Important Information

Check Point R80
For more about this release, see the R80 home page

Latest Version of this Document
Download the latest version of this document

To learn more, visit the Check Point Support Center

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments
goto: mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point
Security Management R80 Administration Guide.

Searching in Multiple PDFs
To search for text in all the R80 PDF documents, download and extract the complete
R80 documentation package

Use Shift-Control-F in Adobe Reader or Foxit reader.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 January 2017</td>
<td>Fixed the procedure for Configuring a Security Gateway to use SecurID Authentication [on page 101]</td>
</tr>
</tbody>
</table>
| 26 September 2016| SIC uses TLS (“Secure Internal Communication (SIC)” [on page 35]).  
|                | Added procedure for searching for rule logs using the Rule UID (“Viewing Rule Logs” [on page 52]).  
|                | Explained how to match an application on any port (“Services & Applications” [on page 65]).  
|                | Changed Protections to Inspection Settings. (“Configuring Inspection Settings” [on page 73])                                               |
| 22 June 2016   | Removed the Security Management Server CLI.                                                                                               |
| 17 May 2016    | Updated The Security Management Server CLI                                                                                               |
| 14 April 2016  | Improved formatting and document layout                                                                                                  |
| 31 March 2016  | First release of this document                                                                                                           |
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Terms</td>
<td>9</td>
</tr>
<tr>
<td>Welcome</td>
<td>11</td>
</tr>
<tr>
<td>Getting Started</td>
<td>12</td>
</tr>
<tr>
<td>Understanding SmartConsole</td>
<td>12</td>
</tr>
<tr>
<td>Tour of SmartConsole</td>
<td>12</td>
</tr>
<tr>
<td>SmartConsole Toolbars</td>
<td>13</td>
</tr>
<tr>
<td>Search Engine</td>
<td>16</td>
</tr>
<tr>
<td>Access and Threat Tools</td>
<td>16</td>
</tr>
<tr>
<td>Shared Policies</td>
<td>17</td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>17</td>
</tr>
<tr>
<td>Connecting to the Security Management Server through SmartConsole</td>
<td>18</td>
</tr>
<tr>
<td>Setting Up for Security Management</td>
<td>18</td>
</tr>
<tr>
<td>Setting up for Team Work</td>
<td>19</td>
</tr>
<tr>
<td>Managing Security through API and CLI</td>
<td>19</td>
</tr>
<tr>
<td>Configuring the API Server</td>
<td>19</td>
</tr>
<tr>
<td>Management API Settings</td>
<td>20</td>
</tr>
<tr>
<td>Planning Security Management</td>
<td>20</td>
</tr>
<tr>
<td>Managing Administrator Accounts</td>
<td>22</td>
</tr>
<tr>
<td>Creating and Changing Administrator Accounts</td>
<td>22</td>
</tr>
<tr>
<td>Configuring Default Expiration for Administrators</td>
<td>23</td>
</tr>
<tr>
<td>Deleting an Administrator</td>
<td>23</td>
</tr>
<tr>
<td>Revoking Administrator Certificate</td>
<td>24</td>
</tr>
<tr>
<td>Assigning Permission Profiles to Administrators</td>
<td>24</td>
</tr>
<tr>
<td>Creating and Changing Permission Profiles</td>
<td>24</td>
</tr>
<tr>
<td>Configuring Customized Permissions</td>
<td>25</td>
</tr>
<tr>
<td>Permissions for Access Control and Threat Prevention</td>
<td>26</td>
</tr>
<tr>
<td>Permissions for Monitoring, Logging, Events, and Reports</td>
<td>26</td>
</tr>
<tr>
<td>Defining Trusted Clients</td>
<td>27</td>
</tr>
<tr>
<td>Configuring Trusted Clients</td>
<td>27</td>
</tr>
<tr>
<td>Administrator Collaboration</td>
<td>28</td>
</tr>
<tr>
<td>Publishing</td>
<td>28</td>
</tr>
<tr>
<td>Working with Sessions</td>
<td>29</td>
</tr>
<tr>
<td>Working with Database Revisions</td>
<td>29</td>
</tr>
<tr>
<td>Configuring Authentication Methods for Administrators</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Check Point Password Authentication for Administrators</td>
<td>30</td>
</tr>
<tr>
<td>Configuring OS Password Authentication for Administrators</td>
<td>30</td>
</tr>
<tr>
<td>Configuring a RADIUS Server for Administrators</td>
<td>31</td>
</tr>
<tr>
<td>Configuring a SecurID Server for Administrators</td>
<td>31</td>
</tr>
<tr>
<td>Configuring a TACACS Server for Administrators</td>
<td>32</td>
</tr>
<tr>
<td>Managing Gateways</td>
<td>34</td>
</tr>
<tr>
<td>Creating a New Security Gateway</td>
<td>34</td>
</tr>
<tr>
<td>Updating the Gateway Topology</td>
<td>35</td>
</tr>
<tr>
<td>Secure Internal Communication (SIC)</td>
<td>35</td>
</tr>
<tr>
<td>Initializing Trust</td>
<td>35</td>
</tr>
<tr>
<td>SIC Status</td>
<td>36</td>
</tr>
<tr>
<td>Trust State</td>
<td>36</td>
</tr>
</tbody>
</table>
Terms

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

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

**Database**
The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

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

**Identity Awareness**
Lets you enforce network access and audit data based on network location, the identity of the user, and the identity of the computer.

**LDAP**

**LDAP Groups**
Groups of users defined on an LDAP account unit.

**Log Server**
Physical server that hosts Check Point product log files.

**Management Server**
A Security Management Server or Multi-Domain Server that manages one or more Security Gateways and security policies.

**Package**
Group of files, and data about those files, delivered as one software archive (usually TGZ or RPM), for distribution and installation.

**Permissions Profile**
A set of access, and feature-based roles for SmartConsole administrators.

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

**Rule Base**
The database that contains the rules in a security policy and defines the sequence in which they are enforced.

**Security Gateway**
A computer or appliance that inspects traffic and enforces Security Policies for connected network resources.

**Security Management Server**
The server that manages, creates, stores, and distributes the security policy to Security Gateways.

**SIC**
Secure Internal Communication. The process by which networking components authenticate over SSL between themselves and the Security Management Server, as the Internal Certificate Authority (ICA), for secure communication. The Security Management Server issues a certificate, which components use to validate the identity of others.

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

**SmartDashboard**
A legacy Check Point client used to create and manage the security policy.
Software Blade
A software blade is a security solution based on specific business needs.
Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

User Database
Check Point internal database that contains all users and administrators defined and managed in SmartConsole.

User Groups
Named groups of users with related responsibilities.

User Template
Property set that defines a type of user on which a security policy will be enforced.

Users
Personnel authorized to use network resources and applications.
Welcome

Check Point offers effective Security Management solutions to help you keep up with constantly growing needs and challenges of your organizational network. This Administration Guide focuses on the basic Security Management Server deployment.

If you are interested in deployments for organizations with multiple sites, refer to the R80 Multi-Domain Server Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=46532.

These are the basic components of Check Point security architecture.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Your environment to protect.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Security Management Server</strong> - Manages Security Gateways with defined security policies and monitors security events on the network.</td>
</tr>
<tr>
<td>3</td>
<td><strong>SmartConsole</strong> - Check Point Graphical User Interface for connection to and management of Security Management Servers.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Security Gateway</strong> - Placed at the perimeter of the network topology, to protect your environment through enforcement of the security policies.</td>
</tr>
</tbody>
</table>
Getting Started

In This Section:

Understanding SmartConsole ................................................................. 12
Connecting to the Security Management Server through SmartConsole ........ 18
Setting Up for Security Management ....................................................... 18
Setting up for Team Work ...................................................................... 19
Managing Security through API and CLI .................................................. 19
Planning Security Management ............................................................... 20

Before you begin deploying a Check Point security solution, familiarize yourself with:

- Check Point SmartConsole
- Basic setup of a Check Point Security Management Server
- Basic setup of Check Point Security Gateways
- Administrative task delegation
- Security management in a non-GUI environment

Understanding SmartConsole

Check Point SmartConsole makes it easy to manage security for complex networks. Before you start to configure your network security environment and policies, become familiar with Check Point SmartConsole.

Tour of SmartConsole

For a guided tour of SmartConsole, click the What’s New button at the bottom left of the window. Click the < and > icons to scroll between the different What’s New screens.
## SmartConsole Toolbars

### Global Toolbar (top of SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The main SmartConsole Menu:</td>
</tr>
<tr>
<td>• Manage policies</td>
</tr>
<tr>
<td>• Manage layers</td>
</tr>
<tr>
<td>• Open Object Explorer</td>
</tr>
<tr>
<td>• New object (opens menu to create a new object)</td>
</tr>
<tr>
<td>• Publish session</td>
</tr>
<tr>
<td>• Discard session</td>
</tr>
<tr>
<td>• Session details</td>
</tr>
<tr>
<td>• Install policy</td>
</tr>
<tr>
<td>• Verify policy</td>
</tr>
<tr>
<td>• Install Database</td>
</tr>
<tr>
<td>• Uninstall Threat policy</td>
</tr>
<tr>
<td>• Management High Availability</td>
</tr>
<tr>
<td>• Manage Licenses and Packages</td>
</tr>
<tr>
<td>• Global Properties</td>
</tr>
<tr>
<td>• View (opens menu to select a View to open)</td>
</tr>
<tr>
<td>• Enter Session Details</td>
</tr>
</tbody>
</table>

Create new objects or open the Object Explorer

Install policy on managed gateways

### Session Management Toolbar (top of SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard changes made during the session</td>
</tr>
<tr>
<td>Enter session details and see the number of changes made in the session</td>
</tr>
<tr>
<td>Commit policy changes to the database and make them visible to other administrators</td>
</tr>
</tbody>
</table>

**Note** - The changes are saved on the gateways and enforced after the next policy install
## Navigation Toolbar (left side of SmartConsole)

<table>
<thead>
<tr>
<th>Keyboard Shortcut</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ctrl+1            | Gateway configuration view:  
|                   | • Manage Security Gateways  
|                   | • Activate Software Blades  
|                   | • Add, edit, or delete gateways and clusters (including virtual clusters)  
|                   | • Run scripts  
|                   | • Backup and restore gateways  
|                   | • Open a command line interface on the gateway  
|                   | • View gateway status  |
| Ctrl+2            | Security Policies Access Control view:  
|                   | • Manage the Access Control Software Blades: DLP, VPN, Application Control and URL Filtering, and Mobile Access  
|                   | • Edit multiple policies at the same time  
|                   | • Add, edit, or delete NAT rules  
|                   | Security Policies Threat Prevention view:  
|                   | • Manage the Threat Prevention Software Blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation  
|                   | • Edit the unified threat Rule Base  
|                   | • Configure threat profiles for all Software Blades  
|                   | • Add, edit, or delete exceptions and exception groups  
|                   | Both views:  
|                   | • Install policies  
|                   | • See logs and details  |
| Ctrl+3            | Logs & Monitor view:  
|                   | • See high level graphs and plots  
|                   | • Search through logs  
|                   | • Schedule customized reports  
|                   | • Monitor gateways  
<p>|                   | • See compliance information  |</p>
<table>
<thead>
<tr>
<th>Keyboard Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+4</td>
<td>Manage &amp; Settings view - review and configure the Security Management Server settings:</td>
</tr>
<tr>
<td></td>
<td>• Administrators - connected and disconnected</td>
</tr>
<tr>
<td></td>
<td>• Permissions profiles</td>
</tr>
<tr>
<td></td>
<td>• Trusted clients</td>
</tr>
<tr>
<td></td>
<td>• Sessions</td>
</tr>
<tr>
<td></td>
<td>• Blades</td>
</tr>
<tr>
<td></td>
<td>• Revisions</td>
</tr>
<tr>
<td></td>
<td>• Network management preferences</td>
</tr>
<tr>
<td></td>
<td>• Idle timeout</td>
</tr>
<tr>
<td></td>
<td>• Login message</td>
</tr>
</tbody>
</table>

**Command Line Interface Button (left bottom corner of SmartConsole)**

<table>
<thead>
<tr>
<th>Keyboard Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F9</td>
<td>Open a command line interface for management scripting and API</td>
</tr>
</tbody>
</table>

**Object Management Tab (right side of SmartConsole)**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects</td>
</tr>
<tr>
<td>Manage security and network objects</td>
</tr>
</tbody>
</table>

**Validations Tab (right side of SmartConsole)**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validations</td>
</tr>
<tr>
<td>See validation warnings and errors</td>
</tr>
</tbody>
</table>

**System Information Area (bottom of SmartConsole)**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
</tr>
<tr>
<td>See management tasks in progress and expand to see recent tasks</td>
</tr>
<tr>
<td>Server Details</td>
</tr>
<tr>
<td>See the IP address of the server to which SmartConsole is connected</td>
</tr>
<tr>
<td>Status of Changes</td>
</tr>
<tr>
<td>See the number of changes made in the session and their status</td>
</tr>
<tr>
<td>Connected Users</td>
</tr>
<tr>
<td>See connected users</td>
</tr>
</tbody>
</table>
Search Engine
In each view you can search the Security Management Server database for information relevant to
the view. For example:
- Gateway, by name or IP address
- Access Control rule
- NAT rule
- Threat Prevention profile
- Specific threat or a threat category
- Object tags

Access and Threat Tools
section in the Security Policies Threat Prevention view give you more management and data
collection tools.

Access Tools in the Security Policies Access Control view:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Communities</td>
<td>Create, edit, or delete VPN Communities.</td>
</tr>
<tr>
<td>Updates</td>
<td>Update the Application Control and URL Filtering database, schedule updates,</td>
</tr>
<tr>
<td></td>
<td>and configure updates.</td>
</tr>
<tr>
<td>UserCheck</td>
<td>Configure UserCheck interaction objects for Access Control policy actions.</td>
</tr>
<tr>
<td>Client Certificates</td>
<td>Create and distribute client certificates that allow users to authenticate to</td>
</tr>
<tr>
<td></td>
<td>the Gateway from handheld devices.</td>
</tr>
<tr>
<td>Application Wiki</td>
<td>Browse to the Check Point AppWiki. Search and filter the Web 2.0 Applications</td>
</tr>
<tr>
<td></td>
<td>Database, to use Check Point security research in your policy rules for ac</td>
</tr>
<tr>
<td></td>
<td>tions on applications, apps, and widgets.</td>
</tr>
<tr>
<td>Installation History</td>
<td>See the Policy installation history for each Gateway, and who made the</td>
</tr>
<tr>
<td></td>
<td>changes. See the revisions that were made during each installation, and</td>
</tr>
<tr>
<td></td>
<td>who made them. Revert to a specific version of the Policy.</td>
</tr>
</tbody>
</table>

Threat Tools in the Security Policies Threat Prevention view:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiles</td>
<td>Create, edit, or delete profiles.</td>
</tr>
<tr>
<td>IPS Protections</td>
<td>Edit IPS protections per profile.</td>
</tr>
<tr>
<td>Protections</td>
<td>See statistics on different protections</td>
</tr>
<tr>
<td>Whitelist Files</td>
<td>Configure Whitelist Files list</td>
</tr>
</tbody>
</table>
### Tool

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Updates</strong>  Configure updates to the Malware database, Threat Emulation engine and images, and the IPS database.</td>
</tr>
<tr>
<td><strong>UserCheck</strong>  Configure UserCheck interaction objects for Threat Prevention policy actions.</td>
</tr>
<tr>
<td><strong>Threat Wiki</strong>  Browse to the Check Point ThreatWiki. Search and filter Check Point’s Malware Database, to use Check Point security research to block malware before it enters your environment, and to best respond if it does get in.</td>
</tr>
</tbody>
</table>

### Shared Policies

The **Shared Policies** section in the **Security Policies** view gives access to granular Software Blades.

Shared policies are installed with the Access Control Policy.

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Access</strong></td>
<td>Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.</td>
</tr>
<tr>
<td><strong>DLP</strong></td>
<td>Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.</td>
</tr>
<tr>
<td><strong>Geo Policy</strong></td>
<td>Create a policy for traffic to or from specific geographical or political locations.</td>
</tr>
<tr>
<td><strong>HTTPS Policy</strong></td>
<td>The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. To launch the HTTPS Policy, click <strong>Manage &amp; Settings &gt; Blades &gt; HTTPS Inspection &gt; Configure in SmartDashboard</strong></td>
</tr>
</tbody>
</table>

### Command Line Interface

You can also configure objects and rules through the command line interface, which you can access from SmartConsole.

1. **Click to open the command line interface.**
2. **Open the Command Line Reference to learn about Session management commands, Host commands, Network commands, and Rule commands.**

In addition to the command line interface, you can create and run API scripts to manage configuration and operations on the Security Management Server. See Managing Security with the API and CLI ("Managing Security through API and CLI" on page 19).
Connecting to the Security Management Server through SmartConsole

To log in to a Security Management Server through Check Point SmartConsole, you must have an administrator account configured on the Security Management Server. You can create an administrator account with cpconfig or with the Check Point First Time Configuration Wizard.

To log in to the Security Management Server through SmartConsole:
1. Launch the SmartConsole application.
2. Enter your administrator authentication credentials.
3. Enter the name or the IP address of the Security Management Server.
4. Click Login.
   The SmartConsole authenticates the Security Management Server and shows the fingerprint.
5. Confirm the fingerprint.

The fingerprint and the IP address of the Security Management Server are saved to the Windows registry and are available for future Security Management Server authentications.

Setting Up for Security Management


To configure the Security Management Server in SmartConsole:
1. Find the Security Management Server object.
   You can search for it by name or IP address in the Search box at the top of the pane.
   When you select the Security Management Server object, the Summary tab at the bottom of the pane shows the Software Blades that are enabled on it.
2. Open the object properties window, and enable the Management Software Blades, as necessary:
   - Network Policy Management - Manage a comprehensive security policy, unified for all security functionalities.
   - Endpoint Policy Management - Manage security and data on end-user computers and hand-held devices. Enable this Software Blade if you have or will install an Endpoint Security Management Server.
   - Logging & Status - Monitor security events and status of gateways, VPNs, users, and more, with advanced visuals and data management features.
   - Identity Awareness - Add user identities, and data of their computers and devices, from Active Directory domains, to log entries.
   - Monitoring - See a complete picture of network and security performance, for rapid response to security events and traffic pattern changes.
   - User Directory - Populate your security scope with user accounts from the LDAP servers in your environment.
   - SmartEvent - Manage and correlate security events in real-time.
To configure the Security Gateways in SmartConsole:

1. From the navigation toolbar, select **Gateways & Servers**.
2. Click **New**, and select **Gateway**.
3. In the **Check Point Security Gateway Creation** window that opens, select a configuration mode:
   - **Wizard Mode** - run the configuration wizard
   - **Classic Mode** - configure the gateway in classic mode ("Creating a New Security Gateway" on page 34)

Setting up for Team Work

As an administrator, you can delegate tasks, such as defining objects and users, to other administrators. Make sure to create administrator accounts ("Managing Administrator Accounts" on page 22) with the privileges that are required to accomplish those tasks.

If you are the only administrator, we recommend that you create a second administrator account with Read Only permissions, which is useful for troubleshooting, consultation, or auditing.

Managing Security through API and CLI

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

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

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

- Standalone management tool, included with SmartConsole. You can copy this tool to Windows or Gaia computers.
  - `mgmt_cli.exe` (Windows)
  - `mgmt_cli` (Gaia)
- Web Services API that allows communication and data exchange between the clients and the Security Management Server through the HTTP protocol. It also lets other Check Point processes communicate with the management server through the HTTPS protocol. The API commands are stored in XML format.

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

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see the [Developers Network](https://community.checkpoint.com) section of the Exchange Point Portal.

Configuring the API Server

To configure the API Server:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Management API** section, click **Advanced Settings**.
The Management API Settings window opens.

3. Configure the Start**up** Settings and the Access Settings.

Management API Settings

- **Startup Settings**
  - Select **Automatic start** to automatically start the API server when the Security Management Server starts.
  
  In these environments, **Automatic start** is selected by default:
  - Distributed Security Management Servers (without gateway functionality) with at least 4GB of RAM
  - Standalone Security Management Servers (with gateway functionality) with at least 8GB of RAM

  In other environments, to reduce the memory consumption on the management server, **Automatic start** is not selected by default.

- **Access Settings**
  Configure IP addresses from which the API server accepts requests:
  
  - **Management server only** (default) - API server will accept scripts and web service requests only from the Security Management Server. You must open a command line interface on the server and use the `mgmt_cli` utility to send API requests.
  - **All IP addresses that can be used for GUI clients** - API server will accept scripts and web service requests from the same devices that are allowed access to the Security Management Server.
  - **All IP addresses** - API server will accept scripts and web-service requests from any device.

  To apply changes, you must publish the session, and run the `api restart` command on the Security Management Server.

Planning Security Management

After installing the Security Management Server and the Security Gateways, you can continue with network security configuration for your environment.

**Define your organization’s topology**

Network topology consists of network components, both physical and logical, such as physical and virtual Security Gateways, hosts, hand-held devices, CA servers, third-party servers, services, resources, networks, address ranges, and groups. Each of these components corresponds to an object in your Check Point security management configuration. Configure those objects ("Network Object Types" on page 41) in SmartConsole.

**Define users and user groups that your security environment protects**

You can add users ("Creating, Modifying, Removing User Accounts" on page 105) and groups ("Managing User Groups" on page 108) to the database manually, through LDAP and User Directory (on page 109), or with the help of Active Directory ("Microsoft Active Directory" on page 131).
Define access rules for protection of your organization's resources

Configure access rules and group them in policies that are enforced on the Security Gateways. You can define access policies ["Policy Management" on page 48] based on traffic, applications, Web sites, and data. Set up preventative actions against known threats with Check Point Anti-Virus and Anti-Malware. Educate users about the validity and security of the operations they attempt with the help of UserCheck. Track network traffic and events through logging and monitoring.

Enforce access policies

Configure the Security Gateways. Make sure to activate the appropriate Software Blades. Then, install your policies on the Security Gateways.
Managing Administrator Accounts

In This Section:
- Creating and Changing Administrator Accounts ........................................................ 22
- Deleting an Administrator ............................................................................................ 23
- Revoking Administrator Certificate ............................................................................. 24
- Assigning Permission Profiles to Administrators ...................................................... 24
- Defining Trusted Clients ............................................................................................... 27
- Administrator Collaboration ........................................................................................ 28
- Configuring Authentication Methods for Administrators ........................................... 30

To successfully manage security for a large network, we recommend that you first set up your administrative team, and delegate tasks.

Creating and Changing Administrator Accounts

We recommend that you create administrator accounts in SmartConsole, with the procedure below or with the First Time Configuration Wizard.

If you create it through the SmartConsole, you can choose one of these authentication methods:
- Check Point Password (on page 99)
- OS Password (see “Operating System Password” on page 99)
- RADIUS (on page 99)
- SecurID (on page 100)
- TACACS (on page 100)

If you create an administrator through cpconfig, the Check Point Configuration Tool:
- Check Point Password is automatically configured as the authentication method.
- You must restart Check Point Services to activate the user.

To create an administrator account using SmartConsole:
1. Click Manage & Settings > Permissions and Administrators.
   The Administrators pane shows by default.
2. Click New Administrator.
   The New Administrators window opens.
3. Enter a unique name for the administrator account.
   Note - This parameter is case-sensitive.
4. Set the Authentication Method, or create a certificate, or the two of them.
   Note - If you do not do this, the administrator will not be able to log in to SmartConsole or other SmartConsole clients, such as SmartEvent.

To define an Authentication Method:
Select a method and follow the instructions in Configuring Authentication Methods for Administrators (on page 30).
Managing Administrator Accounts

To create a Certificate:
In the Certificate Information section, click Create, enter a password, and save the certificate to a secure location.

5. Select a Permissions profile for this administrator, or create a new one ["Creating and Changing Permission Profiles" on page 24].

6. Set the account Expiration date:
   - For a permanent administrator - select Never
   - For a temporary administrator - select an Expire At date from the calendar
The default expiration date shows, as defined in the Default Expiration Settings ["Configuring Default Expiration Settings for Users" on page 107]. After the expiration date, the account is no longer authorized to access network resources and applications.

7. Optional: Configure Additional Info - Contact Details, Email and Phone Number of the administrator.

8. Click OK.

To change an existing administrator account:

1. Click Manage & Settings > Permissions and Administrators.
2. Double-click an administrator account.
   The Administrators properties window opens.

Configuring Default Expiration for Administrators
If you want to use the same expiration settings for multiple accounts, you can set the default expiration for administrator accounts. You can also choose to show notifications about the approaching expiration date at the time when an administrator logs into SmartConsole or one of the SmartConsole clients. The remaining number of days, during which the account will be alive, shows in the status bar.

To configure the default expiration settings:

1. Click Manage & Settings > Permissions and Administrators > Advanced.
2. Click Advanced.
3. In the Default Expiration Date section, select a setting:
   - Never expires
   - Expire at - Select the expiration date from the calendar control
   - Expire after - Enter the number of days, months, or years (from the day the account is made) before administrator accounts expire
4. In the Expiration notifications section, select Show 'about to expire' indication in administrators view and select the number of days in advance to show the message about the approaching expiration date.
5. Click Publish.

Deleting an Administrator
To make sure your environment is secure, it is best practice to delete administrator accounts when personnel leave or transfer.
To remove an administrator account:
1. Click Manage & Settings > Permissions and Administrators. The Administrators pane shows by default.
2. Select an administrator account and click Delete.
3. Click Yes in the confirmation window that opens.

Revoking Administrator Certificate
If an administrator that authenticates through a certificate is temporarily unable to fulfill administrator duties, you can revoke the certificate for the account. The administrator account remains, but no one can authenticate to the Security Management Server with this account’s credentials, until you renew the certificate.

To revoke an administrator certificate:
1. Click Manage & Settings > Permissions and Administrators.
2. Select an administrator account and click Edit.
3. In General > Authentication, click Revoke.

Assigning Permission Profiles to Administrators
A permission profile is a predefined set of Security Management Server and SmartConsole administrative permissions that you can assign to administrators. You can assign a permission profile to more than one administrator. Only administrators with applicable permissions can create and manage permission profiles.

Creating and Changing Permission Profiles
Administrators with Super User permissions can create, edit, or delete permission profiles.

