Important Information

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

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

**Latest Version of this Document**
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=54842.
To learn more, visit the Check Point Support Center https://supportcenter.checkpoint.com.

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

**Searching in Multiple PDFs**
To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package http://downloads.checkpoint.com/dc/download.htm?ID=54846.
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>28 April 2019</td>
<td>Updated Sharing Layers [on page 83]</td>
</tr>
<tr>
<td></td>
<td>Updated: The High Availability Environment [on page 225]</td>
</tr>
<tr>
<td>27 November 2018</td>
<td>Updated High Availability Disaster Recovery [on page 230]</td>
</tr>
<tr>
<td>23 October 2018</td>
<td>Updated Security Management Server Commands [on page 246]</td>
</tr>
<tr>
<td></td>
<td>Updated Initializing Trust [on page 43]</td>
</tr>
<tr>
<td>07 August 2018</td>
<td>Updated cplic [on page 257]</td>
</tr>
<tr>
<td>14 May 2018</td>
<td>Updated Restricting Administrator Login Attempts [on page 36]</td>
</tr>
<tr>
<td></td>
<td>Updated Unlocking Administrators [on page 36]</td>
</tr>
<tr>
<td></td>
<td>Improved formatting and document layout</td>
</tr>
<tr>
<td>11 December 2017</td>
<td>Added Security Management Server Commands [on page 246]</td>
</tr>
<tr>
<td></td>
<td>Added: Cannot have two network objects with the same name [on page 52]</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>16 May 2017</td>
<td>First release of this document</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Compliance Check</td>
<td>142</td>
</tr>
<tr>
<td>Secure Workspace</td>
<td>144</td>
</tr>
<tr>
<td>To Learn More About Mobile Access</td>
<td>144</td>
</tr>
<tr>
<td>Creating a Threat Prevention Policy</td>
<td>145</td>
</tr>
<tr>
<td>Threat Prevention Components</td>
<td>145</td>
</tr>
<tr>
<td>IPS</td>
<td>146</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>147</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>148</td>
</tr>
<tr>
<td>SandBlast</td>
<td>149</td>
</tr>
<tr>
<td>Assigning Administrators for Threat Prevention</td>
<td>151</td>
</tr>
<tr>
<td>Analyzing Threats</td>
<td>151</td>
</tr>
<tr>
<td>Out-of-the-Box Protection from Threats</td>
<td>152</td>
</tr>
<tr>
<td>Getting Quickly Up and Running with the Threat Prevention Policy</td>
<td>152</td>
</tr>
<tr>
<td>Enabling the Threat Prevention Software Blades</td>
<td>152</td>
</tr>
<tr>
<td>Installing the Threat Prevention Policy</td>
<td>155</td>
</tr>
<tr>
<td>Introducing Profiles</td>
<td>155</td>
</tr>
<tr>
<td>Optimized Protection Profile Settings</td>
<td>156</td>
</tr>
<tr>
<td>Predefined Rule</td>
<td>157</td>
</tr>
<tr>
<td>The Threat Prevention Policy</td>
<td>158</td>
</tr>
<tr>
<td>Workflow for Creating a Threat Prevention Policy</td>
<td>158</td>
</tr>
<tr>
<td>Threat Prevention Policy Layers</td>
<td>158</td>
</tr>
<tr>
<td>Threat Prevention Rule Base</td>
<td>160</td>
</tr>
<tr>
<td>Creating Threat Prevention Rules</td>
<td>161</td>
</tr>
<tr>
<td>Configuring IPS Profile Settings</td>
<td>161</td>
</tr>
<tr>
<td>Blocking Viruses</td>
<td>162</td>
</tr>
<tr>
<td>Configuring Anti-Bot Settings</td>
<td>163</td>
</tr>
<tr>
<td>Configuring Threat Emulation Settings</td>
<td>165</td>
</tr>
<tr>
<td>Configuring Threat Extraction Settings</td>
<td>169</td>
</tr>
<tr>
<td>Configuring a Malware DNS Trap</td>
<td>169</td>
</tr>
<tr>
<td>Exception Rules</td>
<td>170</td>
</tr>
<tr>
<td>The Check Point ThreatCloud</td>
<td>172</td>
</tr>
<tr>
<td>Updating IPS Protections</td>
<td>173</td>
</tr>
<tr>
<td>Scheduling Updates</td>
<td>173</td>
</tr>
<tr>
<td>Updating Threat Emulation</td>
<td>174</td>
</tr>
<tr>
<td>To Learn More About Threat Prevention</td>
<td>174</td>
</tr>
<tr>
<td>Managing User Accounts</td>
<td>175</td>
</tr>
<tr>
<td>Authentication Methods for Users and Administrators</td>
<td>175</td>
</tr>
<tr>
<td>Check Point Password</td>
<td>175</td>
</tr>
<tr>
<td>Operating System Password</td>
<td>175</td>
</tr>
<tr>
<td>RADIUS</td>
<td>175</td>
</tr>
<tr>
<td>SecurID</td>
<td>176</td>
</tr>
<tr>
<td>TACACS</td>
<td>176</td>
</tr>
<tr>
<td>Configuring Authentication Methods for Users</td>
<td>176</td>
</tr>
<tr>
<td>Granting User Access Using RADIUS Server Groups</td>
<td>176</td>
</tr>
<tr>
<td>Configuring a Security Gateway to use SecurID Authentication</td>
<td>177</td>
</tr>
<tr>
<td>Configuring TACACS+ Authentication</td>
<td>179</td>
</tr>
<tr>
<td>User Database</td>
<td>180</td>
</tr>
<tr>
<td>Creating, Modifying, Removing User Accounts</td>
<td>180</td>
</tr>
<tr>
<td>Configuring Default Expiration Settings for Users</td>
<td>182</td>
</tr>
<tr>
<td>Delete a User</td>
<td>183</td>
</tr>
<tr>
<td>Managing User Groups</td>
<td>183</td>
</tr>
<tr>
<td>Adding User Groups</td>
<td>183</td>
</tr>
</tbody>
</table>
The ICA Management Tool GUI................................................................. 233
