Important Information

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

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=13953
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R75.40 home page (http://supportcontent.checkpoint.com/solutions?id=sk67581).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 October 2012</td>
<td>Updated User Directory License issue.</td>
</tr>
<tr>
<td>15 April 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Management Server R75.40 Administration Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Security Management Overview</td>
<td>9</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Deployments</td>
<td>9</td>
</tr>
<tr>
<td>Glossary</td>
<td>10</td>
</tr>
<tr>
<td>Management Software Blades</td>
<td>10</td>
</tr>
<tr>
<td>Logging In</td>
<td>11</td>
</tr>
<tr>
<td>Authenticating the Administrator</td>
<td>12</td>
</tr>
<tr>
<td>Authenticating the Security Management Server Using its Fingerprint</td>
<td>12</td>
</tr>
<tr>
<td>SmartDashboard Access Modes</td>
<td>12</td>
</tr>
<tr>
<td>Using SmartDashboard</td>
<td>13</td>
</tr>
<tr>
<td>Objects Tree</td>
<td>13</td>
</tr>
<tr>
<td>Rule Base</td>
<td>17</td>
</tr>
<tr>
<td>Objects List</td>
<td>17</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>17</td>
</tr>
<tr>
<td>SmartWorkflow</td>
<td>17</td>
</tr>
<tr>
<td>SmartMap</td>
<td>18</td>
</tr>
<tr>
<td>Secure Internal Communication (SIC)</td>
<td>18</td>
</tr>
<tr>
<td>The Internal Certificate Authority (ICA)</td>
<td>18</td>
</tr>
<tr>
<td>Initializing the Trust Establishment Process</td>
<td>18</td>
</tr>
<tr>
<td>Testing the SIC Status</td>
<td>19</td>
</tr>
<tr>
<td>Resetting the Trust State</td>
<td>19</td>
</tr>
<tr>
<td>Troubleshooting SIC</td>
<td>19</td>
</tr>
<tr>
<td>LDAP and User Directory</td>
<td>21</td>
</tr>
<tr>
<td>The Check Point Solution for LDAP Servers</td>
<td>21</td>
</tr>
<tr>
<td>User Directory Considerations</td>
<td>21</td>
</tr>
<tr>
<td>Deploying User Directory</td>
<td>22</td>
</tr>
<tr>
<td>Enhancements</td>
<td>22</td>
</tr>
<tr>
<td>Account Units</td>
<td>22</td>
</tr>
<tr>
<td>Defining LDAP Account Units</td>
<td>23</td>
</tr>
<tr>
<td>Defining User Directory Server</td>
<td>23</td>
</tr>
<tr>
<td>Account Units and High Availability</td>
<td>25</td>
</tr>
<tr>
<td>Setting High Availability Priority</td>
<td>25</td>
</tr>
<tr>
<td>Authenticating with Certificates</td>
<td>26</td>
</tr>
<tr>
<td>Managing Users on a User Directory Server</td>
<td>26</td>
</tr>
<tr>
<td>User Directory Groups</td>
<td>26</td>
</tr>
<tr>
<td>Distributing Users in Multiple Servers</td>
<td>27</td>
</tr>
<tr>
<td>Retrieving Information from a User Directory Server</td>
<td>27</td>
</tr>
<tr>
<td>Using User Directory Queries</td>
<td>27</td>
</tr>
<tr>
<td>Example of Query</td>
<td>27</td>
</tr>
<tr>
<td>Querying Multiple LDAP Servers</td>
<td>28</td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td>28</td>
</tr>
<tr>
<td>Updating the Registry Settings</td>
<td>28</td>
</tr>
<tr>
<td>Delegating Control</td>
<td>29</td>
</tr>
<tr>
<td>Extending the Active Directory Schema</td>
<td>29</td>
</tr>
<tr>
<td>Adding New Attributes to the Active Directory</td>
<td>30</td>
</tr>
<tr>
<td>Netscape LDAP Schema</td>
<td>30</td>
</tr>
<tr>
<td>The User Directory Schema</td>
<td>31</td>
</tr>
<tr>
<td>The Check Point Schema</td>
<td>31</td>
</tr>
<tr>
<td>Schema Checking</td>
<td>31</td>
</tr>
<tr>
<td>OID Proprietary Attributes</td>
<td>31</td>
</tr>
<tr>
<td>User Directory Schema Attributes</td>
<td>32</td>
</tr>
</tbody>
</table>
Policy Management

Managing Users and Administrators Internally

Glossary

SmartDashboard
Users Database
User Templates

Configuring Users
Creating or Changing a User
General Properties
Setting the Expiration Date
Assigning a Permissions Profile
Authentication
Locations
Connection Times
Certificates
Encryption

Managing User Groups

Configuring Administrators
Creating or Changing an Administrator
Configuring General Properties
Setting the Expiration Date
Selecting a Permissions Profile
Administrator Groups
Configuring Authentication
Certificates

Configuring Administrator Groups

Managing User and Administrator Expiration

Working with Expiration Warnings
Configuring Default Expiration Parameters

Working with Permissions Profiles
Creating and Changing Permission Profiles
Managing Permissions Profiles

Policy Management

The Need for an Effective Policy Management Tool
Policy Management Overview
Policy Management Considerations
Creating a New Policy Package
Defining the Policy Package's Installation Targets
Adding a Policy to an Existing Policy Package
Adding a Section Title
Configuring a New Query
Intersecting Queries
Querying Objects
Sorting Objects in the Objects List Pane
Policy Packages
File Operations
Installation Targets
Dividing the Rule Base into Sections using Section Titles
Querying Rules
Querying Network Objects
Sorting the Objects Tree and the Objects List Pane
Working with Policies
To Install a Policy Package
To Uninstall a Policy Package
Chapter 1

Security Management Overview

In This Chapter

Introduction ................................................. 9
Logging In ................................................. 11
Using SmartDashboard ................................. 13

Introduction

To make the most of Check Point products and all their capabilities and features, become familiar with some basic concepts and components. This is an overview of usage, terms, and tasks to help you manage your Check Point Security Gateways.

Deployments

Basic deployments:

- Standalone deployment - Gateway and the Security Management server are installed on the same machine.
- Distributed deployment - Gateway and the Security Management server are installed on different machines.

Assume an environment with gateways on different sites. Each gateway connects to the Internet on one side, and to a LAN on the other.

You can create a Virtual Private Network (VPN) between the two gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.
There can be other OPSEC-partner modules (for example, an AntiVirus Server) to complete the network security with the Security Management server and its gateways.

**Glossary**

- **Administrators** are responsible for managing the Security Management environment. They have access permissions to use the SmartConsole clients. At least one administrator must have full Read/Write permissions to manage Security Policies.

- The **Check Point Configuration Tool** lets you configure Check Point products after the installation completes. You can also use this tool to change specified configuration parameters after the initial configuration.
  
  The configuration tool lets you configure important parameters such as Administrators, licenses, management High Availability and GUI Clients.

- **Installation** is the process of installing Check Point product components are installed on a computer.
  
  - **Standalone deployment** - You install a Security Gateway and the Security Management server on one computer.
  
  - **Distributed deployment** - You install the Security Gateways and the Security Management server on different computers.

- **Login** is the procedure by which the administrator connects to the Security Management server using a SmartConsole client.

- **Objects** are defined and managed in SmartDashboard to show physical network components such as a Security Management servers, Security Gateways and networks.

- A **Policy Package** is a collection of policies that enforce security on specified gateways.

- A **Security Policy** is a collection of rules and conditions that enforce security.

- **SmartConsole** is a suite of GUI clients that manage different aspects of your security environment.

- A **Log Server** is a repository for log entries created by Security Gateways and management servers.

- **SmartDashboard** is the SmartConsole client that lets you manage security policies and network objects.

- **Users** are personnel that use applications and network resources. Users cannot access SmartConsole clients or manage Check Point security resources.

**Management Software Blades**

Software Blades are independent and flexible security modules that enable you to select the functions you want to build a custom Check Point Security Gateways. Software Blades can be purchased independently or as pre-defined bundles.

The following Security Management Software Blades are available:

<table>
<thead>
<tr>
<th>Security Management Software Blades</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Policy Management</strong></td>
<td>Gives you control over configuring and managing even the most complex security deployments. Based on the Check Point unified security architecture, the Network Policy Management Software Blade provides comprehensive security policy management using SmartDashboard - a single, unified console for all security features and functionality.</td>
</tr>
</tbody>
</table>

| **Endpoint Policy Management**       | Lets you centrally manage the security products you use on your organization's end-user devices. You control computing devices and the sensitive information they contain. |

| **Logging & Status**                 | Gives comprehensive information on security activity in logs and a complete visual picture of changes to gateways, tunnels, remote users, and security activities. |
## Security Management Overview

<table>
<thead>
<tr>
<th>Security Management Software Blades</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Awareness</strong></td>
<td>Lets you add user and computer identity data in Check Point log entries and configure the Active Directory domains to retrieve logs from. You can also set a user-IP association timeout period and whether to assume that only one user is connected per computer (single user assumption).</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Shows a complete picture of network and security performance, for fast response to changes in traffic patterns or security events</td>
</tr>
<tr>
<td><strong>Management Portal</strong></td>
<td>Extends browser-based management access to outside groups, such as technical support staff or auditors, and maintain centralized control of policy enforcement. Management Portal users can view security policies and status of Check Point products and administrator activity, edit, create and modify internal users, and manage firewall logs.</td>
</tr>
<tr>
<td><strong>User Directory</strong></td>
<td>Lets Check Point Security Gateways use LDAP-based user information stores, eliminating the risks associated with manually maintaining and synchronizing redundant data stores. With the Check Point User Directory Software Blade, Check Point Security Gateways become full LDAP clients which communicate with LDAP servers to obtain identification and security information about network users.</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>Gives centralized provisioning of Check Point security devices. Using profiles, you can easily deploy a security policy or configuration settings to multiple, geographically distributed devices. It also gives centralized backup management and a repository of device configurations, to quickly deploy configurations to new devices.</td>
</tr>
<tr>
<td><strong>SmartReporter</strong></td>
<td>Centralizes reporting on network, security, and user activity and consolidates the data into concise predefined and custom-built reports. Easy report generation and automatic distribution save time and money.</td>
</tr>
<tr>
<td><strong>SmartEvent</strong></td>
<td>Gives centralized, real-time security event correlation and management for Check Point security gateways and third-party devices. This minimizes the time spent analyzing data, and isolates and prioritizes the real security threats.</td>
</tr>
<tr>
<td><strong>SmartEvent Intro</strong></td>
<td>Gives a complete IPS and DLP event management system for situational visibility, easy to use forensic tools, and reporting.</td>
</tr>
</tbody>
</table>

To verify which and how many Software Blades are currently installed on the Security Management Server, look at the SmartDashboard representation of the Security management server. In the General Properties page of the Security management server, the Management tab of the Software Blades section shows all enabled management Software Blades.

In a High Availability environment the Software Blade must be enabled on each High Availability Management.

### Logging In

The login process, in which administrators connect to the Security Management server, is common to all SmartConsole applications (SmartDashboard, SmartUpdate, and so on). This process is bidirectional. The administrator and the Security Management server authenticate each other and create a secure channel of communication between them using Secure Internal Communication (SIC). When SIC is established, the Security Management server launches the selected SmartConsole.
**Authenticating the Administrator**

Administrators can authenticate themselves in different ways, depending on the tool used to create the accounts.

Administrators defined in Check Point Configuration Tool authenticate themselves with a *Username and Password*. This is *asymmetric SIC*. Only the Security Management server uses a certificate to authenticate.

Administrators defined in SmartDashboard can authenticate with a username and password, or with a *Certificate*. If using a certificate, the administrator browses to the certificate and unlocks it with its password. This is *symmetric SIC*. The Security Management server and the administrator authenticate each other using certificates.

After giving authentication data, the administrator enters the name or IP address of the target Security Management server and clicks **OK**. If the administrator is successfully authenticated by the Security Management server:

- If this is the first time this SmartConsole is used to connect to the Security Management server, the administrator must manually authenticate the Security Management server using its Fingerprint.
- If this SmartConsole connected to the Security Management server before, and an administrator already authenticated the Security Management server, Fingerprint authentication is done automatically.

**Authenticating the Security Management Server Using its Fingerprint**

The administrator authenticates the Security Management server using the Security Management server’s Fingerprint. This Fingerprint, shown in the **Fingerprint** tab of the Check Point Configuration Tool, is obtained by the administrator before attempting to connect to the Security Management server.

The first time the administrator connects to the Security Management server, the Security Management server displays a Fingerprint verification window. The administrator, who has the original Fingerprint on hand, compares it to the displayed Fingerprint. If the two are identical, the administrator approves the Fingerprint as valid. This action saves the Fingerprint (along with the Security Management server’s IP address) to the SmartConsole machine’s registry, where it remains available to automatically authenticate the Security Management server in the future.

If the Fingerprints are not identical, the administrator quits the Fingerprint verification window and returns to the initial login window. In this case, the administrator should verify the resolvable name or IP address of the Security Management server.

**SmartDashboard Access Modes**

Many administrators can use SmartDashboard to connect to a Security Management server simultaneously. But only one administrator can have **Read/Write** access to change object definitions, security rules or Security Management server settings at one time. All other administrators connected at the same time have **Read Only** access.

If you connect to a Security Management server while another administrator is connected in the Read/Write mode, a message is shown with these options:

- Connect in the Read Only mode to see the current object definitions, security rules and Security Management server settings.
- Ask to get a notification when Read/Write mode is available. When the administrator who currently has Read/Write access logs out or changes to the Read Only access mode, a message is shown. You can click **Switch to Write mode** to change the access mode immediately.
- Disconnect the administrator currently logged in with Read/Write access and connect with full Read/Write access.

**Important** - Be careful when disconnecting another administrator. Unsaved changes made by the disconnected administrator are lost. Also, it is possible that some policies changed by the disconnected administrator were not installed on Security Gateways.

You can change the access mode after you open SmartDashboard.
To change the access mode:
1. Open the File menu.
2. Select **Switch to Read Only** or **Switch to Read/Write**.

**Using SmartDashboard**

SmartDashboard is your primary tool to manage network and security resources.

**Objects Tree**

You create objects to represent actual hosts and devices, intangible components (such as HTTP and TELNET services) and resources (for example, URI and FTP). Make an object for each component in your organization. Then you can use the objects in the rules of the Security Policy. Objects are stored in the Objects database on the Security Management server.

Objects in SmartDashboard are divided into several categories, which you can see in the tabs of the Objects Tree.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Object Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Network" /></td>
<td><strong>Network Objects</strong></td>
<td>Check Point Gateways, networks</td>
</tr>
<tr>
<td><img src="icon" alt="Services" /></td>
<td><strong>Services</strong></td>
<td>TCP, Citrix</td>
</tr>
<tr>
<td><img src="icon" alt="Resources" /></td>
<td><strong>Resources</strong></td>
<td>URI, FTP</td>
</tr>
<tr>
<td><img src="icon" alt="Servers" /></td>
<td><strong>Servers and OPSEC Applications</strong></td>
<td>Trusted CAs</td>
</tr>
<tr>
<td><img src="icon" alt="Users and Administrators" /></td>
<td><strong>Users and Administrators</strong></td>
<td>Access Roles, User Groups</td>
</tr>
<tr>
<td><img src="icon" alt="VPN Communities" /></td>
<td><strong>VPN Communities</strong></td>
<td>Site to Site, Remote Access</td>
</tr>
</tbody>
</table>

When you create your objects, consider the needs of your organization:
- What are the physical components in your network?
- What are the logical components - services, resources, and applications?
- What components will access the firewall?
- Who are the users, and how should they be grouped?
- Who are the administrators, and what are their roles?
- Will you use VPN, and if so, will it allow remote users?

**Creating Objects in the Objects Tree**

One of the first things to do to protect your environment, is to define the objects in the environment. You can create objects in the Objects Tree, different panes, menus, or toolbars.

To add a new object:
1. In the Objects Tree, select the type of object you want from the Objects Tree list.
2. Right-click the appropriate category.
3. Select the option that best describes the object to add.
   - For example, to make an object that represents a network: in the **Network Objects** tab, right-click **Networks** and select **New Network**.

To see or change the properties of an object, right-click and select **Edit**, or double-click the object.

To delete an object, right-click and select **Delete**.
Typical Object Configuration

There are different ways to create objects and configure them to use in actual management tasks. This is an example of how to create and configure a Check Point Security Gateway object, starting in your Objects Tree.

To define a new Security Gateway object:
1. Open the Objects Tree > Network Objects.
2. Right-click Check Point and select Security Gateway/Management.
3. In the window that opens, click Classic Mode.
   The Check Point gateway properties window shows the default pages.
4. In General Properties, enter the hostname and the IP address of the gateway.
   If you can establish SIC trust now, it will make the rest of the process easier, but you can do this later.
5. Select the platform that describes the gateway computer: hardware, Check Point version, and operating system.
   If you are unsure of the platform data, you can leave this until after trust is established. If you do, you will see a message when you click OK:
   The specified OS on this Security Gateway is 'Unknown'.
   Click Yes to accept the configurations you have now and to fill in the rest later.
6. Select the Software Blades that are installed on the Security Gateway.
   If you are unsure of the installed Software Blades, you can leave them unselected now and edit the object later. If you do not choose a Software Blade, you will see a message when you click OK. Click Yes to accept the configurations you have now and to fill in the rest later.
7. Click OK.
   The Check Point network object is in the Objects Tree, but without Trust, it is just a holder.

Establishing Trust for Objects

The Security Management server manages Check Point components of your environment through SIC (Secure Internal Communication). There must be authentication between the components and the servers, which establishes Trust. See Secure Internal Communication (SIC) (on page 18).

When a network object has Trust with the server, you can manage the object through the SmartDashboard.

To establish trust:
1. Open the network object properties (double-click the object in the Objects Tree).
2. Click Communication.
3. In the window that opens, enter and confirm the Activation Key used when the gateway was installed.
4. Click Initialize.
   With Trust established, you can manage the actual component from its network object.

Completing Basic Configuration

When there is Trust between a Security Gateway and the Security Management server, it easier to configure the network object of the Security Gateway.

To configure a trusted Security Gateway:
1. Double-click the gateway object in the Objects Tree > Network Objects.
2. In the Platform area, click Get.
3. In the Software Blades area, select those that are installed on the gateway.
   Some Software Blades have first time setup wizards. You can do these wizards now or later.
   The left pane of the properties window shows the properties that are related to the selected Software Blades. Continue with the default properties.
4. In Topology, enter the interfaces that lead to and from the Security Gateway.
   If you selected the Firewall Software Blade, you can click Get to have the Security Management server get them for you.
5. In NAT, you can activate NAT and configure the basics of Hide NAT or Static NAT.
6. Click OK.
Network Topology

The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

- Correctly enforce the Security Policy.
- Ensure the validity of IP addresses for inbound and outbound traffic.
- Configure a special domain for Virtual Private Networks.

Each component in the network topology is distinguished on the network by its IP address and net mask. The combination of objects and their respective IP information make up the topology. For example:

- The IP address of the LAN is 10.111.254.0 with Net Mask 255.255.255.0.
- A Security Gateway on this network has an external interface with the following IP address 192.168.1.1, and an internal interface with 10.111.254.254.

In this example, there is one simple internal network. In more complicated scenarios, the LAN is composed of many networks.

The internal network is composed of:

- The IP address of the first is 10.11.254.0 with Net Mask 255.255.255.0.
- The IP address of the second is 10.112.117.0 with Net Mask 255.255.255.0.
- A Security Gateway that protects this network has an external interface with IP address 192.168.1.1, and an internal interface with 10.111.254.254.

In this example, the system administrator defines the topology of the gateway accordingly.

In SmartDashboard:

- An object should be created to represent each network. The definition must include the network’s IP address and netmask.
- A group object should be created which includes both networks. This object represents the LAN.
- In the gateway object, the internal interface should be edited to include the group object. (In the selected gateway, double-click on the internal interface in the Topology page. Select the group defined as the specific IP addresses that lie behind this interface).

Customizing Objects Tree Views

In each category of objects, you can change the view.

For Network Objects the default view is by category of network object. This is recommended for small to medium deployments and for when you are getting started. When you have groups of objects, you can see the objects in their groups. This is recommended for larger deployments, but is relevant only after you have groups of objects.

To create a group: In classic view, right-click Network Objects > Groups and select a group type.

- You can create nested groups.
- If you have many objects in a group, you can sort them by property.
You can show objects in a group by their default category. Right-click and select **Show groups hierarchy**. Therefore, do make groups to take the place of the default network object categories. They are given to you in the hierarchy view of a group of objects.

**To change the Network Objects view:** Right-click and select **Arrange by groups** or **Switch to classic view**.

In all object trees, you can view by default categories or sort by property. **To sort a tree:** Right-click the root, select **Sort** and then select **Name, Type, or Color**.

### Group Conventions

When you create a group, you can set conventions. When an object is created that fits the group conventions, you get a prompt to add the object automatically to the group.

**To define group conventions:**

1. Open a group.
2. Click **Suggest to add objects to this group**.
3. Select conditions and define them.
   - If you define more than one condition, the conditions are met only if the object meets all of them.
   - If an object matches the conventions of multiple groups, a window shows the matching groups. You can add the object to all, none, or a selection of the groups.

   To not add the object to a matching group, in the **Action** column, select **Don't Add**.

If you change the properties of an object so it does not match the conditions of its group, you see this message:

*Your object no longer fits the group *name*. Do you wish to remove it from the group?*

If you can remove an object from a group, the object itself is not changed or removed from the system. If you remove an object from its last group, you can find it in the **Others** group.
Rule Base

The Rule Base is the policy definitions of what is allowed and what is blocked by the firewall. Rules use objects. For example, networks objects are used in the Source and Destination of rules. Time and Group objects are used in the Time of rules.

Objects List

The Objects List shows data for a selected object category. For example, when a Logical Server Network Object is selected in the Objects Tree, the Objects List displays a list of Logical Servers, with certain details displayed.

Identity Awareness

The Identity Awareness pane shows as a tab in the bottom pane of the main window.

Traditionally, firewalls use IP addresses to monitor traffic and are unaware of the user and machine identities behind those IP addresses. Identity Awareness removes this notion of anonymity since it maps users and machine identities. This lets you enforce access and audit data based on identity.

Identity Awareness is an easy to deploy and scalable solution. It is applicable for both Active Directory and non-Active Directory based networks as well as for employees and guest users. It is currently available on the Firewall blade and Application Control blade and will operate with other blades in the future.

Identity Awareness lets you easily configure network access and auditing based on network location and:

- The identity of a user
- The identity of a machine

When Identity Awareness identifies a source or destination, it shows the IP address of the user or machine with a name. For example, this lets you create firewall rules with any of these properties. You can define a firewall rule for specific users when they send traffic from specific machines or a firewall rule for a specific user regardless of which machine they send traffic from.

In SmartDashboard, you use Access Role objects to define users, machines and network locations as one object.

Identity Awareness gets identities from these acquisition sources:

- AD Query
- Browser-Based Authentication
- Identity Agent
- Terminal Servers Identity Agent
- Remote Access

SmartWorkflow

The SmartWorkflow pane shows as a tab in the bottom pane of the main window.

SmartWorkflow Blade is a security policy change management solution that tracks proposed changes to the Check Point network security environment, and ensures appropriate management review and approval prior to implementation.

Managing network operations while accurately and efficiently implementing security policies is a complex process. Security and system administrators find it increasingly difficult to ensure that all security gateways, network components and other system settings are properly configured and conform to organization security policies.

As enterprises evolve and incorporate technological innovations, network and security environments have become increasingly complex and difficult to manage. Typically, teams of engineers and administrators are required to manage configuration settings, such as:

- Security Policies and the Rule Base
- Network Objects
Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install policies on gateways and to send logs between gateways and management servers.

These security measures make sure of the safety of SIC:

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

The Internal Certificate Authority (ICA)

The ICA is created during the Security Management server installation process. The ICA is responsible for issuing certificates for authentication. For example, ICA issues certificates such as SIC certificates for authentication purposes to administrators and VPN certificates to users and gateways.

Initializing the Trust Establishment Process

Communication Initialization establishes a trust between the Security Management server and the Check Point gateways. This trust lets Check Point components communicate securely. Trust can only be established when the gateways and the server have SIC certificates.

**Note** - For SIC to succeed, the clocks of the gateways and servers must be synchronized.

The Internal Certificate Authority (ICA) is created when the Security Management server is installed. The ICA issues and delivers a certificate to the Security Management server.

To initialize SIC:

1. Decide on an alphanumeric Activation Key.
2. In SmartDashboard, open the gateway network object. In the General Properties page of the gateway, click Communication to initialize the SIC procedure.
3. In the Communication window of the object, enter the Activation Key that you created in step 2.
4. Click Initialize.

The ICA signs and issues a certificate to the gateway. Trust state is Initialized but not trusted. The certificate is issued for the gateway, but not yet delivered.
SSL negotiation takes place. The two communicating peers are authenticated with their Activation Key. The certificate is downloaded securely and stored on the gateway.

After successful Initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate, signed by the same ICA. The Activation Key is deleted. The SIC process no longer requires the Activation Key, only the SIC certificates.

Testing the SIC Status

The SIC status reflects the state of the Gateway after it has received the certificate issued by the ICA. This status conveys whether or not the Security Management server is able to communicate securely with the gateway. The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established. In this case an error message will appear, which may contain specific instructions how to remedy the situation.

Resetting the Trust State

Resetting the Trust State revokes the gateway's SIC certificate. This must be done if the security of the gateway has been breached, or if for any other reason the gateway functionality must be stopped. When the gateway is reset, the Certificate Revocation List (CRL) is updated to include the name of the revoked certificate. The CRL is signed by the ICA and issued to all the gateways in this system the next time a SIC connection is made. If there is a discrepancy between the CRL of two communicating components, the newest CRL is always used. The gateways refer to the latest CRL and deny a connection from an impostor posing as a gateway and using a SIC certificate that has already been revoked.

⚠️ Important - The Reset operation must be performed on the gateway's object, using SmartDashboard, as well as physically on the gateway using the Check Point Configuration Tool.

To reset the Trust State in SmartDashboard:

1. In SmartDashboard, in the General Properties window of the gateway, click Communication.
2. In the Communication window, click Reset.
3. To reset the Trust State in the Check Point Configuration tool of the gateway, click Reset in the Secure Internal Communication tab.
4. Install the Security Policy on all gateways. This deploys the updated CRL to all gateways.

If SIC failed to initialize, and you do not have a Rule Base yet (and so cannot install a policy), you can reset Trust on the gateways.

To reset Trust on Check Point Security Gateways:

1. Log in to the Check Point component.
2. Enter: cpconfig
3. Enter the number for Secure Internal Communication and press enter.
4. Enter y to confirm that you are want to reset trust and are prepared to stop Check Point processes.
5. Enter the activation key when prompted.
6. When done, enter the number for Exit.
7. Wait for the processes to stop and automatically start again.
8. On SmartDashboard, establish trust again. Make sure to use the activation key that you entered on the component.

Troubleshooting SIC

If SIC fails to Initialize:

1. Ensure connectivity between the gateway and Security Management server.
2. Verify that server and gateway use the same SIC activation key.
3. If the Security Management server is behind another gateway, make sure there are rules that allow connections between the Security Management server and the remote gateway, including anti-spoofing settings.

4. Ensure the Security Management server's IP address and name are in the /etc/hosts file on the gateway.
   If the IP address of the Security Management server undergoes static NAT by its local Security Gateway, add the public IP address of the Security Management server to the /etc/hosts file on the remote Security Gateway, to resolve to its hostname.

5. Check the date and time of the operating systems and make sure the time is accurate. If the Security Management server and remote gateway reside in two different time zones, the remote gateway may need to wait for the certificate to become valid.

6. On the command line of the gateway, type: `fw unloadlocal`
   This removes the security policy so that all traffic is allowed through.

7. Try again to establish SIC.

**If Remote Access users cannot reach resources and Mobile Access is enabled:**

- After you install the certificate on a Security Gateway, if the Mobile Access Software Blade is enabled, you must Install Policy on the gateways again.
Chapter 2

LDAP and User Directory

In This Chapter

The Check Point Solution for LDAP Servers
User Directory Considerations
Deploying User Directory
Enhancements
Account Units
Managing Users on a User Directory Server
Retrieving Information from a User Directory Server
Microsoft Active Directory
Netscape LDAP Schema
The User Directory Schema
The Check Point Schema
User Directory Profiles

Check Point User Directory integrates LDAP into Check Point.

User Directory requires a special license.

The Check Point Solution for LDAP Servers

LDAP is a cross-platform, open industry standard used by multiple vendors. LDAP is automatically installed on different Operating Systems (for example, the Microsoft Active Directory) and servers (such as Novell).

Check Point products are compliant with LDAP technology.

- Users can be managed externally by an LDAP server.
- The gateways can retrieve CRLs.
- The Security Management can use the LDAP data to authenticate users.
- User data from other applications gathered in the LDAP users database can be shared by different applications.

You can choose to manage Domains on the Check Point users database, or to implement an LDAP server. If you have a large user count, we recommend that you use an external user management database, such as LDAP, for enhanced Security Management performance. For example, if the user database is external, the database will not be reinstalled every time the user data changes.

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution.

User Directory Considerations

Before you begin, plan your use of User Directory.

- Will the User Directory server be for user management, CR retrieval, user authentication, or all of these?
- How many Account Units do you want? You can have one for each LDAP server, or you can divide branches of one LDAP server among different Account Units.
Deploying User Directory

User Directory integrates the Security Management server and an LDAP server and lets the Security Gateways use the LDAP information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Management server - Uses User Directory to manage user information.</td>
</tr>
<tr>
<td>2</td>
<td>LDAP server - Server that holds one or more Account Units.</td>
</tr>
<tr>
<td>3</td>
<td>Security Gateway - Queries LDAP user information, retrieves CRLs, and does bind operations for authentication.</td>
</tr>
<tr>
<td>4</td>
<td>Internet</td>
</tr>
<tr>
<td>5</td>
<td>Security Gateway - Retrieves LDAP user information and CRLs.</td>
</tr>
</tbody>
</table>

Enhancements

Deploy User Directory features to enhance functionality.