To create a new permission profile:
1. In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
2. Click New Profile. The New Profile window opens.
3. Enter a unique name for the profile.
4. Select a profile type:
   - Read/Write All - Administrators can make changes
   - Auditor (Read Only All) - Administrators can see information but cannot make changes
   - Customized - Configure custom settings ("Configuring Customized Permissions" on page 25)
5. Click OK.
To change a permission profile:
1. In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
2. Double-click the profile to change.
3. In the Profile configuration window that opens, change the settings as needed.
4. Click Close.

To delete a permission profile:
1. In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
2. Select a profile and click Delete.
   You cannot delete a profile that is assigned to an administrator. To see which administrators use a profile, in the error message, click Where Used.
   If the profile is not assigned to administrators, a confirmation window opens.
3. Click Yes to confirm.

Configuring Customized Permissions

Configure administrator permissions for Access Control, Threat Prevention, Monitoring and Logging, Events and Reports, Management, and other permissions. For each resource, define if administrators that are configured with this profile can configure the feature or only see it.

Permissions:
• Not selected - The administrator cannot see the feature.
  Note - If you cannot clear a feature selection, the administrator access to it is mandatory and you cannot make it invisible
• Selected - The administrator can see the feature.
• Read - The administrator can see the feature but cannot make changes.
• Write - The administrator can see the feature and make changes.

Some resources do not have the Read or Write option. You can only select (for full permissions) or clear (for no permissions) these resources.

To configure customized permissions:
1. In the Profile object, in the Overview > Permissions section, select Customized.
2. Configure permissions in these pages of the Profile object:
   • Gateways - configure the Provisioning and the Scripts permissions.
   • Access Control - configure Access Control Policy permissions ("Permissions for Access Control and Threat Prevention" on page 26).
   • Threat Prevention - configure Threat Prevention Policy permissions ("Permissions for Access Control and Threat Prevention" on page 26).
   • Monitoring and Logging - configure permissions to generate and see logs and to use monitoring features ("Permissions for Monitoring, Logging, Events, and Reports" on page 26).
   • Events and Reports - configure permissions for SmartEvent features ("Permissions for Monitoring, Logging, Events, and Reports" on page 26).
• Others - configure permissions for Common Objects, user databases, HTTPS Inspection features, and Client Certificates.

3. If this profile is for administrators with permissions to manage other administrator accounts, in the Management section, select Manage Administrators.

4. If this profile is for administrators with permissions to manage sessions, in the Management section, select Manage Sessions.

5. Click OK.

Permissions for Access Control and Threat Prevention

In the Profile object, select the features and the Read or Write administrator permissions for them.

Access Control

To edit a Layer, a user must have permissions for all Software Blades in the Layer.

• Actions
  • Install Policy - Install the Access Control Policy on Security Gateways.
  • Application Control and URL Filtering Update - Download and install new packages of applications and websites, to use in access rules.

Threat Prevention

• Actions
  • Install Policy - Install the Threat Prevention Policy on Security Gateways.
  • IPS Update - Download and install new packages for IPS protections.

Permissions for Monitoring, Logging, Events, and Reports

In the Profile object, select the features and the Read or Write administrator permissions for them.

Monitoring and Logging Features

These are some of the available features:

• Monitoring
• Management Logs
• Track Logs
• Application and URL Filtering Logs

Events and Reports Features

These are the permissions for the SmartEvent GUI:

• SmartEvent
  • Events - The Events tab
  • Policy - Events correlation on the Policy tab
  • Reports - Reports tab
• SmartEvent Application Control and URL Filtering reports only
Defining Trusted Clients

By default, any authenticated administrator can connect to the Security Management Server from any computer. To limit the access to a specified list of hosts, you can configure Trusted Clients. You can configure Trusted Clients in these ways:

- **Any** - All hosts (default)
- **IPv4 Address** - A single host with specified IPv4 address
- **IPv4 Address Range** - Hosts with IPv4 addresses in the specified range
- **IPv4 Netmask** - Hosts with IPv4 addresses in the subnet defined by the specified IPv4 address and netmask
- **IPv6 Address** - A single host with specified IPv6 address
- **IPv6 Address Range** - Hosts with IPv6 addresses in the specified range
- **IPv6 Netmask** - Hosts with IPv6 addresses in the subnet defined by the specified IPv6 address and netmask
- **Name** - A host with the specified name
- **Wild cards (IP only)** - Hosts with IP addresses described by the specified regular expression

Configuring Trusted Clients

Administrators with Super User permissions can add, edit, or delete trusted clients.

To add a new trusted client:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Trusted Clients**.
2. Click **New**.
   The **New Trusted Client** window opens.
3. Enter a unique name for the client.
4. Select a client type and configure corresponding values:
   - **Any** - No values to configure
   - **IPv4 Address** - Enter an IPv4 address of a host
   - **IPv4 Address Range** - Enter the first and the last address of an IPv4 address range
   - **IPv4 Netmask** - Enter the IPv4 address and the netmask
   - **IPv6 Address** - Enter an IPv6 address of a host
   - **IPv6 Address Range** - Enter the first and the last address of an IPv6 address range
   - **IPv6 Netmask** - Enter the IPv6 address and the netmask
   - **Name** - Enter a host name
   - **Wild cards (IP only)** - Enter a regular expression that describes a set of IP addresses
5. Click **OK**.

To change trusted client settings:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Trusted Clients**.
2. Double-click the client you want to edit.
3. In the **Trusted Client** configuration window that opens, change the settings as needed.
Managing Administrator Accounts

4. Click **OK**.

To delete a permission profile:
1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Trusted Clients**.
2. Select a trusted client and click **Delete**.
   The confirmation window opens.
3. Click **Yes** to confirm.

Administrator Collaboration

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

Publishing

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

When you select **Install Policy**, you are prompted to publish all unpublished changes. You cannot install a policy if the included changes are not published.

Before you publish the session, you can add some informative attributes to it.

You can exit SmartConsole without publishing your changes You will see the changes next time you log into SmartConsole.

To publish a session:

In the **SmartConsole** toolbar, click **Publish**.

When a session is published, a new database version is created and shows in the list of database revisions.

**Note** - Before you upgrade the Security Management Server, you must save the database.

To add a name, description, or tag attribute to a session:

1. Before you publish, in the **SmartConsole** toolbar, click **Session**.
   The **Session Details** window opens.
2. Enter a name for the database version.
3. Enter a description.
4. Add a tag.
5. Click **OK**.
To save changes without publishing:
1. From the SmartConsole Menu, select Exit.
2. Click Exit.

Working with Sessions

To see session information:
Click Manage & Settings > Sessions > View Sessions.

When an administrator changes objects, they are saved and locked. To unlock the changed objects, the administrator must do one of these:
- Publish the session - to make the changes available to all the administrators
- Discard the session - to discard the changes

When an administrator that made changes and did not publish the session, is unavailable, and some important objects are locked, you can unlock that session, to continue working with those objects.

To unlock a session that was locked by another administrator:
- To apply session changes and disconnect the administrator's SmartConsole session: right-click the session and select Publish & Disconnect.
- To discard the session changes and disconnect the administrator's SmartConsole session: right-click the session and select Discard & Disconnect.

Working with Database Revisions

After you make changes, you must publish the session, to save changes to the database.

When you publish a session, a new database version is created and shows in the list of database revisions.

Before you publish the session, you can add some informative attributes to it.

To publish a session:
In the SmartConsole toolbar, click Publish.

When you publish a session, a new database version is created and shows in the list of database revisions.

Note - Before you upgrade the Security Management Server, you must save the database.

To add a name, description, or tag attribute to a session:
1. Before you publish, in the SmartConsole toolbar, click Session.
   The Session Details window opens.
2. Enter a name for the database version.
3. Enter a description.
4. Add a tag.
5. Click OK.
To see saved database versions:
In SmartConsole, go to Manage & Settings > Revisions.

To see the changes made during a specific session:
1. In the Manage & Settings > Revisions window, select a session.
2. Click View.
   A separate read-only SmartConsole session opens.

To delete all versions of the database that are older than the selected version:
1. In the Manage & Settings > Revisions window, select a session.
2. Click Purge.
3. In the confirmation window that opens, click Yes.
   Important - Deletion is irreversible. Older revisions are deleted permanently.

Configuring Authentication Methods for Administrators

These instructions show how to configure authentication methods for administrators. For users, see Configuring Authentication Methods for Users (on page 100).

For background information about the authentication methods, see Authentication Methods for Users and Administrators (on page 99).

Configuring Check Point Password Authentication for Administrators

These instructions show how to configure Check Point Password (on page 99) authentication for administrators.

To configure a Check Point password for a SmartConsole administrator:
1. Go to Manage & Settings > Permissions & Administrators > Administrators.
2. Click New.
3. The New Administrator window opens.
4. Give the administrator a name.
5. In Authentication method, select Check Point Password.
6. Click Set New Password, type the Password, and Confirm it.
7. Assign a Permission Profile.
8. Click OK.
9. Click Publish.

Configuring OS Password Authentication for Administrators

These instructions show how to configure OS Password Authentication (see "Operating System Password" on page 99) for administrators.

To configure an OS password for a SmartConsole administrator:
1. Go to Manage & Settings > Permissions & Administrators > Administrators.
2. Click New.
3. The New Administrator window opens.
4. Give the administrator a name.
5. In Authentication method, select OS Password.
6. Assign a Permission Profile.
7. Click OK.
8. Click Publish.

Configuring a RADIUS Server for Administrators

These instructions show how to configure a RADIUS server for SmartConsole administrators. To learn how to configure a RADIUS server, refer to the vendor documentation.

To configure a RADIUS Server for a SmartConsole administrator:
1. In SmartConsole, click Objects > More Object Types > Server > More > New RADIUS.
2. Configure the RADIUS Server Properties:
   a) Give the server a Name. It can be any name.
   b) Click New and create a New Host with the IP address of the RADIUS server.
   c) Click OK.
   d) Make sure that this host shows in the Host field of the Radius Server Properties window.
   e) In the Shared Secret field, type the secret key that you defined previously on the RADIUS server.
   f) Click OK.
3. Add a new administrator:
   a) Go to Manage & Settings > Permissions & Administrators > Administrators.
   b) Click New.
      The New Administrator window opens.
   c) Give the administrator the name that is defined on the RADIUS server.
   d) Assign a Permission Profile.
   e) In Authentication method, select RADIUS.
   f) Select the RADIUS Server defined earlier.
   g) Click OK.
4. Click Publish.

Configuring a SecurID Server for Administrators

These instructions show how to configure a SecurID server for SmartConsole administrators. To learn how to configure a SecurID server, refer to the vendor documentation.

To configure the Security Management Server for SecurID:
2. Copy the sdconf.rec file to the /var/ace/ folder
If the folder does not exist, create the folder.

3. Give the sdconf.rec file full permissions. Run:
   chmod 777 sdconf.rec

To configure a SecurID Server for a SmartConsole administrator:

1. In SmartConsole, click Objects > More Object Types > Server > More > New SecurID.
2. Configure the SecurID Properties:
   a) Give the server a Name. It can be any name.
   b) Click Browse and select the sdconf.rec file. This must be a copy of the file that is on the Security Management Server.
   c) Click OK.
3. Add a new administrator:
   a) Go to Manage & Settings > Permissions & Administrators > Administrators.
   b) Click New.
      The New Administrator window opens.
   c) Give the administrator a name.
   d) Assign a Permission Profile.
   e) In Authentication method, select SecurID.
4. In the SmartConsole Menu, click Install Database.

Configuring a TACACS Server for Administrators

These instructions show how to configure a TACACS (on page 100) server for SmartConsole administrators. To learn how to configure a TACACS server, refer to the vendor documentation.

To configure a TACACS Server for a SmartConsole administrator:

1. In SmartConsole, click Objects > More Object Types > Server > More > New TACACS.
2. Configure the TACACS Server Properties:
   a) Give the server a Name. It can be any name.
   b) Click New and create a New Host with the IP address of the TACACS server.
   c) Click OK.
   d) Make sure that this host shows in the Host field of the TACACS Server Properties window.
   e) In the Shared Secret field, type the secret key that you defined previously on the TACACS server.
   f) Click OK.
3. Add a new administrator:
   a) Go to Manage & Settings > Permissions & Administrators > Administrators.
   b) Click New.
      The New Administrator window opens.
   c) Give the administrator the name that is defined on the TACACS server.
d) Assign a Permission Profile.

e) In Authentication method, select TACACS.

f) Select the TACACS Server defined earlier.

g) Click OK.

4. Click Publish.
Managing Gateways

In This Section:

Creating a New Security Gateway ................................................................. 34
Updating the Gateway Topology ................................................................. 35
Secure Internal Communication (SIC) ....................................................... 35
Check Point Hosts ....................................................................................... 38


Creating a New Security Gateway

To install security policies on the Security Gateways, configure the gateway objects in SmartConsole.

To define a new Security Gateway object:

1. From the navigation toolbar, select Gateways & Servers.
2. Click New, and select Gateway.
   The Check Point Security Gateway Creation window opens.
3. Click Classic Mode.
   The Check Point Gateway properties window opens and shows the General Properties screen.
4. Enter the host Name and the IPv4 Address or IPv6 Address.
5. Click Communication.
   The Trusted Communication window opens.
6. Select a Platform.
7. In the Authentication section, enter and confirm the One-time password.
   If you selected Small Office Appliance platform, make sure Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time is selected.
8. Click Initialize to establish trusted communication with the gateway ("Secure Internal Communication [SIC]" on page 35).
   If trust fails to establish, click OK to continue configuring the gateway.
9. Click OK.
10. The Get Topology Results window that opens, shows interfaces successfully configured on the gateway.
11. Click Close.
12. In the Platform section, select the Hardware, the Version, and the OS.
   If trust is established between the server and the gateway, click Get to automatically retrieve the information from the gateway.
13. Select the Software Blades to enable on the Security Gateway.
   For some of the Software Blades a first-time setup wizard will open. You can run the wizard now or later. For more on the setup wizards, see the relevant Administration Guide.
Updating the Gateway Topology

As the network changes, you must update the gateway topology.

To update the gateway topology:
1. In SmartConsole, click **Gateways & Servers**.
2. Double-click the gateway object.
   - The gateway property window opens.
3. Click **Network Management**.
5. In the window that opens, under **Topology**, click **Modify**.
6. Click **OK**.

Secure Internal Communication (SIC)

Check Point platforms and products authenticate each other through one of these Secure Internal Communication (SIC) methods:
- Certificates.
- Standards-based TLS for the creation of secure channels.
- 3DES or AES128 for encryption.
  - Gateways above R71 use AES128 for SIC. If one of the gateways is below R71, the gateways use 3DES.

SIC creates trusted connections between gateways, management servers and other Check Point components. Trust is required to install polices on gateways and to send logs between gateways and management servers.

Initializing Trust

To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

**Note** - Make sure the clocks of the gateway and Security Management Server are synchronized, before you initialize trust between them. You can control the Time and Date settings of Check Point gateways and servers with `cpconfig`.

To initialize Trust:
1. In SmartConsole, open the gateway network object.
2. In the **General Properties** page of the gateway, click **Communication**.
3. In the **Communication** window, enter the **Activation Key** that you created during installation.
   - This one-time activation password must be on both the gateway and the Security Management Server.
4. Click **Initialize**.
   - The ICA signs and issues a certificate to the gateway.

   Trust state is **Initialized but not trusted**. The Internal Certificate Authority (ICA) issues a certificate for the gateway, but does not yet deliver it.
The two communicating peers authenticate over SSL with the shared Activation Key. The certificate is downloaded securely and stored on the gateway. The Activation Key is deleted. The gateway can communicate with Check Point nodes that have a security certificate signed by the same ICA.

**SIC Status**

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

- **Communicating** - The secure communication is established.
- **Unknown** - There is no connection between the gateway and Security Management Server.
- **Not Communicating** - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

**Trust State**

If the Trust State is compromised (keys were leaked, certificates were lost) or objects changed (user leaves, open server upgraded to appliance), reset the Trust State. When you reset Trust, the SIC certificate is revoked.

The Certificate Revocation List (CRL) is updated for the serial number of the revoked certificate. The ICA signs the updated CRL and issues it to all gateways during the next SIC connection. If two gateways have different CRLs, they cannot authenticate.

**To reset the trust state:**

1. In SmartConsole, open the General Properties window of the gateway.
2. Click Communication.
3. In the Trusted Communication window that opens, click Reset.
   - This deploys the updated CRL to all gateways. If you do not have a Rule Base (and therefore cannot install a policy), you can reset Trust on the gateways.
   - **Important** - Before a new trust can be established, make sure one-time activation password is configured on the gateway and on the Security Management Server.

**To establish a new trust state for a gateway:**

1. Open the command line interface on the gateway.
2. Enter: `cpconfig`
3. Enter the number for Secure Internal Communication and press Enter.
4. Enter y to confirm.
5. Enter and confirm the activation key.
6. When done, enter the number for Exit.
7. Wait for Check Point processes to stop and automatically restart.
In SmartConsole:

1. In the General Properties window of the gateway, click Communication.
2. In the Trusted Communication window, enter the one-time password (activation key) that you entered on the Security Management Server.
3. Click Initialize.
4. Wait for the Certificate State field to show Trust established.
5. Click OK.

Troubleshooting SIC

If SIC fails to Initialize:

1. Make sure there is connectivity between the gateway and Security Management Server.
2. Make sure that the Security Management Server and the gateway use the same SIC activation key (one-time password).
3. If the Security Management Server is behind a gateway, make sure there are rules that allow connections between the Security Management Server and the remote gateway. Make sure Anti-spoofing settings are correct.
4. Make sure the name and the IP address of the Security Management Server are in the /etc/hosts file on the gateway.
   If the IP address of the Security Management Server mapped through static NAT by its local gateway, add the public IP address of the Security Management Server to the /etc/hosts file on the remote gateway. Make sure the IP address resolves to the server’s hostname.
5. Make sure the date and the time settings of the operating systems are correct. If the Security Management Server and remote the gateway reside in different time zones, the remote gateway may have to wait for the certificate to become valid.
6. Remove the security policy on the gateway to let all the traffic through: In the command line interface of the gateway, type: `fw unloadlocal`
7. Try to establish SIC again.

Remote User access to resources and Mobile Access

If you install a certificate on a gateway that has the Mobile Access Software Blade already enabled, you must install the policy again. Otherwise, remote users will not be able to reach network resources.

Understanding the Check Point Internal Certificate Authority (ICA)

The ICA (Internal Certificate Authority) is created on the Security Management Server when you configure it for the first time. The ICA issues certificates for authentication:

- **Secure Internal Communication (SIC)** - Authenticates communication between Security Management Servers, and between gateways and Security Management Servers.
- **VPN certificates for gateways** - Authentication between members of the VPN community, to create the VPN tunnel.
- **Users** - For strong methods to authenticate user access according to authorization and permissions.
ICA Clients

In most cases, certificates are handled as part of the object configuration. To control the ICA and certificates in a more granular manner, you can use one of these ICA clients:

- **The Check Point configuration utility** - This is the `cpconfig` CLI utility. One of the options creates the ICA, which issues a SIC certificate for the Security Management Server.
- **SmartConsole** - SIC certificates for Security Gateways and administrators, VPN certificates, and user certificates.
- **ICA Management tool** - VPN certificates for users and advanced ICA operations ["The ICA Management Tool" on page 158].

See audit logs of the ICA in SmartConsole **Logs & Monitor > New Tab > Open Audit Logs View**.

SIC Certificate Management

Manage SIC certificates in the

- **Communication** tab of the gateway properties window.
- **ICA Management Tool** ["User Certificate Management" on page 160].

Certificates have these configurable attributes:

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>5 years</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>2048 bits</td>
<td></td>
</tr>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>Digital Signature and Key encipherment</td>
</tr>
<tr>
<td>ExtendedKeyUsage</td>
<td>0 (no KeyUsage)</td>
<td>VPN certificates only</td>
</tr>
</tbody>
</table>

To learn more about key size values, see RSA key lengths [http://supportcontent.checkpoint.com/solutions?id=sk96591](http://supportcontent.checkpoint.com/solutions?id=sk96591).

Check Point Hosts

A Check Point Host can have multiple interfaces but no routing takes place. It is an endpoint that receives traffic for itself through its interfaces. (In comparison, a Security Gateway routes traffic between its multiple interfaces.) For example, if you have two unconnected networks that share a common Security Management Server and Log Server, configure the common server as a Check Point Host object.

A Check Point Host has one or more Software Blades installed. But if the Firewall blade is installed on the Check Point Host, it cannot function as a firewall. The Host requires SIC and other features provided by the actual firewall.

A Check Point Host has no routing mechanism, is not capable of IP forwarding, and cannot be used to implement Anti-spoofing. If the host must do any of these, convert it to be a Security Gateway.

**Note** - When you upgrade to R80 from R77.30 or earlier versions, Node objects are converted to Host objects.
Managing Objects

In This Section:

- Object Categories ................................................................. 39
- Adding, Editing, Cloning, Deleting, and Replacing Objects ......................... 40
- Object Tags ........................................................................... 40
- Network Object Types ............................................................ 41

Network Objects, defined in SmartConsole and stored in the proprietary Check Point object database, represent physical and virtual network components (such as gateways, servers, and users), and logical components (such as IP address ranges and Dynamic Objects). Before you create Network Objects, analyze the needs of your organization:

- What are the physical components of your network: devices, hosts, gateways and their active Software Blades?
- What are the logical components: services, resources, applications, ranges?
- Who are the users? How should you group them, and with what permissions?

Object Categories

Objects in SmartConsole represent networks, devices, protocols and resources. SmartConsole divides objects into these categories:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Object Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network Objects</td>
<td>Gateways, hosts, networks, address ranges, dynamic objects, security zones</td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td>Services, Service groups</td>
</tr>
<tr>
<td></td>
<td>Custom Applications/Sites</td>
<td>Applications, Categories, Mobile applications</td>
</tr>
<tr>
<td></td>
<td>VPN Communities</td>
<td>Site to Site or Remote Access communities</td>
</tr>
<tr>
<td></td>
<td>Users</td>
<td>Users, user groups, and user templates</td>
</tr>
<tr>
<td></td>
<td>Servers</td>
<td>Trusted Certificate Authorities, RADIUS, TACACS</td>
</tr>
<tr>
<td></td>
<td>Time Objects</td>
<td>Time, Time groups</td>
</tr>
<tr>
<td></td>
<td>UserCheck Interactions</td>
<td>Message windows: Ask, Cancel, Certificate Template, Inform, and Drop</td>
</tr>
<tr>
<td></td>
<td>Limit</td>
<td>Download and upload bandwidth</td>
</tr>
</tbody>
</table>
Adding, Editing, Cloning, Deleting, and Replacing Objects

You can add, edit, delete, and clone objects. A clone is a copy of the original object, with a different name. You can also replace one object in the Policy with another object.

To work with objects, right-click the object in the object tree or in the Object Explorer, and select the action.

You can delete objects that are not used, and you can find out where an object is used.

To clone an object:
1. In the object tree or in the Object Explorer, right-click the object and select **Clone**.
   The **Clone Object** window opens.
2. Enter a name for the cloned object.
3. Click **OK**.

To find out where an object is used:
In the object tree or in the Object Explorer, right-click the object and select **Where Used**.

To replace an object with a different object:
1. In the object tree or in the Object Explorer, right-click the object and select **Where Used**.
2. Click the **Replace** icon.
3. From the **Replace with** list, select an item.
4. Click **Replace**.

To delete all instances of an object:
1. In the object tree or in the Object Explorer, right-click the object and select **Where Used**.
2. Click the **Replace** icon.
3. From the **Replace with** list, select **None (remove item)**.
4. Click **Replace**.

Object Tags

Object tags are keywords or labels that you can assign to network objects or groups of objects for search purposes.

IPS protections have pre-defined tags. Use the tags
• When configuring a Threat Prevention Profile, to determine which protections are activated.
• As search filters, when searching the list of IPS protections.

You cannot add, change or remove tags on IPS protections.

To add a tag to an object:
1. Open the network object for editing.
2. In the **Add Tag** field, enter the label to associate with this object.
3. Press **Enter**.
The new tag shows to the right of the Add Tag field.

4. Click OK.

Network Object Types

In This Section:
- Networks ....................................................................................................................... 41
- Network Groups ............................................................................................................ 41
- Managing Software Blade Licenses ............................................................................ 41
- Gateway Cluster ............................................................................................................ 44
- More Network Object Types ......................................................................................... 45

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.

Network Groups

A network group is a collection of hosts, gateways, networks or other groups.

Groups are used where you cannot work with single objects, e.g. when working with VPN domains or with topology definitions.

Groups facilitate and simplify network management. Modifications are applied to the group instead of each member of the group.

To create a group of network objects:

1. In the Objects tree, click New > Network Group.
   The New Network Group window opens.
2. Enter a name for the group
3. Set optional parameters:
   - Object comment
   - Color
   - Tag (as custom search criteria)
4. For each network object or a group of network objects, click the [+] sign and select it from the list that shows.
5. Click OK.

Managing Software Blade Licenses

After an administrator runs the First Time Configuration Wizard on an R80 Security Management Server, and the Security Management Server connects to the Internet, it automatically activates its
license and synchronizes with the Check Point User Center. If the Security Management Server loses Internet connectivity before the license is activated, it tries again, on an interval.

If the administrator makes changes to Management Software Blade licenses of an R80 Security Management Server in the Check Point User Center, these changes are automatically synchronized with that Security Management Server.

**Note**
- Automatic activation is supported on Check Point appliances only.
- Automatic synchronization is supported on all R80 servers.

To make sure that your environment is synchronized with the User Center, even when the Security Management Server is not connected to the Internet, we recommend that you configure an R80 Check Point server with Internet connectivity as a proxy.

In SmartConsole, you can see this information for most Software Blade licenses:
- License status
- Alerts
- Check Point User Center details

See the *R80 Release Notes* for a list of supported Software Blades

**Configuring a Proxy gateway**

To configure a proxy on an R80 Check Point server:

1. On the Security Management Server, add these lines to `$CPDIR/tmp/.CPprofile.sh`:
   - `_cpprof_add HTTP_CLIENT_PROXY_SICNAME "<proxy server sic name>" 0 0`
   - `_cpprof_add HTTP_CLIENT_PROXY_IP "<proxy server IP>" 0 0`

**Viewing Licenses**

To view license information:

In SmartConsole, go to the *Gateways & Servers* view, and from the *Columns* drop-down list, select *Licenses*.