User Certificate Management ............................................................... 234
  Modifying the Key Size for User Certificates ........................................... 234
Performing Multiple Simultaneous Operations ........................................... 235
ICA Administrators with Reduced Privileges .............................................. 235
Management of SIC Certificates............................................................... 235
Management of Gateway VPN Certificates ................................................. 235
Management of User Certificates in SmartConsole .................................... 236
Notifying Users about Certificate Initialization .......................................... 236
Retrieving the ICA Certificate ................................................................. 236
Searching for a Certificate ..................................................................... 236
  Basic Search Parameters ........................................................................... 237
  Advanced Search Attributes ....................................................................... 237
  The Search Results.................................................................................... 237
  Viewing and Saving Certificate Details....................................................... 238
Submitting a Certificate Request to the CA.............................................. 238
Initializing Multiple Certificates Simultaneously ....................................... 239
CRL Management.................................................................................... 240
CRL Operations ...................................................................................... 240
CA Cleanup.............................................................................................. 241
Configuring the CA ................................................................................ 241
CA Data Types and Attributes..................................................................... 241
Certificate Longevity and Statuses............................................................. 244
Security Management Server Commands.................................................. 246
  cpca_client ............................................................................................. 246
    cpca_client revoke_cert........................................................................ 246
    cpca_client lscert ................................................................................. 247
    cpca_client init_certs .......................................................................... 247
    cpca_client set_mgmt_tool .................................................................. 248
    cpca_client set_sign_hash .................................................................. 248
    cpca_client search .............................................................................. 248
    cpca_client get_crlkp......................................................................... 249
    cpca_client get_pubkey ........................................................................ 249
    cpca_client double_sign ...................................................................... 250
  cp_conf .................................................................................................... 250
    cp_conf admin .................................................................................... 252
    cp_conf ca .......................................................................................... 252
    cp_conf finger .................................................................................... 252
    cp_conf lic ......................................................................................... 253
    cp_conf client .................................................................................... 253
    cp_conf snmp ..................................................................................... 254
    cp_conf auto ....................................................................................... 254
  cpconfig ............................................................................................... 255
  cpinfo .................................................................................................... 256
  cplic ...................................................................................................... 257
    cplic check ......................................................................................... 258
    cplic db_add ....................................................................................... 259
    cplic db_print ..................................................................................... 260
    cplic db_rm ......................................................................................... 261
    cplic del ............................................................................................. 262
Terms