- **High Availability**, to duplicate user data across multiple servers for backup (see "Account Units and High Availability" on page 25).
- **Multiple Account Units**, for distributed databases.
- **Encrypted User Directory connections** (see "Defining LDAP Account Units" on page 23).
- **Profiles**, to support multiple LDAP vendors (see "User Directory Profiles" on page 38).
Account Units

An Account Unit is the interface between the Security Management server / Security Gateways, and the LDAP servers.

An Account Unit represents one or more branches of the data on the LDAP server. You can have several Account Units, for one or multiple LDAP servers. The users in the system are divided among the branches of an Account Unit, and among all the Account Units.

For example, in a bank with one LDAP server, one Account Unit represents users with businesses accounts and a second Account Unit represents users with private accounts. In the business accounts Account Unit, large business users are in one branch and small business users are in another branch.

Defining LDAP Account Units

To integrate LDAP into your Check Point environment, first define the Account Units. Then enter access data to connect to the LDAP server. When done, the Security Management server and Security Gateways connect to the LDAP server to manage the users or to make queries.

To define an LDAP Account Unit:
1. Click Manage > Servers and OPSEC Applications.
2. Click New > LDAP Account Unit.
   The LDAP Account Unit Properties window opens.
3. Enter a name for the Account Unit.
4. Select a profile that best matches the LDAP server.
5. Define usage:
   - If this Account Unit is a Certificate Revocation List, select CRL retrieval. The Security Management server manages how the CA sends data of revoked licenses to the gateway.
   - If it is a user database, select User Management. Make sure the User Management blade is enabled on the Security Management.

   Note - Single Sign On for LDAP users works only if User management is selected.
• If the profile is Active Directory, you can select **Active Directory Query**. This is available if Identity Awareness is activated on the Security Management.

6. In the **Servers** tab, define the LDAP server settings.

7. In the **Objects Management** tab, select the LDAP server for this Account Unit. The Security Management server searches branches of the LDAP server when queried. To retrieve the branches, click **Fetch branches**. If it is disabled (some versions of User Directory do not support automatic branch retrieval), define the branches manually:
   a) Click **Add**.
   b) In the **LDAP Branch Definition window**, enter the **Branch Path**.

8. Optional: You can set a password SmartDashboard users to access this Account Unit. We recommend this if there are multiple managers with different roles.

9. In the **Authentication** tab, define the authentication limitations. The **Allowed Authentication schemes** limit the user’s authentication to only those authentication schemes. You can set several authentication schemes to each user, or you can set a default scheme for all users.

10. Define the default authentication settings for a user on an Account Unit. Users that are missing authentication definitions, get these definitions from the default authentication scheme or a user template. These default settings are useful if the Check Point schema is not in place. A user template gives the authentication settings.

11. For all users in this Account Unit that are configured for IKE, enter the pre-shared secret. Set the number of acceptable login attempts, and the number of seconds before a frozen account can be unlocked.

To change LDAP server settings:
1. Double-click a server in the **LDAP Account Unit Properties > Servers** tab. The **LDAP Server Properties** window opens.

2. In the **General** tab, you can change:
   • Port of the LDAP server
   • Login DN
   • Password
   • Priority of the LDAP server, if there are multiple servers
   • Security Gateway permissions on the LDAP server

3. In the **Encryption** tab, you can change:
     If the connections are encrypted, enter the encryption port and strength settings.
   • Verify the Fingerprints. Compare the fingerprint shown with the Security Management fingerprint.
Note - User Directory connections can be authenticated by client certificates from a Certificate Authority (CA) ("Authenticating with Certificates" on page 26). To use certificates, the LDAP server must be configured with SSL strong authentication.

**Defining User Directory Server**

Configure SmartDashboard to recognize the LDAP server and to let the management server handle User Directory.

**To define the User Directory Server:**
1. Open **Policy > Global Properties > User Directory**.
2. Select **Use User Directory for Security Gateways**. Select other settings that you want and then click **OK**.
3. Open the object properties of a management server (Security Management server or Multi-Domain Server).
4. In **Software Blades > Management**, select **Network Policy Management** and **User Directory**.

**Account Units and High Availability**

With User Directory replications for High Availability, one Account Unit represents all the replicated User Directory servers. For example, two User Directory server replications can be defined on one Account Unit, and two Security Gateways can use the same Account unit.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Security Management</strong>. Manages user data in User Directory. It has an Account Unit object, where the two servers are defined.</td>
</tr>
<tr>
<td>2</td>
<td><strong>User Directory server</strong> replication.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Security Gateway</strong>. Queries user data and retrieves CRLs from nearest User Directory server replication (2).</td>
</tr>
<tr>
<td>4</td>
<td>Internet</td>
</tr>
<tr>
<td>5</td>
<td><strong>Security Gateway</strong>. Queries user data and retrieves CRLs from nearest User Directory server replication (6).</td>
</tr>
<tr>
<td>6</td>
<td><strong>User Directory server</strong> replication.</td>
</tr>
</tbody>
</table>
**Setting High Availability Priority**

With multiple replications, define the priority of each LDAP server in the Account Unit. Then you can define a server list on the Security Gateways.

Select one LDAP server for the Security Management server to connect to. The Security Management server can work with one LDAP server replication. All other replications must be synchronized for standby.

**To set priority on the Account Unit:**
1. Open the LDAP Account Unit Properties window.
2. Open the Servers tab.
3. Add the LDAP servers of this Account Unit in the order of the priority that you want.

**Authenticating with Certificates**

The Security Management server and Security Gateways can have certificates to communicate with LDAP servers. This is optional. If you choose to not use certificates, the management server, gateways, and LDAP communicate without authentication.

**To configure User Directory to use certificates:**
1. Open dbedit.
2. Set the ldap_use_cert_auth attribute to true for every entry in the fields attribute of the Account Unit.
3. Save and close dbedit.
4. Log in to SmartDashboard.
5. Add a CA object:
   a) Click Manage > Servers and OPSEC Applications > New > Certificate Authority > Trusted. The Certificate Authority Properties window opens.
   b) In Certificate Authority Type, select External Check Point CA.
   c) Set the other options of the CA.
6. Add a certificate for all necessary network objects (such as Security Management server, Security Gateway, Policy Server) that require certificate-based User Directory connections.
   a) In the IPSec VPN page of the object properties, click Add in the Repository of Certificates Available list.
   b) In the Certificate Properties window, select the defined CA.
7. In the Users and Administrators tab of the Objects tree, check the new configuration by opening a connection on one of the Account Units configured to use certificate authentication.

**Managing Users on a User Directory Server**

The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local. You can change the User Directory templates. Users associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

To see User Directory users, open Objects Tree > Users and Administrators. The LDAP group holds the structure and accounts of the server.

**User Directory Groups**

Create User Directory groups to classify users in types and to use as objects in Policy rules. You can add users to groups, or you can create dynamic filters.

**To create groups:**
2. Select the Account Unit for the User Directory group.
3. Apply an advanced filter for dynamic membership.
   Only users who match the defined criteria will be included in the User Directory group:
   - All users in the LDAP server of the Account Unit.
   - Users in a branch.
   - Users in an LDAP group or OU.

**Examples**
- If the User objects for managers in your organization have the object class "myOrgManager", you can define the Managers group with the filter: `objectclass=myOrgManagers`
- If certain users in your organization have an e-mail address ending with us.org.com, you can define the US group with the filter: `mail=*us.org.com`

**Distributing Users in Multiple Servers**
The users of an organization can be distributed across several LDAP servers. Each LDAP server must be represented by a separate Account Unit.

**Retrieving Information from a User Directory Server**
When a gateway requires user information for authentication, it searches in these places:

1. The first place that is queried is the internal users database.
2. If the specified user is not defined in this database, the gateway queries the LDAP servers defined in the Account Unit one at a time, and according to their priority. If the query against an LDAP server fails (for example, connection is lost), the server with the next highest priority is queried. If there is more than one Account Unit, the Account Units are queried concurrently. The results of the query are taken from the first Account Unit to meet the conditions, or from all the Account Units which meet the conditions.
3. If the information still cannot be found, the gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

**Using User Directory Queries**
Use queries to get User Directory user or group data. For best performance, query Account Units when there are open connections. Some connections are kept open by the gateways, to make sure the user belongs to a group that is permitted to do certain operations.

The LDAP server of the Account Unit can be configured to be queried. In the Type of the query, you can choose to find Users, Templates, Groups, or All.

**To query User Directory:**
1. Open Objects Tree > Users and Administrators.
2. Right-click the Account Unit and select Query Users/Group.
3. In the LDAP Query Search window, define the query.
4. To add more conditions, select or enter the values and click Add.

Query conditions:
- **Attributes** - Select a user attribute from the drop-down list, or enter an attribute.
- **Operators** - Select an operator from the drop-down list.
- **Value** - Enter a value to compare to the entry's attribute. Use the same type and format as the actual user attribute. For example, if Attribute is fw1expiration-date, then Value must be in the yyyyMMdd syntax.
- **Free Form** - Enter your own query expression. See RFC 1558 for information about the syntax of User Directory (LDAP) query expressions.
- **Add** - Appends the condition to the query (in the text box to the right of Search Method).
**Example of Query**

If you create a query where:

- **Attributes** = mail
- **Contains**
- **Value** = Andy

The server queries the User Directory with this filter:

```
filter:(&(|(objectclass=fw1person)(objectclass=person)(objectclass=organizationalPerson)(objectclass/inetOrgPerson))
((|(cn=Brad)(mail=*Andy*)))))
```

**Querying Multiple LDAP Servers**

The Security Management server and the gateways can work with multiple LDAP servers concurrently. For example, if a gateway needs to find user information, and it does not know where the specified user is defined, it queries all the LDAP servers in the system. (Sometimes a gateway can find the location of a user by looking at the user DN, when working with certificates.)

**Microsoft Active Directory**

The Microsoft Windows 2000 advanced server (or later) includes a sophisticated User Directory server that can be adjusted to work as a user database for the Security Management server.

By default, the Active Directory services are disabled. In order to enable the directory services:

- run the `dcpromo` command from the **Start > Run** menu, or
- run the Active Directory setup wizard using the **System Configuration** window.

The Active Directory has the following structure:

```
DC=qa, DC=checkpoint, DC=com
CN=Configuration,DCROOT
CN=Schema,CN=Configuration,DCROOT
CN=System,DCROOT
CN=Users,DCROOT
CN=Builtin,DCROOT
CN=Computers,DCROOT
OU=Domain Controllers,DCROOT
...
```

Most of the user objects and group objects created by Windows 2000 tools are stored under the **CN=Users, DCROOT** branch, others under **CN=Builtin, DCROOT** branch, but these objects can be created under other branches as well.

The branch **CN=Schema, CN=Configuration, DCROOT** contains all schema definitions.

Check Point can take advantage of an existing Active Directory object as well as add new types. For users, the existing user can be used "as is" or be extended with fw1person as an auxiliary of "User" for full feature granularity. The existing Active Directory "Group" type is supported "as is". A User Directory template can be created by adding the fw1template objectclass. This information is downloaded to the directory using the `schema_microsoft_ad.ldif` file (see Adding New Attributes to the Active Directory (on page 30)).

**Performance**

The number of queries performed on the directory server is significantly low with Active Directory. This is achieved by having a different object relations model. The Active Directory group-related information is stored inside the user object. Therefore, when fetching the user object no additional query is necessary to assign the user with the group. The same is true for users and templates.
Manageability
SmartDashboard allows the creation and management of existing and new objects. However, some specific Active Directory fields are not enabled via SmartDashboard.

Enforcement
It is possible to work with the existing Active Directory objects without extending the schema. This is made possible by defining an Internal Template object and assigning it with the User Directory Account Unit defined on the Active Directory server.

For example, if you wish to enable all users with IKE+Hybrid based on the Active Directory passwords, create a new template with the IKE properties enabled and "Check Point password" as the authentication method.

Updating the Registry Settings
To modify the Active Directory schema, add a new registry DWORD key named `Schema Update Allowed` with the value different from zero under `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`.

Delegating Control
Delegating control over the directory to a specific user or group is important since by default the Administrator is not allowed to modify the schema or even manage directory objects through User Directory protocol.

To delegate control over the directory:
1. Display the Users and Computers Control console.
2. Right-click on the domain name displayed in the left pane and choose Delegate control from the right-click menu.
   The Delegation of Control wizard window is displayed.
3. Add an Administrator or another user from the System Administrators group to the list of users who can control the directory.
4. Reboot the machine.

Extending the Active Directory Schema
Modify the file with the Active Directory schema, to use SmartDashboard to configure the Active Directory users.

To extend the Active Directory schema:
1. From the Security Gateway, go to the directory of the schema file:
   `/opt/CPsuite-R75/fw1/lib/ldap`.
2. Copy `schmea_microsoft_ad.ldif` to the C:\ drive in the Active Directory server.
3. From Active Directory server, with a text editor open the schema file.
4. Find the value `DOMAINDNAME`, and replace it with the name of your domain in LDIF format.
   For example, the domain `sample.checkpoint.com` in LDIF format is:
   `DC=sample,DC=checkpoint,DC=com`
5. Make sure that there is a dash character - at the end of the modify section.
   This is an example of the modify section.
   ```
   dn:
   CN=User,CN-Schema,CN=Configuration,DC=sample,DC=checkpoint,DC=com
   changetype: modify
   add: auxiliaryClass
   auxiliaryClass: 1.3.114.7.3.2.0.2
   ```
6. Run `ldifde -i -f c:/schema_microsoft_ad.ldif`
Adding New Attributes to the Active Directory

Below is the example in LDAP Data Interchange (LDIF) format that adds one attribute to the Microsoft Active Directory:

```
dn: CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
changetype: add

  adminDisplayName: fw1auth-method
  attributeID: 1.3.114.7.4.2.0.1
  attributeSyntax: 2.5.5.4
  cn: fw1auth-method
distinguishedName:
  CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
  instanceType: 4
  isSingleValued: FALSE
  LDAPDisplayName: fw1auth-method
  name: fw1auth-method
  objectCategory:
    CN=Attribute-Schema,CN=Configuration,CN=Schema,CN=Configuration,DCROOT
  ObjectClass: attributeSchema
cMSyntax: 20
  rangeLower: 1
  rangeUpper: 256
  showInAdvancedViewOnly: TRUE
```

All Check Point attributes can be added in a similar way. The definitions of all attributes in LDIF format are contained in the `schema_microsoft_ad.ldif` file located in the `$FWDIR/lib/ldap` directory.

Before attempting to run the `ldapmodify` command, edit `schema_microsoft_ad.ldif` and replace all instances of `DCROOT` with the specific domain root of your organization. For example if your domain is `support.checkpoint.com`, replace `DCROOT` with `dc=support,dc=checkpoint,dc=com`.

After modifying the file, run the `ldapmodify` command to load the file into the directory. For example if you use the Administrator account of the `dc=support,dc=checkpoint,dc=com` domain the command syntax will be as follows:

```
ldapmodify -c -h support.checkpoint.com -D cn=administrator,cn=users,dc=support,dc=checkpoint,dc=com" -w SeCrEt -f $FWDIR/lib/ldap/schema_microsoft_ad.ldif
```

**Note** - A shell script is available for UNIX gateways. The script is at: `$FWDIR/lib/ldap/update_schema_microsoft_ad`

Netscape LDAP Schema

To add the propriety schema to your Netscape directory server, use the file `schema.ldif` in the `$FWDIR/lib/ldap` directory.

**Important** - This deletes the objectclass definition from the schema and adds the updated one in its place.

We recommend that you back up the User Directory server before you run the command.

The `ldif` file:

- Adds the new attributes to the schema
- Deletes old definitions of `fw1person` and `fw1template`
- Adds new definitions of `fw1person` and `fw1template`

To change the Netscape LDAP schema, run the `ldapmodify` command with the `schema.ldif` file.

On some server versions, the `delete objectclass` operation can return an error, even if it was successful. Use `ldapmodify` with the `-c (continuous)` option.
The User Directory Schema

The User Directory default schema is a description of the structure of the data in a user directory. It has user definitions defined for an LDAP server. This schema does not have Security Management server or Security Gateway specific data, such as IKE-related attributes, authentication schemes, or values for remote users.

You can use the default User Directory schema, if all users have the same authentication scheme and are defined according to a default template. But if users in the database have different definitions, it is better to apply a Check Point schema to the LDAP server.

The Check Point Schema

The Check Point Schema adds Security Management server and Security Gateway specific data to the structure in the LDAP server. Use the Check Point Schema to extend the definition of objects with user authentication functionality.

For example, an Object Class entitled fw1Person is part of the Check Point schema. This Object Class has mandatory and optional attributes to add to the definition of the Person attribute. Another example is fw1Template. This is a standalone attribute that defines a template of user information.

Schema Checking

When schema checking is enabled, User Directory requires that every object class and its associated attributes be defined in the directory schema.

Before working with User Directory, schema checking should be disabled. Once the Check Point object classes and attributes to the User Directory server’s schema, schema checking should be enabled.

OID Proprietary Attributes

Each of the proprietary object classes and attributes (all of which begin with "fw1") has a proprietary Object Identifier (OID), listed below.

<table>
<thead>
<tr>
<th>Object Class OIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>object class</td>
</tr>
<tr>
<td>fw1template</td>
</tr>
<tr>
<td>fw1person</td>
</tr>
</tbody>
</table>

The OIDs for the proprietary attributes begin with the same prefix ("1.3.114.7.4.2.0.X"). Only the value of "X" is different for each attribute. See Attributes (see "User Directory Schema Attributes" on page 32) for the value of "X".
User Directory Schema Attributes

Attributes:

- **cn**: The entry's name. This is also referred to as "Common Name". For users this can be different from the uid attribute, the name used to login to the Security Gateway. This attribute is also used to build the User Directory entry's distinguished name, that is, it is the RDN of the DN.

- **uid**: The user's login name, that is, the name used to login to the Security Gateway. This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication schemes.

The login name is used by the Security Management server to search the User Directory server(s). For this reason, each user entry should have its own unique uid value.
It is also possible to log into the Security Gateway using the full DN. The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing. The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different User Directory servers.

**description**

Descriptive text about the user.

| default | "no value"

**mail**

User's email address.

| default | "no value"

**member**

An entry can have zero or more values for this attribute.

- **In a template:** The DN of user entries using this template. DNs that are not users (object classes that are not one of: "person", "organizationalPerson", "inetOrgPerson" or "fw1person") are ignored.

- **In a group:** The DN of user.

**userPassword**

Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is:

```
{crypt}xxyyyyyyyyyyy
```

where "xx" is the "salt" and "yyyyyyyyyy" is the hashed password.

It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the User Directory server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password.

The Security Gateway never reads this attribute, though it does write it. Instead, the User Directory bind operation is used to verify a password.

**fw1authmethod**

One of the following:

- RADIUS
- TACACS
- SecurID
- OS Password
- Defender

This default value for this attribute is overridden by Default Scheme in the Authentication tab of the Account Unit window in SmartDashboard. For example: a User Directory server can contain User Directory entries that are all of the object-class "person" even though the proprietary object-class "fw1person" was not added to the server's schema. If Default Scheme in SmartDashboard is "Internal Password", all the users will be authenticated using the password stored in the "userPassword" attribute.

**fw1authserver**

A table:

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>y</td>
<td>y</td>
<td>&quot;undefined&quot;</td>
</tr>
</tbody>
</table>

The name of the server that will perform the authentication. This field must be given if fw1auth-method is "RADIUS" or "TACACS". For all other values of fw1auth-method, it is ignored. Its meaning is given below:
<table>
<thead>
<tr>
<th>method</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>name of a RADIUS server, a group of RADIUS servers, or &quot;Any&quot;</td>
</tr>
<tr>
<td>TACACS</td>
<td>name of a TACACS server</td>
</tr>
</tbody>
</table>

"X" in OID  fw1template

| 2       | y                                      |

**fw1pwdLastMod**

The date on which the password was last modified. The format is `yyyyMMdd` (for example, 20 August 1998 is 19980820). A password can be modified through the Security Gateway as a part of the authentication process.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>y</td>
<td>y</td>
<td>If no value is given, then the password has never been modified.</td>
</tr>
</tbody>
</table>

**fw1expiration-date**

The last date on which the user can login to a Security Gateway, or "no value" if there is no expiration date. The format is `yyyyMMdd` (for example, 20 August 1998 is 19980820). The default is "no value".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

**fw1hour-range-from**

The time from which the user can login to a Security Gateway. The format is `hh:mm` (for example, 8:15 AM is 08:15).

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>y</td>
<td>y</td>
<td>&quot;00:00&quot;</td>
</tr>
</tbody>
</table>

**fw1hour-range-to**

The time until which the user can login to a Security Gateway. The format is `hh:mm` (for example, 8:15 AM is 08:15).

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>y</td>
<td>y</td>
<td>&quot;23:59&quot;</td>
</tr>
</tbody>
</table>

**fw1day**

The days on which the user can login to a Security Gateway. Can have the values "SUN","MON",…etc.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>y</td>
<td>y</td>
<td>all days of the week</td>
</tr>
</tbody>
</table>
**fw1allowed-src**
The names of one or more network objects from which the user can run a client, or "Any" to remove this limitation, or "no value" if there is no such client. The names should match the name of network objects defined in Security Management server.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

**fw1allowed-dst**
The names of one or more network objects which the user can access, or "Any" to remove this limitation, or "no value" if there is no such network object. The names should match the name of network objects defined on the Security Management server.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

**fw1allowed-vlan**
Not currently used.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

**fw1SR-keym**
The algorithm used to encrypt the session key in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>y</td>
<td>y</td>
<td>&quot;Any&quot;</td>
</tr>
</tbody>
</table>

**fw1SR-datam**
The algorithm used to encrypt the data in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>y</td>
<td>y</td>
<td>&quot;Any&quot;</td>
</tr>
</tbody>
</table>

**fw1SR-mdm**
The algorithm used to sign the data in SecuRemote. Can be "none" or "MD5".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>y</td>
<td>y</td>
<td>&quot;none&quot;</td>
</tr>
</tbody>
</table>

**fw1enc-fwz-expiration**
The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the Security Gateway.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>
**fw1sr-auth-track**

The exception to generate on successful authentication via SecuRemote. Can be "none", "cryptlog" or "cryptalert".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>y</td>
<td>y</td>
<td>&quot;none&quot;</td>
</tr>
</tbody>
</table>

**fw1groupTemplate**

This flag is used to resolve a problem related to group membership.

The group membership of a user is stored in the group entries to which it belongs, in the user entry itself, or in both entries. Therefore there is no clear indication in the user entry if information from the template about group relationship should be used.

If this flag is "TRUE", then the user is taken to be a member of all the groups to which the template is a member. This is in addition to all the groups in which the user is directly a member.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>y</td>
<td>y</td>
<td>&quot;False&quot;</td>
</tr>
</tbody>
</table>

**fw1ISAKMP-EncMethod**

The key encryption methods for SecuRemote users using IKE. This can be one or more of: "DES", "3DES". A user using IKE (formerly known as ISAMP) may have both methods defined.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>y</td>
<td>y</td>
<td>&quot;DES&quot;, &quot;3DES&quot;</td>
</tr>
</tbody>
</table>

**fw1ISAKMP-AuthMethods**

The allowed authentication methods for SecuRemote users using IKE, (formerly known as ISAMP). This can be one or more of: "preshared", "signatures".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>y</td>
<td>y</td>
<td>&quot;signatures&quot;</td>
</tr>
</tbody>
</table>

**fw1ISAKMP-HashMethods**

The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one or more of: "MD5", "SHA1". A user using IKE must have both methods defined.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>y</td>
<td>y</td>
<td>&quot;MD5&quot;, &quot;SHA1&quot;</td>
</tr>
</tbody>
</table>

**fw1ISAKMP-Transform**

The IPSec Transform method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one of: "AH", "ESP".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>y</td>
<td>y</td>
<td>&quot;ESP&quot;</td>
</tr>
</tbody>
</table>

**fw1ISAKMP-DataIntegrityMethod**

The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one of: "MD5", "SHA1".
fw1ISAKMP-SharedSecret
The pre-shared secret for SecuRemote users using IKE, (formerly known as ISAMP).
The value can be calculated using the `fw_ikecrypt` command line.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>y</td>
<td>y</td>
<td></td>
</tr>
</tbody>
</table>

fw1ISAKMP-DataEncMethod
The data encryption method for SecuRemote users using IKE, (formerly known as ISAMP).

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>y</td>
<td>y</td>
<td>&quot;DES&quot;</td>
</tr>
</tbody>
</table>

fw1enc-Methods
The encryption method allowed for SecuRemote users. This can be one or more of: "FWZ", "ISAKMP" (meaning IKE).

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>y</td>
<td>y</td>
<td>&quot;FWZ&quot;</td>
</tr>
</tbody>
</table>

fw1userPwdPolicy
Defines when and by whom the password should and can be changed.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>y</td>
</tr>
</tbody>
</table>

fw1badPwdCount
Number of allowed wrong passwords entered sequentially.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>y</td>
</tr>
</tbody>
</table>

fw1lastLoginFailure
Time of the last login failure.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>4</td>
</tr>
</tbody>
</table>

memberof template
DN of the template that the user is a member of.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>4</td>
</tr>
</tbody>
</table>
User Directory Profiles

The User Directory profile is a configurable LDAP policy that lets you define more exact User Directory requests and enhances communication with the server. Profiles control most of the LDAP server-specific knowledge. You can manage diverse technical solutions, to integrate LDAP servers from different vendors.

Use User Directory profiles to make sure that the user management attributes of a Security Management are correct for its associated LDAP server. For example, if you have a certified OPSEC User Directory server, apply the OPSEC_DS profile to get enhanced OPSEC-specific attributes.

LDAP servers have difference object repositories, schemas, and object relations.

- The organization's user database may have unconventional object types and relations because of a specific application.
- Some applications use the `cn` attribute in the User object's Relatively Distinguished Name (RDN) while others use `uid`.
- In Microsoft Active Directory, the user attribute `memberOf` describes which group the user belongs to, while standard LDAP schemes define the `member` attribute in the group object itself.
- Different servers implement different storage formats for passwords.
- Some servers are considered v3 but do not implement all v3 specifications. These servers cannot extend the schema.
- Some LDAP servers already have built in support for certain user data, while others require a Check Point schema extended attribute. For example, Microsoft Active Directory has the `accountExpires` user attribute, but other servers require the Check Point attribute `fw1expirationdate`, which is part of the Check Point defined `fw1person` objectclass.
- Some servers allow queries with non-defined types, while others do not.

Default User Directory Profiles

These profiles are defined by default:

- **OPSEC_DS** - the default profile for a standard OPSEC certified User Directory.
- **Netscape_DS** - the profile for a Netscape Directory Server.
- **Novell_DS** - the profile for a Novell Directory Server.
- **Microsoft_AD** - the profile for Microsoft Active Directory.

Modifying User Directory Profiles

Profiles have these major categories:

- **Common** - Profile settings for reading and writing to the User Directory.
- **Read** - Profile settings only for reading from the User Directory.
- **Write** - Profile settings only for writing to the User Directory.

Some of these categories list the same entry with different values, to let the server behave according to type of operation. You can change certain parameters of the default profiles for finer granularity and performance tuning.

To apply a profile:
1. Open the Account Unit.
2. Select the profile.

To change a profile:
1. Create a new profile.
2. Copy the settings of a User Directory profile into the new profile.
3. Change the values.
Fetch User Information Effectively

User Directory servers organize groups and members through different means and relations. User Directory operations are performed by Check Point on users, groups of users, and user templates where the template is defined as a group entry and users are its members. The mode in which groups/templates and users are defined has a profound effect on the performance of some of the Check Point functionality when fetching user information. There are three different modes:

- Defining a "Member" attribute per member, or "Member" user-to-group membership mode. In this case, each member of a specific group gets the "Member" attribute, where the value of this attribute is the DN of that member.

- Defining a "MemberOf" attribute per group, or "MemberOf" user-to-group membership mode. In this case, each group gets the "MemberOf" attribute per group, where the value of this attribute is the DN of a group entry. This is referred to as "MemberOf" user-to-group membership mode.

- Defining a "Memberof" attribute per member and group, or "Both" user-to-group membership mode. In this case both members and groups are given the "Memberof" attribute.

The most effective mode is the "MemberOf" and "Both" modes where user's groups membership information is available on the user itself and no additional User Directory queries are necessary.

Setting User-to-Group Membership Mode

Set the user-to-group membership mode in the profile objects for each User Directory server in objects_5_0.c.

- To specify the user-to-group and template-to-group membership mode set the GroupMembership attribute to one of the following values: Member, MemberOf, Both accordingly.

- To specify the user-to-template membership mode set the TemplateMembership attribute to one of the following values: Member, MemberOf accordingly.