You can see this information:
- **License Status** - The general state of the Software Blade licenses:
  - **OK** - All the blade licenses are valid.
  - **Not Activated** - Blade licenses are not installed. This is only possible in the first 15 days after the establishment of the SIC with the Security Management Server. After the initial 15 days, the absence of licenses will result in the blade error message.
  - **Error with <number> blade(s)** - The specified number of blade licenses are not installed or not valid.
  - **Warning with <number> blade(s)** - The specified number of blade licenses have warnings.
  - **N/A** - No available information.
- **CK (Certificate Key)** - Unique key of the license instance.
- **SKU** - Catalog ID from the Check Point User Center.
• **Account ID** - User's account ID.
• **Support Level** - Check Point level of support.
• **Support Expiration** - Date when the Check Point support contract expires.

To view license information per **Software Blade**:  
1. Select a Security Gateway or a Security Management Server.  
2. In the **Summary** tab below, click the object's license status (for example: **OK**).  
The **Device & License** window opens. It shows basic object information and **License Status**, license **Expiration Date**, and important quota information (in the **Additional Info** column) for each Software Blade.  

**Notes** -  
• Quota information, quota-dependent license statuses, and blade information messages are only supported for R80  
• The tooltip of the SKU is the product name

These are the possible values for the Software Blade **License Status**:

• **Active** - The Software Blade is active and the license is valid.  
• **Available** - The Software Blade is not active, but the license is valid.  
• **No License** - The Software Blade is active but the license is not valid.  
• **Expired** - The Software Blade is active, but the license expired.  
• **About to Expire** - The Software Blade is active, but the license will expire in thirty days (default) or less ('7 days or less for an evaluation license).  
• **Quota Exceeded** - The Software Blade is active, and the license is valid, but the quota of related objects (gateways, files, virtual systems, and so on, depending on the blade) is exceeded.  
• **Quota Warning** - The Software Blade is active, and the license is valid, but the number of objects of this blade is 90% (default) or more of the licensed quota.  
• **N/A** - The license information is not available.

**Monitoring Licenses**

To keep track of license issues, you can use:

• **License Inventory Report** - Shows the status of each Software Blade, gateway, and server license, including warnings and critical issues. You can filter the list of devices and export the report to a file.  
• **License Status View** - Shows the license status for all gateways and servers with the option to click and see more details for each device.  

In the **License Inventory Report** and **License Status View**, you can also see the **Next Expiration Date**, which is the closest expiration date of one or more of the Software Blades.  
The SmartEvent blade allows you to customize the **License Status View** and **License Inventory Report** from the **Logs & Monitor** view of SmartConsole. It is also possible to view license information from the **Gateways & Servers** view of SmartConsole without the SmartEvent blade.

To see the License Inventory report from the **Logs & Monitor** view:  
1. In the **Logs & Monitor** view of SmartConsole, open a new tab.
2. Select **Reports**.
3. Double-click **License Inventory**.
   The **License Inventory** report opens.

To see the License Inventory report from the Gateways & Servers view:
From the **Gateways & Servers** view, click **Actions > License Report**.

To filter the list of devices in the License Status report:
1. In the **License Status** view, click to expand the **Options** menu on the right.
2. Select **View Filter**.
   The **Edit View** Filter window opens.
3. Select a **Field** to filter results.
4. Select the operation - **Equals, Not Equals**, or **Contains**.
5. Enter a filter value.
6. Optional: Click the plus sign to add a filter.
7. Click **OK**.
   The filtered list of devices shows.

To export the License Status report:
1. In the **License Status** view, click to expand the **Options** menu on the right.
2. Select a type of export:
   - **Save as PDF**
   - **Save as Excel** - Can convert to csv file also
   - **Export** - Creates a .cpr file
3. Click **Download**.

To see the License Status view from Logs & Monitor:
1. In the **Logs & Monitor** view of SmartConsole, open a new tab.
2. Select **Views**.
3. Double-click **License Status**.
   The **License Status** view opens.

To see a summary of Licenses from Gateways & Servers:
From the **Gateways & Servers** view, from the **Columns** menu, click **Licenses**.

**Gateway Cluster**
A gateway cluster is a group of Security Gateways with Cluster software installed: ClusterXL, or another Clustering solution. Clustered gateways add redundancy through High Availability or Load Sharing.
More Network Object Types

**Address Ranges**

An address range is a range of IP addresses on the network, defined by the lowest and the highest IP addresses. Use an Address Range object when you cannot define a range of IP addresses by a network IP and a net mask. The Address Range objects are also necessary for the implementation of NAT and VPN.

**Domains**

A Domain object lets you define a host or DNS domain by its name only. You do not need the IP address of the site.

- The format of the name is x.y. For example `mysite.com` or `mysite.co.uk`.
- A period separates each section of the name.
- For successful resolution to an IP address, the specified domain name must be an actual domain name.
- Name resolution takes place on the Security Gateway, and the result is cached for reuse.

You can also configure the domain object to represent a pattern that will watch all sub-domains. For example: `*.mysite.com`. This partial domain name will match all sub-domains of `mysite.com`.

**Note** - The gateway resolves partial names using DNS reverse lookups, which can be inaccurate and take some time.

After defining a domain object, you can use it in the source and destination columns of an access policy.

**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.

Dynamic Objects are predefined for:

- **LocalMachine-all-interfaces** - The DAIP machine interfaces (static and dynamic) are resolved into this object.
- **LocalMachine** - The external interface (dynamic) of the SmartLSM Security Gateway (as declared in `cpconfig` when configuring the gateway).
- **InternalNet** - The internal interface of the SmartLSM Security Gateway (as declared in `cpconfig` when configuring the gateway).
- **AuxiliaryNet** - The auxiliary interface of the SmartLSM Security Gateway (as declared in `cpconfig` when configuring the gateway).
- **DMZNet** - The DMZ interface of the SmartLSM Security Gateway (as declared in `cpconfig` when configuring the gateway).

Externally Managed Gateways/Hosts

An Externally Managed Security Gateway or a Host is a gateway or a Host which has Check Point software installed on it. This Externally Managed gateway 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.

Interoperable Devices

An Interoperable Device is a device that has no Check Point Software Blades installed. The Interoperable Device:

- Cannot have a policy installed on it
- Can participate in Check Point VPN communities and solutions.

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 Command Line Interface Reference Guide http://supportcontent.checkpoint.com/documentation_download?ID=24833.

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.

- Persistence 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.
- Persistence 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 Security Management 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 Security Management 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.
Policy Management

In This Section:

Working with Policy Packages ..................................................................................... 48
Viewing Rule Logs......................................................................................................... 52
Installing and Publishing .............................................................................................. 53
Policy Installation History ............................................................................................ 53
Introducing Policy Layers ............................................................................................. 54
Managing Policy Layers................................................................................................ 54

SmartConsole offers a number of tools that address policy management tasks, both at the definition stage and for maintenance.

At the definition stage:

- **Policy Packages** let you group different types of policies, to be installed together on the same installation targets.
- **Predefined Installation Targets** let you associate each package with a set of gateways. You do not have to repeat the gateway selection process each time you install a Policy Package.

At the maintenance level:

- **Search** gives versatile search capabilities for network objects and the rules in the Rule Base.
- **Database version control** lets you track past changes to the database.

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules:
  - Firewall
  - NAT
  - Application Control and URL Filtering
  - Data Awareness

- **QoS**

- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.

- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
  - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
• Threat Emulation - detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox

The installation process:
• Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.
  If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.
• Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced.
• Distributes the user database and object database to the selected installation targets.
You can create different policy packages for different types of sites in an organization.

Example:
An organization has four sites, each with its own requirements. Each site has a different set of Software Blades installed on the Security Gateways:

<table>
<thead>
<tr>
<th>Item</th>
<th>Security Gateway</th>
<th>Installed Software Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sales California</td>
<td>Firewall, VPN</td>
</tr>
<tr>
<td>2</td>
<td>Sales Alaska</td>
<td>Firewall, VPN, IPS, DLP</td>
</tr>
<tr>
<td>3</td>
<td>Executive management</td>
<td>Firewall, VPN, QoS, and Mobile Access</td>
</tr>
<tr>
<td>4</td>
<td>Server farm</td>
<td>Firewall</td>
</tr>
<tr>
<td>5</td>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>
To manage these different types of sites efficiently, you need to create three different Policy Packages. Each Package includes a combination of policy types that correspond to the Software Blades installed on the site’s gateway. For example:

- A policy package that includes the Access Control policy type. The Access Control policy type controls the firewall, NAT, Application Control and URL Filtering, and Data Awareness blades. This package also determines the VPN configuration.
  
  Install the Access Control policy package on all Security Gateways.

- A policy package that includes the QoS policy type for the QoS blade on gateway that manages bandwidth.
  
  Install this policy package on the executive management Gateway.

- A policy package that includes the Desktop Security Policy type for the gateway that handles Mobile Access.
  
  Install this policy package on the executive management Gateway.

Creating a New Policy Package

1. From the Menu, select Manage Policies. The Manage Policies window opens.
2. Click New. The Policy window opens.
3. Enter a name for the policy package.
4. In the General page > Policy types section, select one or more of these policy types:
   - Access Control
   - QoS, select Recommended or Express
   - Desktop Security
   - Threat Prevention
5. On the Installation targets page, select the gateways the policy will be installed on:
   - All gateways
   - Specific gateways - For each gateway, click the [+|] sign and select it from the list.
  
  To install Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets.
6. Click OK.

Adding a Policy Type to an Existing Policy Package

1. From the Menu, select Manage Policies. The Manage Policies window opens.
2. Select a policy package and click the Edit button.
3. The Policy package window opens.
4. On the **General > Policy types** page, select the policy type to add:
   - **Access Control**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**
   - **Threat Prevention**

5. Click **OK**.

### Installing a Policy Package

1. On the Global Toolbar, click **Install Policy**.
   - The **Install Policy** window opens showing the installation targets (Security Gateways).
2. From the **Select a policy** menu, select a policy package.
3. Select one or more policy types that are available in the package.
4. Select the **Install Mode**:
   - **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn’t affect the installation on the rest of the target gateways.
     - **Note**: If you select **For Gateway Clusters install on all the members, if fails do not install at all**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.
5. Click **Install**.

### Installing the User Database

When you make changes to user or administrator definitions through SmartConsole, they are saved to the user database on the Security Management Server. User authentication methods and encryption keys are also saved in this database. The user database does **not** contain information about users defined externally to the Security Gateway (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). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the Security Management Server.

You must choose to install the policy or the user database, based on the changes you made:

- Install the policy ("Installing a Policy Package" on page 51), if you modified additional components of the Policy Package (for example, added new Security Policy rules) that are used by the installation targets
- Install the user database, if you only changed the user definitions or the administrator definitions - From the Menu, select **Install Database**

The user database is installed on:

- **Security Gateways** - during policy installation
- **Check Point hosts with one or more Management Software Blades enabled** - during database installation
You can also install the user database on Security Gateways and on a remote server, such as a Log Server, from the command line interface on the Security Management Server.

**To install user database from the command line interface:**

On the Security Management Server, run: `fwm dbload <host name>`

**Note:** Check Point hosts that do not have active Management Software Blades do not get the user database installed on them.

**Uninstalling a Policy Package**

You can uninstall a policy package through a command line interface on the gateway.

**To uninstall a policy package:**

1. Open a command prompt on the Security Gateway.
2. Run: `fw unloadlocal`.

**Viewing Rule Logs**

You can search for the logs that are generated by a specified rule, from the Security Policy or from the Logs & Monitor > Logs tab

**To see logs generated by a rule (from the Security Policy):**

1. In SmartConsole, go to the Security Policies view.
2. In the Access Control Policy or Threat Prevention Policy, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Summary** - Rule name, rule action, rule creation information, and the hit count. Add custom information about the rule.
   - **Details** (Access Control Policy only) - Details for each column. Select columns as necessary.
   - **Logs** - Log entries according to filter criteria - Source, Destination, Blade, Action, Service, Port, Source Port, Rule (Current rule is the default), Origin, User, or Other Fields.
   - **History** (Access Control Policy only) - List of rule operations in chronological order, with the information about the rule type and the administrator that made the change.

**To see logs generated by a rule (by Searching the Logs):**

1. In SmartConsole, go to the Security Policies view.
2. In the Access Control Policy or Threat Prevention Policy, select a rule.
3. Right-click the rule number and select Copy Rule UID.
4. In the Logs & Monitor > Logs tab, search for the logs in one of these ways:
   - Paste the Rule UID into the query search bar and press Enter.
   - For faster results, use this syntax in the query search bar:
     ```
     layer_uuid_rule_uuid:*_<UID>
     ```
     For example, paste this into the query search bar:
     ```
     layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10
     ```
Installing and Publishing

It is important to understand the differences between publishing and installing.

<table>
<thead>
<tr>
<th>You must do this:</th>
<th>After you did this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish</td>
<td>Opened a session in SmartConsole and made changes.</td>
</tr>
<tr>
<td></td>
<td>The Publish operation sends all SmartConsole modifications to other administrators, and makes the changes you made in a private session public.</td>
</tr>
<tr>
<td>Install the database</td>
<td>Modified network objects, such as servers, users, services, or IPS profiles, but not the Rule Base.</td>
</tr>
<tr>
<td></td>
<td>Updates are installed on management servers and log servers.</td>
</tr>
<tr>
<td>Install a policy</td>
<td>Changed the Rule Base.</td>
</tr>
<tr>
<td></td>
<td>The Security Management Server installs the updated policy and the entire database on Security Gateways (even if you did not modify any network objects).</td>
</tr>
</tbody>
</table>

Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

Policy Installation History

In the Installation History you can choose a Gateway, a date and time when the Policy was installed, and:

- See the revisions that were installed on the Gateway and who installed the Policy.
- See the changes that were installed and who made the changes.
- Revert to a specific version, and install the last “good” Policy.

To work with the Policy installation history:

1. In SmartConsole, go to Security Policies.
2. Select Installation History:
   - For Access Control Policy, in the Access Tools section
   - For Threat Prevention Policy, in the Threat Prevention Tools section
3. In the Gateways section, select a Gateway.
4. In the Policy Installation History section, select an installation date.
5. To see the revisions that were installed and who made them:
   Click View installed changes.

To see the changes that were installed and who made them:
Click View.

To revert to a specific version of the Policy:
Click Install specific version.

Introducing Policy Layers

To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.

For example, when you upgrade to R80 from earlier versions:

• Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.
  When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

• Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.
  All layers are evaluated in parallel

For Pre-R80 Gateways, the enforcement is the same as with earlier management versions, but it looks different in the SmartConsole.

The layers concept opens more options for policy management. These include:

• Setting different view and edit permissions per layer for different administrator roles.

• Re-using a layer in different places: For example, use the same Application Control layer in different policy packages.


Future versions will include more options with layers, including Actions for Inline Layers.

Managing Policy Layers

You can use the Manage Layers window to work with Policy Layers. To open the Manage Layers window, select Menu > Manage Layers in SmartConsole. The Manage Layers shows:

• Layer - Layer name

• Number of Rules - Number of rules in the Layer

• Policy Package - Policy packages that use the Layer

• Mode:
  • Ordered - A Policy Layer that includes global rules and a placeholder for local, Domain rules
  • Not in use - A Policy Layer that is not used in a Policy package
  • Administrator - The administrator who last changed the Layer configuration
- **Created By** - The administrator who created the Layer
- **Date Created** - Date the Layer was created
- **Rule Grid** - Shows the rules in the selected Layer

To create a new Policy Layer:
1. In SmartConsole, click **Menu > Manage Layers**.
2. Click the **New** icon in the upper toolbar.
3. Configure the settings in the **Layer Editor** window.
4. Optional: It is a best practice to share Policy Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer**.
5. Close the window and publish the session.

   This Policy Layer is not yet assigned to a Policy Package.

To change an existing Policy Layer configuration, right-click it in the **Layer Editor**, and then select **Edit layer**.

To export Layer rules to a .csv file:
1. In SmartConsole, click **Menu > Manage Layers**.
   The **Manage Layers** window opens.
2. Select a Layer, and then click **Actions > Export**.
3. Enter a path and file name.
Introducing the Access Control Policy

In This Section:

Unified Policy ................................................................................................................ 56
The Columns of the Access Control Rule Base .............................................................. 57
Types of Rules in the Rule Base .................................................................................... 57
Visual Division of the Rule Base with Sections ............................................................ 58
Managing Pre-R80 Security Gateways ....................................................................... 59
Order of Rule Enforcement ......................................................................................... 59
Managing Network Access Control ............................................................................. 60
Managing URL Filtering and Application Control ...................................................... 63
Analyzing the Rule Base [Hit Count] .......................................................................... 70
Inspection Settings .................................................................................................... 72

An Access Control Policy Rule Base consists of these types of rules:

- Firewall - Control access to the internal network through different access points (gateways)
- Application Control and URL Filtering - Prevent malicious applications from compromising any internal company data and the internal network resources

Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

- Firewall and VPN
- Application Control and URL Filtering
- Identity Awareness
- Data Awareness
- Mobile Access
- Security Zones

You can create Access Control policy rules that are based on:

- Services
- Protocols
- Applications
- URLs
- File types
- Data types

The information on connections is collected in one log file from all the Software Blades.
The Columns of the Access Control Rule Base

These are the fields of the rules in the Access Control policy. Not all of these are shown by default. To select a field that does not show, right-click on the Rule Base table header, and select it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Rule Base Layer.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of connections that match this rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Services &amp;</td>
<td>Services, Applications, Categories, and Sites.</td>
</tr>
<tr>
<td>Applications</td>
<td>If Application Control and URL Filtering is not enabled, only Services show.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when traffic matches the rule. Options include: Accept,</td>
</tr>
<tr>
<td></td>
<td>Drop, Ask, Inform (UserCheck message), and Reject.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the policy.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that this rule is enforced.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

Types of Rules in the Rule Base

There are three types of rules in the Rule Base - explicit, implied and implicit.

Explicit rules

The rules that the administrator configures explicitly, to allow or to block traffic based on specified criteria.

⚠️ Important - The Cleanup rule is a default explicit rule and is added with every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit cleanup rule as the last rule in each layer.

Implied rules

The default rules that are available as part of the Global properties configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- **First** - Applied first, before all other rules in the Rule Base - explicit or implied
- **Last** - Applied last, after all other rules in the Rule Base - explicit or implied, but before the Implicit Cleanup Rule
- **Before Last** - Applied before the last explicit rule in the Rule Base
Implied rules are configured to allow connections for different services that the Security Gateway uses. For example, the **Accept Control Connections** rules allow packets that control these services:

- Installation of the security policy on a Security Gateway
- Sending logs from a Security Gateway to the Security Management Server
- Connecting to third party application servers, such as RADIUS and TACACS authentication servers

**Implicit cleanup rule**

The default “catch-all” rule that deals with traffic that does not match any explicit or implied rules in the Policy Layers. For R77.30 or earlier versions Security Gateways, the action of the implicit rule depends on the Policy Layer:

- **Drop** - for the Network Layer
- **Accept** - for the Application Control Layer

  **Note** - If you change the default values, the policy installation will fail.

The implicit rules do not show in the Rule Base.

**Configuring the Implied Rules**

Some of the implied rules are enabled by default. You can change the default configuration as necessary.

**To configure the implied rules:**

1. In SmartConsole, from the Menu, select **Global Properties**.
   
   The **Global Properties** window opens.

2. Select a rule to enable it, or clear a rule to disable it.

3. For the enabled rules, select the position of the rules in the Rule Base (“**Order of Rule Enforcement**” on page 59):
   
   - **First** - The rule is applied before any other rule in the Rule Base
     
   - **Last** - The rule is applied if all other rules in the Rule Base were applied and none of them matched
     
   - **Before Last** - The rule is applied before the last explicit rule, if none of the other rules in the Rule Base matched

4. Click **OK** and install the policy.

**Visual Division of the Rule Base with Sections**

To better manage a policy with a large number of rules, you can use **Sections** to divide the Rule Base into smaller, logical components. The division is only visual and does not make it possible to delegate administration of different **Sections** to different administrators.
Managing Pre-R80 Security Gateways

When you upgrade a pre-R80 Security Management Server that manages pre-R80 Security Gateways to R80, the existing Access Control policies are converted in this way:

- The pre-R80 **Firewall** policy is converted into the **Network** Policy Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Drop** all traffic that is not matched by any rule in this Layer.
- The pre-R80 **Application & URL Filtering** policy is converted into the **Application** Policy Layer, which is the second Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Accept** all traffic that is not matched by any rule in this Layer.

**Important** – After upgrade, do not change the **Action** of the implicit cleanup rules, or the order of the Policy Layers. If you do, the policy installation will fail.

New Access Control Policy for pre-R80 Security Gateways on an R80 Security Management Server must have this structure:

1. The first Policy Layer is the Network Layer (with the **Firewall** blade enabled on it).
2. The second Policy Layer is the Application Control and URL Filtering Layer (with the **Application & URL Filtering** blade enabled on it).
3. There are no other Policy Layers.

If the Access Control Policy has a different structure, the policy will fail to install.

You can change the names of the Layers, for example, to make them more descriptive.

Each new Policy Layer will have the explicit default rule, added automatically and set to **Drop** all the traffic that does not match any rule in that Policy Layer. We recommend that the **Action** is set to **Drop** for the Network Policy Layer and **Accept** for the Application Control Policy Layer.

If you remove the default rule, the **Implicit Cleanup Rule** will be enforced. The **Implicit Cleanup Rule** is configured in the Policy configuration window and is not visible in the Rule Base table. Make sure the **Implicit Cleanup Rule** is configured to **Drop** the unmatched traffic for the Network Policy Layer and to **Accept** the unmatched traffic for the Application Control Policy Layer.

Order of Rule Enforcement

When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet.

If the **Action** of the matching rule is **Drop**, the gateway stops matching against later rules in the Policy Rule Base and drops the packet. If the **Action** is **Accept**, the gateway continues to check rules in the next Policy Layer down.

If none of the rules in the Policy Layer match the packet, the explicit **Default Cleanup Rule** is applied. If this rule is missing, the **Implicit Cleanup Rule** is applied.

**Important** - Always add an explicit **Default Cleanup Rule** at the end of each Policy Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Order in which the rules in each Access Control Policy Layer are applied:

1. **First Implied Rule** - No explicit rules can be placed before it.
2. **Explicit Rules** - These are the rules that you create.
3. **Before Last Implied Rule** - Applied before the last explicit rule.

4. **Last Explicit Rule** - We recommend that you use a **Cleanup rule** as the last explicit rule.
   
   **Note** - If you use the Cleanup rule as the last explicit rule, the Last Implied Rule and the Implicit Cleanup Rule are not enforced.

5. **Last Implied Rule** - Remember that although this rule is applied after all other explicit and implied rules, the Implicit Cleanup Rule is still applied last.

6. **Implicit Cleanup Rule** - The default rule that is applied if none of the rules in the Policy Layer match.

**Best practices for performance-efficient Access Control Policy**

- Add all rules that are based only on source and destination IP addresses and ports in a Firewall/Network Policy Layer at the top of the Rule Base
- Create Firewall/Network rules to explicitly accept safe traffic, and add the **Explicit Cleanup Rule** at the bottom of the Policy Layer to drop everything else
- Create Application Control rules to explicitly drop unwanted or unsafe traffic, and add the Explicit Cleanup Rule at the bottom of the Policy Layer to accept everything else
- Turn XFF inspection off, unless the gateway is behind a proxy server. For more, see: sk92839 http://supportcontent.checkpoint.com/solutions?id=sk92839.

**Managing Network Access Control**

A firewall controls access to computers, clients, servers, and applications through a set of rules that comprise an Access Control Rule Base. You need to configure a Rule Base that not only provides highly secure Access Control, but optimizes network performance. A strong Access Control Rule Base:

- Only allows authorized connections and prevents vulnerabilities in a network
- Gives authorized users access to the correct internal resources
- Efficiently inspects connections and uses network resources efficiently

**Ensuring a Secure Network Access**

A robust security policy must have some basic rules in its Rule Base.

**Basic Rules**

These are basic Access Control rules we recommend for all Rule Bases:

- **Stealth rule** that prevents direct access to the Security Gateway
- **Cleanup rule** that drops all traffic that is not allowed by the earlier rules in the policy

**Note** - There is also the implicit drop rule that drops all traffic that did not match all other rules. This rule does not create log entries. If you want to log the traffic, create an explicit cleanup rule.
Sample Firewall Rule Base

This shows a sample Firewall Rule Base for a typical security policy. (The Hits and VPN columns are not shown.)

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stealth</td>
<td>NOT internal</td>
<td>GW-group</td>
<td>Any</td>
<td>Drop</td>
<td>Alert</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>2</td>
<td>Critical subnet</td>
<td>Internal</td>
<td>Finance HR R&amp;D</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>CorpGW</td>
</tr>
<tr>
<td>3</td>
<td>Tech support</td>
<td>TechSupport</td>
<td>Remotel-web</td>
<td>HTTP</td>
<td>Accept</td>
<td>Alert</td>
<td>RemotelGW</td>
</tr>
<tr>
<td>4</td>
<td>DNS server</td>
<td>Any</td>
<td>DNS</td>
<td>Domain UDP</td>
<td>Accept</td>
<td>None</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>5</td>
<td>Mail and Web servers</td>
<td>Any</td>
<td>DMZ</td>
<td>HTTP HTTPS SMTP</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>6</td>
<td>SMTP</td>
<td>Mail</td>
<td>NOT Internal net group</td>
<td>SMTP</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>7</td>
<td>DMZ &amp; Internet</td>
<td>IntGroup</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>8</td>
<td>Clean up rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

1. **Stealth** - All traffic that is NOT from the internal company network to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.

2. **Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and R&D.

3. **Tech support** - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.

4. **DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.

5. **Mail and Web servers** - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.

6. **SMTP** - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.

7. **DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.

8. **Clean up rule** - Drops all traffic. All traffic that is allowed matched one of the earlier rules.

**Preventing IP Spoofing**

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks that packet.
Introducing the Access Control Policy

Example:
The diagram shows a Gateway with interfaces A and B, and C, and some example networks behind the interfaces.