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

**DAIP Gateway**
A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the IP address of the external interface is assigned dynamically by the ISP.

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

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

**Security Management Server**
A computer that runs Check Point software to manage the objects and policies in Check Point environment.

**SIC**
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

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

**SmartDashboard**
A legacy Check Point GUI client used to create and manage the security policy in R77.30 and below.
**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 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.
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 R80.10 Multi-Domain Server Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54841.

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

In This Section:

Understanding SmartConsole ................................................................. 15
Connecting to the Security Management Server through SmartConsole .... 23
Setting Up for Security Management ...................................................... 24
Setting up for Team Work ....................................................................... 25
Managing Security through API and CLI ................................................. 25
Planning Security Management ............................................................... 27

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 cyber security environment and policies, become familiar with Check Point SmartConsole.

SmartConsole
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Global Toolbar</td>
</tr>
<tr>
<td>2</td>
<td>Session Management Toolbar</td>
</tr>
<tr>
<td>3</td>
<td>Navigation Toolbar</td>
</tr>
<tr>
<td>4</td>
<td>System Information Area</td>
</tr>
<tr>
<td>5</td>
<td>Objects Bar (F11)</td>
</tr>
<tr>
<td>6</td>
<td>Validations pane</td>
</tr>
<tr>
<td>7</td>
<td>Command line interface button</td>
</tr>
</tbody>
</table>

---

Security Management Administration Guide R80.10 (Part of Check Point Infinity) | 16
## SmartConsole Toolbars

### Global Toolbar (top of SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The main SmartConsole Menu. When SmartConsole is connected to a Security Management Server, this includes:</td>
</tr>
<tr>
<td>- Manage policies and 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 Access Control Policy</td>
</tr>
<tr>
<td>- Install Database</td>
</tr>
<tr>
<td>- Uninstall Threat Prevention 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new objects or open the Object Explorer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install policy on managed gateways</td>
</tr>
</tbody>
</table>

### 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter session details and see the number of changes made in the session.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish changes, to make them visible to other administrators, and ready to install on gateways.</td>
</tr>
</tbody>
</table>

**Note** - When the policy is installed, published changes are installed on the gateways and enforced.
### Navigation Toolbar (left side of SmartConsole)

<table>
<thead>
<tr>
<th>Keyboard Shortcut</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ctrl+1            | Gateways & Servers 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 Access Control: Content Awareness, VPN, Application & URL Filtering, and Mobile Access  
|                   | • Edit multiple policies at the same time  
|                   | • Add, edit, or delete NAT rules  
|                   | • Use the Access Tools  
|                   | Security Policies Threat Prevention view:  
|                   | • Manage Threat Prevention: IPS, Anti-Bot, Anti-Virus, Threat Emulation  
|                   | • Edit the unified threat Rule Base  
|                   | • Configure threat profiles  
|                   | • Add, edit, or delete exceptions and exception groups  
|                   | • Use the Threat Tools  
|                   | Shared Policies Views:  
|                   | • Manage Mobile Access, DLP, Geo Policy and inspection Settings  |
| 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>
</table>
| Ctrl+4           | Manage & Settings view - review and configure the Security Management Server settings:  
                  • Administrators  
                  • Permissions profiles  
                  • Trusted clients  
                  • Administrator sessions, and session settings  
                  • Blades  
                  • Revisions  
                  • Preferences  
                  • Sync with User Center |

**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>

**Objects Bar (right side of SmartConsole)**

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

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

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

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

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
<td>See management tasks in progress and expand to see recent tasks</td>
</tr>
<tr>
<td>Server Details</td>
<td>See the IP address of the server to which SmartConsole is connected. If Management High Availability is configured, click to see the details.</td>
</tr>
<tr>
<td>Session Status</td>
<td>See the number of changes made in the session and the session status.</td>
</tr>
<tr>
<td>Connected administrators</td>
<td>See connected administrators: Yourself and others.</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

**IP Search**

You can run an advanced search for an IP address, network, or port. It returns direct and indirect matches for your search criteria.

- IP address: xxx.xxx.xxx.xxx
- Network: xxx.xxx.0/16 or xxx.xxx
- Port: svc:<xxx>

These are the different IP search modes:

- **General** – (Default). Returns direct matched results and indirect results in IP ranges, networks, groups, groups with exclusion, and rules that contain these objects.
- **Packet** – Matches rules as if a packet with your IP address arrives at the gateway.

**General IP Search**

This is the default search mode. Use it to search in Rule Bases and in objects. If you enter a string that is not a valid IP or network, the search engine treats it as text.

When you enter a valid IP address or network, an advanced search is done and on these objects and rules:

- Objects that have the IP address as a text value for example, in a comment
- Objects that have an IP address property (direct results)
- Groups, networks, and address ranges that contain objects with the text value or address value
- Rules that contain those objects

**Packet Search**

A Packet Search matches rules as if a packet with your IP address arrives at the gateway. It matches rules that have:

- The IP address in a column of the rule
- “Any”
- A Group-with-exclusion or negated field with the IP address in its declaration

**To run a Packet Search:**

1. Click the search box.
   The search window opens.
2. Click Packet or enter: “mode:Packet”
3. To search a specific rule column, enter: `ColumnName:Criteria`
Rule Base Results

When you enter search criteria and view the matched results, the value that matched the criteria in a rule is highlighted.

<table>
<thead>
<tr>
<th>If there is...</th>
<th>This is highlighted</th>
</tr>
</thead>
<tbody>
<tr>
<td>A direct match on an object name</td>
<td>Only the specific matched characters</td>
</tr>
<tr>
<td>name or on textual columns</td>
<td></td>
</tr>
<tr>
<td>A direct match on object properties</td>
<td>The entire object name</td>
</tr>
<tr>
<td>A negated column</td>
<td>The negated label</td>
</tr>
<tr>
<td>A match on &quot;Any&quot;</td>
<td>&quot;Any&quot;</td>
</tr>
</tbody>
</table>

Known Limitation:
- Packet search does not support IPv6.