After successfully converting the database, set the User Directory server profile in objects_5_0.c to the proper membership setting and start the Security Management server. Make sure to install policy/user database on all gateways to enable the new configuration.
Profile Attributes

Attributes:

UserLoginAttr
UserPasswordAttr
TemplateObjectClass
ExpirationDateAttr
ExpirationDateFormat
PsswdDateFormat
PsswdDateAttr
BadPwdCountAttr
ClientSideCrypt
DefaultCryptAlgorithm
CryptedPasswordPrefix
PhoneNumberAttr
AttributesTranslationMap
ListOfAttrsToAvoid
BranchObjectClass
BranchOCOperator
OrganizationObjectClass
OrgUnitObjectClass
DomainObjectClass
UserObjectClass
UserOCOperator
GroupObjectClass
GroupOCOperator
UserMembershipAttr
TemplateMembership
TemplateMembershipAttr
UserTemplateMembershipAttr
OrganizationRDN
OrgUnitRDN
UserRDN
GroupRDN
DomainRDN
AutomaticAttrs
GroupObjectClass
OrgUnitObjectClass
OrganizationObjectClass
UserObjectClass
DomainObjectClass

UserLoginAttr

The unique username User Directory attribute (uid). In addition, when fetching users by the username, this attribute is used for query.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid (most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>SamAccountName (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>
UserPasswordAttr
This user password User Directory attribute.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>userPassword (most servers)</td>
<td></td>
</tr>
<tr>
<td>unicodePwd (in Microsoft_AD)</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

TemplateObjectClass
The object class for Check Point User Directory templates. If you change the default value with another objectclass, make sure to extend that objectclass schema definition with relevant attributes from fwltemplate.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwltemplate</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

ExpirationDateAttr
The account expiration date User Directory attribute. This could be a Check Point extended attribute or an existing attribute.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwlExpiration-date (most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>accountExpires (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

ExpirationDateFormat
Expiration date format. This format will be applied to the value defined at ExpirationDateAttr.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP format is yyyyymmdd</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

PsswdDateFormat
The format of the password modified date User Directory attribute. This formation will be applied to the value defined at PsswdDateAttr.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP (most servers) format is yyyyymmdd</td>
<td>One value allowed</td>
</tr>
<tr>
<td>MS (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

PsswdDateAttr
The password last modified date User Directory attribute.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwlpwdLastMod (most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>pwdLastSet (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

BadPwdCountAttr
User Directory attribute to store and read bad password authentication count.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwlBadPwdCount</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>
ClientSideCrypt
If 0, the sent password will not be encrypted. If 1, the sent password will be encrypted with the algorithm specified in the DefaultCryptAlgorithm.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 0 for most servers&lt;br&gt;• 1 for Netscape_DS&lt;br&gt;if not using encrypted password, SSL is recommended</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

DefaultCryptAlgorithm
The algorithm used to encrypt a password before updating the User Directory server with a new password.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Plain (for most servers)&lt;br&gt;• Crypt (for Netscape_DS)&lt;br&gt;• SHA1</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

CryptedPasswordPrefix
The text to prefix to the encrypted password when updating the User Directory server with a modified password.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Crypt} (for Netscape_DS)</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

PhoneNumberAttr
User Directory attribute to store and read the user phone number.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>internationalisednumber</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

AttributesTranslationMap
General purpose attribute translation map, to resolve problems related to peculiarities of different server types. For example, an X.500 server does not allow the "-" character in an attribute name. To enable the Check Point attributes containing "-", specify a translation entry: (e.g., "fw1-expiration =fw1expiration").

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

ListOfAttrsToAvoid
All attribute names listed here will be removed from the default list of attributes included in read/write operations. This is most useful in cases where these attributes are not supported by the User Directory server schema, which might fail the entire operation. This is especially relevant when the User Directory server schema is not extended with the Check Point schema extension.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no values by default. If the User Directory server was not extended by the Check Point schema, list here all the new Check Point schema attributes.</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>
**BranchObjectClass**

Use this attribute to define which type of objects (objectclass) is queried when the object tree branches are displayed after the Account Unit is opened in SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Organization OrganizationalUnit Domain (most servers)</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>• Container (extra for Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

**BranchOCOperator**

If One is set, an ORed query will be sent and every object that matches the criteria will be displayed as a branch. If All, an ANDed query will be sent and only objects of all types will be displayed.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**OrganizationObjectClass**

This attribute defines what objects should be displayed with an organization object icon. A new object type specified here should also be in BranchObjectClass.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>organization</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**OrgUnitObjectClass**

This attribute defines what objects should be displayed with an organization object icon. A new object type specified here should also be in BranchObjectClass.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• organizationalUnit (most servers)</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>• Contained (added to Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

**DomainObjectClass**

This attribute defines what objects should be displayed with a Domain object icon. A new object type specified here should also be in BranchObjectClass.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**UserObjectClass**

This attribute defines what objects should be read as user objects. The user icon will be displayed on the tree for object types specified here.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• User (in Microsoft_AD)</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>• Person</td>
<td></td>
</tr>
<tr>
<td>OrganizationalPerson</td>
<td></td>
</tr>
<tr>
<td>InertOrgPerson</td>
<td></td>
</tr>
<tr>
<td>FW1 Person (most servers)</td>
<td></td>
</tr>
</tbody>
</table>
**UserOCOperator**

If 'one' is set, an ORed query will be sent and every object that matches one of the types will be displayed as a user. If 'all' an ANDed query will be sent and only objects of all types will be displayed.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**GroupObjectClass**

This attribute defines what objects should be read as groups. The group icon will be displayed on the tree for objects of types specified here.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groupofnames</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>Groupofuniquenames (most servers)</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Groupoffnames (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

**GroupOCOperator**

If 'one' is set an ORed query will be sent and every object that matches one of the types will be displayed as a user. If 'all' an ANDed query will be sent and only objects of all types will be displayed.

**GroupMembership**

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

Defines the relationship Mode between the group and its members (user or template objects) when reading group membership.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Member mode defines the member DN in the Group object (most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>• MemberOf mode defines the group DN in the member object (in Microsoft_AD)</td>
<td></td>
</tr>
<tr>
<td>• Modes define member DN in Group object and group DN in Member object.</td>
<td></td>
</tr>
</tbody>
</table>

**UserMembershipAttr**

Defines what User Directory attribute to use when reading group membership from the user or template object if GroupMembership mode is 'MemberOf' or 'Both' you may be required to extend the user/template object schema in order to use this attribute.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>MemberOf</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**TemplateMembership**

Defines the user to template membership mode when reading user template membership information.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Member mode defines the member DN in the Group object (most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>• MemberOf mode defines the group DN in the member object (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>
TemplateMembershipAttr
Defines which attribute to use when reading the User members from the template object, as User DNs, if the TemplateMembership mode is Member.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>member</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

UserTemplateMembershipAttr
Defines which attribute to use when reading from the User object the template DN associated with the user, if the TemplateMembership mode is MemberOf.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>member</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

OrganizationRDN
This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when creating a new organization via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

OrgUnitRDN
This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when creating a new organizationalUnit via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>ou</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

UserRDN
This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when creating a new User object via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

GroupRDN
This value will be used as the attribute name for the RDN when creating a new Group object via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

DomainRDN
This value will be used as the attribute name for the RDN when creating a new Domain object via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>dc</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>
**AutomaticAttrs**

This field is relevant when creating objects in SmartDashboard. The format of this field is

`Objectclass:name:value` meaning that if the object being created is of type `ObjectClass` then additional attributes will be included in the created object with name 'name' and value 'value'.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>user:userAccountControl:66048</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>For Microsoft_AD This means that when a user object is created an extra attribute is included automatically: userAccountControl with the value 66048</td>
<td></td>
</tr>
</tbody>
</table>

**GroupObjectClass**

This field is used when modifying an existing group in SmartDashboard. The format of this field is `ObjectClass:memberattr` meaning that for each group objectclass there is a group membership attribute mapping. List here all the possible mappings for this User Directory server profile. When a group is modified, based on the group's objectclass the right group membership mapping will be used.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupOfNames:member</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>groupOfUniqueNames:uniqueMember</td>
<td></td>
</tr>
<tr>
<td>(All other servers)</td>
<td></td>
</tr>
</tbody>
</table>

**OrgUnitObjectClass**

This determines which ObjectClass to use when creating/modifying an OrganizationalUnit object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrganizationalUnit</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**OrganizationObjectClass**

This determines which ObjectClass to use when creating and/or modifying an Organization object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**UserObjectClass**

This determines which ObjectClass to use when creating and/or modifying a user object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>User (in Microsoft_AD)</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>person</td>
<td></td>
</tr>
<tr>
<td>organizationalPerson</td>
<td></td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td></td>
</tr>
<tr>
<td>fW1Person</td>
<td></td>
</tr>
<tr>
<td>(All other servers)</td>
<td></td>
</tr>
</tbody>
</table>
DomainObjectClass

Determines which ObjectClass to use when creating and/or modifying a domain context object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>
Chapter 3

Managing Users and Administrators Internally

In This Chapter

Glossary 48
SmartDashboard 49
Users Database 49
User Templates 49
Configuring Users 50
Managing User Groups 53
Configuring Administrators 53
Configuring Administrator Groups 56
Managing User and Administrator Expiration 57
Working with Permissions Profiles 59

SmartDashboard administrators with permissions can manage user accounts and the permissions of other administrators. You can use the Check Point Users and Administrators objects.

Glossary

This glossary contains important terms that are used in this chapter.

- **Administrator** — Personnel responsible for managing the Security Management environment. Administrators have permissions to use the SmartConsole clients.

- **Administrator Groups** — Named groups of administrators with permissions to install policies on specified gateways.

- **External Users** — Users defined on external servers. External users are not defined in the Security Management database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

- **LDAP Groups** — Groups of users defined on an LDAP account unit. You can specify an LDAP group in policy rules in the same way as individual users or user groups.

- **Permissions Profiles** — Predefined set of access permissions that you assign to individual administrators. This feature lets you assign and manage complex, granular permissions for many administrators with one definition.

- **Templates** — Predefined sets of user properties that let you quickly define new users.

- **Users** — Personnel authorized to use network resources and applications.

- **User Database** — Check Point internal database that contains all users and administrators defined and managed using SmartDashboard. The Check Point User Database does not contain users defined in LDAP groups or external users.

- **User Groups** — Named groups of users with related responsibilities or who do related tasks. You can specify a user group in policy rules in the same way as individual users.
SmartDashboard

The Check Point user management solution is part of SmartDashboard. Users, Administrators and their groups are managed as objects, using the standard object administration tools: the Objects Tree pane and the Objects Manager window.

- **The Objects Tree pane (Users and Administrators tab):**
  - Provides a graphical overview of all users and administrators.
  - Allows you to manage users and administrators by right-clicking the relevant folder (for example, Administrator, Administrator Groups, External User Profiles, etc.) and selecting the appropriate command (Add, Edit, Delete, etc.) from the menu.

- **The Objects Manager (Users and Administrators window):**
  - Lists all users and administrators (you can filter this list to focus on specific types of users or administrators).
  - Allows you to define new objects using the **New...** menu, and to delete or modify an object by selecting them in the list and clicking **Remove** or **Edit** (respectively).

The user's definition includes access permissions to and from specific machines at specific times of the day. The user definition can be used in the Rule Base's Authentication Rules and in Remote Access VPN.

SmartDashboard further facilitates user management by allowing you to define user and administrator **templates**. Templates serve as prototypes of standard users, whose properties are common to many users. Any user you create based on a template inherits all of the template's properties, including membership in groups.

Users Database

The users defined in SmartDashboard (and their authentication schemes and encryption keys) are saved to the proprietary Check Point Internal Users Database (the **Users Databases**) on the Security Management server.

The Users Database is automatically downloaded to Check Point hosts with installed Management Software Blades as part of the Policy installation process. Alternatively, you can manually install the Users Database by selecting **Policy > Install Database** from the menu. Security Gateways that do not include a Management Software Blade do not receive the Users Database.

The Users Database does **not** contain information about users defined externally to the Security Management server (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). For this reason, changes to external groups take effect only after the Security Policy is installed or after the Users Database is downloaded.

User Templates

A user template lets you to create a prototype of a standard user, whose properties are common to many users. Any user you create based on this template will inherit all the properties of the user template, including memberships in groups. Changes in the template do not affect existing users, only future ones.

**To create a new user template:**
1. Click the **Users** tab in the **Objects** tree.
2. Click **Users and Administrators**.
3. Click **General** Properties and enter a template name in the **Template name** field.
   - This property is required and is case sensitive.
4. Do one of these steps to set the expiration date:
   - Select **According to Global Properties** to use the default expiration date.
   - Select **Expire at** to manually set the expiration date. Select a date using the calendar control.
5. Define the remaining user properties (**"Configuring Users"** on page 50).
To use this template to create a new user:
1. Right-click the Users folder and select New User > [Template name].
2. In the General tab, enter the User Name. The user name is not inherited from the template.
3. Define or change other properties ("Configuring Users" on page 50) as required.
Other properties are inherited from the template.

Configuring Users

Users are personnel responsible for managing the Security Management environment. Administrators have permissions to use the SmartConsole clients.

This section includes procedures for configuring users using SmartDashboard.

In this section
Creating or Changing a User 50
General Properties 50
Setting the Expiration Date 51
Assigning a Permissions Profile 51
Authentication 52
Locations 52
Connection Times 52
Certificates 52
Encryption 53

Creating or Changing a User

This section shows you how to create, change or delete a user.

To create a new user:
1. In SmartDashboard, click the Users and Administrators tab.
2. Right-click Users.
   The User Properties window opens.
3. Configure the properties as necessary.

To change an existing user:
1. In SmartDashboard, click the Users and Administrators tab.
2. Double-click a user.
   The User Properties window opens.
3. Configure the properties as necessary.

To delete a user:
1. In SmartDashboard, click the Users and Administrators tab.
2. Select a user.
3. Press Delete and then press OK in the confirmation window.
   If the user is a member of a group, one more confirmation windows opens. Press OK to continue.

General Properties

General properties include the name and other optional properties.

To configure the General Properties:
1. In the User Properties window, click General Properties.
2. Enter a unique name in the User Name field.
   The user name property is required and is case sensitive.
3. Optionally, enter the email address and mobile phone number in the specified fields.
Note - If you generate a user certificate with a non-Check Point Certificate Authority, enter the Common Name (CN) component of the Distinguished Name (DN).

For example, if the DN is: [CN = James, O = My Organization, C = My Country], enter James as the user name.
If you use Common Names as user names, they must contain exactly one string with no spaces.

Setting the Expiration Date
You can assign an expiration date to each administrator. After this expiration date, the administrator cannot log in to the SmartConsole clients or do actions in the Security Management environment.

Note - Account expiration has no effect on operating system administrators. Operating system administrators are different from administrators defined in SmartDashboard and can access the command line.

SmartDashboard includes tools for managing expiration dates and warning administrators of impending expirations.

To configure the expiration date:
1. In the Administrator Properties window, go to the General Properties pane.
2. In the Expiration Date section, click the arrow and select an expiration date using the calendar control.

   The default expiration date shows, as defined in the Default Expiration Settings ("Configuring Default Expiration Parameters" on page 58).

Assigning a Permissions Profile
A permissions profile is a predefined set of Security Management and SmartConsole administrative permissions that you assign to individual administrators. This feature lets you assign and manage complex, granular permissions for many administrators with one definition.

When you configure an administrator, you must assign a permissions profile. Administrators with applicable permissions can create and manage permissions profiles.

To assign permissions to an administrator:
1. In SmartDashboard, create a new administrator or double-click an existing administrator.
2. In the Administrator Properties window, go to the General Properties pane.
3. Select a permissions profile from the list.

You can also do these actions in the Administrator Properties window:
- Click New to create a new permissions profile.
  You must have the applicable permissions to do this.
- Click View to see the selected permissions profile.
**Authentication**

All users must authenticate to access network resources. Select and configure an authentication method for this administrator. If you do not select an authentication method, the administrator cannot log in or use network resources.

**To select an authentication scheme for this user:**
1. In the User Properties window, click Authentication.
2. In the Authentication window, select an authentication scheme.
3. If prompted, enter and confirm a password.
4. For RADIUS or TACACS authentication, select a server.

**Locations**

Define outbound (source) and inbound (destination) connections with network objects that this user can use.

**To add user network locations:**
1. In the User Properties window, click Location.
2. Select one or more Network Objects from the list.
3. Click Add, to add these locations to the source or to the destination list.

**To remove locations from the user permissions:**
1. In the User Properties window, click Location.
2. Select one or more locations from the Source or Destination list.
3. Click Remove.

**Connection Times**

Configure the days and the times during which this user can connect to network resources and applications.

**To configure days and times:**
1. In the User Properties window, click Time.
2. Select or clear the days of the week on which this user can connect to network resources.
3. Enter the time range during which this user can connect in the specified fields.

**Certificates**

You can create and manage certificates for this user. From this pane, you can:
- Send a registration key that lets the user activate a certificate.
- Create a certificate (.p12) file with a private key password for this user.
- Change or Revoke an existing certificate.
To create and Revoke certificates for this user:
1. In the User Properties window, click Certificates.
2. To create a new certificate click New or to edit an existing certificate, double-click it. Do one of these steps:
   - Click Registration Key to send a registration key that activates the certificate. When prompted, select the number of days the user has to activate the certificate before the registration key expires.
   - Click Certificate file to create a .p12 certificate file. Enter and confirm the certificate password when prompted.

Encryption
Select and configure an encryption method for this user.

To select an encryption method:
1. In the User Properties window, click Encryption.
2. Select an encryption method.
3. Click Edit to change the settings for this encryption method.
4. Select Password if this user authenticates with a pre-shared secret password. Enter and confirm the password.
5. Select Public Key if this user authenticates with a public key contained in a certificate file.

Managing User Groups
User groups are collections of related user accounts. These groups let you manage and do operations on many user accounts at the same time.

To create a new user group:
1. In SmartDashboard, click the Users and Administrators tab.
2. Right-click User Groups and select New Group from the options menu.
   The Group Properties window opens.

To change user group settings:
1. In SmartDashboard, click the Users and Administrators tab.
2. Double-click a user group.
   The Group Properties window opens.

To add users or user groups to a group:
1. In the Group Properties window, select users or user groups in the Available Members list.
2. Click Add.
3. If you are adding a group to the list, do one of these tasks when the message window opens:
   - Click Yes to add each member of the group instead of the group.
   - Click No to add only the group.

To remove users or user groups from the group:
1. In the Group Properties window, select users or user groups in the Selected Members list.
2. Click Remove.

To delete a user group:
1. In SmartDashboard, click the Users and Administrators tab.
2. Select a group.
3. Press Delete and then click No to confirm.

Configuring Administrators
Administrators are personnel responsible for managing the Security Management environment. Administrators have permissions to use SmartConsole clients.
Creating or Changing an Administrator

This section shows you how to create, change or delete an administrator.

To create a new user:
1. In SmartDashboard, click the Users and Administrators tab.
3. Configure the user properties as necessary.

To change an existing user:
1. In SmartDashboard, click the Users and Administrators tab.
2. Double-click an existing administrator. The Administrator Properties window opens.
3. Configure the user properties as necessary.

To delete a user:
1. In SmartDashboard, click the Users and Administrators tab.
2. Select an administrator.
3. Click Delete and then click OK in the confirmation window. If the administrator is a member of a group, another confirmation window opens. Click OK to continue.

Configuring General Properties

To configure the General Properties:
1. In the Administrator Properties window, click General Properties.
2. Enter a unique name in the User Name field. The user name property is required and is case sensitive.
3. Optionally, enter the email address and mobile phone number in the specified fields.

Note - If you generate a user certificate with a non-Check Point Certificate Authority, enter the Common Name (CN) component of the Distinguished Name (DN).

For example, if the DN is: [CN = James, O = My Organization, C = My Country], enter James as the user name.

Common names used as user names must have exactly one string with no spaces.

Setting the Expiration Date

You can assign an expiration date to each administrator. After this expiration date, the administrator cannot log in to the SmartConsole clients or do actions in the Security Management environment.

Note - Account expiration has no effect on operating system administrators. Operating system administrators are different from administrators defined in SmartDashboard and can access the command line.

SmartDashboard includes tools for managing expiration dates and warning administrators of impending expirations.

To configure the expiration date:
1. In the Administrator Properties window, go to the General Properties pane.
2. In the Expiration Date section, click the arrow and select an expiration date using the calendar control.
The default expiration date shows, as defined in the Default Expiration Settings ("Configuring Default Expiration Parameters" on page 58).

### Selecting a Permissions Profile

A permissions profile is a predefined set of Security Management and SmartConsole administrative permissions that you assign to individual administrators. This feature lets you assign and manage complex, granular permissions for many administrators with one definition.

When you configure an administrator, you must assign a permissions profile. Administrators with applicable permissions can create and manage permissions profiles.

**To assign a permissions profile:**
1. In the Administrator Properties window, click General Properties.
2. Select a profile from the Permissions Profile list.

You also can do these actions in the General Properties window:
- To create a new permissions profile ("Creating and Changing Permission Profiles" on page 59), click New.
- To see the selected permissions profile, click View Profile.

### Administrator Groups

Administrator groups are collections of related administrator accounts. These groups let you manage and do operations on many administrator accounts the same time.

**To create a new user group:**
1. In SmartDashboard, click the Users and Administrators tab.
2. Right-click User Groups and select New Group
   The Group Properties window opens.
3. To add users or user groups to this group, select them and then click Add.
   If you select a group, a pop-up window shows. Do one of these steps:
   - Click Yes to add each member of the group instead of the group itself.
   - Click No to add only the group.
4. Optionally enter information in the Comment, Email Address or Mobile Phone Number fields.

**To change a user group definition:**
1. In SmartDashboard, click the Users and Administrators tab.
2. To add users or user groups to this group, select them and then click Add.
   If you select a group, a pop-up window shows. Do one of these steps:
   - Click Yes to add each member of the group instead of the group itself.
   - Click No to add only the group.
3. Optionally enter information in the Comment, Email Address or Mobile Phone Number fields.
Configuring Authentication

Administrators must authenticate to access network resources. Select and configure an authentication method for this administrator. If you do not select an authentication method, the administrator cannot log in to SmartConsole clients.

To select an authentication scheme for this administrator:
1. In the Administrator Properties window, click Authentication.
2. In the Authentication window, select an authentication scheme.
3. If prompted, enter and confirm a password.
4. For RADIUS or TACACS authentication, select a server.

Certificates

To create and revoke certificates for this user:
1. In the Administrator Properties window, click Certificates.
2. To create a new certificate, click Generate and save.
3. To revoke an existing certificate, click Revoke.

Configuring Administrator Groups

Administrator groups are collections of related administrators. These groups let you manage and do operations on many administrators at the same time.

To create a new administrator group:
1. In the SmartDashboard, click the Users and Administrators tab.
2. Right-click Administrator Groups and select New Administrators Group.
The Group Properties window opens.
3. Add or remove administrators from the group:
   a) To add administrators and other administrator groups to this group, select them and then click Add.

   Note - If you add a group, a pop-up window shows. Do one of these steps:
   • Click Yes to add each member of the group instead of the group itself.
   • Click No to add only the group.

   a) To remove administrators or other administrator groups, select them and then click Remove.

   Optionally, configure the other settings in this window.

To change administrator group definition:
1. In SmartDashboard, click the Users and Administrators tab.
2. Double-click an administrator group.
The Group Properties window opens.
3. Add or remove administrators from the group:
   a) To add administrators and other administrator groups to this group, select them and then click Add.

   Note - If you add a group, a pop-up window shows. Do one of these steps:
   • Click Yes to add each member of the group instead of the group itself.
   • Click No to add only the group.

   a) To remove administrators or other administrator groups, select them and then click Remove.

4. Optionally, configure the other settings in this window.

To delete an administrator group:
1. In SmartDashboard, click the Users and Administrators tab.
2. Select a group.
3. Press Delete and then click No to confirm.
Managing User and Administrator Expiration

You must assign an expiration date to each administrator. After this expiration date, the administrator cannot log in to the SmartConsole clients or do actions in the Security Management environment.

**Note** - Account expiration has no effect on operating system administrators. Operating system administrators are different from administrators defined in SmartDashboard and can access the command line.

SmartDashboard includes tools for managing expiration dates and warning administrators of impending expirations.

**Working with Expiration Warnings**

There are different methods to give warnings that administrator accounts will expire in a short time or have already expired. This section gives explanations for these warnings and procedures for correcting the issue.

**Log In Warning**

A warning message opens after you log in to SmartConsole clients if your administrator account expiration is about to expire.

Speak to the administrator responsible for managing your administrator account to update the expiration date.

**Using the Expired Accounts Window**

The *Expired Accounts window* shows all administrator accounts that have expired or are near their expiration date. If there are administrators in this condition, the *Expired Accounts* link shows in the SmartDashboard status bar.

To use the *Expired Accounts* window, you must activate this option in the *Administrator Accounts* window. To open the *Expired Accounts* window, click the link.
These icons show the current status of each account.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>Account is active.</td>
</tr>
<tr>
<td>☑️</td>
<td>Account will expire soon.</td>
</tr>
<tr>
<td>☐</td>
<td>Account has expired.</td>
</tr>
<tr>
<td>🔴</td>
<td>Expiration warning ignored.</td>
</tr>
</tbody>
</table>

**To change the expiration date:**
1. Select an administrator account and then click **Update**.
2. In the **Update Expiration Date** window, do one of these steps to change the expiration date:
   - Select **Expire at** and then select an expiration date from the calendar control.
   - OR
   - Select **Never expires** to prevent this administrator account from expiring.

![Expiration Date Window](image)

To change administrator account settings, select an administrator and then click **Edit**.
To deactivate expiration warnings for one administrator account, select the account and then click **Ignore**.
To deactivate expiration warnings for all administrator accounts, do the procedure for setting default expiration parameters.

**Add or Change Administrator Window Warning**
This warning shows in the administrator General Properties pane if the account is about to expire. Make sure that the expiration date is correct and update if necessary.

![Expiration Date Warning](image)

**Configuring Default Expiration Parameters**
The default expiration settings show when you define a new administrator account. These settings include:
- The default expiration date
- The number of days before expiration that warnings show after log in
- The number of days before expiration that the administrator account shows in the **Expired Accounts** window.
To set the default expiration Parameters:
1. In SmartDashboard, select Policy > Global Properties.
2. Select User Accounts or Administrator Accounts.
3. In the User or Administrator Accounts window, set the expiration date using one of these options:
   - Expire after - Enter the number of days (from today) before this user account expires.
   - Expire at - Click the arrow on the text box and then select the expiration date using the calendar control.
4. For Administrator accounts, select Notify during login to show an expiration warning message when the administrator logs in. Enter the number of days before expiration that this warning shows.
5. Select Show indication on the status bar to show expiration warnings in the Expired Accounts window. Enter the number of days before expiration that this warning shows.

Working with Permissions Profiles
A permissions profile is a predefined set of Security Management and SmartConsole administrative permissions that you assign to individual administrators. This feature lets you assign and manage complex, granular permissions for many administrators with one definition.

When you configure an administrator, you must assign a permissions profile. Administrators with applicable permissions can create and manage permissions profiles.

Creating and Changing Permission Profiles
This section includes procedures for creating, changing and deleting permission profiles.

Administrators with the applicable permissions can create, edit or delete permissions profiles.

To create a new permissions profile:
1. In SmartDashboard, select Manage > Permissions Profiles.
2. In the Permissions Profile window, click New and then select Permissions Profile.
3. In the Permissions Profile Properties window, configure permissions profile settings.

To change an existing permissions profile:
1. In SmartDashboard, select Manage > Permissions Profiles.
2. In the Permissions Profile window, click Edit.
3. In the Permissions Profile Properties window, configure permissions profile settings.

To delete an existing permissions profile:
1. In SmartDashboard, select Manage > Permissions Profiles.
2. In the Permissions Profile window, click Remove.
3. Click Yes to confirm.

To configure permissions profile settings:
1. In the Allow access via section, select one of these options:
   - Management Portal and SmartConsole Applications enables access to the Security Management server and SmartConsole applications and Management Portal.
   - Management Portal only enables access to the Security Management server using only Management Portal.
2. In the Permissions section, select one of these options:
   - Read/Write All gives full access to all Check Point products.
     - Manage Administrators lets an administrator with this Permissions Profile can manage other administrators.
     - Read DLP logs including confidential fields and incidents lets an administrator with this Permissions Profile:
       - See all fields of DLP logs in SmartView Tracker.
See the actual message of the incident. This includes permissions to read captured data, therefore, users must understand that their emails can be read if they violate corporate Data Loss Prevention rules.

Send or discard quarantined user emails from SmartView Tracker. With the **Customized** option you can assign a subset of these permissions if necessary. You can give administrator permissions to only see the content of fields in DLP logs in SmartView Tracker and not see/send the actual content of incidents.

- **Read Only All** gives read-only access to all Check Point products.
- **Customized** gives user-defined access to the selected Check Point products and select permissions for each application.

### Configuring Customized Permissions

If you select **Customized Permissions**, you can define permissions for each Security Management resource (object, policy and feature) separately. The resources show on four different panes in the **Administrator Permission Configuration** window.

Each pane contains a list of related resources.

**To configure customized permissions:**

1. In the Permissions section, select **Customized** and then click **Edit**.
2. Select a pane in the **Administrator Permissions Configuration** window:
   - **General** - Security policy, blades and features
   - **Monitoring and Logging** - Monitoring and logging options
   - **Events and Reports** - SmartEvent and SmartReporter features
   - **Provisioning** - SmartProvisioning features and scripting
3. Set permissions for the resources:
   - To prevent the administrator from seeing or configuring a resource, clear its checkbox.
   - To let the administrator see a resource (but not change it), select its checkbox and then select **Read only**.
• To let the administrator see and configure a resource, select its checkbox and then select Read/Write.

Notes:
• You cannot prevent administrators from seeing some resources. These resources have checkboxes with a shaded background.
• Some resources do not have permission selections. You can only select or clear them.

Managing Permissions Profiles
Security Management includes tools to help you manage permissions profiles. You can see information about the latest changes made to a permissions profile and see which administrators are using a permissions profile.

To see information about the latest changes to a permission profile:
1. In SmartDashboard, select Manage > Permissions Profiles.
2. Select a permissions profile.
3. In the Permissions Profiles window, click Actions > Last Modified. The Last Modification window opens.

This window shows:
• Date of the latest change
• Administrator who made the change
• GUI client used to make the change

To see which administrators are using a permissions profile:
1. In SmartDashboard, select Manage > Permissions Profiles.
2. Select a permissions profile.
3. In the Permissions Profiles window, click Actions > Where used. The Object Managers References window opens.

This window shows:
• All administrators using this permissions profile
• If you can delete this permissions profile
Chapter 4

Policy Management

In This Chapter

- The Need for an Effective Policy Management Tool
- Policy Management Overview
- Policy Management Considerations
- Creating a New Policy Package
- Defining the Policy Package's Installation Targets
- Adding a Policy to an Existing Policy Package
- Adding a Section Title
- Configuring a New Query
- Intersecting Queries
- Querying Objects
- Sorting Objects in the Objects List Pane
- Policy Packages
- Dividing the Rule Base into Sections using Section Titles
- Querying Rules
- Querying Network Objects
- Sorting the Objects Tree and the Objects List Pane
- Working with Policies

The Need for an Effective Policy Management Tool

As corporate structures grow in size, more network resources, machines, servers, routers etc. are deployed. It stands to reason that as the Security Policy possesses more and more network objects and logical structures (representing these entities), used in an increasing number of rules, it becomes more complex and more of a challenge for the system administrator to manage.

Because of the complexity of the Security Policy, many system administrators operate according to the "if it ain't broke, don't fix it" axiom:

- New rules are often placed in a "safe" position (e.g. at the end of the Rule Base) rather than in the most effective position.
- Obsolete rules and objects are seldom eliminated.

These practices clutter and inflate the Security Policy and the databases unnecessarily, which invariably affects the performance of the Security Policy and the ability of the system administrator to manage it properly.