For the Gateway, anti-spoofing makes sure that

- All incoming packets to A come from 192.168.33.0
- All incoming packets to B come from 192.0.2.0 or 10.10.10.0
- All incoming packets to C come from the Internet

If an incoming packet to B has a source IP address in network 192.168.33.0, the packet is blocked, because the source address is spoofed.

When you configure Anti-Spoofing on a Check Point Security Gateway, specify the type of networks that each interface faces - External (Internet) or Internal.

Configuring Anti-Spoofing

Make sure to configure Anti-Spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

To configure Anti-Spoofing for an interface:

1. In SmartConsole, go to Gateways & Servers and double-click the gateway object.
   The General Properties window of the gateway opens.
2. From the navigation tree, select Network Management.
3. Click Get Interfaces.
4. Click Accept.
   The gateway network topology shows. If SmartConsole fails to automatically retrieve the topology, make sure that the details in the General Properties section are correct and the Security Gateway, the Security Management Server, and the SmartConsole can communicate with each other.
5. Select an interface and click Edit.
   The Interface properties window opens.
6. From the navigation tree, select General.
7. In the Topology section of the page, click Modify.
   The Topology Settings window opens.
8. Select the type of network the interface leads to:
   - External - All external/Internet addresses
   - Internal -
### Introducing the Access Control Policy

- **Not Defined** - All IP addresses behind this interface are considered a part of the internal network that connects to this interface
- **Network defined by the interface IP and Net Mask** - Only the network that directly connects to this internal interface
- **Specific** - A specific network object (a network, a host, an address range, or a network group) behind this internal interface
- **Interface leads to DMZ** - The DMZ that directly connects to this internal interface

9. In the **Anti-Spoofing** section, make sure that **Perform Anti-Spoofing based on interface topology** is selected.

10. Select an **Anti-Spoofing action**:
   - **Prevent** - Drops spoofed packets
   - **Detect** - Allows spoofed packets. To monitor traffic and to learn about the network topology without dropping packets, select this option together with the **Spoof Tracking Log** option.

11. Configure Anti-Spoofing exceptions (optional) - addresses, from which packets are not inspected by Anti-Spoofing ("Excluding Specific Internal Addresses" on page 63):
   a) Select **Don’t check packets from**.
   b) Select an object from the drop-down list, or click **New** to create a new object.

12. Configure **Spoof Tracking** - select the tracking action that is done when spoofed packets are detected:
   - **Log** - Create a log entry (default)
   - **Alert** - Show an alert
   - **None** - Do not log or alert

13. Click **OK** twice to save Anti-Spoofing settings for the interface.

   For each interface, repeat the configuration steps. When finished, install the policy.

---

### Excluding Specific Internal Addresses

In some configurations, the Firewall must allow connections with an internal IP address from an external source. For example, an external application can assign internal IP addresses to external clients. You can configure the Anti-Spoofing protection on the external interfaces to ignore connections from these IP addresses. The Firewall allows these connections and does not inspect them.

---

### Managing URL Filtering and Application Control

Today there are many challenges for businesses to keep up with security requirements of social media and Web 2.0 applications. It is necessary for system administrators to use the security policy to overcome these challenges. For example:

- **Malware threats** - Popular applications like Twitter, Facebook, and YouTube can cause users to download viruses unintentionally. When users download files and use torrents, they can also let malware into your network.

- **Bandwidth hogging** - Applications that use a lot of bandwidth can reduce the performance for important business applications.

- **Loss of productivity** - Employees can spend time on social networking and other applications that can decrease business productivity.
• **Content control** - Prevent Internet access to websites with inappropriate content, such as sex and violence.

### The Check Point Solution for Internet Browsing

The Check Point URL Filtering and Application Control Software Blades can help organizations of all sizes monitor and control the use of Internet by their employees. You can easily create policies which identify or block thousands of applications and Internet sites.

Use the URL Filtering and Application Control Software Blades to:

- **Create a Granular Policy** - Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels. You can also create an HTTPS policy that enables Security Gateways to inspect HTTPS traffic and prevent security risks related to the SSL protocol.

- **Manage Bandwidth Consumption** - Configure rules to limit the available network bandwidth for specified users or groups. You can define separate limits for uploading and downloading.

- **Keep Your Policies Updated** - The Application Database is updated regularly, which helps you makes sure that your Internet security policy has the newest applications and website categories. Security Gateways connect to the Check Point Online Web Service to identify new social networking widgets and website categories.

- **Communicate with Users** - UserCheck objects add flexibility to URL Filtering and Application Control and let the Security Gateways communicate with users. UserCheck helps users understand that certain websites are against the company’s security policy. It also tells users about the changes in Internet policy related to websites and applications.

- **Create Custom Objects** - In addition to the hundreds of default objects, you can create custom objects, to better manage the use of Internet by your users. Create objects for applications, websites, categories and groups, and use them in your security policy rules.

### UserCheck

UserCheck works with the URL Filtering and Application Control Software Blades and lets the Security Gateways send messages to users about possible non-compliant or dangerous Internet browsing. Create UserCheck objects and use them in the Application Control and URL Filtering rules, to communicate with the users. These actions use UserCheck objects:

- **Inform**
- **Ask**
- **Drop**

### UserCheck on a Security Gateway

You can enable UserCheck on Security Gateways that use URL Filtering and Application Control Software Blades. When UserCheck is enabled, the user’s Internet browser shows the UserCheck messages in a new window.

### UserCheck on a computer

The UserCheck client is installed on endpoint computers. This client:

- Sends messages for applications that are not based on Internet browsers, such as Skype and iTunes, and Internet browser add-ons and plug-ins.
- Shows a message on the computer when it cannot be shown in the Internet browser.
Enabling URL Filtering and Application Control

To enable R80 Application Control and URL Filtering for pre-R80 gateways, enable the Application Control and URL Filtering Software Blades on each gateway. Then, if necessary, create a second Layer for the Application Control and URL Filtering rules. Configure this second Layer for the Access Control Policy.

To enable URL Filtering and Application Control Software Blades on a Security Gateway:

1. In SmartConsole, go to Gateways & Servers and double-click the gateway object. The General Properties window of the gateway opens.
2. From the navigation tree, click General Properties.
3. In the Network Security tab, select URL Filtering, or Application Control, or both.
4. Click OK.

To create a second Layer for URL Filtering and Application Control:

1. In SmartConsole, go to Security Policies.
3. In the Access Control section, click the plus sign.
4. Click New Layer. The Layer Editor window opens and shows the General view.
5. Enable Application Control and URL Filtering on the Layer.
   a) In the Blades section, enter a name for the Layer. We recommend the name Application.
   b) Click Application Control and URL Filtering.
   c) Click OK and the Layer Editor window closes.
   d) Click OK and the Policy window closes.
6. Install the policy.

Special URL Filtering and Application Control Fields

Internet browsing is not easily defined into allowed and prohibited categories. Many websites and applications can be used for legitimate business reasons. The rules that control Internet access must be flexible and granular. The Access Control Policy Rule Base uses these fields to create a strong and flexible URL Filtering and Application Control security policy:

- **Services & Applications**
- **Action**

**Services & Applications**

In the Services & Applications column, define the Web applications, sites, services and protocols that are included in the rule. A rule can contain one or more:

- Applications
- Web sites
Introducing the Access Control Policy

- Services
- Default categories of Internet traffic
- Custom categories or groups that you create, that are not included in the Check Point Application Database.

**Application Matching**

If an application is *allowed* in the policy, the rule is matched only on the recommended services of the application. This default setting is more secure than allowing the application on all services. For example: a rule that allows Facebook, allows it only on the Application Control Web browsing services: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.

If an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can change the default match settings for applications.

**Configuring Matching for an Allowed Application**

You can configure how a rule matches an application or category that is *allowed* in the policy. You can configure the rule to match the application:

- On any service,
- or
- On a specified service.

To do this, change the **Match Settings** of the application or category. The application or category is changed everywhere that it is used in the policy.

**To change the matched services for an allowed application or category:**

1. In a rule which has applications or categories in the **Services & Applications** column, double-click an application or category.
2. Select **Match Settings**.
3. Select an option:
   - To match the application with all services, select **Any**.
   - To match the application on specified services:
     (i) Select **Customize**.
     (ii) Add or remove services.
   - To match the application with all services and exclude specified services:
     (i) Select **Customize**.
     (ii) Add the services to exclude.
     (iii) Select **Negate**.
4. Click **OK**.

**Configuring Matching for Blocked Applications**

By default, if an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.
You can configure the matching for blocked applications so that they are matched on the recommended services. For Web applications, the recommended services are the *Web browsing services*.

If the match settings of the application are configured to **Customize**, the blocked application is matched on the customized services. It is not matched on all ports.

**To configure matching for blocked applications:**

1. In SmartConsole, click **Manage & Settings > Blades > Application Control and URL Filtering > Advanced Settings > Application Control Web Browsing Services.**
2. Configure **Match web application on 'Any' port when used in 'Block' rule**:

   - **Note** - This setting applies to *all* applications, not only to Web applications.
   - **Selected** - This is the default. If an application is *blocked* in the Rule Base, the application is matched to *Any* port.
   - **Not selected** - If an application is *blocked* in the Rule Base, the application is matched to the services that are configured in the application object of the application. However, some applications are still matched on *Any*. These are applications (Skype, for example) that do not limit themselves to a standard set of services.

   **Summary of Application Matching in a "Block" Rule**

<table>
<thead>
<tr>
<th>Application - Match Setting</th>
<th>Checkbox: Match web application on 'Any' port when used in 'Block' rule</th>
<th>Blocked Application is Matched on Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended services (default)</td>
<td>Selected (default)</td>
<td>Any</td>
</tr>
<tr>
<td>Recommended services (default)</td>
<td>Not selected</td>
<td>Recommended services</td>
</tr>
<tr>
<td>Customize</td>
<td><em>Not relevant</em></td>
<td>Customized</td>
</tr>
<tr>
<td>Any</td>
<td><em>Not relevant</em></td>
<td>Any</td>
</tr>
</tbody>
</table>

**Adding Services, Applications, and Sites to a rule**

You can add services to a rule, or applications and sites.

**To add services, applications or sites to a rule:**

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. To add applications to a rule, select the **Application Control** Layer.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.
4. Search for the services, sites, applications, or categories.
5. Click the + next to the ones you want to add.

**Creating Custom Applications, Categories, and Groups**

You can create custom applications, categories or groups, that are not included in the Check Point Application Database.
To create a new application or site:
1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Click New > Custom Applications/Site > User Application.
5. Enter a name for the object.
6. Enter one or more URLs.
   If you used a regular expression in the URL, click URLs are defined as Regular Expressions.
   Note - If the application or site URL is defined as a regular expression you must use the correct syntax.
7. Click OK.

To create a custom category:
1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Click New > Custom Applications/Site > User Category.
5. Enter a name for the object.
6. Enter a description for the object.
7. Click OK.

**Action**

In the Action field, define what occurs to traffic that matches the URL Filtering and Application Control rule. These are the Action options:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Allows the traffic.</td>
</tr>
</tbody>
</table>
| Drop                  | Blocks the traffic.  
                          | Optionally, shows a UserCheck Block message.                              |
| Limit                 | Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for downloads and downloads. |
| Enable Identity Captive Portal | Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication. |
**UserCheck Actions**

These are the Action options that work with UserCheck:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Drop</strong></td>
<td>Blocks the traffic. Optionally, shows a UserCheck Block message.</td>
</tr>
<tr>
<td><strong>Ask</strong></td>
<td>Shows a UserCheck Ask message. The message asks users to confirm that it is necessary that they go to the application or site.</td>
</tr>
<tr>
<td><strong>Inform</strong></td>
<td>Sends a message to the user attempting to access the application</td>
</tr>
<tr>
<td><strong>UserCheck</strong></td>
<td>Defines how often users see the UserCheck message for Ask, Inform, or Block actions.</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>Select the action that triggers a UserCheck message:</td>
</tr>
<tr>
<td><strong>Confirm</strong></td>
<td>• Per rule - UserCheck message shows only once when traffic matches a rule.</td>
</tr>
<tr>
<td><strong>UserCheck</strong></td>
<td>• Per category - UserCheck message shows for each matching category in a rule.</td>
</tr>
<tr>
<td></td>
<td>• Per application/Site - UserCheck message shows for each matching application in a rule.</td>
</tr>
<tr>
<td></td>
<td>• Per Data type - UserCheck message shows for each matching data type.</td>
</tr>
</tbody>
</table>

**Sample URL Filtering and Application Control Rules**

This shows some examples of URL Filtering and Application Control rules for a typical policy that monitors and controls Internet browsing. (The Hits and Install On columns are not shown.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Liability sites</td>
<td>Any</td>
<td>Internet</td>
<td>Potential liability</td>
<td>Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>High risk applications</td>
<td>Any</td>
<td>Internet</td>
<td>High Risk</td>
<td>High Risk Block Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Allow IT</td>
<td>IT</td>
<td>Any</td>
<td>Radmin</td>
<td>Allow</td>
<td>Log</td>
<td>Work-Hours</td>
</tr>
<tr>
<td>4</td>
<td>Allow Facebook for HR</td>
<td>HR</td>
<td>Internet</td>
<td>Facebook</td>
<td>Allow Download 1Gbps Down: 1 Gbps</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td>Block these categories</td>
<td>Any</td>
<td>Internet</td>
<td>Streaming Media</td>
<td>Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Social Networking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>P2P File Sharing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remote Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Log all applications</td>
<td>Any</td>
<td>Internet</td>
<td>Any Recognized</td>
<td>Allow</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remote Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **Liability sites** - Blocks traffic to sites and applications in the Potential_liability category. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.

2. **High risk applications** - Blocks traffic to sites and applications in the High Risk category and blocks the iTunes application. The UserCheck High Risk Block Message is shown to users and explains why their traffic is blocked.
3. **Allow IT department Remote Admin** - Allows the computers in the IT department network to use the Radmin application. Traffic that uses Radmin is allowed only during the Work-Hours (set to 8:00 through 18:30, for example).

4. **Allow Facebook for HR** - Allows computers in the HR network to use Facebook. The total traffic downloaded from Facebook is limited to 1 Gbps, there is no upload limit.

5. **Block these categories** - Blocks traffic to these categories: Streaming Media, Social Networking, P2P File Sharing, and Remote Administration. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.
   
   **Note** - The Remote Administration category blocks traffic that uses the Radmin application. If this rule is placed before rule 3, then this rule can also block Radmin for the IT department.

6. **Log all applications** - Logs all traffic that matches any of the URL Filtering and Application Control categories.

---

**Analyzing the Rule Base (Hit Count)**

Use the Hit Count feature to track the number of connections that each rule matches. You can show Hit Count for the rules in these options:

- The percentage of the rule hits from total hits
- The indicator level (very high, high, medium, low, or zero)

These options are configured in the Access Control Policy Rule Base and also changes how Hit Count is shown in other supported Software Blades.

When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways (from version R75.40 and up). Hit Count works independently from logging and tracks the hits even if the **Track** option is **None**.

You can use the Hit Count data to:

- Analyze a Rule Base - You can delete rules that have no matching connections

  **Note** - If you see a rule with a zero hit count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. There can be matching connections on other Security Gateways.

- Improve Firewall performance - You can move a rule that has a high hit count to a higher position in the Rule Base

- Better understand the behavior of the Access Control Policy

**Enabling or Disabling Hit Count**

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways.

After you enable or disable Hit Count you must install the Policy for the Security Gateway to start or stop collecting data.
To enable or disable Hit Count globally:
1. In SmartConsole, click **Menu > Global properties**.
2. Select **Hit Count** from the tree.
3. Select the options:
   - **Enable Hit Count** - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.
   - **Keep Hit Count data up to** - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.
4. Click **OK**.
5. Install the Policy.

To enable or disable Hit Count on each Security Gateway:
1. From the **Gateway Properties** for the Security Gateway, select **Hit Count** from the navigation tree.
2. Select **Enable Hit Count** to enable the feature or clear it to disable Hit Count.
3. Click **OK**.
4. Install the Policy.

**Configuring the Hit Count Display**
These are the options you can configure for how matched connection data is shown in the **Hits** column:
- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total hit count for:
  - Security Gateways that are not supported
  - Security Gateways that have disabled the hit count feature
The values are shown with these letter abbreviations:
  - **K** = 1,000
  - **M** = 1,000,000
  - **G** = 1,000,000,000
  - **T** = 1,000,000,000,000
  
For example, 259K represents 259 thousand connections and 2M represents 2 million connections.
- **Percentage** - Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.
- **Level** - The hit count level is a label for the range of hits according to the table.
Introducing the Access Control Policy

The hit count range = Maximum hit value - Minimum hit value [does not include zero hits]

<table>
<thead>
<tr>
<th>Hit Count Level</th>
<th>Icon</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td></td>
<td>0 hits</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td>Less than 10 percent of the hit count range</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td>Between 10 - 70 percent of the hit count range</td>
</tr>
<tr>
<td>High</td>
<td></td>
<td>Between 70 - 90 percent of the hit count range</td>
</tr>
<tr>
<td>Very High</td>
<td></td>
<td>Above 90 percent of the hit count range</td>
</tr>
</tbody>
</table>

To show the Hit Count in the Rule Base:
Right-click the heading row of the Rule Base and select **Hits**.

To configure the Hit Count in a rule:
1. Right-click the rule number of the rule.
2. Select **Hit Count** and one of these options (you can repeat this action to configure more options):
   - **Timeframe** - Select **All**, **1 day**, **7 days**, **1 month**, or **3 months**
   - **Display** - Select **Percentage**, **Value**, or **Level**

To update the Hit Count in a rule:
1. Right-click the rule number of the rule.
2. Select **Hit Count > Refresh**.

### Inspection Settings

You can configure inspection settings for the Firewall:
- Deep packet inspection settings
- Protocol parsing inspection settings
- VoIP packet inspection settings

The Security Management Server comes with two preconfigured inspection profiles for the Firewall:
- **Default Inspection**
- **Recommended Inspection**

When you configure a Security Gateway, the **Default Inspection** profile is enabled for it. You can also assign the **Recommended Inspection** profile to the Security Gateway, or to create a custom profile and assign it to the Security Gateway.

To activate the Inspection Settings, install the Access Control Policy.

**Note** - In a pre-R80 SmartConsole, Inspection Settings are configured as IPS Protections.
Configuring Inspection Settings

To configure Inspection Settings:

1. In SmartConsole, go to the Manage & Settings > Blades view.
2. In the General section, click Inspection Settings.

   The Inspection Settings window opens.

You can:

- Edit inspection settings
- Edit user-defined Inspection Settings profiles. You cannot change the Default Inspection profile and the Recommended Inspection profile.
- Assign Inspection Settings profiles to Security Gateways
- Configure exceptions to settings

To edit a setting:

1. In the Inspection Settings > General view, select a setting.
2. Click Edit.
3. In the window that opens, select a profile, and click Edit.

   The settings window opens.
4. Select the Main Action:
   - Default Action - preconfigured action
   - Override with Action - from the drop-down menu, select an action with which to override the default - Accept, Drop, Inactive (the setting is not activated)
5. Configure the Logging Settings
   Select Capture Packets, if you want to be able to examine packets that were blocked in Drop rules.
6. Click OK.
7. Click Close.

To view settings for a certain profile:

1. In the Inspection Settings > General view, click View > Show Profiles.
2. In the window that opens, select Specific Inspection settings profiles.
3. Select profiles.
4. Click OK.

   Only settings for the selected profiles are shown.

You can add, edit, clone, or delete custom Inspection Settings profiles.

To edit a custom Inspection Settings profile:

1. In the Inspection Settings > Profiles view, select a profile.
2. Click Delete, to remove it, or click Edit to change the profile name, associated color, or tag.
3. If you edited the profile attributes, click OK to save the changes.
To clone an Inspection Settings profile:
1. In the Inspection Settings > Profiles view, select the profile, and click Clone.
2. In the New Profile window that opens, edit the profile attributes:
3. Click OK.

To add a new Inspection Settings profile:
1. In the Profiles view, click New.
2. In the New Profile window that opens, edit the profile attributes:
3. Click OK.

To assign an Inspection Settings profile to a Security Gateway:
1. In the Inspection Settings > Gateways view, select a gateway, and click Edit.
2. In the window that opens, select an Inspection Settings profile.
3. Click OK.

To configure exceptions to inspection settings:
1. In the Inspection Settings > Exceptions view, click New to add a new exception, or select an exception and click Edit to modify an existing one. The Exception Rule window opens.
2. Configure the exception settings:
   • Apply To - select the Profile to which to apply the exception
   • Protection - select the setting
   • Source - select the source Network Object, or select IP Address and enter a source IP address
   • Destination - select the destination Service Object, or select Port/Range, TCP or UDP, and enter a destination port number or a range of port numbers
   • Install On - select a gateway on which to install the exception
3. Click OK.

To enforce the changes, install the Access Control Policy.
Creating a Threat Prevention Policy

In This Section:

Threat Prevention Components ................................................................................... 75
ThreatSpect Engine and ThreatCloud Repository ...................................................... 76
Learning about Malware .............................................................................................. 76
IPS ................................................................................................................................. 76
Anti-Bot ......................................................................................................................... 81
Anti-Virus ...................................................................................................................... 82
Anti-Bot and Anti-Virus Rule Base .............................................................................. 83
Threat Emulation .......................................................................................................... 85
Creating a Threat Prevention Policy ............................................................................ 87
Creating Rules .............................................................................................................. 91
Installing the Threat Prevention Policy ....................................................................... 95
Updating the IPS and Malware Databases .................................................................. 96
Anti-Spam ..................................................................................................................... 97

Threat Prevention Components

To challenge today’s malware landscape, Check Point’s comprehensive Threat Prevention solution offers a multi-layered, pre- and post-infection defense approach and a consolidated platform that enables enterprise security to detect and block modern malware. These Threat Prevention Software Blades are available:

- **IPS** - A complete IPS network security solution, for comprehensive protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities.

- **Anti-Bot** - Post-infection detection of bots on hosts. Prevents bot damages by blocking bot C&C (Command and Control) communications. The Anti-Bot Software Blade is continuously updated from ThreatCloud, a collaborative network to fight cybercrime. Anti-Bot discovers infections by correlating multiple detection methods.

- **Anti-Virus** - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus Software Blade is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.

- **Threat Emulation** - Protection against infections from undiscovered exploits, zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The ThreatCloud Emulation service reports to the ThreatCloud and automatically shares the newly identified threat information with other Check Point customers.

Each Software Blade gives unique network protections. When combined, they supply a strong Threat Prevention solution. Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the Anti-Virus database.
ThreatSpect Engine and ThreatCloud Repository

The ThreatSpect engine is a unique multi-tiered engine that analyzes network traffic and correlates information across multiple layers to find bots and other malware. It combines information on remote operators, unique botnet traffic patterns and behavior to identify thousands of different botnet families and outbreak types.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Security Gateway gets automatic binary signature and reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified IP/URL/DNS resources that it finds.

The layers of the ThreatSpect engine:

- **Reputation** - Analyzes the reputation of URLs, IP addresses and external domains that computers in the organization access. The engine searches for known or suspicious activity, such as a C&C.
- **Signatures** - Detects threats by identifying unique patterns in files or in the network.
- **Suspicious Mail Outbreaks** - Detects infected machines in the organization based on analysis of outgoing mail traffic.
- **Behavioral Patterns** - Detects unique patterns that indicate the presence of a bot. For example, how a C&C communicates with a bot-infected machine.

Learning about Malware

The Threat Wiki is an easy-to-use tool that lets you search and filter the ThreatCloud repository to find more information about identified malware. You can filter by category, tag, malware family, and search for malware.

To show the Threat Wiki:

1. In SmartConsole, go to the Security Policies page, and select Threat Prevention.
2. In the Threat Tools section, click Threat Wiki.

   The Threat Wiki web page opens.

IPS

Overview of IPS

The Check Point IPS Software Blade analyzes traffic for possible risks, to enhance the network security of your organization. The IPS detection engine has multiple defense layers, detects and prevents against known threats, and often protects against future ones.

For example IPS protects against drive-by downloads, where a user can go to a legitimate web site and unknowingly download malware. The malware can exploit a browser vulnerability that lets it create a special HTTP response that sends the malware to the client. The firewall allows the HTTP traffic from the web site and the computer is at risk for this malware. IPS protects the computer, because it identifies and then blocks the drive-by download connection.
Enabling the IPS Software Blade

To enable the IPS Software Blade on a Security Gateway:
1. In SmartConsole, go to Gateways & Servers and double-click the gateway object. The General Properties window opens.
2. In the General Properties > Network Security tab, select IPS.
3. Follow the steps in the wizard that opens.
4. Click OK.
5. Click OK.
6. Install the Access Control policy.

Choosing the Level of Protection

Check Point IPS provides instant protection based on pre-defined Threat Prevention Profiles. You can also configure a custom Threat Prevention profile (see “Threat Prevention Profiles” on page 90) to give the exact level of protection for your organization.

When you install an Access Control policy on the Security Gateways, they immediately begin to enforce IPS protection on network traffic.

Default IPS Protection Profiles

SmartConsole includes these default Threat Prevention profiles:
- **Optimized** - Provides excellent protection for common network products and protocols against recent or popular attacks
- **Strict** - Provides a wide coverage for all products and protocols, with impact on network performance
- **Basic** - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

Using the Optimized Profile

The Optimized profile is activated by default, because it gives excellent security with good gateway performance. These are the goals of the Optimized profile:
- Apply settings to all the Threat Prevention Software Blades
- Avoid impact on the gateway performance
- Protect against important threats
- Reduce false-positives

Newly downloaded IPS protections are set to Detect the intrusion attempts. They are activated according to the IPS Updates Policy.

Customizing IPS Protections for Your Network

For additional granularity, in the Additional Activation section of the Profile configuration window, you can select IPS protections to activate and to deactivate. The IPS protections are arranged into categories such as Product, Vendor, Threat Year, and others, for the ease of search. The
gateways enforce activated protections, and do not enforce deactivated protections, regardless of the general profile protection settings.