Access and Threat 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 &amp; URL Filtering database, schedule updates, 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 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 Database, to use Check Point security research in your policy rules for actions 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 changes. See the revisions that were made during each installation, and who made them. Install 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>
<tr>
<td>Indicators</td>
<td>Configure indicators of malicious activity and how to handle it</td>
</tr>
</tbody>
</table>
### Tool | Description
--- | ---
**Updates** | Configure updates to the Malware database, Threat Emulation engine and images, and the IPS database.
**UserCheck** | Configure UserCheck interaction objects for Threat Prevention policy actions.
**Threat Wiki** | 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.
**Installation History** | See the Policy installation history for each Gateway, and who made the changes. See the revisions that were made during each installation, and who made them. Install a specific version of the Policy.

### Shared Policies

The **Shared Policies** section in the **Security Policies** shows the policies that are not in a Policy package. They are shared between all Policy packages.

Shared policies are installed with the Access Control Policy.

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Description</th>
</tr>
</thead>
</table>
**Mobile Access** | Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile. |
**DLP** | 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. |
**Geo Policy** | Create a policy for traffic to or from specific geographical or political locations. |
**HTTPS Inspection** | The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. The HTTPS Policy shows if HTTPS inspection is enabled on one or more Gateways. To learn more about HTTPS Inspection, see the [R80.10 Next Generation Security Gateway Guide](http://downloads.checkpoint.com/dc/download.htm?ID=54806). |
**Inspection Settings** | You can configure Inspection Settings [on page 222](#) for the Firewall:  
  - Deep packet inspection settings  
  - Protocol parsing inspection settings  
  - VoIP packet inspection settings |

### API Command Line Interface

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

Click to open the API reference (in the command line interface).

Use 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 (on page 25).

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. When installing the Security Management Server, you create one administrator in the First Time Configuration Wizard. After that, you can create additional administrators accounts with SmartConsole, or using the Gaia Portal.

To log in to the Security Management Server through SmartConsole:

1. Launch the SmartConsole application.
2. Enter your administrator authentication credentials. These can be a username, or a certificate file, or a CAPI certificate.
   
   **Logging in with a username:**
   - Enter the Username and Password.
   
   **Logging in with a certificate file:**
   - From the drop-down list, select Certificate File.
   - Browse to the file.
   - Enter the password of the certificate file.
   
   **Logging in with a certificate in the CAPI repository:**
   - From the drop-down list, select CAPI Certificate.
   - Select the certificate from drop-down list.
3. Enter the name or the IP address of the Security Management Server.
4. Click Login.
   
   The SmartConsole authenticates the Security Management Server. The first time you connect, SmartConsole shows the fingerprint.
5. Confirm the fingerprint.

The fingerprint and the IP address of the Security Management Server are saved to the user settings in Windows.
Setting Up for Security Management


To configure the Security Management Server in SmartConsole:

1. In the Gateways & Servers view, 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 view. 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. This is automatically enabled.
   - **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 Logging** - Add user identities, and data of their computers and devices, from Active Directory domains, to log entries.
   - **User Directory** - Populate your security scope with user accounts from the LDAP servers in your environment.
   - **Compliance** - Optimize your security settings and comply with regulatory requirements
   - **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 (on page 42)
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 (on page 28) 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 Management Server with the new command line tools and through web services. You must first configure the API server.

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

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

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

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

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


Configuring the API Server

To configure the API Server:

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

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 cyber 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 (on page 53) in SmartConsole.

Define users and user groups that your security environment protects

You can add users (on page 180) and groups (on page 183) to the database manually, through LDAP and User Directory (on page 184), or with the help of Active Directory (on page 202).

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 (on page 61) 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 an Administrator Account ..................................................... 28
Creating a Certificate for Logging in to SmartConsole .............................................. 29
Configuring Default Expiration for Administrators .................................................... 30
Setting SmartConsole Timeout .................................................................................... 30
Deleting an Administrator ............................................................................................ 31
Revoking Administrator Certificate ............................................................................. 31
Assigning Permission Profiles to Administrators ....................................................... 31
Defining Trusted Clients ............................................................................................... 35
Restricting Administrator Login Attempts .................................................................... 36
Unlocking Administrators ............................................................................................. 36
Administrator Collaboration ......................................................................................... 37
Configuring Authentication Methods for Administrators ............................................ 38

Creating and Changing an Administrator Account

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

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

If you create it through the SmartConsole, you can choose one of these authentication methods:

- Check Point Password (on page 175)
- OS Password (on page 175)
- RADIUS (on page 175)
- SecurID (on page 176)
- TACACS (on page 176)

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.
   To define an Authentication Method:
   In the Authentication Method section, select a method and follow the instructions in Configuring Authentication Methods for Administrators (on page 38).
Managing Administrator Accounts

To create a Certificate - If you want to use a certificate to log in:
In the Certificate Information section, click Create, and follow the instructions in Configuring Certificates for Administrators (on page 29).