A simple, seamless solution is needed to facilitate the administration and management of the Security Policy by the system administrator. This easy-to-use policy management tool needs to take into account:

- The complexity of the corporate structure, with its multiple sites and branches, each of which has its own specific corporate needs.
- The need to easily locate objects of interest.
- The need to analyze the Rule Base.
Policy Management Overview

The Security Management server provides a wide range of tools that address the various policy management tasks, both at the definition stage and at the maintenance stage:

- **Policy Packages** allow you to easily group different types of Policies, to be installed together on the same installation target(s).
- **Predefined Installation Targets** allow you to associate each Policy Package with the appropriate set of gateways. This feature frees you of the need to repeat the gateway selection process every time you install (or uninstall) the Package, with the option to easily modify the list at any given time. In addition, it minimizes the risk of installing policies on inappropriate targets.
- **Section Titles** allow you to visually break down your Rule Base into subjects, thereby instantly improving your orientation and ability to locate rules and objects of interest.
- **Queries** provide versatile search capabilities for both objects and the rules in which they are used.
- **Sorting** your objects in the Objects Tree and Objects List pane is a simple and quick way to locate objects. This feature is greatly facilitated by consistent use of naming and coloring conventions.

Policy Management Considerations

It is recommended to define a set of object naming and coloring conventions, which can significantly facilitate locating the object(s) you need. For example, if you use a prefix indicating the object's location (e.g. NYC_Mail_Server), you can easily group all objects by their location, by simply sorting the Object List pane's Name column. Similarly, you can implement a coloring convention that indicates which site an object belongs to, and then sort the relevant Object Tree's tab by color.

Creating a New Policy Package

1. Choose **File > New** from the menu.
   The **New Policy Package** window is displayed.
2. Enter the **New Policy Package name**. This name cannot:
   - Contain any reserved words, spaces, numbers at the beginning, or any of the following characters: %, #, '"', '?', '&', '*', !, @, ?, <, >, /, \, :
   - End with any of the following suffixes: .w, .pf, .W.
3. In the **Include the following Policy types** section, select any or all of the following policy types, to be included in the Policy Package:
   - **Firewall, Address Translation and Application and URL Filtering**.
   - **Anti-Bot & Anti-Virus**.
   - **QoS**: Traditional mode or Express mode.
   - **Desktop Security**.

   The table below lists the Rule Base tabs corresponding to each policy type.

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Rule Base Tabs Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall, Address Translation and Application and URL Filtering</td>
<td>Welcome, Firewall, NAT, Application and URL Filtering, IPS, Data Loss Prevention, Anti-Spam &amp; Mail, Mobile Access, and IPSec VPN</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus</td>
<td>Welcome, Data Loss Prevention, IPS, Anti-Bot, Anti-Virus, Anti-Spam &amp; Mail, Mobile Access The Anti-Bot and Anti-Virus policy package cannot be added to the global policy. It is a separate policy.</td>
</tr>
<tr>
<td>QoS</td>
<td>Welcome, IPS, Data Loss Prevention, Anti-Spam &amp; Mail, Mobile Access, and QoS</td>
</tr>
<tr>
<td>Desktop Security</td>
<td>Welcome, IPS, Data Loss Prevention, Anti-Spam &amp; Mail, Mobile Access, and Desktop</td>
</tr>
</tbody>
</table>
4. Click OK to create the Policy Package.

SmartDashboard displays the new Policy Package, consisting of the selected policy type tabs.

**Defining the Policy Package's Installation Targets**

1. Choose **Policy > Policy Package Installation Targets**... from the menu.

   The **Select Policy Package Installation Targets** window is displayed.

2. Choose one of the following:
   - **All internal modules** (the default option)
   - **Specific modules**, selected by moving the relevant installation targets from the **Not in Installation Targets** list to the **In Installation Targets** list.

3. Click OK.

   The selected modules will be available as installation targets whenever you install or uninstall this Policy Package.

4. To set the default state of all modules to either Selected or Not Selected, thereby facilitating the policy installation (or uninstall) process, choose **Policy > Global Properties** and select the appropriate setting in the **Global Properties** window's **SmartDashboard Customization** page.

5. You can further modify the installation targets as part of the installation (or uninstall) operation:
   - To modify the targets of this operation only, check the relevant modules and Policies and uncheck all others.
   - To modify the targets of all future operations as well, click **Select Targets**... to display the **Select Installation Targets** window and modify the list as needed.

**Adding a Policy to an Existing Policy Package**

1. Choose **File > Add Policy to Package**... from the menu.

   The **Add Policy to Package** window appears.

2. Select one or more of the available policy types (for example, QoS and Desktop Security).

3. Click OK.

**Adding a Section Title**

1. Select the rule above which or under which you want to add a section title.

2. Choose **Rules > Add Section Title > Above** or **Below** (respectively) from the menu.

   The **Header** window is displayed.

3. Specify the title of the new section and click OK.

   The new section title is displayed in the appropriate location. All rules between this title and the next title (or the end of the Rule Base) are now visually grouped together.

4. By default, the section is expanded. To hide the section's rules, collapse its title by clicking the (-) sign.

5. If the rules following this section are not preceded by their own section title, you can mark the end of this section by adding an appropriate title (e.g. "End of Alaska Rules").

**Configuring a New Query**

1. Display the Rule Base you wish to query (Security, Desktop Security or Web Access) and select **Search>Query Rules**... from the menu.

   The **Rule Base Query Clause / View Policy of Gateway** window is displayed.

2. Select the **Column** you wish to query (e.g. Destination) from the drop-down list.

3. Move the object(s) to which your query applies from **Not in List** to **In List**.

4. If you have selected more than one object, specify whether it is enough for the selected column to contain at least one of these objects (the default option), or must it contain all of them.
5. This clause searches for rules where the specified column contains either the selected objects, or other objects they belong to (e.g. groups or networks).
   - To search for rules where the specified column does not contain the selected objects, check **Negate**.
   - To search only for rules where the specified column contains the objects themselves (as opposed to a group of network they belong to), check **Explicit**.
6. To run this query clause, click **Apply**.
   The rules matching the query clause are displayed in the Rule Base, while all other rules are hidden.
7. To save this query clause, click **Save**.
   The **Save Query** window is displayed.
8. Specify this query’s name and click **OK**.
   The **Rule Base Queries** window is displayed, showing the new query in the **SmartDashboard Queries List**.

**Intersecting Queries**

1. Display the Rule Base you wish to query (*Security*, *Desktop Security* or *Web Access*) and select **Search>Manage Rule Queries** from the menu.
   The **Rule Base Queries** window is displayed.
2. Select the first query you wish to run and click **Apply**.
   The rules matching this query are displayed in the Rule Base, while all other rules are hidden.
3. If you cannot find a relevant query on the list, you can define one now as follows:
   a) Click **New...**
      The **Rule Base Query** window is displayed.
   b) Specify the new query’s **Name** and click **New...**
      The **Rule Base Query Clause / View Policy of Gateway** window is displayed.
   c) Define the query (see Configuring a New Query (on page 64) - step 2 to step 5) and click **OK**.
      The query is added to the **Clause** list.
   d) You can add new clauses to the query and use the following logical operations:
      - **And**, to search for rules matching all clauses
      - **Or**, to search for rules matching at least one of the clauses
      - **Negate query**, to search for the negation of these clauses
4. Select the second query you wish to run.
5. Click one of the following:
   - **And**, so that only rules matching both queries are displayed
   - **Or**, to show rules that match either one of the queries
6. Run the selected query by clicking **Apply**.
7. To unhide all rules, click **Clear all**.

**Querying Objects**

1. Choose **Search > Query Network Objects** from the menu.
   The **Network Objects** window is displayed, showing **All** network objects in your system (the default selection) in the **Network objects** section. Alternatively, you can narrow down the display to the relevant object type (e.g. *firewall installed*, *Check Point QoS installed* etc.).
2. In the **Refined Filter** section, specify the appropriate search criterion, for example:
   - To find objects whose names contain a specific string, choose **Search by Name** from the **Refine by** drop-down list, enter the string you wish to search for (you may use wildcards) and click **Apply**.
   - To find objects with duplicate IP addresses, choose **Duplicates** from the **Refine by** drop-down list.
   The objects that match the search criteria are displayed.
3. To find one of these objects in SmartMap, click **Show**.
4. To create a group consisting of the search results, click **Define query results as group...** and specify the new group's name in the **Group Properties** window.

### Sorting Objects in the Objects List Pane

1. Display the Object Tree's relevant tab (e.g. **Services**).
2. In the **Objects List** pane, click the relevant column's title (e.g. **Port**).
   You can now easily locate the object(s) in question. For example, you can find services that are using the same port.

### Policy Packages

Policy Packages allow you to address the specific needs of your organization's different sites, by creating a specific Policy Package for each type of site. The following diagram illustrates an example organization's network, consisting of four sites.

Each of these sites uses a different set of Check Point Software Blades installed on the Security Gateways:
- **Servers Farm** has the firewall blade installed.
- **Sales Alaska** and **Sales California** sites have both the firewall and the VPN blades installed.
- **Executive Management** has the firewall, VPN and QoS blades installed.

Even sites that use the same product may have very different security needs, requiring different rules in their policies.

To manage these different types of sites efficiently, you need three different Policy Packages. Each Package should include a combination of policies that correspond to the products installed on the site in question.

Accordingly, a Policy Package is composed of one or more of the following policy types, each controlling a different Check Point blade:
- A Firewall and NAT Policy, controlling Security Gateways. This Policy also determines the VPN configuration mode.
- A QoS Policy, controlling Check Point QoS gateways.
- A Desktop Security Policy, controlling SecuRemote/SecureClient machines.

Unlike the above Policies, the Security Rule Base does not apply to a specific site but to the relationship between sites. Therefore, this Rule Base is common to all sites.

The Web Access Rule Base is independent of Policy Packages, since it applies to the organization as a whole (as opposed to a specific site). Its appearance in the Rule Base pane is determined by the Global
Properties settings in SmartDashboard (see the SmartDashboard Customization page of the Global Properties window).

**File Operations**

File operations (New, Open, Save etc.) are performed at the Policy Package level (as opposed to the single policy level).

- **New** allows you to either define a new Policy Package, or add a single policy to an existing Policy Package.
- **Open** allows you to display an existing Policy Package. The policy types included in the Policy Package determine which tabs are displayed in the Rule Base.
- **Save** allows you to save the entire Policy Package.
- **Save As** allows you to save the entire Policy Package, or to save a specific policy that is currently in focus in the Rule Base (i.e. Security and Address Translation, QoS or Desktop Security).
- **Delete** allows you to delete the entire Policy Package.
- **Add to Policy Package** allows you to add existing Policies to your Policy Package.
- **Copy Policy to Package** allows you to copy existing Policies to your Policy Package.

**Note** - To back up a Policy Package before you modify it, use the Database Revision Control feature. Do not use File operations for backup or testing purposes, since they clutter the system with extraneous Packages. In addition, as there are multiple Packages but only one Objects Database, the saved Package may not correspond to changes in the Objects Databases.

**Installation Targets**

To install (and uninstall) Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets. This association both eliminates the need to repeat the gateway selection process per installation, and ensures that Policy Package is not mistakenly installed on any inappropriate target.

The installation targets are defined for the whole Policy Package, thereby eliminating the need to specify them per-rule in each policy. The selected targets are automatically displayed every time you perform an Install or Uninstall operation.

You can set the Package’s Policies to be either checked or unchecked by default for all installation targets (in the SmartDashboard customization page of the Global Properties window), and then modify these settings as needed per-installation.
Dividing the Rule Base into Sections using Section Titles

Section Titles enable you to visually group rules according to their subjects. For example, medium-size organizations may have a single policy for all of their sites, and use Section Titles to differentiate between the rules of each site (larger organizations with more complex Policies may prefer to use Policy Packages). Arranging rules in sections must not come at the expense of placing the most commonly matched rules at the beginning of the Rule Base.

Querying Rules

Querying rules can deepen your understanding of the policy and help you identify the most appropriate place for new rules. You can run queries on the Security, Desktop Security and Web Access Rule Bases.

A query consists of one or more clause statements. Each statement refers to the relationship between the selected object(s) and a specific column in the rule. You can apply the query to single objects, groups of objects or both. To further enhance the query, you can use the appropriate logical condition ("Negate", "And" or "Or").

Once you apply the query, only rules matching its criteria are displayed in the Rule Base. Rules that do not match the query are hidden, but remain an integral part of the policy and are included in its installation. You can refine these query results by running additional queries.

An example scenario in which Rule Base queries are useful is when a server running on host A is moved to host B. Such a change requires updating the access permissions of both hosts. To find the rules you need to change, you can run a query that searches for all rules where host A or host B appear in the Destination column.

By default, the query searches not only for rules that include these hosts, but also for rules that include networks or groups that contain them, as well as rules whose Destination is Any. Alternatively, you can search only for rules that explicitly include these objects.

Querying Network Objects

The Network Objects query allows you to find objects that match the query criteria. You can use this query tool to both control and troubleshoot object-related issues.

The query lists either All objects in your system (the default selection) or a specific type of object (e.g. firewall installed, QoS installed, Security Clusters etc.). You can refine this list using a variety of filters (e.g. Search by Name, Search by IP etc.) and use wildcards in the string you search for.

In addition to these basic searches, you can also perform more advanced queries for:

- objects whose IP address does not match their interface(s)
- duplicate IP addresses used by several objects
- objects that are not used

Note - Objects that are used by entities defined on an LDAP server are considered by the query as "not used".

You can further benefit from the query results by defining them as a group. For example, you may wish to create a group of all Mail Servers in your system and use this group in your Rule Base. If your naming convention is to include the word "Mail" in a Mail Server's name, you can easily find these objects by showing All network objects, choosing the Search by Name filter and entering the string "Mail". Then create a group out of the results and use it in the appropriate rule.

This group object is also available through other Check Point SmartConsoles. For example, if you are using the SmartReporter, you can include this group as the source of connections in the Email Activity report.
Sorting the Objects Tree and the Objects List Pane

The Objects Tree features a right-click Sort menu, allowing you to sort each tab by type (the default selection), name or color. This sort parameter applies to the Objects List pane as well. In addition, the Objects List pane can be sorted by clicking the relevant column's title.

Sorting can be a useful troubleshooting tool, for example:

- To easily determine which site an object belongs to, assign a different color to objects in each site and then sort the relevant Objects Tree's tab by color.
- To expose IP address duplications, display the Network Objects tab of the Objects Tree and sort the IP Address column of the Objects List pane.
- To find out which service is occupying the port you wish to use, display the Services tab of the Objects Tree and sort the Port column of the Objects List pane.

Working with Policies

A Policy Package is a set of Policies that are enforced by the gateways. They can be installed or uninstalled together on selected Security Gateways. The Policy Package components include:

- **Advanced Security** — consisting of
  - the Firewall Rule Base
  - the Address Translation (NAT) Rule Base
  - the Users Database — the proprietary Check Point Internal User Database, containing the definitions and authentication schemes of all users defined in SmartDashboard.
  - the Objects Database — the proprietary Check Point Objects Database, containing the definitions of all network objects defined in SmartDashboard.
- **QoS** — the Quality of Service (Check Point QoS) Rule Base
- **Desktop Security** — the Desktop Security Rule Base

The installation process does the following:

1. Performs a heuristic verification on rules, to ensure they are consistent and that no rule is redundant. If there are verification errors (for example, when two of the Policy’s rules are identical) the Policy is not installed. However, if there are verification warnings (for example, when anti-spoofing is not enabled for a gateway with multiple interfaces), the Policy Package is installed with a warning.
2. Confirms that each of the Gateways on which the rule is enforced (known as the Install On objects) enforces at least one of the rules. Install On objects that do not enforce any of the rules enforce the default rule, which rejects all communications.
3. Converts the Security Policy into an Inspection Script and compiles this Script to generate an Inspection Code.
4. Distributes the Inspection Code to the selected installation targets.
5. Distributes the User and Encryption databases to the selected installation targets.

To Install a Policy Package

To install a Policy Package:

1. Display the Policy package in the Rule Base.
2. Choose Policy > Install... from the menu.
   - The Install Policy window is displayed.
     
     **Note** - The Policy to be installed includes implied rules, resulting from the Global Properties settings. To view the implied rules, select View > Implied Rules from the menu.

3. Choose the installation components:
   a) **Installation Targets** — the VPN gateways on which the Policy is installed. By default, all internal Gateways are available for selection. Alternatively, you define specific Gateways per Policy Package through the Select Installation Targets window (accessed by clicking Select Targets...).
b) For each installation target, choose the Policy components (Advanced Security, QoS or Desktop Security) to be installed.

c) The installation Mode — what to do if the installation is not successful for all targets (so different targets enforce different Policies):
   - Install on each gateway independently, or
   - Install on all gateways, or on none of the gateways

   Note - If you are installing the Policy on a gateway Cluster, specify if the installation must be successful for all Cluster Members.

4. Click OK.

   The Installation Process window is displayed, allowing you to monitor the progress of the verification, compilation and installation.

   If the verification is completed with no errors and the Security Management server is able to connect to the gateway securely, the Policy installation succeeds.

   If there are verification or installation errors, the installation fails (in which case you can view the errors to find the source of the problem).

   If there are verification warnings, the installation succeeds with the exception of the component specified in the warning.

To find out which Policy is installed on each Gateway, select File > Installed Policies...

To Uninstall a Policy Package

To uninstall a Policy Package:

1. Display the Policy package in the Rule Base.
2. Choose Policy > Uninstall... from the menu.
   The Uninstall Policy window is displayed.

   Note - Uninstalling the Policy removes its implied rules as well.

3. Choose the Uninstall components.
4. Click OK.
   The Uninstall window is displayed, allowing you to monitor the progress of the operation. You are notified whether the uninstall has been completed successfully or has failed, and if so, for what reason.

Installing the User Database

The changes you make through SmartDashboard to user or administrator definitions are saved to the User Database on the Security Management server.

To provide your Check Point hosts with installed Management Software Blades with the latest user definitions, you must install the User Database on all relevant targets. Security Gateways that do not have an installed Management Software blade do not receive the User Database.

Choose one of the following options:

- **Policy > Install** — Choose this option if you have modified additional Policy Package components (for example, added new Security Policy rules) that are used by the installation targets.

- **Policy > Install Database** — Choose this option if the only changes you wish to implement are in the user or administrator definitions.

Managing Policy Versions

Policies are created by the system administrator and managed via the Security Management server. Different versions of these policies can be saved. Each version includes backups of the various databases (objects, users, Certificate Authority data, etc.). This information is zipped and saved.
The existing versions are recorded in a "Version table". This table can be viewed and the versions which are displayed can be modified. It is possible to:

- Create a Version
- Export and Import a Version (on page 71)
- View a Version (on page 71)
- Revert to a Previous Version (on page 71)
- Delete a Version (on page 72)

Versions can be created manually by the system administrator, or the system can be set to automatically create a new version every time Security Policy installation takes place.

**Create a Version**

A new version can be created manually by the system administrator, or the system can be set to create new versions automatically every time a new policy is installed. Each new version has the following attributes:

- the creation date
- the system administrator who initiated the new version
- the version of the software
- three editable options determined by the system administrator:
  - the name of the version
  - an additional optional comment
  - a checkbox you can select if you want to ensure that this version will not be automatically deleted (if the automatic deletion of database revisions is activated)

  **Note** - It is recommended to create a version before upgrading the system. This enables the administrator to back out to a functioning environment in case of problems during the upgrade operation.

**Export and Import a Version**

It is possible to export existing versions using the Command Line. This can be useful in order to save disk space. When the exported version is necessary, it can be imported back into the Versions table. The imported version appears in the version table as a regular maintained version.

**View a Version**

A saved version can be viewed in SmartDashboard. For every saved version you can view certain entities such as objects, users, rules. Various operations, such as queries can be executed on these entities.

**Revert to a Previous Version**

The revert operation allows you to revert to a previously saved version. Once you initiate the revert operation, the selected version overwrites the current policy. The one type of information that is not overwritten, is Certificate Authority (CA) data. For security reasons, CA data is not overwritten, but it is merged with the CA data of the current policy.

Before the revert operation is done, the system administrator can expect to receive a report on the expected outcome of the revert operation. For example, information certificates that are going to be revoked is supplied. At this point it is necessary for the system administrator to decide whether or not to continue with the revert operation. Of all the entities included in the reverted version, the user database is not automatically reverted. This is because the users database is extremely dynamic; users are added and deleted frequently. The user database is always changing regardless of the policy version. The system administrator can decide to revert to a selected Policy version, but to maintain the current users database. In this manner, the current user base is used with the restored Policy.
Delete a Version

A previously saved version can be deleted. This operation will also delete the various databases included in the policy version.

Version Configuration

Version Operations are performed via the Database Revision Control window. This window can be accessed by selecting File > Database Revision Control.

In this window you can:

- Create a new version of the current policy manually by clicking Create. When automatic deletion of database versions is activated, you can specify here whether to keep the given version to ensure that it will not be deleted automatically.
- View a saved version by clicking Action > View Version.
- Revert to a saved version by clicking Action > Restore Version.
- View the SmartWorkflow Summary of Changes report, which compares the previous policy installation with the currently pending policy installation by clicking Action > Compare Versions.
- View the properties of a selected version by clicking Properties. Certain of the version options are editable.
- Delete a selected version by clicking Delete.
- Configure settings for automatic deletion of database versions by selecting the Automatically delete old versions checkbox and clicking Configure.

Configure Automatic Deletion

You can configure how to automatically delete old database versions by selecting one of the four options:

- **Delete versions older than: X versions** - where X is the number of most recent versions that should be kept and all versions older than that should be deleted. The default is 50.
- **Delete versions older than: X days** - where X is the time period from today backwards for which all versions created during that time frame should be kept and all versions older than that should be deleted.
- **Delete oldest versions when version storage exceeds: X MBytes/Percent** - where X is the maximum storage (in MBs) for all database versions. Alternatively, you can enter a percentage of the total disk space. Upon reaching this limit, the oldest versions are deleted.
- **Delete oldest versions when available disk space is less than: X MBytes/Percent** - where X specifies the minimum allowed available free disk space in MBs or a percent value. When this limit is reached, the oldest versions are deleted.

  **Note** - SmartWorkflow versions are not affected by this feature. They are neither counted nor deleted.

Database Revision Control and Version Upgrade

After upgrade, the DataBase revision control cannot be used to restore versions created by the previous management server. Previous versions can be opened in Read Only mode for viewing purposes only.

Version Diagnostics

The success or failure of version operations that require modification of the Versions table (such as creating, reverting to or deleting a version) are audited in the audit log of the SmartView Tracker. It is recommended to make use of these logs to ensure that operations have taken place successfully.

Saved versions require disk space. If the existing disk space is exhausted, a threshold alert is sent to the SmartView Monitor. Use this SmartConsole in order to make sure that you meet the disk space requirements needed to implement the versioning feature.
Manual versus Automatic Version Creation

It is possible to create a new version of the current policy by clicking Create in the Database Revision Control window.

Alternately, new versions can be configured to be created automatically every time a policy is installed. You can do this by selecting Create new version upon install policy operation in the Install Policy window. You can access this window by selecting Policy > Install.

Backup and Restore the Security Management server

The Backup and Restore operation exports the Security Management server environment from the Security Management server, and allows it to be imported to another machine. This other machine is a working clone of the Security Management server. It has identical functionalities and capabilities as the original Security Management server. This operation supports Operating System (OS) migration, meaning that the OS of the original, as well as the clone machines can be different.

Using the Backup and Restore feature it is possible to:

- Replace the original Security Management server with another clone Security Management server, while the original is being serviced.
- Maintain a backup of the Security Management server to be used in case of failover.
- Upgrade the Security Management server. System administrators are cautious when upgrading the Security Management server in the production environment. It is more secure to upgrade another machine, import the information from the original Security Management server in order to make a clone. Once the clone has been tested thoroughly and it is found to be fully functional, it can be integrated as the official Security Management server operating in the production environment. The imported information is upgraded prior to being integrated into the new machine so that it complies with the new and/or changed features relevant to the software version to which the Security Management server has been upgraded.
Chapter 5

SmartMap

In This Chapter

Overview of SmartMap 74
Working with SmartMap 74

Overview of SmartMap

Most organizations have multiple gateways, hosts, networks and servers. The topology of these organizations is represented in SmartDashboard by network objects. The topology is often highly complex, distributed over many different machines and enforced in many different rules and rule bases. While this layout matches the needs of your organization, it is difficult to visualize, and even harder to translate in a schematic format. While the network objects are easy to use in the Rule Base, it would be easier to understand and troubleshoot the policy if the rules were displayed in a format where they could be understood visually.

The SmartMap Solution

SmartMap view is a visual representation of your network. This view is used to facilitate and enhance the understanding of the physical deployment and organization of your network.

SmartMap is used in order to:

- Convert the logical layout of your organization into a graphical schematic layout which can be exported as an image file, or printed out.
- Show selected network objects, communities and rules within the graphical representation, by right-clicking on these items from numerous places in the various Rule Bases, Object Tree pages and Object List. For enhanced visualization you can zoom into these selected items.
- Edit objects displayed in SmartMap. The changes made will be integrated throughout SmartDashboard.
- Troubleshoot the policy. For instance SmartMap can resolve unresolved objects, and it can make automatic calculations for objects behind the gateway, Install On targets and for anti-spoofing purposes.

Working with SmartMap

Enabling and Viewing SmartMap

Before you begin to work with SmartMap you need to enable it. In this section you can learn how to enable, toggle and launch SmartMap.

Enable SmartMap

It is not possible to work with SmartMap until it has been enabled.

- To enable SmartMap go to Policy > Global Properties > SmartMap.

Toggle SmartMap

In order to clear SmartDashboard of visual clutter, SmartMap can be toggled until such time that you need to work with it again.
Note - When the SmartMap view is hidden or inactive, all of its menus and commands are disabled; however, topology calculations do continue.

- To view SmartMap go to View > SmartMap.
- To disable SmartMap go to View > SmartMap.

**Launching SmartMap**

SmartMap can be displayed, embedded or docked into the GUI window, or it can be displayed outside of the SmartDashboard window.

- To display SmartMap outside the SmartDashboard window, go to SmartMap > Docked View.

**Adjusting and Customizing SmartMap**

All of the following options affect the way that SmartMap is viewed or displayed.

**Magnifying and Diminishing the SmartMap View**

The level of magnification can be selected or customized. The operations that can be executed include:

- enhancing the view so that all or a selected part of SmartMap optimally fits into the display window.
- selecting from one of the displayed zoom values or customizing your own (for example, Zoom In (magnify) or Zoom Out (diminish) the current SmartMap display).
- magnifying an area in SmartMap by dragging the mouse over a specific area. All objects that fall within the area of the selected box will be magnified.

To automatically zoom into a particular area of SmartMap:
1. Select SmartMap > Zoom Mode.
2. Drag the mouse over a specific area in SmartMap.
   The area you selected will zoom into view.

To select the level of magnification
1. Select SmartMap > Select Mode.
2. Drag the mouse over a specific area in SmartMap.
3. Select SmartMap > Zoom > sub menu and select the options that best meet your needs.

**Scrolling**

If you have an IntelliMouse you can use the scroll wheel to scroll SmartMap.

**Adjusting SmartMap using the Navigator**

The Navigator is a secondary window that displays an overview of SmartMap. This view can be adjusted by altering the select box. As parts of SmartMap are selected in the Navigator window, the SmartMap display is altered to match the selected area. When the Navigator window is closed, its coordinates are saved and when it is reopened, the same view of SmartMap is displayed.

- To launch the Navigator, go to SmartMap > View Navigator.

**Affecting SmartMap Layout (Arranging Styles)**

SmartMap enables you to determine the manner in which network objects are placed within SmartMap in one of two possible styles.

- To select a SmartMap style, go to SmartMap > Customization > Arranging Styles and select one of the following:
  - hierarchic — SmartMap resembles a tree graph
  - symmetric — SmartMap resembles star and ring structures

**Optimally arranging SmartMap (Global Arrange)**

Use Global Arrange to optimally arrange the whole SmartMap within the entire view. SmartMap will be arranged according to the currently set arrange style.
To arrange the entire SmartMap, go to **SmartMap > Arrange > Global Arrange.**

**Optimally arranging SmartMap (Incremental Arrange)**

Use **Incremental Arrange** to optimally arrange a selected area of SmartMap within the entire view. SmartMap will be arranged according to the currently set arrange style.

To arrange a selected area, go to **SmartMap > Arrange > SmartMap > Arrange > Incremental Arrange.**

**Working with Network Objects and Groups in SmartMap**

Network Objects are represented by standardized icons in SmartMap. Network Object icons are connected by edges. Edges (also called connections) are the lines or links that are drawn automatically or manually between network objects in SmartMap. These connections can be fixed or they can be editable.

In order to work with objects, you need to be in **SmartMap > Select Mode**, this mode is the default working mode that allows you to select the object in SmartMap.

SmartMap can be used to add and edit network objects. All items in SmartDashboard that are representations of physical network objects, (such as OSE Devices and network objects), can also be seen and edited in the SmartMap view. Objects that are not representations of physical network objects, (such as Address ranges), cannot be seen in SmartMap.

### Add a Network Object to SmartMap

1. Right-click in SmartMap and select **New Network Object** from the displayed menu.
2. Select the object that you would like to add. The Object’s Properties window is displayed. Configure the new object.

   **Note** - You can add a new network object directly to a network. Right-click on a specific network in SmartMap and then continue according to the previous instructions.

### Create a Group

1. Select all the objects that you would like to include in the group.
2. Right-click on the selected objects and select **Group** from the displayed menu.
3. Configure the group by adding or removing objects to and from the group.

### Edit Network Objects

1. Do one of the following
   - Double-click on an object in SmartMap, or
   - Right-click on a selected object in SmartMap and select **Edit** from the displayed menu.
2. Edit the object. Note that if you change the IP address of a selected object, the placement of the object in SmartMap may change accordingly.

### Remove Network Objects

1. Right-click on the selected object(s) that you would like to delete.
2. Select **Remove** from the displayed menu. You are prompted to make sure that you would like to remove the selected object(s)
3. Click **Yes** to continue.

   **Note** - A warning will be displayed if you attempt to remove an object that is used in the policy. If you ignore the warning the object will still be removed and SmartMap will be adjusted accordingly.