**Configuring IPS Profile Settings**

To configure the IPS settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**. The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **IPS > Additional Activation**.
5. Configure the customized protections for the profile. See Additional Activation Fields (on page 78).
6. From the navigation tree, click **IPS > Updates**.
7. Configure the settings for newly downloaded IPS protections.
8. If you are importing IPS profiles from a pre-R80 deployment:
   a) From the navigation tree, click **IPS > Pre-R80 Settings**.
   b) Activate the applicable **Client** and **Server** protections.
   c) Configure the IPS protection categories to exclude from this profile.

   **Note** - These categories are different from the protections in the **Additional Activation** page.
9. Click **OK**.
10. Install the Access Control policy.

**Additional Activation Fields**

- **Activate IPS protections according to the following additional properties** - When selected, the categories configured on this page modify the profile’s IPS protections.
  - **Protections to activate** - The IPS protection categories in this section are enabled on the Security Gateways that use this Threat Prevention profile.
  - **Protections to deactivate** - The IPS protection categories in this section are NOT enabled on the Security Gateways that use this Threat Prevention profile.

These categories will only filter out or add protections that comply with the activation mode thresholds (Confidence, Severity, Performance).

For example, if a protection is inactive because of its Performance rating, it will not be enabled even if its category is in **Protections to activate**.
Creating a Threat Prevention Policy

Changing the Assigned Profile

To assign an IPS profile:
1. In SmartConsole, select Security Policies > Threat Prevention > Policy > IPS.
2. In the rule, right-click the Action cell.
3. Select the Threat Prevention profile with the applicable IPS settings.
4. Install the Access Control policy.

Browsing IPS Protections

The IPS Protections summary lets you quickly browse all IPS protections and their settings. The IPS Protections window lets you use the specified categories and tags to easily filter for IPS protections. For example, the Vendor category contains the Oracle tag with the IPS protections for Oracle products. You can also:

- Find IPS protections using the Filters:
  - Default filters: Activations, Severity, Confidence Level, Performance Impact, and Type
  - Predefined filters: Click the Add filter button
- Change the Action for selected profiles (overrides the profile setting) ("Activating Protections for a Profile" on page 80)

Filtering IPS Protections

To show the IPS protections:
1. In SmartConsole, go to the Security Policies page and select Threat Prevention.
2. In the Threat Tools section, click IPS Protections.

To filter the protections:
1. From the IPS Protections window, click the Filter icon.
   The Filters pane opens and shows IPS protections categories.
2. To add more categories:
   a) Click the Add filter button.
      A window opens and shows the IPS protections categories.
   b) Click the category.
      The category is added to the Filters pane.
3. Click one or more filters to apply to the IPS protections.
4. To show all suggested filters in a category, click View All.
**IPS Protections Columns**

These are some of the default columns in the IPS protections summary table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection.</td>
</tr>
<tr>
<td>Industry Reference</td>
<td>International CVE or CVE candidate name for attack.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>How this protection affects the performance of a Security Gateway.</td>
</tr>
<tr>
<td>Severity</td>
<td>Probable severity of a successful attack on your environment.</td>
</tr>
<tr>
<td>Confidence Level</td>
<td>How confident IPS is in recognizing the attack.</td>
</tr>
<tr>
<td>profile_name</td>
<td>The Activation setting for the protection for each IPS profile.</td>
</tr>
</tbody>
</table>

**Activating Protections for a Profile**

To manually activate a protection for a profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **IPS Protections**.
   - The **IPS Protections** page opens.
3. For the specified protection, find the column for the profile.
   - **Note** - Only the IPS profiles selected in the policy are shown by default.
4. Right-click the cell for the protection and profile and select **Edit**.
   - The **Protection Details** window opens.
5. From the **Main Action** section, click **Override with**.
6. Select the action to apply.
7. Click **OK**.
8. Install the Access Control policy.

**Removing Activation Overrides**

You can remove the manually activated IPS protections and restore them to the settings in the Threat Prevention profile.

To remove IPS protection overrides:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **IPS Protections**.
   - The **IPS Protections** page opens.
3. Click the cell for the profile column.
   - Press CTRL to select more than one protection.
4. Right-click a highlighted cell and select **Restore to profile settings**.
   - A warning message opens.
5. Click **Yes**.
6. Install the Access Control policy.
Adding Network Exceptions

You can configure exceptions for a protection with the **Prevent** action. IPS does not identify the traffic. We recommend that you use IPS exceptions to allow traffic that is legitimate for some computers or services can match the protection criteria for malware. You can also create an exception for a server that does not comply with RFC standards.

**Adding an IPS Exception**

To add a new exception:

1. In SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In the **Threat Tools** section of the Threat Prevention Policy, click **Profiles**.
3. Right-click the profile and select **Edit**. The **Profile** window opens.
4. From the navigation tree, select **IPS > Pre R80 Settings**.
5. In the **Excluded Protections Categories** section, make sure that **Do not activate protections of the following categories** is selected.
6. Click the plus sign and select a protection category.
7. Repeat the previous step for each protection category.
8. Click **OK**.
9. Install the Access Control policy.

Anti-Bot

**Protecting Networks from Bots**

A bot is malicious software that can infect your computer. It is possible to infect a computer when you open attachments that exploit a vulnerability, or go to a web site that results in a malicious download.

When a bot infects a computer, it:

- Takes control of the computer and neutralizes its Anti-Virus defenses. It is not easy to find bots on your computer, they hide and change how they look to Anti-Virus software.
- Connects to a C&C [Command and Control center] for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to do illegal activities without your knowledge. Your computer can do one or more of these activities:
  - Steal data (personal, financial, intellectual property, organizational)
  - Send spam
  - Attack resources [Denial of Service Attacks]
  - Consume network bandwidth and reduce productivity

One bot can often create multiple threats. Bots are frequently used as part of **Advanced Persistent Threats** (APTs) where cyber criminals try to damage individuals or organizations.

The Anti-Bot Software Blade detects and prevents these bot and botnet threats. A botnet is a collection of compromised and infected computers.
Identifying Bot Infected Computers

The Anti-Bot Software Blade uses these procedures to identify bot infected computers:

- **Identify the C&C addresses used by criminals to control bots**
  These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

- **Identify the communication patterns used by each botnet family**
  These communication fingerprints are different for each family and can be used to identify a botnet family. Research is done for each botnet family to identify the unique language that it uses. There are thousands of existing different botnet families and new ones are constantly emerging.

- **Identify bot behavior**
  Identify specified actions for a bot such as, when the computer sends spam or participates in DoS attacks.

Enabling the Anti-Bot Software Blade

To enable the Anti-Bot Software Blade on a Security Gateway:

1. In the *Gateways & Servers* view, double-click the gateway object. The *General Properties* window of the gateway opens.
2. From the *Network Security* tab, select *Anti-Bot*. The *Anti-Bot and Anti-Virus First Time Activation* window opens.
3. Select an activation mode option:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Bot Software Blade and use the Anti-Bot settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click *OK*.
5. Install Policy ["Installing the Threat Prevention Policy" on page 95].

Anti-Virus

Protecting Networks from Viruses

The Anti-Virus Software Blade inspects connections to the Internet and scans file transfers and downloads to the internal network to find and prevent malware attacks. It also gives pre-infection protection from external malware and malicious servers.

Examining Anti-Bot and Anti-Virus Protections

The *Protections* browser shows information about the Anti-Bot and Anti-Virus protections.
To show the Protections browser:
1. In SmartConsole, go to the Security Policies page, and select Threat Prevention.
2. In the Related Tools section, click Protections.
   A detailed summary of the protections is shown in the table.

The table of protections has these fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection type.</td>
</tr>
<tr>
<td>Blade</td>
<td>The Software Blade, by which the protection is used - Anti-Bot or Anti-Virus.</td>
</tr>
<tr>
<td>Engine</td>
<td>Layer of the ThreatSpect engine that is protecting the network.</td>
</tr>
<tr>
<td>Known Today</td>
<td>Number of known protections.</td>
</tr>
<tr>
<td>Last Update</td>
<td>The date when the most recent update.</td>
</tr>
</tbody>
</table>

When you select a protection in the table, the summary and the activation information are shown in the bottom part of the screen. The Summary tab is shown by default. To see the activation information, click the Activations tab.

The table in the Activations tab view shows information in the table with these fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>The profile name.</td>
</tr>
<tr>
<td>Action</td>
<td>The action that is configured in the profile for the selected protection:</td>
</tr>
<tr>
<td></td>
<td>• Ask - Asks user to select an action</td>
</tr>
<tr>
<td></td>
<td>• Prevent - Blocks traffic that matches the protection</td>
</tr>
<tr>
<td></td>
<td>• Detect - Allows all traffic and logs traffic that matches the protection</td>
</tr>
<tr>
<td></td>
<td>• Inactive - Disables the protection</td>
</tr>
</tbody>
</table>

Proofs can have more than one action. The Action column shows the percentage of protections set to each action.

Anti-Bot and Anti-Virus Rule Base

There is one Rule Base for Anti-Bot and Anti-Virus. The Anti-Bot and Anti-Virus rules use the Malware database and network objects. Security Gateways that have Identity Awareness enabled can also use Access Role objects as the Protected Scope in a rule. The Access Role objects let you easily make rules for individuals or different groups of users.

The first Anti-Bot or Anti-Virus rule that matches the traffic is applied. There are no implied rules in this Rule Base, all traffic is allowed unless it is explicitly blocked. A rule that is set to the Prevent action, blocks activity and communication for that malware.
When necessary, you can add an exception directly to a rule. The object in the **Protected Scope**, can have a different **Action** from the specified Anti-Bot and Anti-Virus rule. Here are some examples of exception rules:

- A profile that only detects protections. You can set one or more of the protections for a user to **Prevent**.
- The Research and Development (R&D) network is included in a profile with the **Prevent** action. You can set that network to **Detect**.

### Managing the Anti-Bot and Anti-Virus Rule Base

These are the fields that manage the rules for the Anti-Bot and Anti-Virus threat prevention policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Rule Base. An exception rule contains the letter E and a digit that represents the exception number. For example, E-2.2 is the second exception for the second rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Protected Scope</td>
<td>Objects that are protected against bots and viruses. Traffic to and from these objects is inspected even if the objects did not open the connection.</td>
</tr>
</tbody>
</table>
| Protection  | For rules, the value for this field is always N/A. The protections are set according the profile in the **Action** field.  
For exceptions, set this field to one or more specified protections. |
| Action      | For rules, the value for this field is an Anti-Bot and Anti-Virus profile.  
For exceptions, set this field to **Prevent** or **Detect**. |
| Track       | Tracking and logging action that is done when traffic matches the rule.     |
| Install On  | Network objects that get this rule. The default setting is **All** and installs the policy on all Security Gateways that have Anti-Bot and Anti-Virus enabled. |

### Sample Anti-Bot and Anti-Virus Rule Base

This table shows a sample Anti-Bot and Anti-Virus Rule Base. (The **Install On** column is not shown and is set to **All**.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
</table>
| 1   | High Security | Finance_server  
Corporate_internal  
Corporate_finance | - n/a                  | High_Security_Profile | Log Packet Capture    |
| 2   | Malware Rule | Any                              | - n/a                  | Optimized Profile     | Log                    |
| E-2.1 | R&D Server | Server_1                        | Backdoor.Win32.Shark.A | Detect               | Log                    |
| E-2.2 | Users_3     | Users_3                          | Adware.Win32.CashFiesta.A 
RogueSoftware.Win32. 
Ackantta.A 
Trojan.Win32.Agent.BA | Detect               | Log                    |
Rule number 1, **High Security** - Traffic for the Finance server and two corporate networks are inspected for bots and viruses according to the settings in the **High_Security** profile. The traffic is logged and the packets are captured for analysis in the **Logs & Monitor > Logs** view.

Rule number 2, **Malware Rule** - All traffic in the network is inspected for bots and viruses according to the settings in the **Optimized** profile.

Exception 2.1 to rule 2, **R&D Server** - A global exception rule for the **Server_1** object, that only detects the **Backdoor.Win32.Shark.A** protection.

Exception 2.2 to rule 2, **Users_3** - An exception rule for the **Users_3** Access Role, that sets some protections to Detect instead of Prevent.

### Threat Emulation

#### The Need for Threat Emulation

Cyber-threats continue to multiply and now it is easier than ever for criminals to create new malware that can easily bypass existing protections. On a daily basis, these criminals can change the malware signature and make it virtually impossible for signature based products to protect networks against infection. Threat Emulation can protect your network against new malware, zero-day vulnerabilities and targeted attacks [http://www.checkpoint.com/products/threat-emulation/index.html](http://www.checkpoint.com/products/threat-emulation/index.html).

Threat Emulation gives networks the necessary protection against unknown threats in files that are downloaded from the Internet or attached to emails. When emulation is done on a file:

- The file is opened on more than one virtual computer with different operating system environments
- The virtual computers are closely monitored for unusual and malicious behavior, such as an attempt to change registry keys or run an unauthorized process
- Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network
- The cryptographic hash of a new malicious file is saved to a database and the internal network is protected from that malware
- Information about malicious files and malware is shared with Check Point ThreatCloud and helps to protect all ThreatCloud users

#### ThreatCloud Emulation

You can securely send files to the Check Point ThreatCloud for emulation. The ThreatCloud is always up-to-date with the latest Threat Emulation releases.

**Sample ThreatCloud Emulation Workflow**

1. The Security Gateway gets a file from the Internet or an external network.
2. The Security Gateway compares the cryptographic hash of the file with the database.
   - If the file is already in the database, no additional emulation is necessary
   - If the file is not in the database, it is necessary to run full emulation on the file
3. The file is sent over an SSL connection to the ThreatCloud.
4. The virtual computers in the ThreatCloud run emulation on the file.
5. The emulation results are sent securely to the Security Gateway for the applicable action.

Sample ThreatCloud Deployment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet and external networks</td>
</tr>
<tr>
<td>2</td>
<td>Perimeter Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Computers and servers in the internal network</td>
</tr>
<tr>
<td>4</td>
<td>Check Point ThreatCloud servers</td>
</tr>
</tbody>
</table>

Using Cloud Emulation

Files are sent to the Check Point ThreatCloud over a secure SSL connection for emulation. The emulation in the ThreatCloud is identical to emulation in the internal network, but it uses only a small amount of CPU, RAM, and disk space of the Security Gateway. The ThreatCloud is always up-to-date with all available operating system environments.

**Best Practice** - For ThreatCloud emulation, it is necessary that the Security Gateway connects to the Internet. Make sure that the DNS and proxy settings are configured correctly in **Global Properties**.

To enable ThreatCloud emulation:

1. In the **Gateways & Servers** view, double-click the Security Gateway object.
   - The **Gateway Properties** window opens.
2. From the **Network Security** tab, select **Threat Emulation**.
   - The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.
3. Select **ThreatCloud Emulation Service**.
4. Click **Next**.
   - The **Summary** page opens.
5. Click **Finish** to enable Threat Emulation and close the First Time Configuration Wizard.
Creating a Threat Prevention Policy

The Threat Prevention profile applies to these Software Blades:

- IPS - There is a dedicated layer for the IPS Rule Base for pre-R80 gateways. After you make changes to IPS, install the Access Control policy.

- Anti-Bot, Anti-Virus, Threat Emulation - These Software Blades are configured in the Threat Prevention Rule Base and policy. After you make changes to one of them, install the Threat Prevention policy.

**Note** - If you make changes to IPS and one of the other Threat Prevention Software Blades, you must install both the Access Control and Threat Prevention policy.

Overview of Creating a Threat Prevention Policy

After you enable the IPS and Threat Prevention Software Blades on the Security Gateways, configure the Threat Prevention policy.

This is the high-level workflow create and deploy a Threat Prevention policy:

1. Update the IPS database and Malware database with the latest protections.
2. Configure an IPS and Threat Prevention Rule Base with the Threat Prevention profile as the Action of the rule.
3. Install the Access Control and Threat Prevention policy.

Optimized Protection Profile Settings

Check Point defined the **Optimized** profile to give excellent security with good performance for the gateway.

These are the goals of the Optimized profile, and the settings that achieve those goals:

<table>
<thead>
<tr>
<th>Goal</th>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply settings to the IPS and Threat Prevention Software Blades</td>
<td>Blades Activation</td>
<td>Activate the profile for IPS, Anti-Bot, Anti-Virus, and Threat Emulation.</td>
</tr>
<tr>
<td>Do not have a critical effect on performance</td>
<td>Performance impact</td>
<td>Activate protections that have a Medium or lower effect on performance.</td>
</tr>
<tr>
<td>Protect against important threats</td>
<td>Severity</td>
<td>Protect against threats with a severity of Medium or above.</td>
</tr>
<tr>
<td>Reduces false-positives</td>
<td>Confidence</td>
<td>Set to Prevent the protections with an attack confidence of Medium or High. Set to Detect the protections with a confidence of Low.</td>
</tr>
</tbody>
</table>
Newly downloaded IPS protections are set to **Detect**. They are activated according to the **IPS Newly Updated Protections**.

**To get quickly up and running with a Threat Prevention policy:**
To get quickly up and running with IPS without making changes to the IPS profile, install this Threat Prevention Rule Base with the **Optimized** profile:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat</td>
<td>Any</td>
<td>Optimized</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Prevention policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPS and Threat Prevention Policy Use Cases**
This section shows some sample IPS and Threat Prevention policies for different scenarios.

**Getting up and Running with IPS and Threat Prevention**

*Scenario: I want to quickly protect my organization against intrusions*

**IPS Policy**

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box IPS policy</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Optimized profile with these</td>
<td>One or more Security Gateways with IPS enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>settings:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Activated for Threat</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Prevention Software Blades:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• <strong>Performance impact:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium or lower</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• <strong>Severity:</strong> Medium or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>above</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• <strong>Confidence</strong> (Low\Medium\High):</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Detect\Prevent\Prevent</td>
<td></td>
</tr>
</tbody>
</table>

**Note** - Install the Access Control and Threat Prevention policies.
### Threat Prevention Policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
</table>
| Out-of-the-box Threat Prevention policy | Any | Optimized profile with these settings:  
- Activated for Threat Prevention Software Blades: All  
- **Performance impact**: Medium or lower  
- **Severity**: Medium or above  
- **Confidence** (Low\Medium\High): Detect\Prevent\Prevent | Log Packet Capture | Policy Targets |

This scenario used the Optimized Threat Prevention profile ("Optimized Protection Profile Settings" on page 87).

Note - The Protection/Site column is used only for protection exceptions ("Disabling a Protection on a Specified Server" on page 94).

### Monitoring bot activity without blocking traffic

*Scenario: I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?*

Add this rule above the Out-of-the-box Threat Prevention policy to monitor bot activity ("Monitoring Bot Activity" on page 93):

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
</table>
| Monitor bot activity | Any | A profile, with these changes relative to the Recommended_Profile:  
**Confidence** (Low\Medium\High): Prevent\Prevent\Prevent | Log Packet Capture | Policy Targets |

### Blocking bots

*Scenario: I want to block bots in my organization. How can I do this?*

You can block bots ("Blocking Bots" on page 92) using the out-of-the-box Threat Prevention policy rule, with the Optimized profile:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat Prevention policy</td>
<td>Any</td>
<td>Optimized profile</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
Blocking viruses and malware

Scenario: I want to block viruses and malware in my organization. How can I do this?

You can block viruses ("Blocking Viruses" on page 95) using the out-of-the-box Threat Prevention policy rule, with the Optimized profile:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat Prevention policy</td>
<td>Any</td>
<td>Optimized profile</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

Disabling some protections for one server

Scenario: The protection Backdoor.Win32.Agent.AH detects malware on a server [Server_1]. How can I disable this protection for this server only?

Add an exception to the specified Anti-Bot rule. This policy monitors bots activity in the organization without blocking traffic, but disables the Backdoor.Win32.Agent.AH protection on Server_1 ("Disabling a Protection on a Specified Server" on page 94).

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Bot</td>
<td>Any</td>
<td>- N/A</td>
<td>A profile based on the Optimized profile, with these changes: Confidence (Low\Medium\High): Prevent\Prevent\Prevent</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Exclude Server_1</td>
<td>Server_1</td>
<td>Backdoor.Win32.Agent.AH</td>
<td>Detect</td>
<td>Log</td>
<td>Server_1</td>
</tr>
</tbody>
</table>

Threat Prevention Profiles

A Threat Prevention profile determines which protections are activated, and which Software Blades are enabled for the specified rule or policy. The protections that the profile activates depend on the:

- Performance impact of the protection.
- Severity of the threat.
- Confidence that a protection can correctly identify an attack.
- Settings that are specific to the Software Blade.

A Threat Prevention profile applies to one or more of these Software Blades: IPS, Anti-Bot, Anti-Virus, and Threat Emulation.
Creating a Threat Prevention Policy

Editing Profiles

You can change the settings of the IPS and Threat Prevention profile according to your requirements.

To edit a profile:

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile and select Edit.

Creating Rules

The Threat Prevention policy determines how the system inspects connections for bots and viruses. The primary component of the policy is the Rule Base. The rules use the Malware database and network objects.

If you enable Identity Awareness on your gateways, you can also use Access Role objects as the scope in a rule. This lets you easily make rules for individuals or different groups of users.

There are no implied rules in the Rule Base. All traffic is allowed unless it is explicitly blocked.

Predefined Rule

When you enable the IPS or one of the Threat Prevention Software Blades, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope value equals any) is inspected for all protections according to the recommended profile. By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

   Note - You cannot edit the settings of the predefined rule for the IPS Security Gateway.

The result of this rule (according to the Optimized profile) is that:

- All protections that can identify an attack with a high or medium confidence level and have a medium or lower performance impact are set to Prevent mode.
- All protections that can identify an attack with a low confidence level and have a medium or lower performance impact are set to Detect mode.

Use the Logs & Monitor page to show logs related to IPS and Threat Prevention traffic. Use the data there to better understand the use of these Software Blades in your environment and create an effective Rule Base. You can also directly update the Rule Base from this page.

You can add more exceptions that prevent or detect specified protections or have different tracking settings.
Creating Anti-Bot Rules

Here are examples of how to create different types of Anti-Bot rules.

Creating an Anti-Bot Policy

Create and manage the policy for the Anti-Bot Software Blade as part of the Threat Prevention Policy ("Creating Rules" on page 91).

- The Threat Prevention page shows the rules and exceptions for the Anti-Bot policy. The rules specify the Threat profiles set for network objects or locations defined as a protected scope. Click the Add Rule button to get started.
- To learn about bots and protections, look through the Threat Wiki.

Blocking Bots

Scenario: I want to block bots in my organization. How can I do this?

In this example you will install this default Threat Policy rule that uses the recommended policy, or create a new rule.

<table>
<thead>
<tr>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Optimized</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet Capture</td>
<td></td>
</tr>
</tbody>
</table>

To block bots in your organization:

1. In SmartConsole, click Gateways & Servers.
2. Enable the Anti-Bot Software Blade on the Gateways that protect your organization. For each Gateway:
   a) Double-click the Gateway object.
   b) In the Gateway Properties page, select the Anti-Bot Software Blade.
      The First Time Activation window opens.
   c) Select According to the Anti-Bot and Anti-Virus policy
   d) Click OK.
   You can block bots using the out-of-the-box Threat Prevention policy rule, with the default Optimized Profile and the previous rule.
   Alternatively, add a new Threat Prevention rule:
   a) Click Add Rule.
      A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
   b) Make a rule that includes these components:
      - **Name** - Give the rule a name such as Block Bot Activity.
      - **Protected Scope** - The list of network objects you want to protect. By default, the Any network object is used.
Creating a Threat Prevention Policy

- **Action** - The Profile that contains the protection settings you want. The default profile is **Optimized**.
- **Track** - The type of log you want to get when detecting malware on this scope.
- **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.

4. Install the Threat Prevention policy (see “Installing the Threat Prevention Policy” on page 95).

**Monitoring Bot Activity**

*Scenario: I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?*

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor bot activity</td>
<td>Any</td>
<td>A profile that has these changes relative to the <strong>Optimized</strong> profile: Confidence {High\Medium\Low}: Detect\Detect\Detect</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

To monitor all bot activity:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. Create a new profile:
   a) From the **Threat Tools** section, click **Profiles**.
      The **Profiles** page opens.
   b) Right-click a profile and select **Clone**.
   c) Give the profile a name such as **Monitoring_Profile**.
   d) Edit the profile, and under **Activation Mode**, configure all confidence level settings to **Detect**.
   e) Select the **Performance Impact** - for example, **Medium or lower**.
      This profile detects protections that are identified as an attack with low, medium or high confidence and have a medium or lower performance impact.
3. Create a new rule:
   a) Click **Threat Prevention > Policy > Threat Prevention**.
   b) Add a rule to the Rule Base.
      The first rule that matches is applied.
   c) Make a rule that includes these components:
      - **Name** - Give the rule a name such as **Monitor Bot Activity**.
      - **Protected Scope** - Keep **Any** so the rule applies to all traffic in the organization.
      - **Action** - Right-click in this cell and select **Monitoring_Profile**.
      - **Track** - Keep **Log**.
      - **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.
4. Install the Threat Prevention policy (see “Installing the Threat Prevention Policy” on page 95).
Disabling a Protection on a Specified Server

**Scenario:** The protection Backdoor.Win32.Agent.AH detects malware on a server [Server_1]. How can I disable this protection for this server only?

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection/Site</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Bot Activity</td>
<td>Any</td>
<td>- N/A</td>
<td>Optimized Profile</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Exclude</td>
<td>Server_1</td>
<td>Backdoor.Win32.Agent.AH</td>
<td>Detect</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

To add an exception to a rule:

1. In SmartConsole, click **Access Control > Threat Prevention > Policy > Threat Prevention**.
2. Click the rule that contains the scope of Server_1.
3. Click the **Add Exception** toolbar button to add the exception under the rule. The first exception matched is applied.
4. Right-click the rule and select **New Exception**.
5. Configure these settings:
   - **Name** - Give the exception a name such as **Exclude**.
   - **Protected Scope** - Change it to **Server_1** so that it applies to all detections on the server.
   - **Protection/Site** - Click + in the cell. From the drop-down menu, click the category and select one or more of the items to exclude.
     - **Note** - To add EICAR files as exceptions, you must add them as Whitelist Files. Adding EICAR files through Exceptions in Policy rules will still get them blocked.
   - **Action** - Keep it as **Detect**.
   - **Track** - Keep it as **Log**.
   - **Install On** - Keep it as **Policy Targets** or choose specified gateways to install the rule on.
6. Install the Threat Prevention policy.