5. Select a Permissions profile for this administrator, or create a new one (on page 31).

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 (on page 182). 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.

Creating an administrator with cpconfig

We do not recommend creating an administrator with cpconfig, the Check Point Configuration Tool. Use it only if there is no access to SmartConsole or the Gaia Portal. If you use cpconfig to create an administrator:

• You must restart Check Point Services to activate the administrator.
• It does not show the other administrators
• Check Point Password is automatically configured as the authentication method.

Creating a Certificate for Logging in to SmartConsole

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

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

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

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

To create a certificate file:

1. In the New Administrator window, in the Certificate Information section, click Create.
2. Enter a password.
3. Click OK.
4. Save the certificate file to a secure location on the SmartConsole computer. The certificate file is in the PKCS #12 format, and has a .p12 extension.

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

To Import the certificate file to the CAPI repository:

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

**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**.

**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, but all changes are preserved.
Deleting an Administrator

To make sure your environment is secure, the best practice is 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 the certificate. However, if the account has an additional authentication method (a password, for example), that method can be used to authenticate to the account.

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 Security Management Server administrators with the Manage Administrators permission in the profile can create and manage permission profiles.


Changing and Creating Permission Profiles

Administrators with Super User permissions can edit, create, or delete permission profiles.

These are the predefined, default permission profiles. You cannot change or delete the default permission profiles. You can clone them, and change the clones:

- **Read Only All** - Full Read Permissions. No Write permissions.
- **Read Write All** - Full Read and Write Permissions.
- **Super User** - Full Read and Write Permissions, including managing administrators and sessions.
To change the permission profile of an administrator:
1. Click Manage & Settings > Permissions and Administrators.
2. Double-click the administrator account.
   The Administrators properties window opens.
3. In the Permissions section, select another Permission Profile from the list.
4. 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 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 to all features
   - Auditor (Read Only All) - Administrators can see all information but cannot make changes
   - Customized - Configure custom settings (on page 32)
5. Click OK.

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

Permissions:
- Selected - The administrator has this feature.
- Not selected - The administrator does not have this feature.
  Note - If you cannot clear a feature selection, the administrator access to it is mandatory.
Some features have Read and Write Options. If the feature is selected:

- **Read** - The administrator has the feature but cannot make changes.
- **Write** - The administrator has the feature and can make changes.

**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 (on page 34).
   - **Threat Prevention** - configure Threat Prevention Policy permissions (on page 34).
   - **Others** - configure permissions for Common Objects, user databases, HTTPS Inspection features, and Client Certificates.
   - **Monitoring and Logging** - configure permissions to generate and see logs and to use monitoring features (on page 34).
   - **Events and Reports** - configure permissions for SmartEvent features (on page 34).
3. In the Management section, configure this profile with permissions to:
   - **Manage Administrators** - Manage other administrator accounts.
   - **Manage Sessions** - Lets the administrator configure the session management settings (single or multiple sessions)
   - the session mode for single or multiple sessions
   - **High Availability Operations** - Configure and work with High Availability.
   - **Management API Login** - Log in with the management API.
4. Click OK.

**Configuring Permissions for Access Control Layers**

You can simplify the management of the Access Control Policy by delegating ownership of different Layers to different administrators.

To do this, assign a permission profile to the Layer. The permission Profile must have this permission: **Edit Layer by the selected profiles in a layer editor**.

An administrator that has a permission profile with this permission can manage the Layer.

**Workflow:**

1. Give Layer permissions to an administrator profile.
2. Assign the permission profile to the Layer.

**To give Layer permissions to an administrator profile:**

1. In the Profile object, in the Access Control > Policy section, select Edit Layer by the selected profiles in a layer editor.
2. Click OK.

**To assign a permission profile to a Layer:**

1. In SmartConsole, click Menu > Manage policies and layers.
2. In the left pane, click Layers.
3. Select a Layer.
4. Click Edit.
5. In the left pane, select Permissions.
6. Click +
7. Select a profile with Layer permissions.
8. Click OK.
9. Click Close.
10. Publish the session.

Configuring 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
  - Application & URL Filtering Update - Download and install new packages of applications and websites, to use in access rules.

Threat Prevention

- Actions
  - IPS Update - Download and install new packages for IPS protections.

Configuring 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 SmartEvent:

- SmartEvent
  - Events - views in SmartConsole > Logs & Monitor
  - Policy - Events correlation on the Policy tab
  - Reports - in SmartConsole > Logs & Monitor
- SmartEvent Application & 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, 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.
4. Click OK.

To delete a trusted client:
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.

Restricting Administrator Login Attempts
For administrators that login to the Security Management Server using a Check Point password, you can configure these login restrictions:

- The number of login attempts before SmartConsole automatically locks an administrator.
- The number of minutes before SmartConsole unlocks the administrator’s account after it was locked.