### Fixed Connections versus Editable Connections

- **Automatic connections** — these are non-editable connections that exist between objects whose topology can be deterministically calculated. These connections can only be changed if the objects connected by them are edited. A non-editable connection can be made into an editable one, if other objects are added or modified. For example, if a host is uniquely connected to a network and later an
identical network is defined, the host's connection will be changed from a fixed connection to an editable one to allow for the host to be moved from the one network to the other.

- **Editable connections** — these are editable connections that can be created automatically by SmartMap by adding or modifying objects (for instance by modifying the connection between contained and containing networks), or they can be manually defined by the user. For example, when ambiguous networks are resolved, or when networks are connected to the Internet or to other networks (either by a containment relation or using a connectivity cloud), these connections can be disconnected by right-clicking on the connecting UTM-1 Edge and selecting **Disconnect**.

### Select an area in SmartMap (Select Mode)

Select an area in SmartMap by dragging the mouse over a specific area. All objects that fall within the area of the select box will be selected. Objects that are selected in Select Mode can be dragged to another area in SmartMap.

To move to **Select Mode**, go to **SmartMap > Select Mode**.

#### Customize color and width of objects and edges

Only the width of edges can be customized.

To change options, go to **SmartMap > Customization > View Options**.

### Setting the Layers for SmartMap

Not all object types can be viewed automatically in SmartMap. You can decide what types of layers you would like to add to your view. You can select from the basic layer which provides you all default objects, and from the OPSEC layer which adds certain OPSEC object types.

To set layers, go to **SmartMap > Customization > View Options**.

#### Customize Tooltips for Objects

Select the Information about the network object to be displayed when the cursor passes over the object in SmartMap.

To customize tooltip information, go to **SmartMap > Customization > Tooltips Information**.

#### Customize the Display of Object Labels and IP Addresses

Select Object Label and IP Address attributes and limitations.

To customize, go to **SmartMap > Customization > Object Label Options**.

### Working with SmartMap Objects

SmartMap maintains graphic connectivity between different parts of the network by creating and adding several new topology objects, such as:

- **Internet Objects** — represents the Internet.
- **Connectivity Clouds** — represents a private web or an Intranet.
- **Implied Networks** — a network that is created when a created network object has no viable network to which it can be connected. This network is read-only and non-editable although it can be *actualized*, that is, made into a real network.
- **Ambiguous Networks** — a network that is created when a created network object has multiple viable networks to which it can be connected. The network object is connected to the ambiguous network and the user must decide to which network the network object should be connected.

**Note** - Topology objects, or objects created by the SmartMap view, such as clouds and implied networks, etc., cannot be defined as protected objects. They cannot be included in any group, nor can they be pasted into the SmartDashboard Rule Base.

- **Contained Networks** — A Contained Network is always derived from the same or lower net mask class as the Containing Network.
Add an Internet Cloud

The Internet Cloud defines connectivity between the network object and a public network without supplying technical details of the path between them. Multiple Internet clouds can be added to SmartMap. These clouds are non-editable. When SmartMap performs calculations it looks for Internet clouds and uses them to identify whether interfaces are external or internal.

To create a new cloud, go to **SmartMap > New Internet Cloud**.

Add a Connectivity Cloud

The Connectivity Cloud defines connectivity between the network object and a private network without supplying technical details of the path between them. Multiple Connectivity clouds can be added to SmartMap. These clouds are editable.

To add a connectivity cloud, go to **SmartMap > New Connectivity Cloud**.

Connecting a Network to Internet Clouds

There is always at least one Internet cloud in SmartMap. This cloud cannot be deleted. A line is automatically drawn between an existing network and the sole Internet cloud.

Connecting a network to Connectivity clouds/an Internet cloud, where there is more than one/a Containing Network

1. Right-click on the network you would like to connect to the Connectivity cloud by holding down the `ctrl` key until all networks are selected.
2. Right-click the last selected network.
3. Select `Connect to` and select the option that you would like.

Connecting multiple networks to a Connectivity Cloud

Since SmartMap connects networks according to their IP addresses hierarchy, contained networks are automatically connected to their parent network. This connection is editable and can be removed.

1. Select the networks that you would like to connect to the Connectivity cloud.
2. Select `Connect Networks`.
3. Specify the Connectivity cloud settings.

Viewing the Settings of an Implied network

The Implied network is named by its IP address and a superimposed "I". It is Read Only, unless it is actualized, or made into a real network.

1. Right-click the Implied Network.
2. Select `View` from the displayed menu.

Actualizing an Implied network

The Implied network is Read Only, unless it is actualized, or made into a real network. This means that it is made into a functioning network with its own specification and legitimate (legal or illegal) IP address.

1. Right-click the Implied network.
2. Select `Actualize` from the displayed menu.
3. Configure the settings.

Removing the Connection between a Containing and a Contained network

1. Right-click the UTM-1 Edge of the Contained Network.
2. Select `Disconnect` from the displayed menu.

Working with Folders in SmartMap

Topology collapsing, often referred to as folding, facilitates the use of SmartMap by expanding or collapsing topology structures. This collapsing mechanism simplifies SmartMap, by ridding it of visual clutter, but still preserving its underlying structure. The folding mechanism allows you to collapse certain topology structure types.
The folders can be created at the following points:

- On a UTM-1 Edge that is an interface as well as all the objects behind it.
- On any network which has hosts or containing networks.
- On any gateway and its locales.

There are two special folders which can be collapsed:

- **Objects To Resolve** — contains network objects and unresolved hosts that are ambiguous.
- **External Objects** — contains hosts which have no networks to which they can be connected (because they do not fit into any network's IP address range) as well as any standalone networks. This folder does not include Check Point installed objects.

### Collapsing locales

1. Right-click the locale.
2. Select **Collapse Locale** from the displayed menu.

### Collapsing other Topology Structures

1. Right-click on the object that you would like to collapse.
2. Select **Collapse Object** where object is a variable depending on the object that you selected.

### Expanding Topology folders

1. Right-click the folder which contains the content that you would like to view.
2. Select **Expand** from the displayed menu.

### Viewing the Content of "special" folders

**External Objects** and **Unresolved Objects** are two special types of folders which cannot be expanded, but whose contents can be viewed:

1. Right-click the folder whose contents you would like to view.
2. Select **Show Contents** from the displayed menu.

### Hiding the contents of "special" folders

**External Objects** and **Unresolved Objects** are two special types of folders which cannot be expanded, but whose contents can be hidden:

1. Right-click the folder whose contents you would like to hide.
2. Select **Hide Contents** from the displayed menu.

### Defining the contents of a "special" folder as a group

1. Right-click the folder whose member you would like to group.
2. Select **Define as Group** from the displayed menu.
3. Configure the **Group Properties** window.

### Renaming Topology folders

Folders are given a default name. This name can be edited.

1. Right-click the folder that you would like to rename.
2. Select **Rename** from the displayed menu.
3. Enter a new name for the folder.

### Adding the contents of a SmartMap folder to the Rule Base

When the contents of the folder are dragged and copied into the Rule Base you will be prompted to decide whether or not to save the members of the folder as a group, or to add the contents member by member.

1. Select the folder whose contents you would like to add to the Rule Base.
2. Press the Shift key.
3. Drag the selected folder to the desired location in the Rule Base.
4. If the contents are added as a group, configure the **Group Properties** window.

**Editing External Objects**

External Objects are hosts which have no viable networks to which they can be connected. That is to say their IP address is not within the range of the IP address of any currently defined network.

1. Right-click the **External Objects** folder.
2. Select **Edit** from the displayed menu.
3. Configure the **Properties** window of the selected external object.

**Viewing Gateway Clusters**

The gateway cluster objects are never included in the **Objects to Resolve** folder, even though they may be unresolved.

1. Right-click the selected gateway cluster.
2. Select **Show Members** from the displayed menu.

**Integrating SmartMap and the Rule Base**

You can drag rules from the Rule Base and show them in SmartMap. You can enhance your understanding of the displayed rule by adding a Legend. You can paste objects and folders from SmartMap. You can show network objects selected in the Rule Base and some other locations in SmartMap.

**Display a Legend for regular and/or NAT rules**

The Legend provides a key to the understanding of rules displayed in SmartMap.

- To display a legend, go to **SmartMap > Customization > View Options**.

**Adding the contents of a SmartMap folder to the Rule Base**

See Working with Folders in SmartMap (on page 78).

**Pasting Network Objects in the Rule Base**

Topology objects (for instance clouds, ambiguous networks, etc.) cannot be pasted into the Rule Base.

1. Right-click on a selected network object.
2. Select **Copy to Rule Base** from the displayed menu.
3. Right-click the column in which the selected network object should be pasted.
4. Select **Paste** from the displayed menu.

**Viewing a Network Object selected in the Rule Base in SmartMap**

1. Select the Network Object in the Rule Base that you would like to show in SmartMap.
2. Drag the network object using the left mouse button, and drop it into SmartMap.

**Viewing Network Objects selected in SmartMap in the Rule Base**

1. Select the Network Object in SmartMap that you would like to show in the Rule Base.
2. Drag the network object using the left mouse button and the **shift** and **alt** buttons of the keyboard, and drop it into SmartMap.

**Showing a rule in SmartMap**

A rule that you select to show in SmartMap can be shown in a magnified view or according to the current zoom level.

**Note** - Only Security Policy rules can be shown in SmartMap View.

1. Select a rule in the Rule Base that you would like to display in SmartMap from the rule number.
2. Select **Show** and a view option from the displayed menu.
Display the Rule Color Legend

Rules appear as combinations of highlighted colors and arrows on SmartMap. For instance, colors are designated to represent the Source, Destination and Install On columns of SmartDashboard. These colors can be viewed in the Rule Color Legend window, which is displayed when a rule is shown.

Drag a rule into SmartMap and the Rule Color Legend is automatically displayed.

Understanding the Rule Color Legend

Rules appear as combinations of highlighted colors and arrows on SmartMap. The colors assigned to the arrows represent the action being performed. The arrow also indicates the direction of the rule; from whence the rule came (source), and to where it is going (destination).

- **Red**—Drop, Reject
- **Green**—Accept
- **Blue**—User Auth, Client Auth, Session Auth
- **Purple**—Encrypt, Client Encrypt

Rules that require special attention

When rules are shown in SmartMap, the “Any” value is represented by the icon at the base or the head of the arrow, to indicate that the Source or Destination, respectively, is Any.

The rules mentioned below are mapped and displayed in a specific manner:

- Where the Source is **Any**, the rule is mapped from the Install On to the Destination.
- Where the Destination is **Any**, the rule is mapped out from the Source to the Install On.
- Where both Source and Destination are **Any**, only the paths between the Install Ons are shown.

Troubleshooting with SmartMap

SmartMap can be used as a troubleshooting tool, mostly for topology calculations and certain connectivity issues such as duplicated networks and unresolved object interfaces.

For what objects are topology calculations made?

Topology information specifies data about the object interfaces and the IP addresses behind the interfaces.

- Security Gateways with two or more interfaces
- OSE Devices

Calculating topology information

You can calculate topology for objects selected in the following places:

- SmartMap
- Objects Tree
- Objects List

The Legend in the Topology Calculation Results window explains how you are meant to read the Interfaces topology list.

- **Red**—the results of the calculation are different from the currently defined topology information. This information needs to be approved. Click Approve to display and contrast the current topology information with the resulting topology information. Click Approve all to automatically approve all calculations without comparing and contrasting results.
- **Blue**—the calculation has been automatically approved.
- **Regular**—no change has been made to the topology information.

To calculate topology for a selected object

1. Right-click the selected object.
2. Select Calculate Topology from the displayed menu.
3. The **Topology Calculation Results** window displays the topology information after a calculation has been made for the selected object.

**What is SmartMap Helper?**
SmartMap Helper teaches you how to solve tasks relating to connectivity such as:

- Duplicated networks
- Unresolved object interfaces

The Helper is a learning tool. Once you understand how to solve these connectivity tasks, you can solve them directly in SmartMap View, and not via the Helper.

**Troubleshooting duplicated networks**
Duplicated networks occur if there is more than one network with an identical net mask and IP address.

Note - Some network systems may require duplicated networks. Consider the needs of your system before modifying duplicated networks.

To solve duplicated networks you can modify the shared IP address so that they are all unique. Alternately you can delete the duplicated network.

**Troubleshooting unresolved object interfaces**
When there is more than one viable network to which a network object can be connected, the network object is temporarily connected to an Ambiguous network until such time that it can be properly resolved. See Ambiguous Networks in Working with SmartMap Objects (on page 77).

**What objects can be defined as protected objects?**
Any object which does not lead to the Internet can be defined as a protected object. This includes:

- Gateway clusters
- Security Gateways with two or more interfaces
- OSE Devices

**Defining Protected Objects as Groups**
Any object which does not lead to the Internet can be defined as a protected object group.

1. Right-click the selected object(s).
2. Select **Define Protected Objects as Group** from the displayed menu.
3. Configure the **Group Properties** window.

**Working with SmartMap Output**
Once you have set up your deployment there are several operations that can be performed. Make sure that you save and/or install your policy in order to ensure that all the changes made in SmartMap are applied. SmartMap is always displayed in the layout and with the last coordinates that it had when it was last saved. Once SmartMap is saved you can print SmartMap or even export it to another format for ease of use.

The following options are accessible from the **SmartMap** menu in SmartDashboard:

**Print SmartMap**
Set the attributes by which SmartMap will be printed. This includes how the output is to be scaled, the size of the margins and finally information to be included (such as page numbers, borders, crop marks, or even a customized caption).

**Export SmartMap (as an image file)**
Configure the attributes for images that are exported to an image file. Include the type and size of the image. Specify the treatment of folders in the exported image. Specify general information, including name, label,
the date of export as well as a logical prefix that can be referred to and understood. This is especially important when saving multiple image files. Finally specify the location to which the image file will be saved and whether you want to open or to print the image files once they have been exported.

**Export SmartMap (to Microsoft Visio)**

You can configure the settings for SmartMap exported to Microsoft Visio. Specify object data that you would like to include. This includes general information about the object such as name, IP address and net mask. Specify the treatment of folders and icons during the export operation. You can preserve the Check Point icons and colors or you can choose to use icons from the Microsoft Visio stencil. Finally, decide which general information should be included on the output, for instance, the date, a label and the location to which the exported SmartMap will be saved.
Chapter 6

The Internal Certificate Authority

In This Chapter

- The Need for the ICA
- The ICA Solution
- ICA Configuration

The Need for the ICA

The Internal Certificate Authority is needed for strong authentication. Authentication for:

- Secure Internal Communication (SIC) between internal Check Point entities
- VPN – for both gateways and users

The ICA Solution

Introduction to the ICA

The ICA is a Certificate Authority which is an integral part of the Check Point product suite. It is fully compliant with X.509 standards for both certificates and CRLs. See the relevant X.509 and PKI documentation, as well as RFC 2459 standards for more information. You can read more about Check Point and PKI in the R75.40 VPN Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).

The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

The ICA issues certificates for:

- SIC – certificates are issued for the Security Management server, its gateways, OPSEC modules, and product administrators in order to enable secure communication for all Check Point-related operations (such as policy installation on gateways, logging, SmartConsole-Security Management server connectivity, etc.).
- VPN certificates for gateways – to enable efficient and seamless strong authentication in VPN tunnel creation.
- Users – to enable strong authentication between remote access users and gateways, as well as other features, such as clientless VPN Security Management server.

The ICA issues Certificate Revocation Lists (CRLs) in order to publish a list of certificates that have been revoked. This revocation may be due to a number of factors: key compromise, certificate loss, etc. The CRLs are published on an HTTP server running on the Security Management server, and can be retrieved by any Check Point gateway for certificate validation.

ICA Clients

ICA operations are performed using the following clients:

- Check Point configuration tool or cpconfig on the Command Line. Using this tool, the ICA is created and a SIC certificate is issued for the Security Management server.
- SmartDashboard. This SmartConsole is used to manage:
  - SIC certificates for the various gateways, as well as for administrators.
  - VPN certificates
- ICA Management tool. This tool is used to manage VPN certificates for users that are either managed on the internal database or on a LDAP server. Additionally it is used to perform ICA management operations.

The ICA generates audit logs when ICA operations are performed. These logs can be viewed in the SmartView Tracker.

**Certificate Longevity and Statuses**

Each certificate issued by the ICA has a defined validity period. When this validity period is over, the certificate becomes *expired*.

An administrator can revoke a certificate. This may be done for a number of reasons, for instance, when a user leaves the organization. If a certificate is revoked, the serial number of the certificate is published on the CRL indicating that the certificate has been officially revoked, and cannot be used or recognized by any entity in the system.

Certificates are created in different stages. SIC certificates, VPN certificates for gateways and User certificates are created in one step via SmartDashboard, although the latter can also be created in a two step process using either SmartDashboard or the ICA Management Tool. If the User certificate is created in two steps, these steps include:

- **Initialization** – during this stage a registration code is created for the user. When this is done, the certificate state is *pending*.
- **Registration** – when the user completes the registration process in the remote client (SecuRemote/SecureClient) using the registration code the certificate becomes *valid*.

The advantages are:

- **Enhanced security**
  - the private key is created and stored on the user's machine
  - the certificate issued by the ICA is downloaded securely to the client machine (and not handed to the user by the administrator)

*Pre-issuance automatic and administrator-initiated certificate removal*

If a user does not complete the registration process within a given period of time (which is by default two weeks), the registration code is automatically removed. An administrator can remove the registration key before the user completes the registration process. After that, the administrator can revoke the user certificate.

*Explicit or Automatic Renewal of User certificates ensuring continuous User connectivity*

A user certificate of type PKCS12 can be renewed explicitly by the user or it can be set to be renewed automatically when it is about to expire. This renewal operation ensures that the user can continuously connect to the organization's network. The administrator can choose when to set the automatic revocation of the old user certificate.

Another added advantage is:

*Automatic renewal of SIC certificates ensuring continuous SIC connectivity*

SIC certificates are renewed automatically after 75% of the validity time of the certificate has passed. If, for example, the SIC certificate is valid for five years, 3.75 years after it was issued, a new certificate is created and downloaded automatically to the SIC entity. This automatic renewal ensures that the SIC connectivity of the gateway is continuous. The administrator can decide to revoke the old certificate automatically or after a set period of time. By default, the old certificate is revoked one week after the certificate renewal has taken place.
SIC Certificate Management

SIC certificates are managed in the Communication window of the gateway object.

**SIC Certificate Attributes**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Configurable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>5 years</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>1024 bits</td>
<td>yes</td>
<td>Can be set to 2048 or 4096 bits</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>yes</td>
<td>Digital Signature and Key encryption</td>
</tr>
</tbody>
</table>

All the attributes in the previous table can be set in the ICA Management Tool.

Gateway VPN Certificate Management

VPN certificate for gateways are managed in the VPN tab of the corresponding network object.

**VPN Certificate Attributes**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Configurable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>5 years</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>1024 bits</td>
<td>yes</td>
<td>Can be set to 2048 or 4096 bits</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>yes</td>
<td>Digital Signature and Key encryption</td>
</tr>
<tr>
<td>ExtendedKeyUsage</td>
<td>0 (no KeyUsage)</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

All the attributes in the previous table can be set in the ICA Management Tool.

Note - If the gateway certificate is stored on a hardware token, the key size is configured in the Objects_5_0.C file using the dbedit utility, see Modifying the Key Size (on page 87).

User Certificate Management

Internally managed User Certificates can be managed (for example, operations such as initialization, revocation or the removal of registrations can be performed) either from the User Properties window in SmartDashboard or by using the ICA Management Tool.

User Certificates of users who are managed on an LDAP server can only be managed via the ICA Management Tool.

**User Certificate Attributes**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Configurable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>2 years</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>1024 bits</td>
<td>yes</td>
<td>Can be set to 2048 or 4096 bits</td>
</tr>
<tr>
<td>DN of User certificates managed by the internal database</td>
<td>CN=user name, OU=users</td>
<td>no</td>
<td>This DN is appended to the DN of the ICA</td>
</tr>
<tr>
<td>DN of User certificates managed on an LDAP server</td>
<td></td>
<td>yes</td>
<td>Depends on LDAP branch</td>
</tr>
</tbody>
</table>
### Modifying the Key Size

If the user completes the registration from the Remote Access machine, the key size can be configured in the Advanced Configuration page in SmartDashboard. This page can be accessed by selecting Policy > Global Properties > SmartDashboard Customization > Advanced. This is the recommended method.

Alternately you can edit the key size using the `dbedit` utility of the `Objects_5_0.C` by modifying the size of the key as it is listed in `users_certs_key_size` Global Property. The new value is downloaded when the user updates his site.

**How is it done?**

In SmartDashboard or in the `dbedit` utility:

1. Change the attribute `ica_key_size` to one of the following values: 1024, 2048 or 4096.
2. Run `fwmsic_reset`.
3. Run `cpconfig` and define the CA name in the Certificate Authority tab.
4. When you are done, click OK.
5. Run `cpstart`.

### CRL Management

By default, the CRL is valid for one week. This value can be configured. Fresh CRLs are issued:

- when approximately 60% of the CRL validity period has passed
- immediately following the revocation of a certificate

It is possible to recreate a specified CRL via the ICA Management Tool. This acts as a recovery mechanism in the event that the CRL is deleted or corrupted. Moreover, an administrator can download a DER encoded version of the CRL using the ICA Management Tool.

### CRL Modes

The ICA is able to issue multiple CRLs. The purpose of multiple CRLs is to eliminate any CRL from becoming larger than 10K. If the CRL exceeds 10K, IKE negotiations may fail when trying to establish VPN tunnels.

Multiple CRLs are achieved by attributing every certificate which is issued to a specific CRL. If revoked, the serial number of the certificate appears in this specific CRL.

The CRL Distribution Point (CRLDP) extension of the certificate contains the URL of the specific CRL. This ensures that the correct CRL is retrieved when the certificate is validated.

### ICA Advanced Options

**Modifying the ICA Key**

The ICA is created with a key of size 2048 bits. There are certain cases in which a key of a different size is required (of either 1024 or 4096 bits). In such a case, the ICA must be re-created. This can be done using the command lines and the ICA Configuration file.
The ICA Management Tool

The ICA Management Tool is a user-friendly tool that allows an administrator to perform multiple operations on and for the ICA, such as:

- Certificate management and searches
- CRL recreation and download
- ICA configuration
- ICA cleanup resulting in the removal of expired certificates

Note - The ICA Management Tool is supported by SSL version 3 and TLS.

The ICA Management Tool GUI

The Interface is divided into three panes:

- The **Menu** pane - select the operation to be performed from the menu pane.
- The **Operations** pane - the operation is configured and applied in this pane. From this window you can:
  - **Manage Certificates** - this window is divided into search attributes configuration and bulk operation configuration.
  - **Create Certificates** - from this window you can create certificates.
  - **Configure the CA** - this window contains the configuration parameters and enables the administrator to configure them. You can also view the CA's time, name, and the version and build number of the Security Management server.
  - **Manage CRLs** - from this window you can download, publish, or recreate CRLs.
- The **Search Results** pane - the results of the applied operation are displayed in this pane. This window consists of a table with a list of searched certificates attributes.

The ICA Management Tool is operational from any browser on any platform. Using HTTPS it is possible to connect securely from the ICA Management Tool to the ICA provided that an administrator certificate is added to the browser.

Note - The ICA Management Tool can connect to the ICA in clear, however for the sake of security it is recommended to work encrypted in HTTPS.

Notifying Users about Certificate Initialization

The ICA Management Tool can be used to send mail to users to notify them about certificate initialization. In order to send mail notifications, the administrator must configure:

1. the mail server.
2. the mail "From" address.
3. an optional "To" address, which can be used if the users' address is not known. In this case, when the certificates are issued, the administrator can get the mails and forward them to the corresponding address.

Performing Multiple Simultaneous Operations

In order to ease the management of user certificates the ICA Management Tool can perform multiple simultaneous operations. For example, it is possible to:

1. Make a single LDAP query for getting the details of all the organization employees.
2. Create a file out of this data, and then use this file to:
   - initiate the creation of certificates for all employees
   - notify all employees of these new certificates
The following are the types of operations that can be performed simultaneously:

- initiate user certificates
- revoke user certificates
- send mail to users
- remove expired certificates
- remove certificates for which the registration process was not completed

**ICA Administrators with Reduced Privileges**

The ICA Management Tool supports administrators with reduced privileges. These administrators can make basic searches and initialize certificates for new users. Multiple concurrent operations cannot be executed by these administrators. These administrators may typically be help desk operators who are charged with the handling of new employees.

**ICA Configuration**

**Retrieving the ICA Certificate**

In certain scenarios it is required to obtain the ICA certificate. Peer gateways that are not managed by the Security Management server need to use it for Trust purposes. Also, clients using Clientless VPN, as well as the machine on which the ICA Management Tool is run, require this certificate. In this case, these peers are requested to proceed as follows:

1. Open a browser and enter the appropriate URL (in the format http://<smart_dns_name>:18264)
   The Certificate Services window is displayed.

2. In the Certificate Services window, you can download a CA certificate to your computer or in Windows you can install the CA certification path.

**Management of SIC Certificates**

SIC certificates are managed using SmartDashboard.
Management of Gateway VPN Certificates

VPN Certificates are managed in the VPN page of the corresponding network object. These certificates are issued automatically when the IPSec VPN blade is defined for the Check Point gateway or host. This definition is specified in the General Properties window of the corresponding network object, as shown below:

![Management of Gateway VPN Certificates](Image)

If this certificate is revoked, a new one is issued automatically.

Management of User Certificates via SmartDashboard

The User certificates of users that are managed on the internal database are managed using SmartDashboard. For more information, see the Remote Access VPN chapter in the R75.40 VPN Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).

Invoking the ICA Management Tool

The ICA Management Tool is disabled by default, and can be enabled via the command line.

1. Enable or disable the ICA Management tool using the command line on the Security Management server.

   Usage

   \[c pca\_client \[-d\] set\_mgmt\_tool on|off \[-p <ca\_port>\] \[-no\_ssl\] \[-a|-u "administrator|user DN" ... \]

   where:

   - **on** means to start the ICA Management Tool (by opening port 18265)
   - **off** means to stop the ICA Management Tool (by closing port 18265)
   - **-p** changes the port used to connect to the CA (if the default port is not being used)
• **-no_ssl** configures the server to use clear HTTP rather than HTTPS
• **-a "administrator DN"** ... - sets the DNs of the administrators that will be allowed to use the ICA Management Tool
• **-u "user DN"** ... - sets the DNs of the users that will be allowed to use the ICA Management Tool. This option is intended for administrators with limited privileges.

  Note - If cpca_client is run without -a or -u, the list of the allowed users and administrators will not be changed and the server will be started/stopped with the previously allowed users/administrators.

2. In order to connect to the ICA, add the administrator's certificate to the browser's certificate repository.
3. Open the ICA Management tool from the browser.
   Open the browser and type the location: https://<Management_Host_Name>:18265
   You will be requested to authenticate.
   
   Note - The ICA Management Tool should not be on the same subnet as the Security Management server.

**Search for a Certificate**

**Initiating a Search**

This is performed in the Create Certificates - Operations Pane.

There are two search options, a basic search that includes only the user name, type, status and serial number fields, as well as an advanced search that includes all the search fields. The second option can only be performed by administrators with unlimited privileges.

**Search Attributes**

**Basic Search Attributes**

- **User name** - the exact string which is user name. By default this field is empty.
- **Type** - a drop-down list with the following options: Any, SIC, Gateway, Internal User or LDAP user, where the default is Any.
- **Status** - a drop-down list with the following options: Any, Pending, Valid, Revoked, Expired or Renewed (superseded), where the default is Any.
- **Serial Number** - the serial number of the requested certificate. By default this field is empty.

**Advanced Search Attributes**

This search includes all of the attributes described for the Basic Search, as well as the following:

- **Sub DN** - the string that represents the DN substring. By default this field is empty.
- **Valid From** - a text box with an option to open a calendar and select a date with the format dd-mmm-yyyy [hh:mm:ss] (for example 15-Jan-2003). By default this field is empty.
- **Valid To** - a text box with an option to open a calendar and select a date with the format dd-mmm-yyyy [hh:mm:ss] (for example 14-Jan-2003 15:39:26). By default this field is empty.
- **CRL Distribution Point** - a drop-down list with the following options: Any, No CRLDP (for certificates issued before the management upgrade - old CRL mode certificates) or any CRL number available, where the default is Any.

**The Search Results**

The results of the search are displayed in the Search Results pane. This pane consists of a table with a list of searched certificate attributes such as:

- (SN) Serial Number - the SN of the certificate.
User Name (CN), a user name is considered a string that appears after the first "=" until the next comma.

DN.

Status (where the statuses may be any of the following: Pending, Valid, Revoked, Expired, Renewed (superseded).

The date from which the certificates are valid until the date that they are due to expire.

Search statistics will be displayed in the status bar after every search is performed.

Viewing and Saving Certificate Details

Click on the DN link in the Search Results pane in order to display certificate details.

- If the status is pending a window will be displayed which displays certificate information, including its registration key. In this case a log will be created and displayed in the SmartView Tracker.

- If the certificate was already created, a new window is displayed in which the certificate can be saved on a disk or opened directly, (assuming that this file extension is known to the operating system).

Certificate Operations Using the ICA Management Tool

Certificate operations (such as certificate creation) when done via the ICA Management Tool can only be used for user certificates.

⚠️ Important - SIC certificates and VPN certificates should not be modified using the ICA Management Tool, but via SmartDashboard.

Check the certificates on which you would like to perform the operations.

Removing & Revoking Certificates and Sending Email Notifications

1. Select Manage Certificates in the Menu pane. In the Manage Certificates - Operations pane:
2. Configure a search according to the required attributes, and click Search (see The ICA Management Tool GUI (on page 88)). The results are shown in the Search Results pane.
3. Select the requested certificates from the search results and click on one of the following three options:
   - Revoke Selected - this operation revokes the selected certificates. If a certificate is pending then this operation will remove it from the CA's database.
   - Remove Selected - this operation removes the selected certificates from the Database of the CA and from the CRL if it was found there. You can only remove expired or pending certificates.
   - Mail to Selected - this operation sends mail for all selected pending certificates that include the authorization codes to the selected users. Messages to users that do not have an email defined will be sent to a default address that can be defined in the CA Configuration window (select Menu pane > Configure the CA). For more information, see Notifying Users about Certificate Initialization (on page 88).