Creating Anti-Virus Rules

Here are examples of how to create different types of Anti-Virus rules.

You can also use Anti-Virus rules to disable a specified malware protection ("Disabling a Protection on a Specified Server" on page 94).

Creating an Anti-Virus Policy

Create and manage the policy for the Anti-Virus Software Blade as part of the Threat Prevention Policy.

- The **Threat Prevention** page shows the rules and exceptions for the Anti-Virus policy. The rules specify the Threat profiles set for network objects or locations defined as a protected scope.
  Add a new rule to the Threat Prevention policy.
• You can configure the Anti-Virus settings in the Threat Prevention profile for the specified rule.
• To learn about bots and protections, look through the Threat Wiki.

Blocking Viruses

To block viruses and malware in your organization:

1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway.
2. In the General Properties page, select the Anti-Virus Software Blade.
   The First Time Activation window opens.
3. Select According to the Anti-Bot and Anti-Virus policy and click OK.
4. Close the gateway Properties window and publish the changes.
6. Click Add Rule.
   A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule
   that matches the traffic.
7. Make a rule that includes these components:
   • Name - Give the rule a name such as Block Virus Activity.
   • Protected Scope - The list of network objects you want to protect. In this example, the Any
     network object is used.
   • Action - The Profile that contains the protection settings you want. The default profile is
     Optimized.
   • Track - The type of log you want to get when detecting malware on this scope. In this
     example, keep Log and also select Packet Capture to capture the packets of malicious
     activity. You will then be able to view the actual packets in SmartConsole > Logs & Monitor
     > Logs.
   • Install On - Keep it as All or choose specified gateways to install the rule on.
8. Install the Threat Prevention policy.

Installing the Threat Prevention Policy

The Anti-Bot, Anti-Virus and Threat Emulation Software Blades have a dedicated Threat
Prevention policy. You can install this policy separately from the policy installation of the Access
Control Software Blades. Install only the Threat Prevention policy to minimize the performance
impact on the Security Gateways.

Settings for the IPS Software Blade are installed with the Access Control policy.

You can update the IPS, Anti-Bot, Anti-Virus and Threat Emulation Rule Base to give immediate
coverage for new malware threats.

To install the Threat Prevention and Access Control policies:

1. From the Global toolbar, click Install Policy.
   The Install Policy window opens showing the installation targets (Security Gateways).
3. Expand the Install Mode options, and click the applicable settings:
   - **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.
     
     If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.

4. Click **OK**.

---

**Updating the IPS and Malware Databases**

The IPS protection database and the Malware database automatically download updates at regular intervals. This ensures that you have the latest IPS protections, and the most current data and newly added signatures and URL reputations in your Anti-Bot and Anti-Virus policy.

The Malware database only updates if you have a valid Anti-Bot, Threat Emulation and/or Anti-Virus contract.

By default, updates for Anti-Virus and Anti-Bot run on the Security Gateway every two hours. For IPS and Threat Emulation you must configure an update schedule. You can change the update schedule or choose to manually update the Security Gateway. The updates are stored in a few files on each Security Gateway.

---

**Updating IPS Proctions**

Check Point constantly develops and improves its protections against the latest threats. You can manually update the database with latest IPS protections.

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

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

To manually update the IPS protections:

1. In SmartConsole, click **Security Policies > Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the **IPS** section, click **Update Now**.
4. Install the Access Control policy.

To revert to an earlier protection package:

1. In the **IPS** section of the Threat Prevention **Updates** page, click **Switch to version**.
2. In the window that opens, select an **IPS Package Version**, and click **OK**.
3. Install the Access Control policy.
Scheduling Updates

You can change the default automatic schedule for when updates are automatically downloaded and installed. If you have Security Gateways in different time zones, they are not synchronized when one updates and the other did not yet update.

To configure Threat Prevention scheduled updates:

1. In SmartConsole, go to the Security Policies page and select Threat Prevention.
2. In the Threat Tools section of the Threat Prevention Policy, click Updates.
3. In the section for the applicable Software Blade, click Schedule Update.
   The Scheduled Update window opens.
4. Make sure Enable <feature> scheduled update is selected.
5. Click Configure.
6. In the window that opens, set the Update at time and the frequency:
   - Daily - Every day
   - Days in week - Select days of the week
   - Days in month - Select dates of the month
7. Click OK.
8. Click Close.
9. Install the policy for the applicable Software Blade:
   - IPS updates, install the Access Control policy (for Pre-R80 gateways)
   - Anti-Bot, Anti-Virus, and Threat Emulation updates, and R80.x IPS gateways, install the Threat Prevention policy

Anti-Spam

Employees waste more and more time to sort through bulk emails commonly known as spam. The amount of resources (disk space, network bandwidth, CPU) devoted to handling spam also increases from year to year. In addition, unwanted emails continue to grow and can be an unexpected security threat to networks. Cyber-criminals can use emails to let viruses and malware into your network. The Anti-Spam and Mail Software Blade gives system administrators an easy and central tool to eliminate most of the spam that reaches their networks.

Enabling Anti-Spam

Use the Overview page in the Anti-Spam & Mail tab of the SmartDashboard to enable Anti-Spam on a Security Gateway.

To enable Anti-Spam:

1. In SmartConsole, go to Manage & Settings > Blades.
2. In the Anti-Spam & Mail section, click Configure in SmartDashboard.
   SmartDashboard opens and shows the Overview page in the Anti-Spam & Mail tab.
3. Click Anti-Spam.
   The Anti-Spam Enforcing Gateways window opens.
4. Select one or more Security Gateways.
5. Click OK.
## Sample Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content based Anti-Spam</td>
<td>High protection</td>
<td>Identifies spam based on email content</td>
</tr>
<tr>
<td>IP Reputation Anti-Spam</td>
<td>High protection</td>
<td>Identifies spam based on IP address database of known spammers</td>
</tr>
<tr>
<td>Block List Anti-Spam</td>
<td>Block</td>
<td>Identifies spam based on domains or IP addresses that you define</td>
</tr>
<tr>
<td>Mail Anti-Virus</td>
<td>Block</td>
<td>Scans and filters emails for viruses and other malware</td>
</tr>
<tr>
<td>Zero hour malware protection</td>
<td>Off</td>
<td>Does not scan the Internet to identify and filter new virus email attacks</td>
</tr>
</tbody>
</table>

The **Zero hour malware protection** feature is set to **Off** because enabling the feature has a negative effect on network performance.
Managing User Accounts

In This Section:

- Authentication Methods for Users and Administrators ............................................. 99
- Configuring Authentication Methods for Users ........................................................ 100
- User Database .............................................................. 105
- Managing User Groups .............................................................. 108
- LDAP and User Directory .............................................................. 109
- Access Roles .............................................................. 143
- Authentication Rules .............................................................. 144

Authentication Methods for Users and Administrators

Check Point supports different methods of authenticating end users and administrators.


Users and Administrators authenticate using credentials. All the methods required a username and password.

Users and administrators can be stored in the Check Point User Database (on page 105) or on an LDAP server.

The following sections describe the supported authentication methods.

Check Point Password

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

Operating System Password

OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.
The RADIUS protocol uses UDP to communicate with the gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

SecurID

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA ACE/server and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the ACE/server.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the ACE/server. For administrators, it is the Security Management Server that forwards the requests. ACE manages the database of RSA users and their assigned hard or soft tokens. The gateway or the Security Management Server act as an ACE/Agent 5.0 and direct all access requests to the RSA ACE/server for authentication. For additional information on agent configuration, refer to ACE/server documentation.

There are no specific parameters required for the SecurID authentication method.

TACACS

Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

Configuring Authentication Methods for Users

These instructions show how to configure authentication methods for users. For administrators, see Configuring Authentication Methods for Administrators (on page 30).

For background information about the authentication methods, see Authentication Methods for Users and Administrators (on page 99).

Granting User Access Using RADIUS Server Groups

The Security Gateway lets you control access privileges for authenticated RADIUS (on page 99) users, based on the administrator's assignment of users to RADIUS groups. These groups are used in the Security Rule Base to restrict or give users access to specified resources. Users are unaware of the groups to which they belong.
To use RADIUS groups, you must define a return attribute in the RADIUS user profile of the RADIUS server. This attribute is returned to the Security Gateway and contains the group name (for example, `RAD_<group to which the RADIUS users belong>`) to which the users belong.

Use these RADIUS attributes [refer to RFC 2865]:

- For SecurePlatform - attribute “Class” [25]
- For other operating systems, including Gaia, Windows, and IPSO- attribute “Vendor-Specific” [26]

Sample workflow for RADIUS authentication configuration:

1. Create a RADIUS host object.
2. Configure the RADIUS server object settings.
3. Configure gateways to use RADIUS authentication.
4. Define user groups.
5. Configure RADIUS authentication settings for user.
6. Complete the RADIUS authentication configuration.

Configuring a Security Gateway to use SecurID Authentication

Sample workflow for SecurID (on page 100) authentication configuration:

1. Configure gateways for SecurID authentication.
2. Define user groups.
3. Configure SecurID authentication settings for users.
   - The procedure for doing this is different for Internal Users (that are defined in the internal User Database on the Security Management Server) and for External Users.
4. Complete the SecurID authentication configuration.

To configure a Security Gateway to use SecurID:

1. Generate the `sdconf.rec` file on the ACE/Server and copy it to:
   - `/var/ace/sdconf.rec` on UNIX, Linux or IPSO
   - `%SystemRoot%\System32\sdconf.rec` on 32-bit Windows
   - `%SystemRoot%\SysWOW64\sdconf.rec` on 64-bit Windows
   

2. In SmartConsole, go to the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.

3. In the gateway property window that opens, select **Other > Legacy Authentication**.

4. In the **Enabled Authentication Schemes** section, select **SecurID**.

5. Click **OK**.

To define a user group:

1. In SmartConsole, open the **Objects Bar (F11)**.
2. Click **New > More > User > User Group**.
   - The **New User Group** window opens.
3. Enter the name of the group, for example **SecurID_Users**.
Make sure the group is empty.

4. Click **OK**.
5. Publish the changes and install the policy.

To configure SecurID authentication settings for Internal Users:

Internal users are users that are defined in the internal User Database on the Security Management Server.

1. Create a new user. In SmartConsole, open the **Objects Bar (F11)**.
2. Click **New > More > User > User**.
   The **New User** window opens.
3. Choose a template.
4. Click **OK**.
5. In the **General** page:
   - Enter a default **Name**. This name will be used to authenticate users on the ACE/Server.
   - Set the **Expiration** date.
6. In the **Authentication** page, from the **Authentication Method** drop-down list, select **SecurID**.
7. Click **OK**.

To configure SecurID authentication settings for External Users:

External users are users that are not defined in the internal Users Database on the Security Management Server.

1. Create a new user profile. In SmartConsole, click **Manage & Settings > Blades**.
2. In the **Mobile Access** section, click **Configure in SmartDashboard**.
   SmartDashboard opens.
3. Go to the objects pane, and click **Users**.
4. Right-Click and select **New > External User Profile**.
5. If you support more than one external authentication scheme, select **Match By Domain**.
   In the **External User Profile Properties** window, **General Properties** page:
   - Enter an **External User Profile Name**. This name will be used to authenticate users on the ACE/Server.
   - Set the **Expiration Date**.
   If you support one external authentication scheme, select **Match all users**.
   In the **External User Profile Properties** window, **General Properties** page, set the **Expiration Date**.
6. In the **Authentication** page, from the **Authentication Scheme** drop-down list, select **SecurID**.
7. Click **OK**.
8. Click **Update** (Ctrl + S).
9. Close SmartConsole.
To complete the SecurID authentication configuration:

1. Make sure that connections between the gateway and the ACE/Server are not NATed in the Address Translation Rule Base.
   
   On a Virtual System, follow the instructions in sk107281

2. Save, verify, and install the policy in SmartConsole.

When a Security Gateway has multiple interfaces, the SecurID agent on the Security Gateway sometimes uses the wrong interface IP to decrypt the reply from the ACE/Server, and authentication fails.

To overcome this problem, place a new text file, named sdopts.rec in the same directory as sdconf.rec. The file should contain the CLIENT_IP=<ip> line, where <ip> is the primary IP address of the Security Gateway, as defined on the ACE/Server. This is the IP address of the interface to which the server is routed.

Configuring a Security Gateway to use TACACS+ Authentication

Sample workflow for TACACS [on page 100] authentication configuration:

1. Create a TACACS host object.
2. Configure the TACACS server object settings.
3. Configure gateways to use TACACS authentication.
4. Define user groups.
5. Configure TACACS authentication settings for user.
6. Complete the TACACS authentication configuration.

To create a new TACACS host object:

1. In SmartConsole, the Object Management tab, click New > Host. The New Host window opens.
2. Enter the Object Name and the IP Address of the new TACACS host object, and click OK.
3. Publish the changes.

To configure the TACACS server object settings:

1. In the Object Management tab, click New > More > Server > More > TACACS. The TACACS Server Properties window opens.
2. Configure new server properties:
   - Enter the Name of the TACACS server object
   - Select the TACACS Host object with which to associate the TACACS server object
     This is the host object you created previously.
   - Select the TACACS Type (the default is TACACS, but TACACS+ is recommended)
   - Select the Service - match the TACACS service (UDP or TCP) to the Type selected above
3. Click OK.
4. Publish the changes.
To configure a Security Gateway to use TACACS authentication:

1. In SmartConsole, go to the Gateways & Servers view, right-click a Security Gateway object and select Edit.
2. In the gateway property window that opens, select Other > Legacy Authentication.
3. In the Enabled Authentication Schemes section, select TACACS.
4. Click OK.

To define a TACACS user group:

1. In SmartConsole, the Objects tab, click New > More > Users > User Group.
   The New User Group window opens.
2. Enter the name of the group.
   Make sure the group is empty.
3. Click OK.
4. Publish the changes and install the policy.

To configure TACACS authentication settings for users:

1. Create new user profiles -
   - For users with Security Gateway user accounts - in SmartConsole, go to the Objects tab and click New > More > Users > User.
   - For users without Security Gateway user accounts - go to the Objects tab and click New > More > Users > External User Profile > Match all users (or Match by domain). If you support more than one external authentication scheme, set up External User Profiles with the Match By Domain setting.
   The User Properties window opens.
2. In the General Properties tab, configure these settings:
   - Enter a User Name for the TACACS server. (When configuring Match all users as an External User Profile, the name “generic*” is automatically assigned)
   - Set the Expiration Date.
3. In the Authentication tab, configure these settings:
   - Select TACACS from the Authentication Scheme drop-down list
   - From the Select a TACACS Server drop-down menu, select the TACACS object that you configured earlier
4. Click OK.

To complete the TACACS authentication configuration:

1. Verify that communication between the firewall and the TACACS server is not NATed in the Address Translation Rule Base.
2. Save, verify, and install the policy.
User Database

Users defined in SmartConsole are saved to the User Database on the Security Management Server, together with the user authentication schemes and encryption keys. Then, the user database is installed on Security Gateways and Check Point hosts:

- On Security Gateways - When the policy is installed (Install Policy)
- On Check Point hosts with an active Management blade (such as Log Server) - When the database is installed (Install Database)

The user database does not contain information about users defined elsewhere than on 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). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the management server.

Creating, Modifying, Removing User Accounts

To create a new user:
1. In the object tree, click New > More > Users > User.
   
   The Users Properties window opens.
   
   Important! If you do not select an authentication method, the user cannot log in or use network resources.
4. In Location (“User > Authentication” on page 106), select objects from which this user can access or send data and traffic.
5. If the user has specified working days or hours, configure when (“User > Time “ on page 106) the user can be authenticated for access.
6. Click OK.

To change an existing user:
1. In the object tree, click Users > Users.
2. Double-click a user.
   
   The User Properties window opens.
3. Change the properties as necessary.
4. Click OK.

User > General Properties

Required settings:
- User Name - A unique, case sensitive character string.

   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.
• **Expiration Date** - The date, after which the user is no longer authorized to access network resources and applications. By default, the date defined in the Default Expiration Settings ("Configuring Default Expiration Settings for Users" on page 107) shows as the expiration date.

Optional settings:

• **Comment**
• **Email Address**
• **Mobile Phone Number**

**User > Authentication**

Select an **Authentication Scheme**:

• **SecurID**
• **Check Point Password** - Enter the password string (between 4 and 8 characters) and confirm it
• **OS Password**
• **RADIUS** - Select a RADIUS server or a group of servers
• **TACACS** - Select a TACACS server

**User > Authentication**

**Network Objects** - List of defined objects in the environment.

**Source** - Click **Add**, to add selected objects to this user’s permitted resources. The user can get data and traffic from these objects.

**Destination** - Click **Add**, to add selected objects to this user’s permitted destinations. The user can send data and traffic to these objects.

**User > Time**

**Days in week** - Select the days that the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

**Time of day [hh:mm]** - Enter start time and end time of an expected workday. This user will not be authenticated if a login attempt is made on a time outside the given range.

**Managing Certificates**

Generate and register SIC certificates for user accounts. This authenticates the user in the Check Point system. Use certificates with required authentication for added access control.

**To create a new certificate:**

1. Open the **User Properties** window > **Certificates** page.
2. Click **New**.
3. Select key or .p12 file:
   • **Registration key for certificate enrollment** - Select 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.
   • **Certificate file (.p12)** - Select to create a .p12 certificate file with a private password for the user. When prompted, enter and confirm the certificate password.
4. Click **OK**.

If a user will not be in the system for some time (for example, going on an extended leave), you can revoke the certificate. This leaves the user account in the system, but it cannot be accessed until you renew the certificate.

**To revoke a certificate**, select the certificate and click **Revoke**.

### Configuring Encryption

If the user will access resources from a remote location, traffic between the remote user and internal resources will be encrypted. Configure encryption settings for remote access users.

**To configure encryption:**

1. Open the **User Properties** window > **Encryption** page.
2. Select an encryption method for the user.
3. Click **Edit**.

   The encryption **Properties** window opens.

   The next steps are for **IKE Phase 2**. The options can be different for different methods.
4. Open the **Authentication** tab.
5. Select the authentication schemes:
   a) **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.
   b) **Public Key** - The user authenticates with a public key contained in a certificate file.
6. Click **OK**.
7. Click **OK**.

### Configuring Default Expiration Settings for Users

If a user account is about to expire, notifications show at the time when the owner of that account logs into SmartConsole or one of the SmartConsole clients.

**To configure the default expiration settings:**

1. From the **Menu**, select **Global Properties**.
   
   The **Global Properties** window opens.
2. Click **User and Administrator Accounts**.
3. Click **User Accounts**.
4. Select **Expire at** or **Expire after**.
   a) **Expire at** - Select the expiration date from the calendar control.
   b) **Expire after** - Enter the number of days (from the day the account is made) before user accounts expire.
5. Select **Show accounts expiration indication**, and enter the number of days.

Expiration warnings in the **Expired Accounts** window will show this number of days before an account expires. During this time, if the user account is to be active for longer, you can edit the user account expiration configuration. This will avoid loss of working time.
Delete a User

To delete a user:
1. In the object tree, click **Users > Users**.
2. Right-click the account and select **Delete**.
   The confirmation window opens.
3. Click **Yes**.

Managing User Groups

User groups are collections of user accounts. Add the user group to the *Source* or *Destination* of a rule. You cannot add individual users to a rule.

You can also edit user groups, and delete user groups that are not used in the Rule Base.

Adding User Groups

To create a new user group:
1. In the object tree, click **New > More > Users > User Group**.
   The **New User Group** window opens.
2. Enter a name for the new group.
3. For each user or a group of users, click the [*] sign and select the object from the list.
4. Configure the optional settings:
   - **Mailing List Address**
   - **Comment**
   - **Tag**
   - **Color**
5. Click **OK**.

To add new users or other user groups to a group:
1. In the object tree, select **Users > User Groups**
2. Select the User group and click **Edit**.
   The **Group Properties** window opens.
3. In the **Group Properties** window, select users or user groups in the **Available Members** list.
4. Click **Add**.
   If you are adding a group to the list, a message window opens:
   - Click **Yes** to add each member of the group instead of the group or
   - Click **No** to add only the group.
LDAP and User Directory

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

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

You can choose to manage Domains on the Check Point users database, or to implement an external LDAP server.

**Note:** User Directory requires a special license. If you have the Mobile Access Software Blade, you have the User Directory license.

User Directory lets you configure:

- **High Availability**, to duplicate user data across multiple servers for backup (see “Account Units and High Availability” on page 140).
- **Multiple Account Units**, for distributed databases.
- **Define LDAP Account Units**, for encrypted User Directory connections (see “Modifying the LDAP Server” on page 139).
- **Profiles**, to support multiple LDAP vendors (see “User Directory Profiles” on page 119).

User Directory and Identity Awareness

Identity Awareness uses User Directory.

Identity Awareness lets you enforce network access and audit data, based on network location, the identity of the user, and the identity of the computer. You can use Identity Awareness in the Access Control, Threat Prevention and DLP Rule Bases.

User Directory Considerations

Before you begin, plan your use of User Directory.

- Decide whether you will use the User Directory servers for user management, CRL retrieval, user authentication (“Working with LDAP Account Units” on page 136), or all of those.
- Decide how many Account Units you will need. You can have one for each User Directory server, or you can divide branches of one User Directory server among different Account Units (on page 136).
- Decide whether you will use High Availability (“Account Units and High Availability” on page 140) setup.
- Determine the order of priority (“Setting High Availability Priority” on page 140) among the User Directory servers for High Availability and querying purposes.
• Assign users ["Managing Users on a User Directory Server" on page 141] to different Account Units, branches, and sub-branches, so that users with common attributes (such as their role in the organization, permissions, etc.) are grouped together.

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 methods, or values for remote users.

You can use the default User Directory schema, if all users have the same authentication method 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 (see “Check Point Schema for LDAP” on page 110).

In This Section

- Schema Checking .......................................................... 110
- OID Proprietary Attributes .............................................. 111
- User Directory Schema Attributes .................................. 112
- Netscape LDAP Schema .................................................. 119

Check Point Schema for LDAP

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 Check Point object class and its associated attributes be defined in the directory schema.

Before you work with User Directory, make sure that schema checking is disabled. Otherwise the integration will fail. After the Check Point object classes and attributes are applied to the User Directory server's schema, you must enable schema checking again.
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.

Object Class OIDs

<table>
<thead>
<tr>
<th>object class</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw1template</td>
<td>1.3.114.7.4.2.0.1</td>
</tr>
<tr>
<td>fw1person</td>
<td>1.3.114.7.4.2.0.2</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 112) for the value of “X”. 
**User Directory Schema Attributes**

**Attributes:**

- **cn** ................................................................................................................................. 112
- **uid** ................................................................................................................................. 113
- **description** .................................................................................................................. 113
- **mail** ................................................................................................................................ 113
- **member** ....................................................................................................................... 113
- **userPassword** ............................................................................................................. 113
- **fw1authmethod** ........................................................................................................... 114
- **fw1authserver** ............................................................................................................. 114
- **fw1pwdLastMod** .......................................................................................................... 114
- **fw1expiration-date** ...................................................................................................... 114
- **fw1hour-range-from** .................................................................................................. 114
- **fw1hour-range-to** ....................................................................................................... 115
- **fw1day** ......................................................................................................................... 115
- **fw1allowed-src** ........................................................................................................... 115
- **fw1allowed-dst** ........................................................................................................... 115
- **fw1allowed-vlan** ........................................................................................................ 115
- **fw1SR-keym** ................................................................................................................ 116
- **fw1SR-datam** ................................................................................................................ 116
- **fw1SR-mdm** ................................................................................................................ 116
- **fw1enc-fwz-expiration** ................................................................................................ 116
- **fw1sr-auth-track** ........................................................................................................ 116
- **fw1groupTemplate** ...................................................................................................... 117
- **fw1ISAKMP-EncMethod** ............................................................................................. 117
- **fw1ISAKMP-AuthMethods** .......................................................................................... 117
- **fw1ISAKMP-HashMethods** ......................................................................................... 117
- **fw1ISAKMP-Transform** .............................................................................................. 117
- **fw1ISAKMP-DataIntegrityMethod** .............................................................................. 118
- **fw1ISAKMP-SharedSecret** ......................................................................................... 118
- **fw1ISAKMP-DataEncMethod** ..................................................................................... 118
- **fw1enc-Methods** ......................................................................................................... 118
- **fw1userPwdPolicy** .................................................................................................... 118
- **fw1badPwdCount** ........................................................................................................ 118
- **fw1lastLoginFailure** .................................................................................................... 119
- **memberof template** .................................................................................................... 119

**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 methods.

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 login to 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 SmartConsole is “Internal Password”, all the users will be authenticated using the password stored in the “userPassword” attribute.

fw1authserver

<table>
<thead>
<tr>
<th>“X” 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>“undefined”</td>
</tr>
</tbody>
</table>

The name of the server that will do 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 “Any”</td>
</tr>
<tr>
<td>TACACS</td>
<td>name of a TACACS server</td>
</tr>
</tbody>
</table>

fw1pwdLastMod

The date on which the password was last modified. The format is yyyyymmdd (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>“X” 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 yyyyymmdd (for example, 20 August 1998 is 19980820). The default is “no value”.

<table>
<thead>
<tr>
<th>“X” 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>“no value”</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).
### Managing User Accounts

#### “X” in OID

<table>
<thead>
<tr>
<th>“X” 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>“00:00”</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>“X” 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>“23:59”</td>
</tr>
</tbody>
</table>

#### fw1day

The days on which the user can login to a Security Gateway. Can have the values “SUN”, “MON”, and so on.

<table>
<thead>
<tr>
<th>“X” 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>“X” 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>“no value”</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>“X” 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>“no value”</td>
</tr>
</tbody>
</table>

#### fw1allowed-vlan

Not currently used.

<table>
<thead>
<tr>
<th>“X” 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>“no value”</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>“X” 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>“Any”</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>“X” 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>“Any”</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>“X” 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>“none”</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>“X” 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>“X” 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>“none”</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>“X” 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>“X” 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>“X” 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>“X” 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>“X” 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”.

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>y</td>
<td>y</td>
<td>&quot;SHA1&quot;</td>
</tr>
</tbody>
</table>

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>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>“X” 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>“X” 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>“X” 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>“X” in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>y</td>
</tr>
</tbody>
</table>
Managing User Accounts

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 user 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>

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.