To configure login restrictions:
1. Go to the Manage & Settings view or to the Multi-Domain view.
2. Go to Permissions & Administrators > Advanced > Login Restrictions.

Note - these restrictions apply only to administrators that authenticate to the Security Management Server using a Check Point password.

Unlocking Administrators
An administrator who has the Manage Administrators permission can unlock another administrator if the locked administrator authenticates to the Security Management Server using a Check Point password.

To unlock an administrator:
1. Go to the Manage & Settings view or to the Multi-Domain view.
2. Right-click the locked administrator and select Unlock Administrator.

Or:


Note - the Unlock Administrator feature does not apply to administrators using other authentication methods.
Administrator Collaboration

Multiple administrators can work with SmartConsole on the same Security Management Server with the same policies at the same time. To avoid configuration conflicts, 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. Changes are saved automatically.

Usually, an administrator will make changes to the policy in a private session and publish the changes when finished.

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 in the current session. You cannot install a policy if the included changes in the session are not published. Unpublished changes from other sessions will not be included in the policy installation.

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

There is no need to save changes when working on a session. Changes are saved automatically. You can exit SmartConsole without publishing your changes from the session. 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.

To add a name or description 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. Click OK.

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.

Working with Sessions

You can see information about the SmartConsole sessions that are connected to the Security Management Server.
When an administrator changes objects, they are saved and locked. Another administrator with Manage Sessions permissions can unlock the changed objects, by publishing, or discarding the session. This allows other administrators to work with those objects. You can also publish, discard, or take over sessions that are disconnected. Disconnecting a session does not unlock the locked objects.

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

To unlock a session that is locked by another administrator:
- To make the changes available to all administrators, 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.
- To take over a session of another administrator, and disconnect the other administrator’s SmartConsole session: right-click the session and select Take over.

Note - Publish your changes before you take over a session of another administrator, if you want to keep them. Otherwise, you lose those changes.

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 176).

For background information about the authentication methods, see Authentication Methods for Users and Administrators (on page 175).

Configuring Check Point Password Authentication for Administrators

These instructions show how to configure Check Point Password (on page 175) 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 (on page 175) 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 (on page 175) 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.
   g) Click Publish.
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 [on page 176] 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 176) 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.
   g) Click Publish.
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 ................................................................. 42
Updating the Gateway Topology ................................................................. 43
Secure Internal Communication (SIC) .......................................................... 43
Managing Software Blade Licenses .............................................................. 46

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 (on page 43).
   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. This is necessary for SIC to succeed. To set the time settings of the gateway and Security Management Server, go to the **Gaia Portal > System Management > Time**.

**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 of the gateway.
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 hosts 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.

1. In SmartConsole, open the **General Properties** window of the gateway.
2. Click **Communication**.
3. In the **Trusted Communication** window that opens, click **Reset**.
4. **Install Policy** on the gateways.
   - 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 in SmartConsole, make sure the same one-time activation password is configured on the gateway.

**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 gateway.
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.
Managing Gateways

- **SmartConsole** - SIC certificates for Security Gateways and administrators, VPN certificates, and user certificates.
- **ICA Management tool** - VPN certificates for users and advanced ICA operations (on page 232).

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 (on page 234).

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).

**Managing Software Blade Licenses**

After an administrator runs the First Time Configuration Wizard on a 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 a Security Management Server in the Check Point User Center, these changes are automatically synchronized with that Security Management Server.

**Notes:**

- Automatic activation is supported on Check Point appliances only.
- Automatic synchronization is supported on all R80.10 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 a 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 **R80.10 Release Notes** for a list of supported Software Blades
Configuring a Proxy gateway

To configure a proxy on a 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 in SmartConsole

To view license information:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In SmartConsole, from the left navigation panel, click Gateways &amp; Servers.</td>
</tr>
<tr>
<td>2</td>
<td>From the Columns drop-down list, select Licenses.</td>
</tr>
</tbody>
</table>

You can see these columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Status</td>
<td>The general state of the Software Blade licenses:</td>
</tr>
<tr>
<td></td>
<td>• <strong>OK</strong> - All the blade licenses are valid.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Activated</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Error with &lt;number&gt; blade(s)</strong> - The specified number of blade licenses are not installed or not valid.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Warning with &lt;number&gt; blade(s)</strong> - The specified number of blade licenses have warnings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>N/A</strong> - No available information.</td>
</tr>
<tr>
<td>CK</td>
<td>Unique Certificate Key of the license instance.</td>
</tr>
<tr>
<td>SKU</td>
<td>Catalog ID from the Check Point User Center.</td>
</tr>
<tr>
<td>Account ID</td>
<td>User’s account ID.</td>
</tr>
<tr>
<td>Support Level</td>
<td>Check Point level of support.</td>
</tr>
<tr>
<td>Support Expiration</td>
<td>Date when the Check Point support contract expires.</td>
</tr>
</tbody>
</table>

To view license information for each Software Blade:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select a Security Gateway or a Security Management Server.</td>
</tr>
</tbody>
</table>
2. In the **Summary** tab below, click the object’s **License Status** (for example: **OK**).