Submitting a Certificate Request to the CA Using the ICA Management Tool

There are three methods of submitting certificates:

- Initiate ("Initiating a Certificate" on page 93) - a registration key is created on the CA and used once by a user to create a certificate.

- Generate ("Generating a Certificate" on page 93) - a certificate file is created and associated with a password which must be entered whenever the certificate is accessed.

- PKCS#10 ("Creating a PKCS#10 Certificate" on page 93) - when a PKCS#10 request for a certificate has been received, a certificate is created and delivered to the requester.
**Initiating a Certificate**

To initiate a certificate, proceed as follows:

1. In the Menu pane, select Create Certificates.
2. Select Initiate.
3. Enter a User Name or Full DN, or fill in the Form.
4. If you would like to enter expiration details for certificates or registration keys, click Advanced.
   - Certificate Expiration Date: open the calendar to select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss]. The default is two years from now.
   - Registration Key Expiration Date: open the calendar to select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss]. The default is two weeks from now.
5. Click Go. A registration key is created and displayed in the Results pane.
6. If desired, click Send mail to user to email the registration key. Note that the number of characters in the email is limited to 1900.
7. The certificate becomes usable upon supplying the proper registration key.

**Generating a Certificate**

To generate a certificate, proceed as follows:

1. In the Menu pane, select Create Certificates.
2. Select Generate.
3. Enter a User Name or Full DN, or fill in the Form.
4. If you would like to enter expiration details for certificates or registration keys, click Advanced.
   - Certificate Expiration Date: open the calendar to select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss]. The default is two years from now.
   - Registration Key Expiration Date: open the calendar to select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss]. The default is two weeks from now.
5. Enter a password.
6. Click Go.
7. Save the P12 file, and deliver it to the user.

**Creating a PKCS#10 Certificate**

To create a PKCS#10 certificate, proceed as follows:

1. In the Menu pane, select Create Certificates.
2. Select PKCS#10.
3. Either paste into the space the encrypted base-64 buffer text provided or click on Browse for a file to insert (IE only) to import the request file.
4. Click Create and save the resulting certificate.
5. Deliver the certificate to the requester.

**Initializing Multiple Certificates Simultaneously**

Bulk certificate initialization can be done as follows:

1. Create a file with the list of DNs that you want to initialize. There are two possible syntaxes for this file creation: LDAP or non-LDAP.
2. Browse for this file in the Advanced page of the Create Certificate page.
3. To send registration keys to the users, check the field Send registration keys via email.
4. To receive a file that lists the initialized DNs along with their registration keys, check the field Save results to file. This file can later be used by a script.
5. Click Initiate from file.
Using an LDAP Query

The format of the file initiated by the LDAP search is as follows:

- Each line after a blank line or the first line in the file represents one DN to be initialized.
- If the line starts with "mail=" the string after contains the mail of that user. When no email is given the email address will be taken from the ICA's "Management Tool Mail To Address" attribute.
- If the line is not_after then the value at the next line is the Certificate Expiration Date in seconds from now.
- If the line is otp_validity then the value at the next line is the Registration Key Expiration Date in seconds from now.

Example of Output of an LDAP Search

```plaintext
not_after
86400
otp_validity
3600
uid=user_1,ou=People,o=intranet,dc=company,dc=com
mail=user_1@company.com
<blank_line>
uid=...
```

For more information, see User Directory ("LDAP and User Directory" on page 21).

Using a Simple Non-LDAP Query

It is possible to create a simple (non-LDAP) query by configuring the DN + email in a file in the following format:

```
<email address> space <DN>
... blank line as a separator ...
<email address> space <DN>
```

CRL Operations

In the Menu pane, select Manage CRL and:

1. Either:
   - select Download and enter the number of the CRL that you would like to download, or
   - select Publish to immediately renew the current CRL after changes have been made to the CRL database (this operation is performed automatically at an interval set by the CRL Duration attribute).
   - select Recreate and enter the number of the CRL that you would like to recreate

2. Click Go.

CA Cleanup

On the Manage CRLs page, select Clean the CA's Database and CRLs from expired certificates. This operation gets rid of all expired certificates. Before performing this operation, make sure that the time set on the Security Management server is accurate.

Configuring the CA

In the Menu pane, select Configure the CA. The Configure the CA - Operations pane displays all the configurable fields of the CA. There are three possible operations that can be performed:

- Select Apply to save and enter the CA configuration settings. If the values are valid, the configured settings will take effect immediately. All non-valid strings will be changed to the default value.
- Select **Cancel** to reset all values to the last configuration.
- Select **Restore Default** to revert the CA to its default configuration settings.

Entering the string **Default** in one of the attributes will also reset it to the default after pressing **Configure**. Values that are valid will be changed as requested and others will change to default values.

**CA Data Types**

Edit the CA data by modifying the values displayed in the **Configure the CA - Operations Pane**. The CA data types can be any of the following:

- **Time** - displayed in the format: `<number> days <number> seconds`. For example: **CRL Duration**: 7 days 0 seconds.
  - When changing the attribute, it can be entered as `<number> days <number> seconds` or just as a single number of seconds.
- **Integer** - a regular integer, for example: **SIC Key Size**: 1024.
- **Boolean** - the values can be true or false (not case sensitive), for example: **Enable renewal**: true.
- **String** - for example: **Management Tool DN prefix**: `cn=tests`.

The following attributes are listed in alphabetical order:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Comment</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Code Length</td>
<td>The number of characters of the authorization codes.</td>
<td>min-6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>max-12</td>
<td></td>
</tr>
<tr>
<td>CRL Duration</td>
<td>The period of time for which the CRL is valid.</td>
<td>min-5 minutes</td>
<td>1 week</td>
</tr>
<tr>
<td></td>
<td></td>
<td>max-1 year</td>
<td></td>
</tr>
<tr>
<td>Enable Renewal</td>
<td>For User certificates. This is a Boolean value setting which stipulates whether to enable renewal or not.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>Grace Period Before Revocation</td>
<td>The amount of time the old certificate will remain in Renewed (superseded) state.</td>
<td>min-0</td>
<td>1 week</td>
</tr>
<tr>
<td></td>
<td></td>
<td>max-5 years</td>
<td></td>
</tr>
<tr>
<td>Grace Period Check Period</td>
<td>The amount of time between sequential checks of the Renewed (superseded) list in order to revoke those whose duration has passed.</td>
<td>min-10 minutes</td>
<td>1 day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>max-1 week</td>
<td></td>
</tr>
<tr>
<td>IKE Certificate Validity Period</td>
<td>The amount of time an IKE certificate will be valid.</td>
<td>min-10 minutes</td>
<td>5 years</td>
</tr>
<tr>
<td></td>
<td></td>
<td>max-20 years</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Comment</td>
<td>Values</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>IKE Certificate Extended Key Usage</td>
<td>Certificate purposes for describing the type of the extended key usage for IKE certificates. Refer to RFC 2459.</td>
<td>means no KeyUsage</td>
<td></td>
</tr>
<tr>
<td>IKE Certificate Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459.</td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
<tr>
<td>Management Tool DN prefix</td>
<td>Determines the DN prefix of a DN that will be created when entering a user name.</td>
<td>possible values</td>
<td>CN=</td>
</tr>
<tr>
<td>Management Tool DN suffix</td>
<td>Determines the DN suffix of a DN that will be created when entering a user name.</td>
<td>ou=users</td>
<td></td>
</tr>
<tr>
<td>Management Tool Hide Mail Button</td>
<td>For security reasons the mail sending button after displaying a single certificate can be hidden.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>Management Tool Mail Server</td>
<td>The SMTP server that will be used in order to send registration code mails. It has no default and must be configured in order for the mail sending option to work.</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Management Tool Registration Key Validity Period</td>
<td>The amount of time a registration code is valid when initiated using the Management Tool.</td>
<td>min-10 minutes max-2 months</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Management Tool User Certificate Validity Period</td>
<td>The amount of time that a user certificate is valid when initiated using the Management Tool.</td>
<td>min-one week max-20 years</td>
<td>2 years</td>
</tr>
<tr>
<td>Management Tool Mail From Address</td>
<td>When sending mails this is the email address that will appear in the from field. A report of the mail delivery status will be sent to this address.</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Comment</td>
<td>Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Management Tool Mail Subject</strong></td>
<td>The email subject field.</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td><strong>Management Tool Mail Text Format</strong></td>
<td>The text that appears in the body of the message. 3 variables can be used in addition to the text: $REG_KEY (user’s registration key); $EXPIRE (expiration time); $USER (user’s DN).</td>
<td></td>
<td>Registration Key: $REG_KEY Expiration: $EXPIRE</td>
</tr>
<tr>
<td><strong>Management Tool Mail To address</strong></td>
<td>When the send mail option is used, the emails to users that have no email address defined will be sent to this address.</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Max Certificates Per Distribution Point</strong></td>
<td>The maximum capacity of a CRL in the new CRL mode.</td>
<td>min-3 max-400</td>
<td>400</td>
</tr>
<tr>
<td><strong>New CRL Mode</strong></td>
<td>A Boolean value describing the CRL mode.</td>
<td>0 for old CRL mode 1 for new mode</td>
<td>true</td>
</tr>
<tr>
<td><strong>Number of certificates per search page</strong></td>
<td>The number of certificates that will be displayed in each page of the search window.</td>
<td>min-1 max-approx 700</td>
<td>approx 700</td>
</tr>
<tr>
<td><strong>Number of Digits for Serial Number</strong></td>
<td>The number of digits of certificate serial numbers.</td>
<td>min-5 max-10</td>
<td>5</td>
</tr>
<tr>
<td><strong>Revoke renewed certificates</strong></td>
<td>This flag determines whether to revoke an old certificate after it has been renewed. The reason for not revoking this is to prevent the CRL from growing each time a certificate is renewed. If the certificate is not revoked the user may have two valid certificates.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>Attribute</td>
<td>Comment</td>
<td>Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>SIC Key Size</strong></td>
<td>The key size in bits of keys used in SIC.</td>
<td>possible values:</td>
<td>1024</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4096</td>
<td></td>
</tr>
<tr>
<td><strong>SIC Certificate Key usage</strong></td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SIC Certificate Validity Period</strong></td>
<td>The amount of time a SIC certificate will be valid.</td>
<td>min-10 minutes max-20 years</td>
<td>5 years</td>
</tr>
<tr>
<td><strong>User Certificate Extended Key Usage</strong></td>
<td>Certificate purposes for describing the type of the extended key usage for User certificates. Refer to RFC 2459.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User Certificate Key Size</strong></td>
<td>The key size in bits of the user's certificates.</td>
<td>Possible values are</td>
<td>1024</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4096</td>
<td></td>
</tr>
<tr>
<td><strong>User Certificate Key usage</strong></td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7

Management Portal

Overview of Management Portal

Management Portal enables web-based administration and troubleshooting of the Security Management server. The Management Portal product is included on the release DVD.

The product can be deployed on a dedicated server, or alongside the Security Management server. SSL encrypted connections are used to access the Management Portal web interface. Administrative access can be limited to specific IP addresses. Dedicated administrator users can be limited to Management Portal access only.

Deploying the Management Portal on a Dedicated Server

When deploying the Management Portal on a dedicated server, the following actions should be taken to successfully integrate the Management Portal Server with the Security Management server.

1. During the Management Portal installation you will be asked to choose a SIC (Secure Internal Communication) password that will be used to establish trust with the Security Management server.

   - Fill in the network objects properties.
   - Select Management Portal from the Management tab of the Software Blades list.

3. Add access rules to allow administrative access to the Management Portal Server.

4. Create administrator users with Management Portal permissions if you want to restrict access to the Management Portal.
   - Administrator users can be limited to Management Portal access only using a Permission profile. Create a Permission profile by selecting the Allow access via Management Portal only permission for the specific administrator.
Deploying the Management Portal on the Security Management server

When deploying the Management Portal alongside the Security Management server, the following actions should be taken to successfully integrate the Management Portal component with the Security Management server.

1. Modify the Security Management server network object to include the Management Portal in its Software Blades list if the Management Portal was installed after the Security Management server. If the Management Portal and the Security Management server were installed from the same wrapper this step is unnecessary.

2. Add access rules to allow administrative access using TCP 4433 to the Security Management server itself.

3. Create administrator users with Management Portal permissions if you want to restrict access to the Management Portal.
   - Administrator users can be limited to Management Portal access only using a Permission profile. Create a Permission profile by selecting the **Allow access via Management Portal only** permission for the specific administrator.

Management Portal Commands

- **smartportalstop**: Stops Management Portal services.
- **smartportalstart**: Starts Management Portal services.

Limiting Access to Specific IP Addresses

To allow only specific IP addresses or networks to access the Management Portal, stop the Management Portal and create the `hosts.allow` file under the Management Portal `conf` directory (in Windows: `C:\program files\CheckPoint\R71\SmartPortal\portal\conf` and in Solaris, Linux and SecurePlatform: `/opt/CPportal-R71/portal/conf`). If the `hosts.allow` file is not in the Management Portal `conf` directory you should create it if it is required.

The file format is:

- **ALL: ALL** (to allow all IPs)
- **ALL: x.x.x.x** (to allow specific IPs)
- **ALL: x.x.x.x/y.y.y.y** (to allow specific networks where x.x.x.x is the IP address and y.y.y.y is the netmask)

Management Portal Configuration

The following Management Portal product properties can be modified by editing the `cp_httpd_admin.conf` file. This file can be found in the Management Portal `conf` directory.

- **Note** - Any modifications to the `cp_httpd_admin.conf` file should be done after performing `SmartPortalStop`.

- To change the web server port, modify the **PORT** attribute (default is TCP 4433).
- To use HTTP instead of HTTPS set the **SSL** attribute to 0. It is not recommended to do this for security reasons and should only be used when troubleshooting.
- To change the Web Server certificate modify the **SERVCERT** (the full path to the certificate) and **CERTPWD** (the certificate password) attributes.
Client Side Requirements

The Management Portal can be used with the following web browsers:

- Internet Explorer
- Mozilla
- FireFox
- Netscape

The Management Portal requires that you enable JavaScript and disable Popup blockers in your browser.

Connecting to the Management Portal

Connect to the Management Portal by opening one of the supported browsers and pointing it to:


Using the Management Portal

Once you have authenticated, click on the HELP button to display the Management Portal Online Help. The Online help explains the functionality of each window.

Troubleshooting Tools

- **The web demon (cpwmd) error log file is cpwmd.elg and can be found in the Management Portal log directory.** (in Windows: C:\program_files\CheckPoint\R71\SmartPortal\portal\log and in Solaris, Linux and SecurePlatform: /opt/CPportal-R71/portal/log) directory.
- **The web server (cp_http_server) error log file is cphttpd.elg and can be found in the Management Portal log directory.**
- **To see debug cpwmd messages perform the following:**
  - cpwmd debug -app the Management Portal on
- **To see debug cpwmd messages with greater detail perform the following:**
  - cpwmd debug -app SmartPortal on TERROR_ALL_ALL=5
- **To see additional cp_http_server debug messages you should stop the daemon using cpwd_admin stop -name CPHTTPD and perform the following:**
  - set the TERROR_CPHTTPD_ALL environment variable to 5.
  - set the OPSEC_DEBUG_LEVEL environment variable to 3.
  - execute cp_http_server -v -f <full path to the cp_httpd_admin.conf file>.
- **To see CGI log messages of incoming and outgoing data, you should stop the cp_http_server daemon, set the CFWM_DEBUG environment variable to 1 and run cp_http_server.**
- **The output will be written to the cgi_log.txt and cgi_out.txt files in the temp directory (c:\temp on Windows and /tmp on Unix/Linux/SPLAT).**
Chapter 8

Management High Availability

The Need for Management High Availability

The Security Management server consists of several databases with information on different aspects of the system, such as objects, users and policy information. This data changes each time the system administrator makes modifications to the system. It is important to maintain a backup for this data, so that crucial information is not permanently lost in the event of Security Management server failure.

Moreover, if the Security Management server fails or is down for administrative purposes, a backup server needs to be in place in order to take over its activities. In the absence of the Security Management server, essential operations performed by the gateways, such as the fetching of the Security Policy and the retrieval of the CRL, cannot take place.

The Management High Availability Solution

**Backing Up the Security Management server**

In Management High Availability, the Active Security Management server (Active SMS) always has one or more backup Standby Security Management servers (Standby SMS) which are ready to take over from the Active Security Management server. These Security Management servers must all be of the same Operating System and version. The existence of the Standby SMS allows for crucial backups to be in place:

- for the Security Management server - the various databases in the corporate organization, such as the database of objects and users, policy information and ICA files are stored on both the Standby SMSs as well as the Active SMS. These Security Management servers are synchronized so data is maintained and ready to be used. If the Active SMS is down a Standby SMS needs to become Active in order to be able to edit and install the Security Policy.

- for the Security Gateway - certain operations that are performed by the Security Gateways via the Active SMS, such as fetching a Security Policy, or retrieving a CRL from the Security Management server, can be performed on Standby SMS.
Management High Availability Deployment

In a Management High Availability deployment, the first installed Security Management server is specified as the Primary Security Management server. This is a regular Security Management server used by the system administrator to manage the Security Policy. When any subsequent Security Management server is installed, these must be specified as Secondary Security Management servers. Once the Secondary Security Management server has been installed and manually synchronized, the distinctions between Primary versus Secondary are no longer significant. These servers are now referred to according to their role in the Management High Availability scenario as Active or Standby, where any Security Management server can function as the Active SMS.

The Management High Availability Environment

The Management High Availability environment requires an Active SMS and at least one Standby SMS. The Secondary SMS is created with empty databases. These databases are filled with information that the newly created Secondary SMS gleans from the Active SMS. The Secondary SMS is ready once:

- it is represented on the Primary Security Management server by a network object
- SIC has been initialized between it and the Primary Security Management server
- manual synchronization has been done with the Primary Security Management server for the first time.

It is possible to install a gateway on any of the Security Management servers. The role of these gateways is to protect the Security Management servers. Although the Security Management servers backup one another, High Availability is not implemented between the gateways installed on Security Management servers.

Active versus Standby

All management operations such as editing and installing the Security Policy and modifying users and objects, are done by the Active SMS. If the Active SMS is down, and any of the aforementioned operations need to be performed, one of the Standby SMSs should be made active by the system administrator. This transition from Standby to Active should be *initiated manually*.

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

The frequency of the synchronization between the Standby SMS and the Active SMS is set by the System Administrator. This process can be configured to take place automatically, or it can be set to occur manually.
What Data is Backed Up by the Standby Security Management servers?

In order for Management High Availability to function properly, the following data must be synchronized and backed up:

- configuration and ICA data, such as:
  - databases (such as the Objects and Users).
  - certificate information such as Certificate Authority data and the CRL which is available to be fetched by the Check Point Security Gateways.
- the latest installed Security Policy. The installed Security Policy is the applied Security Policy. The Security Gateways must be able to fetch the latest Security Policy from either the Active or the Standby SMS.

Note - Previous versions of the Database, SmartMap data, as well as View Installed Policy data are not synchronized.

Synchronization Modes

There are two ways to perform synchronization:

- **manual synchronization** is a process initialized by the system administrator. It can be set to synchronize
  - databases, or
  - databases as well as the installed Security Policy.
  The former option synchronizes quicker than the latter option. It should be the preferred mode of synchronization provided that the system administrator has edited the objects or the Security Policy, but has not installed the newly edited Security Policy since the previous synchronization.
- **automatic synchronization** is a process configured by the system administrator to allow the Standby SMSs to be synchronized with the Active SMSs at set intervals of time. This is generally the preferred mode of synchronization, since it keeps the Standby SMSs updated. The basis for the synchronization schedule is that when the Security Policy is installed, both the installed Security Policy and all the databases are synchronized. Additionally, it is possible to synchronize the Standby SMSs when:
  - the system administrator saves the Security Policy
  - at a specified scheduled time
  Even when automatic synchronization has been selected as the synchronization mode, it is possible to perform a manual synchronization.

Synchronization Status

The synchronization status indicates the status of the peer SMSs in relation to that of the selected Security Management server. This status can be viewed in the Management High Availability Servers window or in SmartView Monitor, whether you are connected to the Active or Standby SMS.

The possible synchronization statuses are:

- **Never been synchronized** - immediately after the Secondary Security Management server has been installed, it has not yet undergone the first manual synchronization that brings it up to date with the Primary Security Management server.
- **Synchronized** - the peer is properly synchronized and has the same database information and installed Security Policy.
- **Lagging** - the peer SMS has not been synchronized properly.
For instance, on account of the fact that the Active SMS has undergone changes since the previous synchronization (objects have been edited, or the Security Policy has been newly installed), the information on the Standby SMS is lagging.

- **Advanced** - the peer SMS is more up-to-date.

  For instance, in the above figure, if a system administrator logs into Security Management server B before it has been synchronized with the Security Management server A, the status of the Security Management server A is **Advanced**, since it contains more up-to-date information which the former does not have.

  In this case, manual synchronization must be initiated by the system administrator by changing the Active SMS to a Standby SMS. Perform a **synch me** operation from the more advanced server to the Standby SMS. Change the Standby SMS to the Active SMS.

- **Collision** - the Active SMS and its peer have different installed policies and databases. The administrator must perform manual synchronization and decide which of the SMSs to overwrite.

  For instance, in the above figure, when Security Management server A fails before a synchronization takes place, the changes made (to databases or to the Security Policy) cannot be synchronized with Security Management server B. When Security Management server B takes over from Security Management server A, the system administrator may decide to modify the Security Policy.

  In this case, both Security Management server A and B have some information which is not synchronized with its peer. In order to remedy the collision state, one of the Security Management servers will need to be overwritten. The Security Management server which is found to have the dominant or significant changes should be the Security Management server on which manual synchronization is initiated.

  At this point the system administrator needs to decide which of the Security Management server’s should become the Standby SMS, and change its status, if necessary.

  **Note** - Changes made by the CA, such as the issuance of certificates, could lead to breaches of security if they are overwritten; therefore, any CA changes that are made are merged in order to eliminate security issues.

### Changing the Status of the Security Management server

Although Security Gateways can use the Standby Security Management server to fetch a Security Policy or a fresh CRL, in the event that the Active SMS fails, the Standby SMS must become the Active SMS for two predominant reasons:

1. The Standby SMS cannot perform management operations such as editing and installing the Security Policy. While the Standby is identical in its databases and installed Security Policy to the Active SMS, if changes are needed for the Security Policy the Standby SMS does not have the capacity to make them.
2. The ICA database can only be modified on the Active SMS.

If the Active SMS is going down for administrative purposes, the system administrator should login to the Standby SMS and manually set it as the Active SMS.

Thereafter manual synchronization should be initiated. Once the Standby SMS has become the Active SMS, it is recommended to perform an Install Policy operation, in order to verify that this machine is functioning properly as an Active SMS.

If the Active SMS is in failover, it is likely that the synchronization status of the Active SMS and its peer will be **collision**. In this case the system administrator will need to decide which information will be overwritten.

### Synchronization Diagnostics

The status of all Security Management servers can be viewed in the Management High Availability Servers window in SmartDashboard or via SmartView Monitor.

Audit Logs can be used to view and track management operations as well as Synchronization operations in the SmartView Tracker.
When Synchronization Fails

There are several instances in which the synchronization process might fail:

- synchronization failure - for instance, the Active SMS was unable to make a connection with the Standby SMS at the moment of synchronization. To solve this:
  - manually synchronize the Standby SMS at a later opportunity, or
  - if you are working in automatic mode, reinstall the Security Policy when the Standby SMS can be reached. After the install operation takes place, synchronization occurs automatically.

- Collision between the Security Management servers. In this case the system administrator should perform a manual synchronization and decide which database is the dominant database. The CA is always merged in order to eliminate security issues.

When a collision occurs and one of the Security Management servers is overwritten, it is very useful to follow management operations performed on the overwritten Security Management server in the audit logs of the SmartView Tracker. In this manner it is possible to track and redo these operations, where necessary, on the dominant Security Management server.

Management High Availability Considerations

Remote versus Local Installation of the Secondary SMS

In the Management High Availability deployment the Secondary SMS is often installed locally on the LAN. The system administrator should consider the usefulness of maintaining a remote Standby SMS. This remote Security Management server will not be affected in the case of networking problems on the LAN. This Standby SMS can be made into the Active SMS by the remote system administrator.

Different Methods of Synchronization

Automatic synchronization keeps the peer SMSs updated. However the synchronization may take some time and affect the system performance. It may be useful to schedule a synchronization event that automatically synchronizes the Security Management servers after working hours when the system performance cannot affect the regular work of the employees.

Manual synchronization can be initiated at any stage by the system administrator. Manual synchronization is recommended when changing the Standby SMS to Active (if the Active SMS is about to go down for administrative purposes). It is essential when the synchronization status is collision.

Data Overload During Synchronization

The data saved during the synchronization process is very heavy. Synchronization is optimized if the connectivity between the Security Management server is fast and efficient.

Management High Availability Configuration

Secondary Management Creation and Synchronization - the First Time

1. When installing the Security Management server in a Management High Availability deployment you will be prompted to specify whether it is the Primary Management or the Secondary Management. Select the latter.
2. In SmartDashboard, create a network object to represent the Secondary Security Management server, as follows:
   a) In the Network Objects tree, right-click Check Point.
   b) Select Host from the options menu.
c) In the Check Point Host window > General Properties pane, enter the host name and IP address in the applicable fields.

d) In the Software Blades, section, select the Management tab, and then select Secondary Server. This automatically selects the Logging & Status blades.

a) If necessary, configure a secondary Security Management to work as a Log Server when the Primary Security Management server is not available.

   (i) Access the Security Gateway properties window, and select Logs and Masters > Log Servers.

   (ii) Add the Secondary Security Management server to the When a Log Server is unreachable, send logs to list.

b) Select other blades as necessary.

c) Initialize SIC between the Secondary Security Management server and the Active SMS by selecting Communication.


**Changing the Active SMS to the Standby SMS**

1. On the Active SMS, display the Management High Availability Server window by selecting Policy > Management High Availability.
2. In the displayed window, click **Change to Standby**.

### Changing the Standby SMS to the Active SMS

1. When logging in to the Standby SMS, the **Standby** window is displayed.
2. In the displayed window, select **Change to Active**.
**Refreshing the Synchronization Status of the SMS**

If you suspect that the status of the Security Management server has changed, you may decide to do a refresh operation.

1. Display the Management High Availability Servers window for the selected SMS by selecting **Policy > Management High Availability**
2. In the displayed window, click **Refresh**.

**Selecting the Synchronization Method**

The manner in which the Standby SMSs synchronize with the Active SMS is defined in the **Global Properties - Management High Availability** window. This window is displayed by selecting **Policy > Global Properties > Management High Availability**. The Standby SMS can be synchronized automatically when the policy is installed, saved or on a specified scheduled event. Alternatively, the Standby SMS can be synchronized manually. If manual synchronization is the method of choice, the system administrator will need to initiate the manual synchronization in the **Management High Availability Servers** window. For more information, see Synchronization Modes (on page 104).

**Tracking Management High Availability Throughout the System**

The statuses of all the Security Management servers in the system are displayed in the Management High Availability window. This window is displayed by selecting **Policy > Management High Availability**. Details about the Security Management server and its peers that are displayed include the name, status and type of Security Management server.

All Management High Availability management operations can be viewed in the SmartView Tracker in Audit mode.
Chapter 9

Working with SNMP Management Tools

In This Chapter

The Need to Support SNMP Management Tools 110
The Check Point Solution for SNMP 110
Special Consideration for the Unix SNMP Daemon 112
Configuring Security Gateways for SNMP 112
SNMP Monitoring Thresholds 114

The Need to Support SNMP Management Tools

SNMP management tools are used to monitor the activity of various devices on the network. Because system administrators prefer to work with familiar tools, they might feel more comfortable obtaining status information regarding Check Point products through their regular SNMP Network Management Station (NMS).

The Check Point Solution for SNMP

Check Point addresses this issue by running SNMP agents on Security Gateways. These Security Gateways need to respond to requests from an SNMP Management Station.

Understanding the SNMP MIB

SNMP management systems consist of an SNMP management station and the managed devices, such as bridges, routers, or network servers. SNMP agents constitute the software elements that interface with the device being managed. The agents relate to the configuration and performance characteristics of a managed device as separate identifiable objects. These objects are arranged in an hierarchical namespace,
a tree-like database structure known as a Management Information Block, or MIB. Check Point has a
registered MIB sub-tree with the Internet Assigned Numbers Authority (IANA). The MIB:

1. Gives structure to the data in the registered Check Point tree, assigning a unique number to a Check
Point Security Gateway. The number, a string of integers separated by decimal points, is the OID or
Object Identifier.
   - For Check Point, the root of the registered Object Identifier (OID) is 1.3.6.1.4.1.2620. The notation
     is: Check point OBJECT IDENTIFIER:: = {enterprises 2620}. For example, the MIB on the
     management station resolves a string such as 1.3.6.1.4.1.2640.1.1 to:
   - The object definitions for Check Point are located in the Check Point MIB. The Check Point MIB can
     be read by any third party SNMP Management Station once the MIB has been imported.

2. Provides name resolution, resolving the OID integer string to a user-friendly name. For example, if an
   administrator wants to know the version number of a particular firewall, the administrator selects "version
   number" as the property of the managed device and the MIB maps "version number" to an integer string
   before sending the information request to the agent.
   
   Note - The SNMP management station can read but not modify the
   object definitions for Check Point products.

**Handling SNMP Requests on Windows**

When the Security Management server is installed, a special Check Point dynamic link library (DLL) is listed
in the Windows registry. The SNMP service running on the Operating System loads this DLL. The SNMP
service listens in the standard way on port 161 for incoming SNMP requests from the SNMP Network
Management Station. The Check Point DLL extends the Windows SNMP service to identify those status
requests directed at Check Point products. The relevant data is then retrieved by the DLL and sent to the
SNMP management station.

   Note - The Check Point SNMP agent is an extension of the Windows
   SNMP agent. If you have not installed the standard Windows SNMP
   agent, you cannot use the Check Point SNMP agent.