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 Server 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 methods 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 users’ group 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:**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserLoginAttr</td>
<td>123</td>
</tr>
<tr>
<td>UserPasswordAttr</td>
<td>123</td>
</tr>
<tr>
<td>TemplateObjectClass</td>
<td>123</td>
</tr>
<tr>
<td>ExpirationDateAttr</td>
<td>123</td>
</tr>
<tr>
<td>ExpirationDateFormat</td>
<td>123</td>
</tr>
<tr>
<td>PsswdDateFormat</td>
<td>124</td>
</tr>
<tr>
<td>PsswdDateAttr</td>
<td>124</td>
</tr>
<tr>
<td>BadPwdCountAttr</td>
<td>124</td>
</tr>
<tr>
<td>ClientSideCrypt</td>
<td>124</td>
</tr>
<tr>
<td>DefaultCryptAlgorithm</td>
<td>124</td>
</tr>
<tr>
<td>CryptedPasswordPrefix</td>
<td>125</td>
</tr>
<tr>
<td>PhoneNumberAttr</td>
<td>125</td>
</tr>
<tr>
<td>AttributesTranslationMap</td>
<td>125</td>
</tr>
<tr>
<td>ListOfAttrsToAvoid</td>
<td>125</td>
</tr>
<tr>
<td>BranchObjectClass</td>
<td>125</td>
</tr>
<tr>
<td>BranchOCOperator</td>
<td>126</td>
</tr>
<tr>
<td>OrganizationObjectClass</td>
<td>126</td>
</tr>
<tr>
<td>OrgUnitObjectClass</td>
<td>126</td>
</tr>
<tr>
<td>DomainObjectClass</td>
<td>126</td>
</tr>
<tr>
<td>UserObjectClass</td>
<td>126</td>
</tr>
<tr>
<td>UserOCOperator</td>
<td>126</td>
</tr>
<tr>
<td>GroupObjectClass</td>
<td>127</td>
</tr>
<tr>
<td>GroupOCOOperator</td>
<td>127</td>
</tr>
<tr>
<td>UserMembershipAttr</td>
<td>127</td>
</tr>
<tr>
<td>TemplateMembership</td>
<td>128</td>
</tr>
<tr>
<td>TemplateMembershipAttr</td>
<td>128</td>
</tr>
<tr>
<td>UserTemplateMembershipAttr</td>
<td>128</td>
</tr>
<tr>
<td>OrganizationRDN</td>
<td>128</td>
</tr>
<tr>
<td>OrgUnitRDN</td>
<td>128</td>
</tr>
<tr>
<td>UserRDN</td>
<td>129</td>
</tr>
<tr>
<td>GroupRDN</td>
<td>129</td>
</tr>
<tr>
<td>DomainRDN</td>
<td>129</td>
</tr>
<tr>
<td>AutomaticAttrs</td>
<td>129</td>
</tr>
<tr>
<td>GroupObjectClass</td>
<td>129</td>
</tr>
<tr>
<td>OrgUnitObjectClass</td>
<td>130</td>
</tr>
<tr>
<td>OrganizationObjectClass</td>
<td>130</td>
</tr>
<tr>
<td>UserObjectClass</td>
<td>130</td>
</tr>
<tr>
<td>DomainObjectClass</td>
<td>130</td>
</tr>
</tbody>
</table>
**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>One value allowed</td>
</tr>
<tr>
<td>unicodePwd (in Microsoft_AD)</td>
<td></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 fw1template.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw1template</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>fw1expiration-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 <code>yyyyymmdd</code></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>fw1pwdLastMod (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>fw1BadPwdCount</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</td>
<td>One value allowed</td>
</tr>
<tr>
<td>1 for Netscape_DS</td>
<td></td>
</tr>
<tr>
<td>if not using encrypted password, SSL is recommended</td>
<td></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)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>Crypt (for Netscape_DS)</td>
<td></td>
</tr>
<tr>
<td>SHA11</td>
<td></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. In case the User Directory server was not extended by the Check Point schema, the best thing to do is to 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>
</table>
| • Organization OrganizationalUnit Domain (most servers)  
• Container (extra for Microsoft_AD) | Multiple values allowed |
**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) Contained (added to Microsoft_AD)</td>
<td>Multiple values allowed</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) Person OrganizationalPerson InertOrgPerson FW1 Person (most servers)</td>
<td>Multiple values allowed</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>Groupofnames (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>
</tbody>
</table>

For Microsoft_AD This means that when a user object is created an extra attribute is included automatically: `userAccountControl` with the value 66048

**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.
### Default vs. Other

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default</th>
<th>Other</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>groupOfNames:member</code></td>
<td></td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td><code>groupOfUniqueNames:uniqueMember</code></td>
<td></td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td>(All other servers)</td>
<td></td>
<td>Multiple values allowed</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>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>OrganizationalUnit</code></td>
<td>Multiple values allowed</td>
<td></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>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Organization</code></td>
<td>Multiple values allowed</td>
<td></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>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User (in Microsoft_AD)</td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td>person</td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td>organizationalPerson</td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td>fw1Person</td>
<td>Multiple values allowed</td>
<td></td>
</tr>
<tr>
<td>(All other servers)</td>
<td>Multiple values allowed</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>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Multiple values allowed</td>
<td></td>
</tr>
</tbody>
</table>
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 133]).

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

SmartConsole allows the creation and management of existing and new objects. However, some specific Active Directory fields are not enabled via SmartConsole.

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 SmartConsole 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: `$FWDIR/lib/ldap`.
2. Copy `schema_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 `DOMAINNAME`, 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.

   ```ldif
   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
oMSyntax: 20
rangeLower: 1
rangeUpper: 256
showInAdvancedViewOnly: TRUE
```

All Check Point attributes can be added in the same 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 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`

Retrieving Information from a User Directory Server

When a gateway requires user information for authentication, it goes through this process:

1. The gateway searches for the user in the internal users database.
2. If the specified user is not defined in the internal users database, the gateway queries the LDAP server defined in the Account Unit with the highest priority.
3. If the query against an LDAP server with the highest priority fails (for example, the connection is lost), the gateway queries the server with the next highest priority.
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.

4. If the query against all LDAP servers fails, the gateway matches the user against the generic external user profile.

**Running 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 a specified operation.

To query User Directory:

1. Open Objects Tree > Users and Administrators.
2. Double-click the Account Unit to open a connection to the LDAP server.
3. Right-click the Account Unit and select Query Users/Group.
   - The LDAP Query Search window opens.
   - Click Advanced to select specified objects types, such as Users, groups, or templates.
4. Define the query.
5. 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 a Query**

If you create a query where:

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

The server queries the User Directory with this filter:

```plaintext
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.)

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

Enabling User Directory

In SmartConsole, enable the Security Management Server to manage users in the Account Unit (“Working with LDAP Account Units” on page 136).

Note: You cannot use the SmartConsole User Database when the User Directory LDAP server is enabled.

To enable User Directory on the Security Management Server:

1. From the Menu, select Global Properties > User Directory.
   The User Directory page opens.
3. Configure login and password settings.
4. Click OK.
5. In Object Categories > Network Objects > Check Point Host, open the Security Management Server object for editing.
7. Click OK.
8. Install the policy.

Account Units

An Account Unit represents branches of user information on one or more LDAP servers. The Account Unit is the interface between the LDAP servers and the Security Management Server and Security Gateways.

You can have a number of Account Units representing one or more LDAP servers. Users are divided among the branches of one Account Unit, or between different Account Units.

Note: When you enable the Identity Awareness and Mobile Access Software Blades, SmartConsole opens a First Time Configuration Wizard. The Active Directory Integration window of this wizard lets you create a new AD Account Unit. After you complete the wizard, SmartConsole creates the AD object and Account Unit.

Working with LDAP Account Units

Use the LDAP Account Unit Properties window in SmartConsole to edit an existing Account Unit or to create a new one manually.

To edit an existing LDAP Account Unit:
1. In SmartConsole, open the Object Explorer (Ctrl+E).
2. Select Servers > LDAP Account Units.
3. Right-click the LDAP Account Unit and select Edit.
   The LDAP Account Unit Properties window opens.
4. Edit the settings in these tabs:
   - General ("General Tab" on page 137) - Configure how the Security Management Server uses the Account Unit
   - Servers ("Configuring an LDAP Server" on page 137) - Manage LDAP servers that are used by this Account Unit
   - Objects Management ("Objects Management Tab" on page 138) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - Authentication ("Authentication Tab" on page 139) - Configure the authentication scheme for the Account Unit
5. Click OK.
6. Install the policy.

To create a new LDAP Account Unit:
1. In the Objects tab, click New > More > Server > LDAP Account unit.
   The LDAP Account Unit Properties window opens.
2. Configure the settings on these tabs:
   - **General** ("General Tab" on page 137) - Configure how the Security Management Server uses the Account Unit
   - **Servers** ("Configuring an LDAP Server" on page 137) - Manage LDAP servers that are used by this Account Unit
   - **Objects Management** ("Objects Management Tab" on page 138) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - **Authentication** ("Authentication Tab" on page 139) - Configure the authentication scheme for the Account Unit

3. Click **OK**.

4. Install the policy.

**General Tab**

These are the configuration fields in the **General** tab:

- **Name** - Name for the Account Unit
- **Comment** - Optional comment
- **Color** - Optional color associated with the Account Unit
- **Profile** - LDAP vendor
- **Domain** - Domain of the Active Directory servers, when the same user name is used in multiple Account Units (this value is also necessary for AD Query and SSO)
- **Prefix** - Prefix for non-Active Directory servers, when the same user name is used in multiple Account Units
- **Account Unit usage** - Select applicable options:
  - **CRL retrieval** - The Security Management Server manages how the CA sends information about revoked licenses to the Security Gateways
  - **User Management** - The Security Management Server uses the user information from this LDAP server (User Directory must be enabled on the Security Management Server)
    
    **Note** - LDAP SSO (Single Sign On) is only supported for Account Unit objects that use **User Management**.
  - **Active Directory Query** - This Active Directory server is used as an Identity Awareness source.
    
    **Note** - This option is only available if the **Profile** is set to **Microsoft_AD**.
- **Enable Unicode support** - Encoding for LDAP user information in non-English languages
- **Active Directory SSO configuration** - Click to configure Kerberos SSO for Active Directory - Domain Name, Account Name, Password, and Ticket encryption method

**Configuring an LDAP Server**

You can add, edit, or delete LDAP server objects.

To configure an LDAP server for the Account Unit:

1. To add a new server, click **Add**. To edit an existing one, select it from the table and click **Edit**.
   
   The **LDAP Server Properties** window opens.

2. From the **Host** drop-down menu, select the server object.
If necessary, create a new SmartConsole server object:
   a) Click New.
   b) In the New Host window opens, enter the settings for the LDAP server.
   c) Click OK.

3. Enter the login credentials and the Default priority.
4. Select access permissions for the Check Point Gateways:
   • Read data from this server
   • Write data to this server
5. In the Encryption tab, configure the optional SSL encryption settings.
6. Click OK.

To remove an LDAP server from the Account Unit:
1. Select a server from the table.
2. Click Remove.

If all the configured servers use the same login credentials, you can modify those simultaneously.

To configure the login credentials for all the servers simultaneously:
1. Click Update Account Credentials.
   The Update Account to All Servers window opens.
2. Enter the login credentials.
3. Click OK.

Objects Management Tab
Configure the LDAP server for the Security Management Server to query and the branches to fetch.

Note - Make sure there is LDAP connectivity between the Security Management Server and the LDAP Server that holds the management directory.

To configure LDAP query parameters:
1. From the Manage objects on drop-down menu, select the LDAP server object.
2. Click Fetch branches.
   The Security Management Server queries and shows the LDAP branches.
3. Configure Branches in use:
   • To add a branch, click Add and in the LDAP Branch Definition window that opens, enter a new Branch Path
   • To edit a branch, click Edit and in the LDAP Branch Definition window that opens, modify the Branch Path
   • To delete a branch, select it and click Delete
4. Select Prompt for password when opening this Account Unit, if necessary (optional).
5. Configure the number of Return entries that are stored in the LDAP database (the default is 500).
**Authentication Tab**

These are the configuration fields in the Authentication tab:

- **Use common group path for queries** - Select to use one path for all the LDAP group objects (only one query is necessary for the group objects)

- **Allowed authentication schemes** - Select one or more authentication schemes allowed to authenticate users in this Account Unit - **Check Point Password**, **SecurID**, **RADIUS**, **OS Password**, or **TACACS**

- **Users’ default values** - The default settings for new LDAP users:
  - **User template** - Template that you created
  - **Default authentication scheme** - one of the authentication schemes selected in the **Allowed authentication schemes** section

- **Limit login failures** (optional):
  - **Lock user’s account after** - Number of **login failures**, after which the account gets locked
  - **Unlock user’s account after** - Number of **seconds**, after which the locked account becomes unlocked

- **IKE pre-shared secret encryption key** - Pre-shared secret key for IKE users in this Account Unit

**Modifying the LDAP Server**

1. On the **LDAP Account Unit Properties > Servers** tab, double-click a server. The **LDAP Server Properties** window opens.

2. On 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


   If the connections are encrypted, enter the encryption port and strength settings.

**Note** - User Directory connections can be authenticated by client certificates from a Certificate Authority (CA) (“Authenticating with Certificates” on page 141). To use certificates, the LDAP server must be configured with SSL strong authentication.
**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 Server</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 use certificates to secure communication with LDAP servers. If you do not configure certificates, the management server, Security Gateways, and LDAP servers communicate without authentication.

To configure User Directory to use certificates:
1. Open GuiDBedit.
2. Search for the `ldap_use_cert_auth` attribute.
3. For each entry in the field **Name** column, set the `ldap_use_cert_auth` attribute to **true**.
4. Save and close GuiDBedit.
5. Log in to SmartConsole.
6. 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.
7. For all necessary network objects (such as Security Management Server, Security Gateway, Policy Server) that require certificate-based User Directory connections:
   a) On the **IPSec VPN** page of the network object properties, click **Add** in the **Repository of Certificates Available** list.
      
      **Note**: a management-only server does not have an IPSec VPN page. The User Directory on a management-only server cannot be configured to authenticate to an LDAP server using certificates.
   b) In the **Certificate Properties** window, select the defined CA.
8. In the **Users and Administrators** tab of the Objects tree, make sure the new configuration works.
   Open a connection on one of the Account Units configured to use certificate authentication.

### Managing Users on a User Directory Server

In R80 SmartDashboard, users and user groups in the Account Unit show in the same tree structure as on the LDAP server.

- To see User Directory users, open **Users and Administrators**. The **LDAP Groups** folder holds the structure and accounts of the server.
- You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartDashboard, the changes are immediate on the server.
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.

Managing LDAP Information

User Directory lets you use R80 SmartDashboard to manage information about users and OUs (Organizational Units) that are stored on the LDAP server.

To manage LDAP information from SmartDashboard:
1. From the object tree, select Users and Administrators.
2. Double-click the Account Unit.
   The LDAP domain is shown.
3. Double-click the LDAP branch.
   The Security Management Server queries the LDAP server and SmartConsole shows the LDAP objects.
4. Expand the Objects List pane.
5. Double-click the LDAP object.
   The Objects List pane shows the user information.
6. Right-click a user and select Edit.
   The LDAP User Properties window opens.
7. Edit the user information and settings and then click OK.

LDAP Groups for the User Directory

Create LDAP groups for the User Directory. These groups classify users according to type and can be used in Policy rules. You can add users to groups, or you can create dynamic filters.

To create LDAP groups for User Directory:
1. In SmartConsole, open Object Categories > New > More > Users > LDAP group.
2. In the New LDAP Group window that opens, select the Account Unit for the User Directory group.
3. Define Group’s Scope - select one of these:
   - All Account-Unit’s Users - All users in the group
   - Only Sub Tree - Users in the specified branch
   - Only Group in branch - Users in the branch with the specified DN prefix
4. Apply an advanced LDAP filter:
   a) Click Apply filter for dynamic group.
   b) Enter the filter criteria.
5. Click OK.

Examples
- If the User objects for managers in your organization have the object class “myOrgManager”, define the Managers group with the filter: objectclass=myOrgManagers
• If 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**

**Access Roles**

Access role objects let you configure network access according to:

• Networks
• Users and user groups
• Computers and computer groups
• Remote access clients - will be supported with R80.x gateways

After you activate the Identity Awareness Software Blade, you can create access role objects and
use them in the **Source** and **Destination** columns of Access Control Policy rules.

**Adding Access Roles**

**Important:** Before you add Active Directory users, machines, or groups to an access role, make
sure there is LDAP connectivity between the Security Management Server and the AD Server that
holds the management directory. The management directory is defined on the **Objects**
Management tab in the **Properties** window of the **LDAP Account Unit**.

To create an access role:

1. In the object tree, click **New > More > Users > Access Role**.
   
   The **New Access Role** window opens.
2. Enter a **Name** for the access role.
3. Enter a **Comment** (optional).
4. Select a **Color** for the object (optional).
5. In the **Networks** pane, select one of these:
   
   • Any network
   • **Specific networks** - For each network, click **+** and select the network from the list
6. In the **Users** pane, select one of these:
   
   • Any user
   • **All identified users** - includes any user identified by a supported authentication method
     (internal users, Active Directory users, or LDAP users).
   • **Specific users/groups** - For each user or user group, click **+** and select the user or the
     group from the list
7. In the **Machines** pane, select one of these:
   
   • Any machine
   • **All identified machines** - includes machines identified by a supported authentication
     method (Active Directory).
   • **Specific machines** - For each machine, click **+** and select the machine from the list
8. In the **Remote Access Clients** pane, select the clients for remote access.
9. Click **OK**.
Identity Awareness engine automatically recognizes changes to LDAP group membership and updates identity information, including access roles. For more, see the R80 Identity Awareness Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=46529.

Authentication Rules

To make an authentication rule:

1. Add users to user groups.
2. Define an access role ("Access Roles" on page 143) for networks, users and user groups, and computers and computer groups.
3. Make the authentication rules with the access roles in the Source.
Client Certificates for Smartphones and Tablets

In This Section:

- Managing Client Certificates ...................................................................................... 145
- Creating Client Certificates ........................................................................................ 146
- Revoking Certificates ................................................................................................. 147
- Creating Templates for Certificate Distribution ....................................................... 147
- Cloning a Template ..................................................................................................... 148
- Giving Permissions for Client Certificates ................................................................ 148

To allow your users to access their resources using their handheld devices, make sure they can authenticate to the Gateway with client certificates.

In many organizations, the daily task of assigning and maintaining client certificates is done by a different department than the one that maintains the Security Gateways. The computer help desk, for example. You can create an administrator that is allowed to use SmartConsole to create client certificates, while restricting other permissions (“Giving Permissions for Client Certificates” on page 148).

To configure client certificates, open SmartConsole and go to Security Policies > Access Control > Access Tools > Client Certificates.

To configure the Mobile Access policy, go to Security Policies > Shared Policies > Mobile Access. This opens SmartDashboard. The Client Certificates page in SmartConsole is a shortcut to the SmartDashboard Mobile Access tab, Client Certificates page.

Managing Client Certificates

Check Point Mobile Apps for mobile devices can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.


The page has two panes.

- In the Client Certificates pane:
  - Create, edit, and revoke client certificates.
  - See all certificates, their status, expiration date and enrollment key. By default, only the first 50 results show in the certificate list. Click Show more to see more results.
  - Search for specified certificates.
  - Send certificate information to users.

- In the Email Templates for Certificate Distribution pane:
  - Create and edit email templates for client certificate distribution.
  - Preview email templates.
Creating Client Certificates

Note - If you use LDAP or AD, creation of client certificates does not change the LDAP or AD server. If you get an error message regarding LDAP/AD write access, ignore it and close the window to continue.

To create and distribute certificates with the client certificate wizard:


2. In the Client Certificates pane, click New.
   The Certificate Creation and Distribution wizard opens.

3. In the Certificate Distribution page, select how to distribute the enrollment keys to users. You can select one or both options.
   a) Send an email containing the enrollment keys using the selected email template - Each user gets an email, based on the template you choose, that contains an enrollment key.
      ▪ Template - Select the email template that is used.
      ▪ Site - Select the gateway that users connect to.
      ▪ Mail Server - Select the mail server that sends the emails.
      You can click Edit to view and change its details.
   b) Generate a file that contains all of the enrollment keys - Generate a file for your records that contains a list of all users and their enrollment keys.

4. Optional: To change the expiration date of the enrollment key, edit the number of days in Users must enroll within x days.

5. Optional: Add a comment that will show next to the certificate in the certificate list on the Client Certificates page.

6. Click Next.
   The Users page opens.

7. Click Add to add the users or groups that require certificates.
   • Type text in the search field to search for a user or group.
   • Select a type of group to narrow your search.

8. When all included users or groups show in the list, click Generate to create the certificates and send the emails.

9. If more than 10 certificates are being generated, click Yes to confirm that you want to continue.
   A progress window shows. If errors occur, an error report opens.

10. Click Finish.
11. Click Save.
12. From SmartConsole, install the Policy.
Revoking Certificates

If the status of a certificate is Pending Enrollment, after you revoke it, the certificate does not show in the Client Certificate list.

To revoke one or more certificates:
1. Select the certificate or certificates from the Client Certificate list.
2. Click **Revoke**.
3. Click **OK**.

After you revoke a certificate, it does not show in the Client Certificate list.

Creating Templates for Certificate Distribution

To create or edit an email template:
2. To create a new template: In the Email Templates for Certificate Distribution pane, select **New**.
   - To edit a template: In the Email Templates for Certificate Distribution pane, double-click a template.
   - The Email Template opens.
3. Enter a **Name** for the template.
4. **Optional:** Enter a **Comment**. Comments show in the Mail Template list on the Client Certificates page.
5. **Optional:** Click **Languages** to change the language of the email.
6. Enter a **Subject** for the email. Click **Insert Field** to add a predefined field, such as a Username.
7. In the message body add and format text. Click **Insert Field** to add a predefined field, such as Username, Registration Key, or Expiration Date.
8. Click **Insert Link** to add a link or QR code and select the type of link to add.
   - For each link type, you select which elements will be added to the mail template:
     - **QR Code** - Users scan the code with their mobile devices.
     - **HTML Link** - Users tap the link on their mobile devices.
   - The text in **Display Text** is the text that shows on the link.
   - **Certificate and Site Creation** - For users who already have a Check Point app installed.
     - When users scan the CR code or go to the link, it creates the site and registers the certificate.
     - Select the client type that will connect to the site.
       - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
       - **Capsule Connect/VPN** - A full L3 tunnel app that gives users network access to all mobile applications.
   - **Download Application** - Direct users to download a Check Point App for their mobile devices.
• **Select the client device operating system:**
  - iOS
  - Android

• **Select the client type to download:**
  - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN** - A full L3 tunnel app that gives users network access to all mobile applications.

• **Select which elements will be added to the mail template:**
  - **QR Code** - Users scan the code with their mobile devices
  - **HTML Link** - Users tap the link on their mobile devices.
  - **Display Text** - Enter the text to show on the HTML link.

9. Click **OK**.
10. **Optional:** Click **Preview in Browser** to see a preview of how the email will look.
11. Click **OK**.
12. Publish the changes

---

**Cloning a Template**

Clone an email template to create a template that is similar to one that already exists.

**To create a clone of an email template:**

1. Select a template from the template list in the **Client Certificates** page.
2. Click **Clone**.
3. A new copy of the selected template opens for you to edit.

---

**Giving Permissions for Client Certificates**

You can create an administrator that is allowed to use SmartConsole to create client certificates, and restrict other permissions.

**To make an administrator for client certificates:**

2. Create a customized profile for the administrator ("Assigning Permission Profiles to Administrators" on page 24), with permission to handle client certificates. Configure this in the **Others** page of the Administrator Profile. Restrict other permissions.
Preferences and Management Settings

In This Section:
- Setting IP Address Versions of the Environment ...................................................... 149
- Restoring Window Defaults ........................................................................................ 149
- Setting SmartConsole Timeout .................................................................................. 149
- Configuring the Login Window ................................................................................... 150

Setting IP Address Versions of the Environment

Many objects and rules use IP addresses. Configure the version that your environment uses to see only relevant options.

To set IP address version:
1. Click Manage & Settings.
2. Click Preferences.
3. Select the IP address version that your environment uses: IPv4, IPv6, or IPv4 and IPv6.
4. Select how you want to see subnets: Mask Length or Subnet Mask.

Restoring Window Defaults

Some windows in the SmartConsole offer administrators the option to not see the window again. You can undo this selection, and restore all windows to show again.

This option is available only if administrators selected do not show in a window.

To restore windows from "do not show":
1. Click Manage & Settings.
2. Click Preferences.
3. In the User Preferences area, click Restore All Messages.

Setting SmartConsole Timeout

Use the SmartConsole in a secure manner, and enforce secure usage for all administrators. Setting a SmartConsole timeout is a basic requirement for secure usage. When an administrator is not using the SmartConsole, it logs out.

To set the SmartConsole timeout:
1. Click Manage & Settings.
2. Select Permissions & Administrators > Advanced.
3. In the Idle Timeout area, select Perform logout after being idle.
4. Enter a number of minutes.
When a SmartConsole is idle after this number of minutes, the SmartConsole automatically logs out the connected administrator.

Configuring the Login Window

Administrators in your environment use SmartConsole daily. Customize the Login window, to set the environment to comply with your organization’s culture.

To customize the Login window:

1. Click Manage & Settings.
2. Open Preferences > Login Message.
3. Select Show custom message during login.
4. In Customize Message, enter a title and message for administrators to see.
   The default suggestion is:
   
   Warning
   This system is for authorized use only

5. If you want the message to have a warning icon, in Customize Layout, click Add warning sign.
6. If you want the Login window to show your organization’s logo, in Customize Layout, click Add logo and then browse to an image file.
Management High Availability

In This Section:

- The High Availability Environment ................................................................. 151
- Planning for Management High Availability .................................................... 152
- Configuring a Secondary Server in SmartConsole .......................................... 152
- Monitoring High Availability ............................................................................. 153
- Synchronizing Active and Standby Servers ....................................................... 153
- Failover Between Active and Standby ............................................................... 156
- Changing a Server to Active or Standby ............................................................ 156
- High Availability Disaster Recovery ................................................................. 156

High Availability is redundancy and database backup for management servers. Synchronized servers have the same policies, rules, user definitions, network objects, and system configuration settings. The first management server installed is the primary. If the primary Security Management Server fails, or is off line for maintenance, the secondary server takes over.


The High Availability Environment

A Management High Availability environment includes:

- One Active Security Management Server
- One or more Standby Security Management Server

For full redundancy, the primary management server periodically synchronizes its database with the secondary server or servers.

Active vs. Standby

The active server lets you manage gateways, network objects and system configuration. The synchronized standby server gives backup and redundancy. Only one Security Management Server can be Active at a time. If the Active server fails, you can manually change the Active server to Standby, or the Standby server to Active. The standby server always opens in Read Only mode.

Primary Server vs. Secondary Server

The order in which you install management servers defines them as Primary or Secondary. The first management server installed becomes the Primary active server. When you install more Security Management Servers, you define them as Secondary. Secondary servers are Standby servers.
Planning for Management High Availability

When you plan your High Availability deployment, think about:

- **Remote versus Local Installation of the Standby Security Management Server**
  Connectivity issues on the LAN will not affect a standby server installed remotely.

- **Different physical locations**
  As a best practice for successful disaster recovery, install at least one standby Security Management Server in a physical location different from that of the active server.

Configuring a Secondary Server in SmartConsole

In the SmartConsole connected to the Primary server, create a network object to represent the Secondary Security Management Server. Then synchronize the Primary with the Secondary.

To configure the secondary server in SmartConsole:

1. Open SmartConsole.
2. In **Object Categories**, click **New > More > Network Object > Gateways and Servers > Check Point Host**.
3. On the **General Properties** page, enter a unique name and IP address for the server. **Note**: Do not initialize SIC at this time.
4. In the **Software Blades**, section, select the **Management** tab.
5. Select **Network Policy Management**.
   This automatically selects the **Secondary Server, Logging and Status**, and **Provisioning**.
6. Create SIC trust between the Secondary Security Management Server and the Primary:
   a) Click **Communication**.
   b) Enter the SIC Activation Key of the secondary server.
   c) Click **Initialize**.
   d) Click **Close**.
7. Click **OK**.
8. Click **Publish** to save these session changes to the database.
   On publish, the databases of the primary and secondary server synchronize and continue to synchronize every three minutes.
9. Wait for the Task List in the System Information Area to show that a full sync has completed.
10. Open the **High Availability Status** window and make sure there is one active server and one standby.
Monitoring High Availability

The High Availability Status window shows the status of each Security Management Server in the High Availability configuration.

To see the status of the servers in your High Availability environment:

1. Open SmartConsole and connect to a primary or secondary server.
2. On the Menu, click High Availability.
   The High Availability Status window opens.
   For the management server and its peer or peers in the High Availability configuration, the window shows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>The name of the Security Management Server.</td>
</tr>
<tr>
<td>Mode</td>
<td>If the server is Active or Standby.</td>
</tr>
<tr>
<td>Status</td>
<td>The synchronization status between the Security Management Servers:</td>
</tr>
<tr>
<td></td>
<td>• Last sync</td>
</tr>
<tr>
<td></td>
<td>• There is an HA conflict in the system</td>
</tr>
<tr>
<td></td>
<td>• Some servers could not be synchronized</td>
</tr>
<tr>
<td></td>
<td>• Synchronized</td>
</tr>
<tr>
<td></td>
<td>See Synchronization Status (on page 154) for a complete description.</td>
</tr>
</tbody>
</table>

Synchronizing Active and Standby Servers

The Active server periodically sends the latest changes to the standby server or servers. Active and Standby servers also synchronize when you publish a session.

How Synchronization Works

Synchronization can run automatically or you can start it manually. When synchronizing, the system does these steps without user intervention:

1. Locks the policy and object databases on the Active Security Management Server.
2. Takes a snapshot of the databases and save it to local disk.
3. Unlocks policy and object databases.
5. The Standby Security Management Servers overwrite their databases with the snapshot.
7. The Active and Standby servers delete the snapshots.

While the Active Security Management Server is taking a snapshot [step 2 above], the databases are locked and you cannot add, change or delete these system objects:
Management High Availability

- Security Gateways, Security Management Servers and other network objects
- VPN Communities
- Services, resources and OPSEC applications
- Policies and rules
- Deployment rules and packages
- Reports and queries

This is necessary to prevent database corruption and other errors.

If the environment includes Endpoint Security, the Active Security Management Server and clients continue to dynamically update these database objects even while the Security Management Server takes a snapshot:
- Full Disk Encryption recovery data
- Media Encryption & Port Protection recovery data
- Endpoint monitoring data
- Endpoint heartbeat data

Synchronization Status

The High Availability status window shows this information about synchronization between the active and standby servers:
- Name, status, and actions of the connected server
- Names, statuses, and actions of peers

Status messages can be general, or apply to a specified active or standby server. General messages show in the yellow overview banner.

<table>
<thead>
<tr>
<th>General Status messages in overview banner</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronized</td>
<td>The database of the primary Security Management Server is identical with the database of the secondary.</td>
</tr>
<tr>
<td>Some servers could not be synchronized</td>
<td>A communication issue prevents synchronization, or some other synchronization issue exists.</td>
</tr>
<tr>
<td>No HA</td>
<td>The active and standby servers are not communicating.</td>
</tr>
<tr>
<td>Communication Problem</td>
<td>The <code>fwm</code> service is down or cannot be reached.</td>
</tr>
<tr>
<td>Collision or HA conflict</td>
<td>More than one management server configured as active. Two active servers cannot sync with each other.</td>
</tr>
</tbody>
</table>
When connected to a specified *active* management server:

<table>
<thead>
<tr>
<th>Status window area:</th>
<th>Specified Status Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected to:</td>
<td>Active</td>
<td>SmartConsole is connected to the active management server.</td>
</tr>
</tbody>
</table>
| Peers               | Standby                   | The peer is in standby. The message can also show:  
|                     |                           | - Sync problem, last time sync  
|                     |                           | - Ok, last sync time: <time>  
|                     |                           | - Last sync failed: <date>  
|                     |                           | - Error, partial error  
|                     |                           | - No SIC  
|                     | Not communicating, last sync time | |
|                     | Active                    | A state of collision exists between two servers both defined as active. |

When connected to a specified *standby* management server:

<table>
<thead>
<tr>
<th>Status window area:</th>
<th>Specified Status Messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected to:</td>
<td>Standby</td>
<td>The message also shows: last sync time.</td>
</tr>
</tbody>
</table>
| Peers               | Active                    | The peer is in standby. The message can also show:  
|                     |                           | - No communication, last sync time  
|                     |                           | - OK, last sync time: <time>  
|                     |                           | - Sync problem, last sync time (in any direction)  
|                     | Standby/Master unknown    | The message can also show: no communication. |

**High Availability Troubleshooting**

These error messages show in the *High Availability Status* window when synchronization fails:

**No SIC**

Solution:

2. On the *General Properties* page, click *Test SIC Status*.
3. Follow the instructions in the *SIC Status* window.
Not communicating

Solution:
1. From the main SmartConsole menu, select Management High Availability. The High Availability Status window opens.
2. For the active server, click Actions > Sync now.

Collision or HA Conflict

More than one management server is configured as active. Solution:
1. From the main SmartConsole menu, select Management High Availability. The High Availability Status window opens.
2. Use the Actions button to set one of the active servers to standby.

Failover Between Active and Standby

Failover between the primary (active) and secondary (standby) management server is not automatic. If the Active fails or it is necessary to change the Active to a Standby, you must do so manually. The two servers synchronize before failover to the new active server. After the failover, you cannot use the former active server to make changes.

If the Active Security Management Server is responsive:
In the High Availability status window, change the active server to standby or the standby to active.

Changing a Server to Active or Standby

To change the status of a server:
1. Open SmartConsole.
2. Connect to the Active server.
4. Using the Action buttons, Change the Active server to standby, or one of the standby servers to active.
   The servers synchronize before a failover occurs to the new active server.

High Availability Disaster Recovery

If the primary management server becomes permanently unavailable:
- Create a new Primary server with the IP address of the original Primary server ("Recovery By Creating a New Primary Server" on page 157)
  Note: This is not supported for environments with Endpoint Security.
- Promote the Secondary server to Primary and create new licenses.
  IMPORTANT: Check Point product licenses are linked to IP addresses. At the end of the disaster recovery you must make sure that licenses are correctly assigned to your servers.
Recovery By Creating a New Primary Server

1. Change the Secondary management server from Standby to Active.
2. Install a new Primary server with the same IP address and hostname as the original Primary server.
3. Synchronize the new Primary server with your Active server.
   - Create the active server as an object in the new primary, establish SIC and synchronize the databases.
4. Change the new Primary server to Active server
   - The original Secondary server returns to Standby.
5. Reassign licenses.

Promoting a Secondary Server to Primary

The first management server installed is the Primary Server and all servers installed afterwards are Secondary servers. The Primary server acts as the synchronization master. When the Primary server is down, secondary servers cannot synchronize their databases until a Secondary is promoted to Primary and the initial syncs completes.

To promote a Secondary server to become the Primary server:

1. On the Secondary Server that you will promote, run:
   
   ```bash
   #$FWDIR/bin/promote_util
   #cpstop
   ```

2. Remove the $FWDIR/conf/mgha* files. They contain information about the current Secondary settings. These files will be recreated when you start the Check Point services.

3. Make sure you have a mgmtha license on the newly promoted server.
   - **Note** - All licenses must have the IP address of the promoted Security Management Server.

4. Run cpstart on the promoted server.

5. Open SmartConsole, and:

   a) Make the secondary server active.

   b) Remove all instances of the old Primary Management object. To see all of the instances, right-click the object and select **Where Used**.
      - **Note** - When you remove the old Primary server, all previous licenses are revoked.

   c) Install database.
The ICA Management Tool

The ICA Management Tool lets you:

- Manage certificates
- Run searches
- Recreate CRLs
- Configure the ICA
- Remove expired certificates

**Note**: The ICA management tool supports TLS.

Check Point ICA is fully compliant with X.509 standards for both certificates and CRLs. See the related X.509 and PKI documentation, and RFC 2459 for more information.

**In This Appendix**

- CRL Management .................................................................158
- Using the ICA Management Tool .............................................159
- Enabling and Connecting to the ICA Management Tool ..........159
- The ICA Management Tool GUI .............................................160
- User Certificate Management ................................................160
- Performing Multiple Simultaneous Operations .......................161
- ICA Administrators with Reduced Privileges .........................162
- Management of SIC Certificates .............................................162
- Management of Gateway VPN Certificates ..........................162
- Management of User Certificates in SmartConsole ................162
- Notifying Users about Certificate Initialization ......................162
- Retrieving the ICA Certificate ...............................................162
- Searching for a Certificate ....................................................163
- Removing and Revoking Certificates and Sending Email Notifications 164
- Submitting a Certificate Request to the CA .........................165
- Initializing Multiple Certificates Simultaneously ..................166
- CRL Operations .................................................................167
- CA Cleanup ......................................................................167
- Configuring the CA ............................................................167
- CA Data Types and Attributes ............................................168
- Certificate Longevity and Statuses ......................................171

CRL Management

By default, the CRL is valid for one week. This value can be configured. New 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 using the ICA Management Tool. The utility acts as a recovery mechanism in the event that the CRL is deleted or corrupted. An administrator can download a DER encoded version of the CRL using the ICA Management Tool.

**CRL Modes**

The ICA can issue multiple CRLs. Multiple CRLs prevent one CRL from becoming larger than 10K. If the CRL exceeds 10K, IKE negotiations can fail when trying to open VPN tunnels.

Multiple CRLs are created by attributing each certificate issued to a specified CRL. If revoked, the serial number of the certificate shows in the specified CRL.

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

**Using the ICA Management Tool**

Use the ICA management tool for user certificate operations only, such as certificate creation. Do not use the ICA management tool to change SIC certificates or VPN certificates. Change SIC and VPN certificates in SmartConsole.

To use the ICA management tool, you must first enable it on the Security Management Server.

**Enabling and Connecting to the ICA Management Tool**

The ICA Management Tool is disabled by default.

To enable the ICA Management tool

Run this command on the Security Management Server:

```
cpca_client [-d] set_mgmt_tool on|off [-p <ca_port>] [-a|-u "administrator|user DN" ... ]
```

The command options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Starts the ICA Management Tool (by opening port 18265)</td>
</tr>
<tr>
<td>off</td>
<td>Stops the ICA Management Tool (by closing port 18265)</td>
</tr>
<tr>
<td>-p</td>
<td>Changes the port used to connect to the CA (if the default port is not being used)</td>
</tr>
<tr>
<td>-a &quot;administrator DN&quot; ...</td>
<td>Sets the DNs of the administrators that will be allowed to use the ICA Management Tool</td>
</tr>
<tr>
<td>-u &quot;user DN&quot; ...</td>
<td>Sets the DNs of users allowed to use the ICA Management Tool. An option intended for administrators with limited privileges.</td>
</tr>
</tbody>
</table>

**Note:** If `cpca_client` is run without `-a` or `-u` parameters, the list of the allowed users and administrators remains unchanged.
To Connect to the ICA Management Tool
1. Add the administrator’s certificate to the browser’s certificate repository.
2. Open the ICA Management tool from the browser using this address:
   https://<Management_Host_Name>:18265
   Authenticate when requested.

The ICA Management Tool GUI

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu Pane</td>
</tr>
<tr>
<td></td>
<td>Shows a list of operations</td>
</tr>
<tr>
<td>2</td>
<td>Operations Pane</td>
</tr>
<tr>
<td></td>
<td>Manage certificates. The window divides into <strong>Search attributes configuration</strong> and <strong>Bulk operation configuration</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Create Certificates</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Configure the CA</strong>. Contains configuration parameters You can also view the CA’s time, name, and the version and build number of the Security Management Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Manage CRLs</strong>. Download, publish, and recreate CRLs.</td>
</tr>
<tr>
<td>3</td>
<td>Search Results Pane. The results of the applied operation show in this pane. This window consists of a table with a list of certificates and certificate attributes.</td>
</tr>
</tbody>
</table>

Connect to the ICA Management tool using a browser and HTTPS connection.

**Important**: Before connecting, make sure to add an administrator certificate to the browser’s store.

User Certificate Management

Internally managed User Certificates can be initialized, revoked or have their registrations removed using the ICA Management Tool. User Certificates of users managed on an LDAP server can only be managed using the ICA Management Tool.

This table shows User Certificate attributes that can be configured using the ICA Management Tool.

<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</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>Attributes</td>
<td>Default</td>
<td>Configurable</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------</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>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>yes</td>
<td>Digital signature and Key encipherment</td>
</tr>
<tr>
<td>ExtendedKeyUsage</td>
<td>0 [no KeyUsage]</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

**Modifying the Key Size for User Certificates**

If the user completes the registration from the Remote Access machine, the key size can be configured in the **Advanced Configuration** page in SmartConsole.

**To configure the key size:**

1. From the **Menu**, select **Global Properties**.
2. Open the **SmartConsole Customization** page.
3. In the **Advanced Configuration** section, click **configure**.
   The **Advanced Configuration** window opens.
4. Go to the **Certificates and PKI properties** page.
5. Set the new key size for this property: `user_certs_key_size`.
6. Click **OK**.

You can also change the key size using the GuiDBedit utility. Change the key size as it is listed in `users_certs_key_size` Global Property. The new value is downloaded when you update the site.

**Performing Multiple Simultaneous Operations**

The ICA Management Tool can do multiple operations at the same time. For example:

- Run an LDAP query for the details of all the organization's employees
- Create a file out of this data, and then use this file to:
  - Start (initialize) the creation of certificates for all employees
  - Send a notification about the new certificates to each of those employees

These operations can be done simultaneously:

- Start (initialize) user certificates
- Revoke user certificates
- Send mail to users
- Remove expired certificates
- Remove certificates for which the registration procedure was not completed
ICA Administrators with Reduced Privileges

The ICA Management Tool supports administrators with limited privileges. These administrators cannot execute multiple concurrent operations, and their privileges include only these:

- Basic searches
- Initialization of certificates for new users

Management of SIC Certificates

SIC certificates are managed using SmartConsole.

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.

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

Management of User Certificates in SmartConsole

The user certificates of users that are managed on the internal database are managed using SmartConsole. For more information, see User Certificates in the R80 VPN Administration Guide.

Notifying Users about Certificate Initialization

The ICA Management Tool can be configured to send a notification to users about certificate initialization. To send mail notifications

1. In the Menu pane, click Configure the CA.
2. In the Management Tool Mail Attributes area, configure:
   - The mail server
   - The mail "From" address
   - An optional 'To' address, which can be used if the users' address is not known
     The administrator can use this address to get the certificates on the user's behalf and forward them later.
3. Click Apply.

Retrieving the ICA Certificate

For trust purposes, some gateways and remote clients, such as peer gateways that are not managed by the Security Management Server or clients using Clientless VPN, must retrieve the ICA certificate.
To retrieve the ICA Certificate:

1. Open a browser and enter the applicable URL.
   Use this format:
   `http://<smart_dns_name>:18264`
   The Certificate Services window opens.
2. Use the links to download the CA certificate to your computer or (in Windows) install the CA certification path.

Searching for a Certificate

There are two search options:

- A basic search that includes only the user name, type, status and the serial number
- An advanced search that includes all the search fields (can only be performed by administrators with unlimited privileges)

To do a certificate search:
In the Manage Certificates page, enter the search parameters, and click Search.

Basic Search Parameters

- **User Name** - Username string (by default, this field is empty)
- **Type** - a drop-down list with these options:
  - Any (default)
  - SIC
  - Gateway
  - Internal User or LDAP user
- **Status** - Drop-down list with these options:
  - Any (default)
  - Pending
  - Valid
  - Revoked
  - Expired
  - Renewed (superseded)
- **Serial Number** - Serial number of the requested certificate (by default, this field is empty)

Advanced Search Attributes

In addition to the parameters of the basic search, specify these parameters:

- **Sub DN** - DN substring (by default, this field is empty)
- **Valid From** - Date, from which the certificate is valid, in the format dd-mmm-yyyy [hh:mm:ss]
  (for example 15-Jan-2003) (by default, this field is empty)
- **Valid To** - Date until which the certificate is valid, in 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** - Drop-down list with these options:
  - *Any* [default]
  - *No CRL Distribution Point* (for certificates issued before the management upgrade - old CRL mode certificates)

The list also shows all available CRL numbers.

**The Search Results**

The results of a search show 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)** - The string between the first equals sign ("=") and the next comma (","),
- **DN**
- **Status** - One of these: *Pending*, *Valid*, *Revoked*, *Expired*, *Renewed* (superseded)
- The date from which certificates are valid until the date they expire

**Note**: The status bar shows search statistics after each search.

**Viewing and Saving Certificate Details**

You can view or save the certificate details that show in the search results.

**To view and save certificate details:**

Click on the **DN** link in the **Search Results** pane.

- If the status is *pending*, the certificate information together with the registration key shows, and a log entry is created and shows in SmartView Tracker
- If the certificate was already created, you can save it on a disk or open directly (if the operating system recognizes the file extension)

**Removing and Revoking Certificates and Sending Email Notifications**

1. In the Menu pane, click **Manage Certificates**.
   The results show in the **Search Results** pane.
3. Select the certificates, as needed, and click one of these options:

   - **Revoke Selected** - revokes the selected certificates and removes pending certificates from the CA’s database
   - **Remove Selected** - removes the selected certificates from the CA’s database and from the CRL

   **Note** - You can only remove expired or pending certificates.

   - **Mail to Selected** - sends mail for all selected *pending* certificates
The mail includes the authorization codes. Messages to users that do not have an email defined are sent to a default address. For more, see Notifying Users about Certificate Initialization (on page 162).

## Submitting a Certificate Request to the CA

There are three ways to submit certificate requests to the CA:

- **Initiate** - A registration key is created on the CA and used once by a user to create a certificate
- **Generate** - A certificate file is created and associated with a password which must be entered when the certificate is accessed
- **PKCS#10** - When the CA receives a PKCS#10 request, the certificate is created and delivered to the requester

### To initiate a certificate:

1. In the Menu pane, select **Create Certificates > Initiate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form:
   - **Certificate Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two weeks from the date of creation)
3. Click **Go**.
   A registration key is created and show in the **Results** pane.
   If necessary, click **Send mail to user** to email the registration key. The number of characters in the email is limited to 1900.
4. The certificate becomes usable after entering the correct registration key.

### To generate a certificate:

1. In the Menu pane, select **Create Certificates > Generate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form:
   - **Certificate Expiration Date** - Select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss] (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss] (the default value is two weeks from the date of creation)
3. Enter a password.
4. Click **Go**.
5. Save the P12 file, and supply it to the user.

### To create a PKCS#10 certificate:

1. In the Menu pane, select **Create Certificates > PKCS#10**.
2. Paste into the space the encrypted base-64 buffer text provided.
   You can also click on **Browse for a file to insert (IE only)** to import the request file.
3. Click **Create** and save the created certificate.
4. Supply the certificate to the requester.
Initializing Multiple Certificates Simultaneously

You can initialize a batch of certificates at the same time.

**To initialize several certificates simultaneously:**

1. Create a file with the list of DNs to initialize.
   
   **Note** - There are two ways to create this file - through an LDAP query or a non-LDAP query.

2. In the Menu pain, go to **Create Certificates > Advanced**.

3. Browse to the file you created.
   - To send registration keys to the users, select **Send registration keys via email**
   - To receive a file that lists the initialized DNs with their registration keys, select **Save results to file**

   This file can later be used in a script.

4. Click **Initiate from file**.

**Files created through LDAP Queries**

The file initiated by the LDAP search has this format:

- 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 continues with the mail of the user
  
  If no email is given, the email address will be taken from the ICA’s “Management Tool Mail To Address” attribute.

- If there is a line with the not_after attribute, then the value at the next line is the Certificate Expiration Date
  
  The date is given in seconds from now.

- If there is a line with the is otp_validity attribute, then the value at the next line is the Registration Key Expiration Date.
  
  The date is given in seconds from now.

Here is an example of an LDAP Search output:

```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 109).
Files created through a Simple Non-LDAP Query

It is possible to create a simple (non-LDAP) query by configuring the DN + email in a file using this format:

```
<email address> space <DN>
... blank line as a separator ...
<email address> space <DN>
```

CRL Operations

You can download, update, or recreate CRLs through the ICA management tool.

To do operations with CRLs:
1. In the Menu pane, select **Manage CRLs**.
2. From the drop-down box, select one or more CRLs.
3. Select an action:
   - Click **Download** to download the CRL.
   - Click **Publish** to renew the CRL after changes have been made to the CRL database.
     This operation is done at an interval set by the **CRL Duration** attribute.
   - Click **Recreate** to recreate the CRL.

CA Cleanup

To clean up the CA, you must remove the expired certificates. Before you do that, make sure that the time set on the Security Management Server is correct.

To remove the expired certificates:
In the Menu pane, select **Manage CRLs > Clean the CA's Database and CRLs from expired certificates**.

Configuring the CA

To configure the CA:
1. In the Menu pane, select **Configure the CA**.
2. Edit the CA data values ("CA Data Types and Attributes" on page 168) as necessary.
3. In the **Operations** pane, select an operation:
   - **Apply** - Save and enter the CA configuration settings.
     If the values are valid, the configured settings become immediately effective. All non-valid strings are changed to the default values.
   - **Cancel** - Reset all values to the values in the last saved configuration.
   - **Restore Default** - 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 you click **Configure**. Values that are valid will be changed as requested, and others will change to default values.
CA Data Types and Attributes

The CA data types are:

- **Time** - displayed in the format: `<number> days <number> seconds`, for example: CRL Duration: 7 days 0 seconds
  
  You can enter the values in the format in which they are displayed (`<number> days <number> seconds`) or as a 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** - an alphanumeric string, for example: Management Tool DN prefix: cn=tests

These are the CA attributes, 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>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>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 Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459.</td>
<td></td>
<td>Digital signature and Key encipherment</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></td>
<td>ou=users</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</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>max-2 months</td>
<td></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>Management Tool Mail Subject</td>
<td>The email subject field.</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>
</tbody>
</table>
| **Management Tool Mail Text Format** | 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). |                       | Registration Key: $REG_KEY  
Expiration: $EXPIRE |
| **Management Tool Mail To address** | When the send mail option is used, the emails to users that have no email address defined will be sent to this address. |                       | -             |
| **Max Certificates Per Distribution Point** | The maximum capacity of a CRL in the new CRL mode. | min-3 max-400         | 400           |
| **New CRL Mode** | A Boolean value describing the CRL mode. | 0 for old CRL mode  
1 for new mode | true           |
| **Number of certificates per search page** | The number of certificates that will be displayed in each page of the search window. | min-1 max-approx 700 | approx 700 |
| **Number of Digits for Serial Number** | The number of digits of certificate serial numbers. | min-5 max-10          | 5             |
| **Revoke renewed certificates** | 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. | true or false         | true          |
| **SIC Key Size** | The key size in bits of keys used in SIC. | possible values:  
1024  
2048  
4096 | 1024           |
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Comment</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<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>Digital signature and Key encipherment</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>means no KeyUsage</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 1024, 2048, 4096</td>
<td>1024</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>Digital signature and Key encipherment</td>
</tr>
</tbody>
</table>

**Certificate Longevity and Statuses**

Certificates issued by the ICA have a defined validity period. When period ends, the certificate expires.

SIC certificates, VPN certificates for Security Gateways and User certificates can be created in one step in SmartConsole. User certificates can also be created in two steps using SmartConsole or the ICA Management Tool. The two steps are:

- Initialization – during this step a registration code is created for the user. When this is done, the certificate status is **pending**.
- Registration – when the user completes the registration procedure in the remote client. After entering 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.

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

If a user does not complete the registration procedure in a given period (two weeks by default), the registration code is automatically removed. An administrator can remove the registration key before the user completes the registration procedure. 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. A PKCS12 certificate can also be set to renew 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 revoke old user certificates.

One more 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. After 3.75 years, 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 revoke the old certificate automatically or after a set period of time. By default, the old certificate is revoked one week after certificate renewal.