The **Device & License Information** 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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td>The Software Blade is active and the license is valid.</td>
</tr>
<tr>
<td><strong>Available</strong></td>
<td>The Software Blade is not active, but the license is valid.</td>
</tr>
<tr>
<td><strong>No License</strong></td>
<td>The Software Blade is active but the license is not valid.</td>
</tr>
<tr>
<td><strong>Expired</strong></td>
<td>The Software Blade is active, but the license expired.</td>
</tr>
<tr>
<td><strong>About to Expire</strong></td>
<td>The Software Blade is active, but the license will expire in thirty days (default) or less (7 days or less for an evaluation license).</td>
</tr>
<tr>
<td><strong>Quota Exceeded</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Quota Warning</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>N/A</strong></td>
<td>The license information is not available.</td>
</tr>
</tbody>
</table>
Monitoring Licenses in SmartConsole

To keep track of license issues, you can use these options:

- **License Status** view - To see and export license information for Software Blades on each specific Security Management Server, gateway, or Log Server object.
- **License Status** report - To see, filter and export license status information for all configured Security Management Server, gateway, or Log Server objects.
- **License Inventory** report - To see, filter and export license information for Software Blades on all configured Security Management Server, gateway, or Log Server objects.

The SmartEvent Software Blade lets you customize the **License Status** and **License Inventory** information from the **Logs & Monitor** view of SmartConsole.

It is also possible to view license information from the **Gateways & Servers** view of SmartConsole without enabling the SmartEvent blade on Security Management Server.

The **Gateways & Servers** view in SmartConsole lets you see and export the **License Inventory** report.

1. **To see the License Inventory report from the Gateways & Servers view:**
   a) In SmartConsole, from the left Navigation Toolbar, click **Gateways & Servers**.
   b) From the top toolbar, click Actions > License Report.
   c) Wait for the **SmartView** to load and show this report.
   
   By default, this report contains:
   - **Inventory** page: Blade Names, Devices Names, License Statuses
   - **License by Device** page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date

2. **To export the License Inventory report from the Gateways & Servers view:**
   a) In the top right corner, click the **Options** button.
   b) Select the applicable export option - Export to Excel, or Export to PDF.

The **Logs & Monitor** view in SmartConsole lets you see, filter and export the **License Status** report.

1. **To see the License Status report from the Logs & Monitor view:**
   a) In SmartConsole, from the left Navigation Toolbar, click **Logs & Monitor**
   b) At the top, open a new tab by clicking New Tab, or [+].
   c) In the left section, click Views.
   d) In the list of reports, double-click **License Status**.
   e) Wait for the **SmartView** to load and show this report.
   
   By default, this report contains:
   - Names of the configured objects, License status for each object, CK, SKU, Account ID, Support Level, Next Expiration Date

2. **To filter the License Status report in the Logs & Monitor view:**
   a) In the top right corner, click the Options button > View Filter.
Managing Gateways

The Edit View Filter window opens.

b) Select a Field to filter results. For example, Device Name, License Status, Account ID.

c) Select the logical operator - Equals, Not Equals, or Contains.

d) Select or enter a filter value.

Note - Click the X icon to delete a filter.

e) Optional: Click the + icon to configure additional filters.

f) Click OK to apply the configured filters.

The report is filtered based on the configured filters.

3. To export the License Status report in the Logs & Monitor view:

   a) In the top right corner, click the Options button.

   b) Select the applicable export option - Export to Excel, or Export to PDF.

The Logs & Monitor view in SmartConsole lets you see, filter and export the License Inventory report.

1. To see the License Inventory report from the Logs & Monitor view:

   a) In SmartConsole, from the left Navigation Toolbar, click Logs & Monitor

   b) At the top, open a new tab by clicking New Tab, or [+].

   c) In the left section, click Reports.

   d) In the list of reports, double-click License Inventory.

   e) Wait for the SmartView to load and show this report.

   By default, this report contains:

   • Inventory page: Blade Names, Devices Names, License Statuses
   • License by Device page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date

2. To filter the License Inventory report in the Logs & Monitor view:

   a) In the top right corner, click the Options button > Report Filter.

   The Edit Report Filter window opens.

   b) Select a Field to filter results. For example, Blade Name, Device Name, License Overall Status, Account ID.

   c) Select the logical operator - Equals, Not Equals, or Contains.

   d) Select or enter a filter value.

   Note - Click the X icon to delete a filter.

   e) Optional: Click the + icon to configure additional filters.

   f) Click OK to apply the configured filters.

   The report is filtered based on the configured filters.