**Handling SNMP Requests on Unix**

For the Unix platform, a special Check Point SNMP daemon, called cpsnmpd, is installed. This daemon
provides status information on Check Point specific objects. This daemon is not run by default. The daemon
is enabled or disabled through cpconfig. Once enabled, the daemon runs with other Check Point
processes. The SNMP Network Management Station queries the daemon for status information. The
daemon retrieves the information, and replies.

   Note - While the Check Point daemon is SNMP compliant, the
   daemon listens on port 260 instead of 161. The standard Unix SNMP
daemon loads before the Check Point daemon and binds to port 161.
   If the regular daemon is not running, cpsnmpd binds to both ports (161
   and 260). If both ports are occupied by a previous process, the Check
   Point daemon will not run. Further, if the Check Point daemon receives
   a request for an unrecognized OID, it does not forward this to the
   standard snmp unix daemon.

**Handling SNMP Requests on SecurePlatform**

SNMP support is fully integrated in SecurePlatform:

- Net-SNMP Support for full OS-MIB-II.
- Monitoring of Check Point Status Information (AMON) through SNMP.
- SNMP V.2 and V.3 Support.

For additional information about SNMP and SecurePlatform refer to the SNMP Support section in the
SNMP Traps

While Check Point has Alert as one of its tracking types, you might prefer to receive alert messages through your regular SNMP Management Station in the form of an SNMP trap. An SNMP trap is notification that a certain event has occurred. Check Point offers SNMP traps as one of its tracking types. When the conditions of the trap are met, the gateway sends a log to Security Management. Security Management saves the log and sends (via port 162) an SNMP trap to the configured catcher—the SNMP Network Management station. The trap includes the text of the log file.

For example, if any machine outside of the organization tries to make an http connection to a machine within the internal network, the packet is dropped and an SNMP trap is sent:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Internal_private_network</td>
<td>Any</td>
<td>HTTP</td>
<td>Drop</td>
<td>SnmpTrap</td>
</tr>
</tbody>
</table>

The Check Point MIB file describes the SNMP traps that are used by Security Management. The MIB file is located in:

- Windows - %CPDIR%\lib\snmp\chkpnt-trap.mib
- Other OS - %CPDIR%/lib/snmp/chkpnt-trap.mib

Special Consideration for the Unix SNMP Daemon

If you need to run the standard Unix SNMP daemon on port 161, run this daemon before you start cpsnmpd, otherwise cpsnmpd will take the port.

Configuring Security Gateways for SNMP

To handle SNMP requests and traps, the various supported platforms need to be configured in slightly different ways.

Configuring Security Gateways for SNMP Requests

1. On the SNMP Management Station, import the Check Point MIB file from $CPDIR/lib/snmp/chkpnt.mib.
2. If the platform is Windows NT, verify that the Operating System is running the SNMP service. On the Unix platform, verify that port 260 is not bound to another process. If port 260 is available, run cpconfig to enable the cpsnmpd daemon.
3. In the Security Policy Rule Base:
   - Open port 161 if the platform is Windows NT.
   - Open port 260 if the platform is Unix.
   Do this only on the Security Gateways through which the SNMP packets need to pass.
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>If Via</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP_Management_Station</td>
<td>Firewall_Modules</td>
<td>Any</td>
<td>snmp</td>
<td>accept</td>
</tr>
</tbody>
</table>

This policy rule allows the SNMP Management Station to communicate with the Security Gateways.
4. Install the new Security Policy.

Configuring Security Gateways for SNMP Traps

To configure Security Gateways for SNMP traps, the built-in trap script has to be assigned an appropriate catcher.

To assign an appropriate catcher:
1. Open the Global Properties window, Alert Commands page.
2. Select the Run SNMP trap alert script option.
3. In the corresponding text box, replace `internal_snmp_trap localhost` with `internal_snmp_trap <snmpTrapCatcher>`, where the `<variable>` is replaced with the name of the configured catcher. For example, if the configured catcher is a machine called Alaska, the new script would read `internal_snmp_trap Alaska`.

4. For the relevant rules in the Security Policy Rule Base, set the tracking type to `snmp_trap`.

5. If Security Management server and the SNMP Management Station do not reside on the same network segment, open port 162 on all Security Gateways between them. This allows SNMP traps to pass through.
6. Install the Security Policy.

SNMP Monitoring Thresholds

This release lets you configure a variety of SNMP Thresholds that generate SNMP traps, or alerts. You can use the thresholds to monitor many system components automatically without requesting information from each object or device. The categories of thresholds that you can configure include:

- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments.

In each category are many individual thresholds that you can set. For example, the hardware category includes alerts for the state of the RAID disk, the state of the temperature sensor, the state of the fan speed sensor, and others. For each individual threshold, you can configure:

- If it is enabled or disabled
- How frequently alerts are sent
- The severity of the alert
- The threshold point (if necessary)
- Where the alerts are sent to

You can also configure some settings globally, such as how often alerts are send and where they are sent to.

Types of Alerts

There are two different types of alerts:

- **Active alerts** are sent when a threshold point is passed or the status of a monitored component is problematic.
- **Clear alerts** are sent when the problem is resolved and the component has returned to its normal value. Clear alerts look like active alerts but the severity is set to 0.

Configuring SNMP Monitoring

Configure the SNMP monitoring thresholds in the command line of the Security Management server. When you install the policy on the gateways the SNMP monitoring thresholds are applied globally to all gateways.

Configuring in Multi-Domain Security Management

In a Multi-Domain Security Management environment, you can configure thresholds on the Multi-Domain Server and on each individual Domain Management Server. Thresholds that you configure on the Multi-Domain Server are for the Multi-Domain Server only. Thresholds that you configure for a Domain Management Server are for that Domain Management Server and its gateways. If a threshold applies to the Multi-Domain Server and the Domain Management Server gateways, set it on the Multi-Domain Server and Domain Management Server. However, in this situation you might only get alerts from the Multi-Domain Server if the threshold is passed.

For example, because the Multi-Domain Server and Domain Management Server are on the same machine, if the CPU threshold is passed, it applies to both of them. However, only the Multi-Domain Server generates alerts.

You can see the **Multi-Domain Security Management level** for each threshold with the `threshold_config` utility.
• If the Multi-Domain Security Management level for a threshold is Multi-Domain Server, alerts are generated for the Multi-Domain Server when the threshold point is passed.

• If the Multi-Domain Security Management level for a threshold is Multi-Domain Server, Domain Management Server, alerts are generated for the Multi-Domain Server and Domain Management Servers separately when the threshold point is passed.

Configuring a Local Gateway Policy
You can configure SNMP thresholds locally on a gateway with the same procedure that you do on a Security Management server. However, each time you install a policy on the gateway, the local settings are erased and it reverts to the global SNMP threshold settings.

You can use the threshold_config utility to save the configuration file and load it again later. Or you can manually back up the configuration file so that you can copy the configuration to the gateway again after you install the policy.

On SecurePlatform and Linux, the configuration file that you can back up is:
$FWDIR/conf/thresholds.conf

On Windows the configuration file that you can back up is: %FWDIR%\conf\thresholds.conf

Configuration Procedures
There is one primary command to configure the thresholds in the command line, threshold_config. You must be in expert mode to run it. After you run threshold_config, follow the on-screen instructions to make selections and configure the global settings and each threshold.

When you run threshold_config, you get these options:
• Show policy name - Shows you the name configured for the threshold policy.
• Set policy name - Lets you set a name for the threshold policy.
• Save policy - Lets you save the policy.
• Save policy to file - Lets you export the policy to a file.
• Load policy from file - Lets you import a threshold policy from a file.
• Configure global alert settings - Lets you configure global settings for how frequently alerts are sent and how many alerts are sent.
• Configure alert destinations -Lets you configure a location or locations where the SNMP alerts are sent.
• View thresholds overview - Shows a list of all thresholds that you can set including: The category of the threshold, if it is active or disabled, the threshold point (if relevant), and a short description of what it monitors.
• Configure thresholds - Open the list of threshold categories to let you select thresholds to configure.

Configure Global Alert Settings
If you select Configure global alert settings, you can configure global settings for how frequently alerts are sent and how many alerts are sent. You can also configure these settings for each threshold. If a threshold does not have its own alert settings, it uses the global settings by default.

You can configure these options:
• Enter Alert Repetitions - How many alerts will be sent when an active alert is triggered. If you enter 0, alerts will be sent until the problem is fixed.
• Enter Alert Repetitions Delay - How long the system waits between sending active alerts.
• Enter Clear Alert Repetitions - How many clear alerts will be sent after a threshold returns to a normal value.
• Enter Clear Alert Repetitions Delay - How long the system waits between sending clear alerts.
Configure Alert Destinations

If you select Configure Alert Destinations, you can add and remove destinations for where the alerts are sent. You can also see a list of the configured destinations. A destination is usually an NMS (Network Management System) or a Check Point log server.

After entering the details for a destination, the CLI asks if the destination should apply to all thresholds.

- If you enter yes, alerts for all thresholds are sent to that destination, unless you remove the destination from an individual threshold.
- If you enter no, no alerts are sent to that destination by default. However, for each individual threshold, you can configure the destinations and you can add destinations that were not applied to all thresholds.

For each threshold, you can choose to which of the alert destinations its alerts are sent. If you do not define alert destination settings for a threshold, it sends alerts to all of the destinations that you applied to all thresholds.

For each alert destination enter:

- **Name** - An identifying name.
- **IP** - The IP address of the destination.
- **Port** - Through which port it is accessed
- **Ver** - the version on SNMP that it uses
- **Other data** - Some versions of SNMP require more data. Enter the data that is supplied for that SNMP version.

Configure Thresholds

If you select Configure thresholds, you see a list of the categories of thresholds, including:

- **Hardware**
- **High Availability**
- **Networking**
- **Resources**
- **Log Server Connectivity**

Some categories apply only to some machines or deployments. For example, Hardware applies only to Check Point appliances and High Availability applies only to clusters or high availability deployments.

Select a category to see the thresholds in it. Each threshold can have these options:

- **Enable/Disable Threshold** - If the threshold is enabled, the system sends alerts when there is a problem. If it is disabled it does not generate alerts.
- **Set Severity** - You can give each threshold a severity setting. The options are: Low, Medium, High, and Critical. The severity level shows in the alerts and in SmartView Monitor and lets you know quickly how important the alert is.
- **Set Repetitions** - Set how frequently and how many alerts will be sent when the threshold is passed. If you do not configure this, it uses the global alert settings.
- **Set Threshold Point** - Enter the value that will cause active alerts when it is passed. Enter the number only, without a unit of measurement.
- **Configure Alert Destinations** - See all of the configured alert destinations. By default, active alerts and clear alerts are sent to the destinations. You can change this for each destination. Select the destination and you see these options:
  - **Remove from destinations** - If you select this, alerts for this threshold are not sent to the selected destination.
  - **Add a destination** - If you configured a destination in the global alert destinations but did not apply it to all thresholds, you can add it to the threshold.
  - **Disable clear alerts** - If you select this, clear alerts for this threshold are not sent to the selected destination. Active alerts are sent.
Completing the Configuration

To complete threshold configuration and activate the settings:

- On the Security Management server, install the policy on all gateways.
- For a local gateway threshold policy or a Multi-Domain Security Management Multi-Domain Server environment, restart the CPD process using the cpwd_admin utility:
  
a) Run: cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"

b) Run: cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"

Monitoring SNMP Thresholds

You can see an overview of the SNMP thresholds that you configure in SmartView Monitor.

To see an overview of the SNMP thresholds:

1. Open SmartView Monitor and select a gateway.
2. In the summary of the gateway data that open in the bottom pane, click System Information.
3. In the new pane that opens, click Thresholds.
4. In the pane that opens, you can see these details:

   - **General Info** - A summary of the total SNMP Threshold policy.
     - **Policy name** - The name that you set for the policy in the CLI.
     - **State** - If the policy is enabled or disabled.
     - **Thresholds** - How many thresholds are enabled.
     - **Active events** - How many thresholds are currently sending alerts.
     - **Generated Events** - How many thresholds went from not active to active since the policy was installed.

   - **Active Events** - Details for the thresholds that are currently sending alerts.
     - **Name** - The name of the alert (given in the CLI)
     - **Category** - The category of the alert (given in the CLI), for example, Hardware or Resources.
     - **MIB object** - The name of the object as recorded in the .mib file.
     - **MIB object's value** - The value of the object when the threshold became active, as recorded in the .mib file.
     - **State** - The current state of the object, either active or clearing (passed the threshold but is returning to normal value).
     - **Severity** - The severity of that threshold, as you configured for it in the CLI.
     - **Activation time** - When the alert was first sent.

   - **Alert Destinations** - A list of the destinations that alerts are sent to.
     - **Name** - The name of the location.
     - **Type** - The type of location, for example, a log server or NMS.
     - **State** - If logs are being sent from the gateway or Security Management server to the destination machine.
     - **Alert Count** - How many alerts were sent to the destination from when the policy was started.

   - **Errors** - Shows thresholds that cannot be monitored. For example, the gateway cannot monitor RAID sensors on a machine that does not have RAID sensors. Therefore it will show an error for the RAID Sensor Threshold.
     - **Threshold Name** - The name of the threshold with an error.
     - **Error** - A description of the error.
     - **Time of Error** - When the error first occurred.
Chapter 10

Security Management Servers on DHCP Interfaces

In This Chapter

Requirements 118
Enabling and Disabling 118
Using a Dynamic IP Address 118
Licensing a Dynamic Security Management 119
Limitations for a Dynamic Security Management 119

Requirements

Beginning with version R71, Security Management Servers are supported with Dynamic IP addresses on DHCP. To use this:

- The Security Management must be on a Windows system with a DHCP adapter.
- The Security Management must be part of a distributed deployment.

Enabling and Disabling

When you install a Security Management on a Windows machine with a DHCP interface, the Security Management recognizes the DHCP interface. As a result, a Dynamic Address checkbox appears in the General Properties of the Security Management object. This checkbox is automatically selected to enable using the Security Management with a dynamic IP address.

If the Security Management object is not shown in SmartDashboard, make sure that at least one interface is defined with a valid IP address and run cpstop and cpstart to restart Check Point services.

Clear the checkbox to disable the feature and to indicate that a static IP address is being used. When the Dynamic Address checkbox is cleared, Security Gateways will only accept connections from the exact last known IP address of the Security Management.

Using a Dynamic IP Address

For the Security Management to install policy, it should use an IP address that is defined as an allowed Network or Address Range. If no range is defined, a default address range is created from the first 3 octets of the first assigned IP address. For example, if the server is configured with the IP address 192.168.184.55, the default range will be 192.168.184.0 - 192.168.184.255. You can define a new allowed address network or range at any time.

When the managed Security Gateway is of version R71 or higher, policy installation fails if the IP address of the Security Management is outside of the defined ranges and networks.

When the IP address of the Security Management changes, the change is reflected in the database after you restart the SmartDashboard.

To define an allowed Network or Address Range:

1. From the General Properties window of the Security Management object, click Manage.
   The Management DHCP Ranges window opens.
2. Click Add to add a new Network or Address Range.
   - **Network** - Define the first IP address and a subnet mask
   - **Address Range** - Define the first and last IP address of the range.
3. When all networks and address ranges are added, click OK to activate them.

**Licensing a Dynamic Security Management**

A Security Management uses constant IP address based on a MAC address.

**To obtain a license for a Security Management with a dynamic IP address:**

1. Run `cplic dynlic` from the CLI.
   - An IP address is returned.
2. Use this IP address to obtain a license from the Check Point User Center
   (http://usercenter.checkpoint.com).
3. Run `cplic put` in the CLI to install the license. Do not install it using SmartUpdate.

**Limitations for a Dynamic Security Management**

- You cannot configure a Security Management on a DHCP interface in a standalone deployment.
- A dynamic Security Management can only manage remote UTM-1 gateways, Power-1 gateways, and IPS-1 Sensors if they have static IP addresses and are of version R70 or higher.
- Management High Availability is not supported together with automatic IP Address replacement of the Security Management.
Appendix A

Network Objects

In This Appendix
- Introduction to Objects 120
- Network Objects 121

Introduction to Objects

Network Objects are created in order to represent actual physical machines and components such as gateway, servers, as well as logical components such as IP Address Ranges and Dynamic Objects.

Objects are created and managed by the system administrator via SmartDashboard.

All objects are managed using SmartDashboard; therefore, it is recommended that the objects database must not be accessed or edited directly. In this appendix you will find general information about network objects, including configuration specifications, where necessary.

The Objects Creation Workflow

1. Objects created by the system administrator, are automatically stored in the objects database on the Security Management server in $FWDIR/conf/objects_5_0.c.
2. When the Security Policy is installed on the Security Gateway, Security Management server computes the objects.c file for the Security Gateway. This file is computed and derived from the objects_5_0.c file.
4. When a policy is installed, all changes made to objects are applied and saved. These changes are also registered in the objects database which is automatically updated.

Viewing and Managing Objects

When an object is created it is allocated an iconic representation that can be viewed and applied from any of the following locations:

- **Objects Tree** is the Objects manager from which objects are created, viewed and managed. To make sure that all network objects folders are displayed, right-click on the Network Objects root, and uncheck Do not show empty folders.
- **Objects List** is the view from which detailed information about specific objects categories is displayed (such as all the available networks).
- **Rule Base** is the view in which objects are implemented and applied to the rules which make up the Security Policy.
- **SmartMap** is the view in which the objects implemented in the Rule Base are displayed in a graphical representation.
Network Objects

Check Point Objects

Security Gateways

A Security Gateway object is a gateway with more than one interface on which Check Point Software Blades are installed. At least a firewall blade is installed, although other Check Point Software Blade such as QoS or Monitoring may also be installed. This gateway sits on the network that serves as an entry point to the LAN and is managed by the Security Management server. A Security Gateway is characterized as follows:

- it has one or more Software Blades installed
- where the IPSec VPN blade is installed, it requires a VPN license
- it is a routing mechanism that is capable of IP forwarding
- since it has more than one interface it can be used in order to implement anti-spoofing.

If the Security Gateway that you defined does not need to perform IP forwarding or anti-spoofing, you can convert it to a Check Point host.

Converting a Security Gateway into a Check Point host

You can convert a Security Gateway to a Check Point host by right-clicking the Security Gateway in the Objects Tree and selecting Convert to Host.

UTM-1 Edge Gateway

A UTM-1 Edge gateway object is a network object that represents a UTM-1 Edge gateway. This gateway sits on the network and can be managed by the Security Management server or by an external management server.

Defining UTM-1 Edge Gateway Objects

1. In the Network Objects tab of the Objects Tree, create a new UTM-1 Edge gateway.
2. Configure the general settings of the window, including its name and IP address (whether static or dynamic) and version information.
3. To define the UTM-1 Edge gateway as a member of a VPN community, select the VPN Enabled check box and select the VPN Community type (whether Site to Site or Remote Access).

Check Point Host

A Check Point host is a host with only one interface, on which Check Point software has been installed, and which is managed by the Security Management server.

A Check Point host is characterized as follows:

- It has one or more Check Point Software Blades installed.
- It is not a routing mechanism and is not capable of IP forwarding.
- Since it only has one interface, its topology cannot be modified and therefore it cannot be used to implement Anti-spoofing.
- It requires a SecureServer license and not a VPN license.

If you have defined a Check Point host and you are trying to use it to perform IP forwarding or anti-spoofing, you must convert it to a Security Gateway.

Converting a Check Point host into a Security Gateway

You can convert a Check Point host to a Security Gateway by right-clicking the Check Point host in the Objects Tree and selecting Convert to Gateway.
Gateway Cluster
A gateway cluster is a group of Security Gateway machines on which Check Point software has been installed which have been configured to provide failover services using ClusterXL or another Cluster solution.

**Converting a Cluster Member into a Security Gateway**
You can detach a Cluster member from a gateway cluster and convert it into a Security Gateway as follows:
1. Right-click on a Cluster object in the Objects Tree or List.
2. Select **Detach Cluster Members** from the menu.
3. Select the member from the displayed window and click **Detach**.
4. Ignore the displayed warning in order to complete the conversion.
5. The gateway Properties window of the converted cluster member is displayed. Click **OK** to finalize the conversion.

Externally Managed Gateway/Host
An Externally Managed Security Gateway or Host is a gateway or Host which has been installed with Check Point software. This Externally Managed gateway is a Security Gateway which is managed by an external Security Management server. While it does not receive the Check Point Security Policy, it can participate in Check Point VPN communities and solutions.

**Nodes**
A node can represent any network entity. The two most common uses of this object are to create non-Security Gateways and Hosts.
- A gateway node is a gateway which does not have Check Point software installed.
- A host node is a host which does not have Check Point software installed.

**Converting Nodes**
- Gateway Nodes can be converted to Host Nodes and vice versa. Right-click on the specified Node in the Objects Tree and selecting **Convert to Host** or **Gateway**.
- Gateway Nodes can be converted to Security Gateways. Right-click on the gateway Node in the Objects Tree and select **Convert to Check Point Gateway**.
- Host Nodes can be converted to Check Point hosts. Right-click on the specified Host Node in the Objects Tree and select **Convert to Check Point Host**.

Interoperable Device
An Interoperable Device is a device which has no Check Point Software Blades installed. This device is managed by any Management Server, including Security Management server, although it cannot receive the Check Point Security Policy, and it can participate in Check Point VPN communities and solutions.

**Networks**
A Network is a group of IP addresses defined by a network address and a net mask. The net mask indicates the size of the network.
A Broadcast IP address is an IP address which is destined for all hosts on the specified network. If this address is included, the Broadcast IP address will be considered as part of the network.

**Domains**
This object defines a DNS domain name.
The format of the domain name is \texttt{.x.y}, where each section of the domain name is demarcated by a period. For instance \texttt{.mysite.com} or \texttt{.mysite.co.uk}. The domain name that is specified must be an actual domain name in order that it can be resolved to a valid IP address. The first time that a domain name is resolved by the Security Management server a brief delay may occur. Once the domain name has been resolved it is entered into the cache, and no further delays will take place on any subsequent access attempts. On account of the initial delays which may occur for each new domain name, the rules that contain Domain objects in their Source or Destination should be placed towards the end of the Rule Base.

**Groups**

A network objects group is a collection of hosts, gateways, networks or other groups. Groups are used in cases where you cannot work with single objects, e.g. when working with VPN domains or with topology definitions.

In addition, groups can greatly facilitate and simplify network management, since they allow you to perform operations only once instead of repeating them for every group member.

The Group Properties window lists the network objects included from the group versus those excluded from the group. To configure the group, move objects between the lists as needed.

To include an unlisted network object in the group, create it now by clicking New.... This window shows collapsed sub-groups, without listing their members. For a list of all group members (including the sub-groups' members), click View Expanded Group....

**Open Security Extension (OSE) Devices**

**Overview to OSE Devices**

The Open Security Extension features enable Check Point to manage third-party open security extension devices (OSE). The number of managed devices depends on your license. Devices include hardware and software packet filters. Check Point also supports hardware security devices which provide routing and additional security features, such as Network Address Translation and Authentication. Security devices are managed in the Security Policy as Embedded Devices. The Security Management server generates Access Lists from the Security Policy and downloads them to selected routers and open security device. Check Point supports the following devices, as shown in the following table:

**Check Point Supported OSE Devices**

<table>
<thead>
<tr>
<th>OSE Device</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Systems</td>
<td>9.x, 10.x, 11.x, 12.x</td>
</tr>
<tr>
<td>Nortel</td>
<td>13.x, 14.x</td>
</tr>
</tbody>
</table>

When working with a Cisco Router (that is, OSE object), the Rule Base should not contain one of the following. If one of the following is included in the Rule Base, the Security Management server will fail to generate Access Lists from the rules.

- Drop (in the Action column)
- Encrypt (Action)
- Alert (Action)
- RPC (Service)
- <??AH>(Service)
- ACE (Service)
- Authentication Rules
- Negate Cell
OSE Device Properties Window — General Tab

- **Name** — the name of the OSE device
  
  The name given here should be identical to the name as it appears in the system database on the server.

- **IP Address** — the device's IP address

- **Get Address** — click this button to resolve the name to an address
  
  **Note** - It is recommended that you list OSE device objects in your hosts (Unix) and lmhosts (Windows) files in addition to defining them in the Check Point database.

- **Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

- **Color** — Select a color from the drop-down list. The OSE device will be represented in the color selected throughout the SmartMap for easier user tracking and management.

- **Type** — choose one of the following from the drop-down menu:
  - Cisco Systems
  - Nortel

OSE Device Properties Window — Topology Tab

OSE devices report their network interfaces and setup at boot time. Each OSE device has a different command for listing its configuration.

**Note** - At least one interface must be defined in the **Topology** tab or Install Policy will fail.

To add an interface, click **Add**. The **Interface Properties** window is displayed.

To edit an interface, select the interface and click **Edit**, or double-click the interface. The **Interface Properties** window is displayed.

To delete an interface, select the interface and click **Remove**.

The manner in which names are specified for OSE device interfaces is different from the manner in which they are specified for interfaces of other network objects.

- **Name** — name of the network interface as specified in the router's interface configuration scheme.
  
  This name does not include a trailing number.

- **IP Address** — the IP address of the device

- **Net Mask** — the net mask of the device.

Defining Router Anti-Spoofing Properties

The **Interface Properties** window allows you to define router anti-spoofing parameters when installing Access Lists on routers. The **Interface Properties** window is almost identical to the **Interface Properties** window for network objects.

**Note** - To implement anti-spoofing for Cisco (version 10.x and higher), you must define additional properties in the **Setup** tab of each router after you define the Valid Addresses in the Interfaces Properties window. For more information, see Anti-spoofing Parameters and OSE Devices Setup (Cisco and Nortel) (on page 124).

Logging for spoofing attempts is available for external interfaces only.

**Anti-spoofing Parameters and OSE Devices Setup (Cisco and Nortel)**

For Cisco (Version 10.x and higher) and Nortel OSE devices, you must specify the direction of the filter rules generated from anti-spoofing parameters. The direction of enforcement is specified in the **Setup** tab of each router.
For Cisco routers, the direction of enforcement is defined by the **Spoof Rules Interface Direction** property.

**Access List No** — the number of Cisco access lists enforced.

Cisco routers Version 12x and below support an ACL number range from 101-200. Cisco routers Version 12x and above support an ACL range number from 101-200 and also an ACL number range from 2000-2699. Inputting this ACL number range enables the support of more interfaces.

**Username** — the name required to logon to the OSE device.

**Password** — the Administrator password (Read only) as defined on the router.

**Enable Username** — the user name required to install Access Lists.

**Enable Password** — the password required to install Access Lists.

The security administrator must select one of the following options from the drop-down list for the above **Username** and **Password** fields (this includes the Enable fields):

- **None** — Indicates the parameter is not needed.
- **Known** — the value of the parameter must be entered.
- **Prompt** — Indicates that the security administrator will be prompted for this parameter.

**Version** — the Cisco OSE device version (9.x, 10.x, 11.x, 12.x).

**OSE Device Interface Direction** — Installed rules are enforced on data packets traveling in this direction on all interfaces.

**Spoof Rules Interface Direction** — The spoof tracking rules are enforced on data packets traveling in this direction on all interfaces.

---

**Logical Servers**

A Logical Server is a group of machines that provides the same services. The workload of this group is distributed between all its members.

When a Server group is stipulated in the **Servers group** field, the client is bound to this physical server. In Persistent server mode the client and the physical server are bound for the duration of the session.

- **Persistency by Service** — once a client is connected to a physical server for a specified service, subsequent connection to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.
- **Persistency by Server** — once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

**Balance Method**

The load balancing algorithm stipulates how the traffic is balanced between the servers. There are several types of balancing methods:

- **Server Load** — The Security Gateway determines which Server is best equipped to handle the new connection.
- **Round Trip Time** — On the basis of the shortest round trip time between Security Gateway and the servers, executed by a simple ping, the Security Gateway determines which Server is best equipped to handle the new connection.
- **Round Robin** — the new connection is assigned to the first available server.
- **Random** — the new connection is assigned to a server at random.
- **Domain** — the new connection is assigned to a server based on domain names.

**Address Ranges**

An Address Range object stipulates the range of IP addresses used in the network from the first to the last IP address.

This object is used when the networks themselves do not have IP address-net mask alignment, so an Address Range is necessary for the implementation of:
Network Objects

- NAT, and
- VPN

**Dynamic Objects**

A dynamic object is a "logical" object where the IP address will be resolved differently per Security Gateway using the `dynamic_objects` command.

The following are the predefined Dynamic Objects:

- **LocalMachine-all-interfaces** – The DAIP machine interfaces (static and dynamic) are resolved into this object.
- **LocalMachine** – The external interface (dynamic) of the ROBO gateway (as declared in `cpconfig` when configuring the ROBO gateway).
- **InternalNet** – The internal interface of the ROBO gateway (as declared in `cpconfig` when configuring the ROBO gateway).
- **AuxiliaryNet** – The auxiliary interface of the ROBO gateway (as declared in `cpconfig` when configuring the ROBO gateway).
- **DMZNet** – The DMZ interface of the ROBO gateway (as declared in `cpconfig` when configuring the ROBO gateway).

For more information see the [R75.40 Command Line Interface Reference Guide](http://supportcontent.checkpoint.com/solutions?id=sk67581).

**VoIP Domains**

There are five types of VoIP Domain objects:

- VoIP Domain SIP Proxy
- VoIP Domain H.323 Gatekeeper
- VoIP Domain H.323 Gateway
- VoIP Domain MGCP Call Agent
- VoIP Domain SCCP CallManager

In many VoIP networks, the control signals follow a different route through the network than the media. This is the case when the call is managed by a signal routing device. Signal routing is done in SIP by the Redirect Server, Registrar, and/or Proxy. In SIP, signal routing is done by the Gatekeeper and/or gateway.

Enforcing signal routing locations is an important aspect of VoIP security. It is possible to specify the endpoints that the signal routing device is allowed to manage. This set of locations is called a **VoIP Domain**. For more information refer to [R75.40 Command Line Interface Reference Guide](http://supportcontent.checkpoint.com/solutions?id=sk67581).
Appendix B

CLI Appendix


**Security Management server Command Line Interface**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpca_client</td>
<td>This command and all its derivatives are used to execute operations on the ICA.</td>
</tr>
<tr>
<td>cpca_client create_cert</td>
<td>This command prompts the ICA to issue a SIC certificate for the Security Management server.</td>
</tr>
<tr>
<td>cpca_client revoke_cert</td>
<td>This command is used to revoke a certificate issued by the ICA.</td>
</tr>
<tr>
<td>cpca_client set_mgmt_tools</td>
<td>This command is used to invoke or terminate the ICA Management Tool.</td>
</tr>
<tr>
<td>cpconfig</td>
<td>This command is used to run a Command Line version of the Check Point Configuration Tool. This tool is used to configure/reconfigure a Check Point installation.</td>
</tr>
<tr>
<td>cplic</td>
<td>This command and all its derivatives relate to the subject of Check Point license management. All cplic commands are located in $CPRID/bin.</td>
</tr>
<tr>
<td>cplic check</td>
<td>Use this command to check whether the license on the local machine will allow a given feature to be used.</td>
</tr>
<tr>
<td>cplic db_add</td>
<td>The cplic db_add command is used to add one or more licenses to the license repository on the Security Management server. When local licenses are added to the license repository, they are automatically attached to its intended Security Gateway, central licenses need to undergo the attachment process.</td>
</tr>
<tr>
<td>cplic db_print</td>
<td>The cplic db_print command displays the details of Check Point licenses stored in the license repository on the Security Management server.</td>
</tr>
<tr>
<td>cplic db_rm</td>
<td>The cplic db_rm command removes a license from the license repository on the Security Management server. It can be executed ONLY after the license was detached using the cplic del command. Once the license has been removed from the repository, it can no longer be used.</td>
</tr>
<tr>
<td>cplic del</td>
<td>Use this command to delete a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. This command is used for both local and remote machines.</td>
</tr>
<tr>
<td>cplic del &lt;object name&gt;</td>
<td>Use this command to detach a Central license from a Security Gateway. When this command is executed, the License Repository is automatically updated. The Central license remains in the repository as an unattached license. This command can be executed only on a Security Management server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cplic get</td>
<td>The cplic get command retrieves all licenses from a Security Gateway (or from all Security Gateways) into the license repository on the Security Management server. Do this to synchronize the repository with the Security Gateway (or with all the Security Gateways). When the command is run, all local changes will be updated.</td>
</tr>
<tr>
<td>cplic put</td>
<td>The cplic put command is used to install one or more Local licenses on a local machine.</td>
</tr>
<tr>
<td>cplic put &lt;object name&gt; ...</td>
<td>Use the cplic put command to attach one or more central or local license remotely. When this command is executed, the License Repository is also updated.</td>
</tr>
<tr>
<td>cplic print</td>
<td>The cplic print command (located in $CPDIR/bin) prints details of Check Point licenses on the local machine.</td>
</tr>
<tr>
<td>cplic upgrade</td>
<td>Use the cplic upgrade command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.</td>
</tr>
<tr>
<td>cp_merge</td>
<td>This utility has two main functionalities:</td>
</tr>
<tr>
<td>cp_merge delete_policy</td>
<td>This command provides the options of deleting an existing policy package. Note that the default policy can be deleted by delete action.</td>
</tr>
<tr>
<td>cp_merge export_policy</td>
<td>This command provides the options of leaving the policy package in the active repository, or deleting it as part of the export process. The default policy cannot be deleted during the export action.</td>
</tr>
<tr>
<td>cp_merge import_policy</td>
<td>This command provides the options to overwrite an existing policy package with the same name, or prevent overwriting when the same policy name already exists.</td>
</tr>
<tr>
<td>cp_merge list_policy</td>
<td>This command lists the Policy Packages that are available.</td>
</tr>
<tr>
<td>cppkg</td>
<td>This command is used to manage the Package Repository. It is always executed on the Security Management server.</td>
</tr>
<tr>
<td>cppkg add</td>
<td>The cppkg add command is used to add a package to the Package Repository. Only packages can be added to the Package Repository.</td>
</tr>
<tr>
<td>cppkg delete</td>
<td>The command is used to delete a package from the Package Repository. To delete a package you must specify a number of options. To see the format of the options and to view the contents of the Package Repository, use the cppkg print command.</td>
</tr>
<tr>
<td>cppkg get</td>
<td>This command synchronizes the Package Repository database with the content of the actual Package Repository under $SUROOT.</td>
</tr>
<tr>
<td>cppkg getroot</td>
<td>The command is used to find out the location of the Package Repository. The default Package Repository location on Windows machines is C:\SUroot. On UNIX it is /var/SUroot.</td>
</tr>
<tr>
<td>cppkg print</td>
<td>The command is used to list the contents of the Package Repository.</td>
</tr>
<tr>
<td>cppkg setroot</td>
<td>The command is used to create a new repository root directory location, and to move existing packages into the new Package Repository.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cpridrestart</td>
<td>Stops and starts the Check Point Remote installation Daemon (cprid). This is the daemon that is used for remote upgrade and installation of products. It is part of the SVN Foundation. In Windows it is a service.</td>
</tr>
<tr>
<td>cpridstart</td>
<td>Starts the Check Point Remote installation Daemon (cprid). This is the service that allows for the remote upgrade and installation of products. It is part of the SVN Foundation. In Windows it is a service.</td>
</tr>
<tr>
<td>cpridstop</td>
<td>Stops the Check Point Remote installation Daemon (cprid). This is the service that allows for the remote upgrade and installation of products. It is part of the SVN Foundation. In Windows it is a service.</td>
</tr>
<tr>
<td>cprinstall</td>
<td>Use cprinstall commands to perform remote installation of packages, and associated operations.</td>
</tr>
<tr>
<td>cprinstall boot</td>
<td>This command is used to boot the remote computer.</td>
</tr>
<tr>
<td>cprinstall cprestart</td>
<td>This command enables cprestart to be run remotely.</td>
</tr>
<tr>
<td>cprinstall cpstart</td>
<td>This command enables cpstart to be run remotely.</td>
</tr>
<tr>
<td>cprinstall cpstop</td>
<td>This command enables cpstop to be run remotely.</td>
</tr>
<tr>
<td>cprinstall get</td>
<td>The cprinstall get command is used to obtain details of the packages and the Operating System installed on the specified Security Gateway, and to update the database.</td>
</tr>
<tr>
<td>cprinstall install</td>
<td>The cprinstall install command is used to install Check Point packages, UTM-1 Edge firmware packages, OPSEC partner packages (SU compliant) and Check Point IPSO images on remote Security Gateways. To install a package you must specify a number of options. Use the cppkg print command and copy the required options.</td>
</tr>
<tr>
<td>cprinstall uninstall</td>
<td>The cprinstall uninstall command is used to install Check Point packages, UTM-1 Edge firmware packages, OPSEC partner packages (SU compliant) and Check Point IPSO images on remote Security Gateways. To uninstall a package you must specify a number of options. Use the cprinstall get command and copy the required options.</td>
</tr>
<tr>
<td>cprinstall verify</td>
<td>The cprinstall verify command is used to verify:</td>
</tr>
<tr>
<td></td>
<td>• If a specific product can be installed on the remote Security Gateway.</td>
</tr>
<tr>
<td></td>
<td>• That the Operating System and currently installed products are appropriate for the package.</td>
</tr>
<tr>
<td></td>
<td>• That there is enough disk space to install the product.</td>
</tr>
<tr>
<td></td>
<td>• That there is a CPRID connection.</td>
</tr>
<tr>
<td>cpstart</td>
<td>This command is used to start all Check Point processes and applications running on a machine.</td>
</tr>
<tr>
<td>cpstat</td>
<td>cpstat displays the status of Check Point applications, either on the local machine or on another machine, in various formats.</td>
</tr>
<tr>
<td>cpstop</td>
<td>This command is used to terminate all Check Point processes and applications running on a machine.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cpwd_admin</td>
<td>cpwd (also known as WatchDog) is a process that invokes and monitors critical processes such as Check Point daemons on the local machine, and attempts to restart them if they fail. Among the processes monitored by Watchdog are cpd, fwd, fwm. cpwd is part of the SVN Foundation. cpwd writes monitoring information to the $CPDIR/log/cpwd.elg log file. In addition, monitoring information is written to the console on UNIX platforms, and to the Windows Event Viewer. The cpwd_admin utility is used to show the status of processes, and to configure cpwd.</td>
</tr>
<tr>
<td>cpwd_admin config</td>
<td>This command is used to set cpwd configuration parameters. When parameters are changed, these changes do not take effect until cpwd has been stopped and restarted.</td>
</tr>
<tr>
<td>cpwd_admin exist</td>
<td>This command is used to check whether cpwd is alive.</td>
</tr>
<tr>
<td>cpwd_admin kill</td>
<td>This command is used to kill cpwd.</td>
</tr>
<tr>
<td>cpwd_admin list</td>
<td>This command is used to print a status of the selected processes being monitored by cpwd.</td>
</tr>
<tr>
<td>cpwd_admin monitor_list</td>
<td>This command is used to print the list of processes actively being monitored.</td>
</tr>
<tr>
<td>cpwd_admin start</td>
<td>Start a new process by cpwd.</td>
</tr>
<tr>
<td>cpwd_admin start_monitor</td>
<td>This command is used to start continuous monitoring on this machine.</td>
</tr>
<tr>
<td>cpwd_admin stop</td>
<td>Stop a process which is being monitored by cpwd.</td>
</tr>
<tr>
<td>cpwd_admin stop_monitor</td>
<td>This command is used to stop continuous monitoring on this machine.</td>
</tr>
<tr>
<td>dbedit</td>
<td>This command is used by administrators to edit the objects file on the Security Management server. There is an objects file on the gateway and a file, objects_5_0.C on the Security Management server. A new objects.C file is created on the gateway (based on the objects_5_0.C on the Security Management server) whenever a Policy is installed. Editing the objects.C file on the gateway is not required or desirable, since it will be overwritten the next time a Policy is installed.</td>
</tr>
<tr>
<td>DBTableStat</td>
<td>This utility provides a daily summary of the number of log records that match the consolidation rules, and the number of consolidated records that were stored in the specified database table. The format of the output is a comma separated value. The execution time of this utility depends on the number of records in the SmartReporter table.</td>
</tr>
<tr>
<td>dbver</td>
<td>The dbver utility is used to export and import different revisions of the database. The properties of the revisions (last time created, administrator responsible for, etc.) can be reviewed. The utility can be found in $FWDIR/bin.</td>
</tr>
<tr>
<td>dbver create</td>
<td>Create a revision from the current state of $fwdir/conf, including current objects, rule bases, etc.</td>
</tr>
<tr>
<td>dbver export</td>
<td>Archive the revision as an archive file in the revisions repository: $fwdir/conf/db_versions/export.</td>
</tr>
<tr>
<td>dbver import</td>
<td>Add an exported revision to the repository a version from $fwdir/conf/db_versions/export. Give filename of revision as input.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dbver print</td>
<td>Print the properties of the revision.</td>
</tr>
<tr>
<td>dbver print_all</td>
<td>Print the properties of all revisions to be found on the server side: $fwdir/conf/db_versions.</td>
</tr>
<tr>
<td>dynamic_objects</td>
<td>dynamic_objects specifies an IP address to which the dynamic object will be resolved on this machine.</td>
</tr>
<tr>
<td>fw</td>
<td>The fw commands are used for working with various aspects of the firewall component of the Security Gateway. All fw commands are executed on the gateway. Typing fw at the command prompt sends a list of available fw commands to the standard output.</td>
</tr>
<tr>
<td>fw ctl</td>
<td>The fw ctl command controls the Security Gateway kernel.</td>
</tr>
<tr>
<td>fw expdate</td>
<td>This command is used to modify the expiration date of all users and administrators.</td>
</tr>
<tr>
<td>fw fetch</td>
<td>This command fetches the Inspection Code from the specified host and installs it to the kernel.</td>
</tr>
<tr>
<td>fw fetchlogs</td>
<td>fw fetchlogs fetches Log Files from a remote machine. You can use the fw fetchlogs command to transfer Log Files to the machine on which the fw fetchlogs command is executed. The Log Files are read from and written to the directory $FWDIR/log.</td>
</tr>
<tr>
<td>fw hastat</td>
<td>The fw hastat command displays information about High Availability machines and their states.</td>
</tr>
<tr>
<td>fw kill</td>
<td>This command prompts the kernel to shut down all the daemon processes in the firewall component of the Security Gateway. The command is located in the $FWDIR/bin directory on the Security Management server or gateway. The Security Gateway daemons and Security Servers write their pids to files in the $FWDIR/tmp directory upon startup. These files are named $FWDIR/tmp/daemon_name.pid. For example, the file containing the pid of the Security Gateway snmp daemon is $FWDIR/tmp/snmpd.pid.</td>
</tr>
<tr>
<td>fw lea_notify</td>
<td>This command should be run from the Security Management server. It sends a LEA_COL_LOGS event to all connected lea clients (see the LEA Specification documentation). It should be used after new log files have been imported (manually or automatically) to the $FWDIR/log directory in order to avoid the scheduled update which takes 30 minutes.</td>
</tr>
<tr>
<td>fw lichosts</td>
<td>This command prints a list of hosts protected by the Security Gateways. The list of hosts is in the file $fwdir/database/fwd.h</td>
</tr>
<tr>
<td>fw log</td>
<td>fw log displays the content of Log files.</td>
</tr>
<tr>
<td>fw logswitch</td>
<td>fw logswitch creates a new active Log File. The current active Log File is closed and renamed by default $FWDIR/log/current_time_stamp.log unless you define an alternative name that is unique. The format of the default name current_time_stamp.log is YYYY-MM-DD_HHMMSS.log. For example: 2003-03-26_041200.log</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>fw mergefiles</code></td>
<td>This command merges several Log Files into a single Log File. The merged file can be sorted according to the creation time of the Log entries, and the times can be &quot;fixed&quot; according to the time zones of the origin Log Servers. When the combined size exceeds 2GB, the merge creates a list of &quot;merged files&quot; where each file size is not more than 2GB. The user receives the following warning: &quot;Warning: The size of the files you have chosen to merge is greater than 2GB. The merge will produce two or more files.&quot; The files names will be: [Requested name].log, [Requested name]_1.log, [Requested name]_2.log, ..., [Requested name]_n.log. Log entries with the same Unique-ID are unified. If a Log switch was performed before all the segments of a specific log were received, this command will merge the records with the same Unique-ID from two different files into one fully detailed record.</td>
</tr>
<tr>
<td><code>fw lslogs</code></td>
<td>This command displays a list of Log Files residing on a remote or local machine. You must initialize SIC between the Security Management server and the remote machine.</td>
</tr>
<tr>
<td><code>fw putkey</code></td>
<td>This command installs an authentication password on a host. This password is used to authenticate internal communications between Check Point Security Gateways and between a Check Point Security Gateway and its Security Management server. A password is used to authenticate the control channel the first time communication is established. This command is required for backward compatibility scenarios.</td>
</tr>
<tr>
<td><code>fw repairlog</code></td>
<td><code>fw repairlog</code> rebuilds a Log file's pointer files. The three files name.logptr, name.loginitial_ptr and name.logaccount_ptr are recreated from data in the specified Log file. The Log file itself is modified only if the -u flag is specified.</td>
</tr>
<tr>
<td><code>fw sam</code></td>
<td>This command is used to manage the Suspicious Activity Monitoring (SAM) server. Use the SAM server to block connections to and from IP addresses without the need to change the Security Policy. SAM commands are logged. Use this command to (also) monitor active SAM requests (see -M option). To configure the SAM Server on the Security Management server or firewall gateway machine, use SmartDashboard to edit the Advanced&gt;SAM page of the Security Gateway object.</td>
</tr>
<tr>
<td><code>fwm</code></td>
<td>This command is used to perform Security Management server operations. It controls fwd and all Check Point daemons.</td>
</tr>
<tr>
<td><code>fwm dbimport</code></td>
<td><code>fwm dbimport</code> imports users into the Security Management server User Database from an external file. You can create this file yourself, or use a file generated by fwm dbexport.</td>
</tr>
</tbody>
</table>
| `fwm dbexport`| `fwm dbexport` exports the Security Management server User Database to a file. The file may be in one of the following formats:  
  - The same Usage as the import file for fwm dbimport  
  - LDIF format, which can be imported into an LDAP Server using ldapmodify                                                                                                                                                                                                                                                                                                                                                     |
<p>| <code>fwm dbload</code>  | This command downloads the user database and network objects information to selected targets. If no target is specified, then the database is downloaded to localhost.                                                                                                                                                                                                                                                                                                                                         |
| <code>fwm ikecrypt</code>| <code>fwm ikecrypt</code> command line encrypts the password of a SecuRemote user using IKE. The resulting string must then be stored in the LDAP database.                                                                                                                                                                                                                                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| fwm load       | This command compiles and installs a Security Policy or a specific version of the Security Policy on the target's VPN Security Gateways. This is done in one of two ways:  
- fwm load compiles and installs an Inspection Script (*.pf) file on the designated Security Gateways.  
- fwm load converts a Rule Base (*.W) file created by the GUI into an Inspection Script (*.pf) file then installs it to the designated Security Gateways.  
Versions of the Security Policy and databases are maintained in a version repository on the Security Management server. Using this command, specific versions of the Security Policy can be installed on a Security Gateway (local or remote) without changing the definition of the current active database version on the Security Management server.  
To protect a target, you must load a Policy that contains rules whose scope matches the target. If none of the rules are enforced on the target, then all traffic through the target is blocked. |
| fwm lock_admin | This command enables you to view and unlock locked administrators.                                                                                                                                     |
| fwm logexport  | fwm logexport exports the Log file to an ASCII file.                                                                                                                                                    |
| fwm unload <targets> | This command uninstalls the currently loaded Inspection Code from selected targets.                                                                                                               |
| fwm ver        | fwm ver displays the build number.                                                                                                                                                                      |
| fwm verify <policy-name> | This command verifies the specified Policy Package without installing it.                                                                                                                                  |
| GeneratorApp   | This command generates a report for the SmartReporter. Both command line parameters are required.                                                                                                        |
| inet_alert     | This command notifies a company's Internet Service Provider (ISP) when the company's corporate network is under attack. The inet_alert utility forwards log messages generated by the alert daemon to an external Security Management server, typically located at the ISP site. The ISP can then analyze the alert and decide how to react. inet_alert uses the ELA Protocol to send the alert. The Security Management server receiving the alert must be running the ELA Proxy.  
If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the Security Management server running the ELA Proxy and the gateway generating the alert.  
To use this utility, enter it into a script. From Global Properties > Logs and alert > alert commands and enter the name of the script. |
| ldapcmd        | ldapcmd is used to manage processes running on the firewall collectively or individually. It includes:  
  - Cache - cache operations, such as emptying the cache, as well as providing debug information.  
  - Statistics - lookup statistics such as all user search, pending lookups (when two or more lookups are identical) and total lookup time (the total search time for a specific lookup)  
  - cache statistics such as hits and misses  
  - Logging - view the alert and warning log regarding debug |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldapcompare</td>
<td>ldapcompare is used to perform compare queries that print a message whether the result returned a match or not. ldapcompare opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.</td>
</tr>
<tr>
<td>ldapconvert</td>
<td>ldapconvert is a utility program to port from Member mode to MemberOf mode. This is done by searching all specified group/template entries and fetching their Member attribute values. Each value is the DN of a member entry. The entry identified by this DN will be added to the MemberOf attribute value of the group/template DN at hand. In addition, those Member attribute values will be deleted from the group/template unless Both mode is specified. While running the program, a log file named ldapconvert.log is generated in the current directory, logging all modifications done and errors encountered.</td>
</tr>
<tr>
<td>ldapmodify</td>
<td>ldapmodify imports users to an LDAP server. The input file must be in the LDIF format.</td>
</tr>
<tr>
<td>ldapsearch</td>
<td>ldapsearch queries an LDAP directory and returns the results.</td>
</tr>
<tr>
<td>log_export</td>
<td>log_export is a utility that allows you to transfer Log data to an external database. This utility behaves as a LEA client. LEA (Log Export API) enables Security Gateway log data to be exported to third-party applications. log_export receives the Logs from the Security Management server via LEA so it can be run from any host that has a SIC connection with the Security Management server and is defined as an OPSEC host. log_export should be defined as a reporting Security Gateway in order to act in a distributed environment. To run log_export, you need a basic understanding and a working knowledge of: - Oracle database administration - LEA</td>
</tr>
<tr>
<td>queryDB_util</td>
<td>queryDB_util enables searching the object database according to search parameters.</td>
</tr>
<tr>
<td>rs_db_tool</td>
<td>rs_db_tool is used to manage DAIP Modules in a DAIP database.</td>
</tr>
<tr>
<td>sam_alert</td>
<td>This tool executes Check Point SAM (Suspicious Activity Monitoring) actions according to information received through Standard input. This tool is for executing SAM actions with the Check Point User Defined alerts mechanism.</td>
</tr>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Account Units • 23</td>
<td></td>
</tr>
<tr>
<td>Account Units and High Availability • 25</td>
<td></td>
</tr>
<tr>
<td>Active versus Standby • 103</td>
<td></td>
</tr>
<tr>
<td>Actualizing an Implied network • 78</td>
<td></td>
</tr>
<tr>
<td>Add a Connectivity Cloud • 78</td>
<td></td>
</tr>
<tr>
<td>Add a Network Object to SmartMap • 76</td>
<td></td>
</tr>
<tr>
<td>Add an Internet Cloud • 78</td>
<td></td>
</tr>
<tr>
<td>Add or Change Administrator Window Warning • 58</td>
<td></td>
</tr>
<tr>
<td>Adding a Policy to an Existing Policy Package • 64</td>
<td></td>
</tr>
<tr>
<td>Adding a Section Title • 64</td>
<td></td>
</tr>
<tr>
<td>Adding New Attributes to the Active Directory • 30</td>
<td></td>
</tr>
<tr>
<td>Adding the contents of a SmartMap folder to the Rule Base • 79, 80</td>
<td></td>
</tr>
<tr>
<td>Address Ranges • 125</td>
<td></td>
</tr>
<tr>
<td>Adjusting and Customizing SmartMap • 75</td>
<td></td>
</tr>
<tr>
<td>Adjusting SmartMap using the Navigator • 75</td>
<td></td>
</tr>
<tr>
<td>Administrator Groups • 55</td>
<td></td>
</tr>
<tr>
<td>Advanced Search Attributes • 91</td>
<td></td>
</tr>
<tr>
<td>Affecting SmartMap Layout (Arranging Styles) • 75</td>
<td></td>
</tr>
<tr>
<td>Anti-spoofing Parameters and OSE Devices Setup (Cisco and Nortel)• 124</td>
<td></td>
</tr>
<tr>
<td>Assigning a Permissions Profile • 51</td>
<td></td>
</tr>
<tr>
<td>AttributesTranslationMap • 42</td>
<td></td>
</tr>
<tr>
<td>Authenticating the Administrator • 12</td>
<td></td>
</tr>
<tr>
<td>Authenticating the Security Management Server Using its Fingerprint • 12</td>
<td></td>
</tr>
<tr>
<td>Authenticating with Certificates • 26</td>
<td></td>
</tr>
<tr>
<td>Authentication • 52</td>
<td></td>
</tr>
<tr>
<td>AutomaticAttrs • 46</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>Backing Up the Security Management server • 102</td>
<td></td>
</tr>
<tr>
<td>Backup and Restore the Security Management server • 73</td>
<td></td>
</tr>
<tr>
<td>BadPwdCountAttr • 41</td>
<td></td>
</tr>
<tr>
<td>Balance Method • 125</td>
<td></td>
</tr>
<tr>
<td>Basic Search Attributes • 91</td>
<td></td>
</tr>
<tr>
<td>BranchObjectClass • 43</td>
<td></td>
</tr>
<tr>
<td>BranchOCOperator • 43</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CA Cleanup • 94</td>
<td></td>
</tr>
<tr>
<td>CA Data Types • 95</td>
<td></td>
</tr>
<tr>
<td>Calculating topology information • 81</td>
<td></td>
</tr>
<tr>
<td>Certificate Longevity and Statuses • 85</td>
<td></td>
</tr>
<tr>
<td>Certificate Operations Using the ICA Management Tool • 92</td>
<td></td>
</tr>
<tr>
<td>Certificates • 52, 56</td>
<td></td>
</tr>
<tr>
<td>Changing the Active SMS to the Standby SMS • 107</td>
<td></td>
</tr>
<tr>
<td>Changing the Standby SMS to the Active SMS • 108</td>
<td></td>
</tr>
</tbody>
</table>

**Index**

Changing the Status of the Security Management server • 105
Check Point Host • 121
Check Point Objects • 121
CLI Appendix • 127
Client Side Requirements • 101
ClientSideCrypt • 42
cn • 32
Collapsing locales • 79
Collapsing other Topology Structures • 79
Completing Basic Configuration • 14
Completing the Configuration • 117
Configuration Procedures • 115
Configure Alert Destinations • 116
Configure Automatic Deletion • 72
Configure Global Alert Settings • 115
Configure Thresholds • 116
Configuring a New Query • 64
Configuring Administrator Groups • 56
Configuring Administrators • 53
Configuring Authentication • 56
Configuring Customized Permissions • 60
Configuring Default Expiration Parameters • 58
Configuring General Properties • 54
Configuring Security Gateways for SNMP • 112
Configuring Security Gateways for SNMP Requests • 112
Configuring Security Gateways for SNMP Traps • 112
Configuring SNMP Monitoring • 114
Configuring the CA • 94
Configuring Users • 50
Connecting a network to Connectivity clouds/an Internet cloud, where there is more than one/a Containing Network • 78
Connecting a Network to Internet Clouds • 78
Connecting multiple networks to a Connectivity Cloud • 78
Connecting to the Management Portal • 101
Connection Times • 52
Converting a Check Point host into a Security Gateway • 121
Converting a Cluster Member into a Security Gateway • 122
Converting a Security Gateway into a Check Point host • 121
Converting Nodes • 122
Create a Group • 76
Create a Version • 71
Creating a New Policy Package • 63
Creating a PKCS#10 Certificate • 93
Creating and Changing Permission Profiles • 59
Creating Objects in the Objects Tree • 13
Creating or Changing a User • 50
Creating or Changing an Administrator • 54
CRL Management • 87
CRL Modes • 87
CRL Operations • 94
CryptedPasswordPrefix • 42
Customize color and width of objects and edges • 77
Customize the Display of Object Labels and IP Addresses • 77
Customize Tooltips for Objects • 77
Customizing Objects Tree Views • 15
D
Data Overload During Synchronization • 106
Database Revision Control and Version Upgrade • 72
Default User Directory Profiles • 38
DefaultCryptAlgorithm • 42
Defining LDAP Account Units • 23
Defining Protected Objects as Groups • 82
Defining Router Anti-Spoofing Properties • 124
Defining the contents of a • 79
Defining the Policy Package’s Installation Targets • 64
Defining User Directory Server • 25
Defining UTM-1 Edge Gateway Objects • 121
Delegating Control • 29
Delete a Version • 72
Deploying the Management Portal on a Dedicated Server • 99
Deploying the Management Portal on the Security Management server • 100
Deploying User Directory • 22
Deployments • 9
description • 33
Different Methods of Synchronization • 106
Display a Legend for regular and/or NAT rules • 80
Display the Rule Color Legend • 81
Distributing Users in Multiple Servers • 27
Dividing the Rule Base into Sections using Section Titles • 68
DomainObjectClass • 43, 47
DomainRDN • 45
Domains • 122
Dynamic Objects • 126
E
Edit Network Objects • 76
Editing External Objects • 80
Enable SmartMap • 74
Enabling and Disabling • 118
Enabling and Viewing SmartMap • 74
Encryption • 53
Enhancements • 22
Establishing Trust for Objects • 14
Example of Query • 28
Expanding Topology folders • 79
ExpirationDateAttr • 41
ExpirationDateFormat • 41
Export and Import a Version • 71
Export SmartMap (as an image file) • 82
Export SmartMap (to Microsoft Visio) • 83
Extending the Active Directory Schema • 29
Externally Managed Gateway/Host • 122
F
Fetch User Information Effectively • 39
File Operations • 67
Fixed Connections versus Editable Connections • 76
For what objects are topology calculations made? • 81
fw1allowed-vlan • 35
fw1authmethod • 33
fw1authserver • 33
fw1badPwdCount • 37
fw1day • 34
fw1enc-fwz-expiration • 35
fw1enc-Methods • 37
fw1expiration-date • 34
fw1groupTemplate • 36
fw1hour-range-from • 34
fw1hour-range-to • 34
fw1ISAKMP-AuthMethods • 36
fw1ISAKMP-DataEncMethod • 37
fw1ISAKMP-DataIntegrityMethod • 36
fw1ISAKMP-EncMethod • 36
fw1ISAKMP-HashMethods • 36
fw1ISAKMP-SharedSecret • 37
fw1ISAKMP-Transform • 36
fw1lastLoginFailure • 37
fw1pwdLastMod • 34
fw1sr-auth-track • 36
fw1SR-datam • 35
fw1SR-keym • 35
fw1SR-mdm • 35
fw1userPwdPolicy • 37
G
Gateway Cluster • 122
Gateway VPN Certificate Management • 86
General Properties • 50
Generating a Certificate • 93
Glossary • 10, 48
Group Conventions • 16
GroupObjectClass • 44, 46
GroupOCOperator • 44
GroupRDN • 45
Groups • 123
H
Handling SNMP Requests on SecurePlatform • 111
Handling SNMP Requests on Unix • 111
Handling SNMP Requests on Windows • 111
Hiding the contents of • 79
How is it done? • 87
I
ICA Administrators with Reduced Privileges • 89
ICA Advanced Options • 87
ICA Clients • 84
ICA Configuration • 89
Identity Awareness • 17
Important Information • 3
Initializing Multiple Certificates Simultaneously • 93
Initializing the Trust Establishment Process • 18
Initiating a Certificate • 93
Initiating a Search • 91
Installation Targets • 67
Installing the User Database • 70
Integrating SmartMap and the Rule Base • 80
Interoperable Device • 122
Intersecting Queries • 65
Introduction • 9

Page 136
What Data is Backed Up by the Standby Security Management servers? • 104
What is SmartMap Helper? • 82
What objects can be defined as protected objects? • 82
When Synchronization Fails • 106
Working with Expiration Warnings • 57
Working with Folders in SmartMap • 78
Working with Network Objects and Groups in SmartMap • 76
Working with Permissions Profiles • 59
Working with Policies • 69
Working with SmartMap • 74
Working with SmartMap Objects • 77
Working with SmartMap Output • 82
Working with SNMP Management Tools • 110