3. To export the License Inventory report in the Logs & Monitor view:

   a) In the top right corner, click the Options button.

   b) Select the applicable export option - Export to Excel, or Export to PDF.
Managing Objects

In This Section:

Object Categories .......................................................................................................................... 51
Adding, Editing, Cloning, Deleting, and Replacing Objects .......................................................... 52
Object Tags ....................................................................................................................................... 52
Network Object Types ................................................................................................................... 53

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><img src="image" alt="Network Objects" /></td>
<td>Network Objects</td>
<td>Gateways, hosts, networks, address ranges, dynamic objects, security zones</td>
</tr>
<tr>
<td><img src="image" alt="Services" /></td>
<td>Services</td>
<td>Services, Service groups</td>
</tr>
<tr>
<td><img src="image" alt="Custom Applications/Sites" /></td>
<td>Custom Applications/Sites</td>
<td>Applications, Categories, Mobile applications</td>
</tr>
<tr>
<td><img src="image" alt="VPN Communities" /></td>
<td>VPN Communities</td>
<td>Site to Site or Remote Access communities</td>
</tr>
<tr>
<td><img src="image" alt="Users" /></td>
<td>Users</td>
<td>Users, user groups, and user templates</td>
</tr>
<tr>
<td><img src="image" alt="Data Types" /></td>
<td>Data Types</td>
<td>International Bank Account Number - IBAN, HIPAA - Medical Record Number - MRN, Source Code.</td>
</tr>
<tr>
<td><img src="image" alt="Servers" /></td>
<td>Servers</td>
<td>Trusted Certificate Authorities, RADIUS, TACACS</td>
</tr>
<tr>
<td><img src="image" alt="Time Objects" /></td>
<td>Time Objects</td>
<td>Time, Time groups</td>
</tr>
<tr>
<td><img src="image" alt="UserCheck Interactions" /></td>
<td>UserCheck Interactions</td>
<td>Message windows: Ask, Cancel, Certificate Template, Inform, and Drop</td>
</tr>
<tr>
<td><img src="image" alt="Limit" /></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.

**Note** - Do not create two objects with the same name. You will see a validation error when you try to publish. To resolve, change one of the object names.

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 the network objects or groups of objects for search purposes. These are the types of tags you can assign:

- User tags - Assigned manually to individual objects or groups of objects
- System tags - Predefined keywords, such as "application"

Each tag has a name and a value. The value can be static, or dynamically filled by detection engines.

**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 .......................................................... 53
Network Groups .................................................. 53
Check Point Hosts .............................................. 54
Gateway Cluster .................................................. 54
More Network Object Types ................................. 54

**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.
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.

The Security Management Server object is a Check Point Host.

Note - When you upgrade to R80.10 from R77.30 or earlier versions, Node objects are converted to Host objects.

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. It is not necessary to have the IP address of the site.

You can use the Domain object in the source and destination columns of an Access Control Policy.

You can configure a Domain object in two ways:

- Select FQDN
  In the object name, use the Fully Qualified Domain Name (FQDN). Use the format .x.y.z (with a dot "." before the FQDN). For example, if you use www.example.com then the Gateway matches www.example.com
  This option is supported for R80.10 and higher, and is the default. It is more accurate and faster than the non-FQDN option.
  The Security Gateway looks up the FQDN with a direct DNS query, and uses the result in the Rule Base.
Managing Objects

This option supports SecureXL Accept templates. Using domain objects with this option in a rule has no effect on the performance of the rule, or of the rules that come after it.

- **Clear FQDN**
  This option enforces the domain and its sub-domains. In the object name, use the format .x.y for the name. For example, use .example.com or .example.co.uk for the name. If you use .example.com, then the Gateway matches www.example.com and support.example.com.
  The Gateway does the name resolution using DNS reverse lookups, which can be inaccurate. The Gateway uses the result in the Rule Base, and caches the result to use again.
  When upgrading from R77, this option is enforced.

**Dynamic Objects**

A dynamic object is a "logical" object where the IP address is resolved differently for each Security Gateway, using the `dynamic_objects` command.

For R80.10 Security Gateways and higher, dynamic objects support SecureXL Accept templates. Therefore, there is no performance impact on a rule that uses a dynamic object, or on rules that come after it.

Dynamic Objects are predefined for **LocalMachine-all-interfaces**. The DAIP computer interfaces (static and dynamic) are resolved into this object.

**Security Zones**

Security Zones let you to create a strong Access Control Policy that controls the traffic between parts of the network.

A Security Zone object represents a part of the network (for example, the internal network or the external network). You assign a network interface of a Security Gateway to a Security Zone. You can then use the Security Zone objects in the Source and Destination columns of the Rule Base.

Use Security Zones to:

- Simplify the Policy. Apply the same rule to many Gateways.
- Add networks to Gateways interfaces without changing the Rule Base.

For example, in the diagram, we have three Security Zones for a typical network: **ExternalZone** [1], **DMZZone** [2] and **InternalZone** [3].

- Gateway [4] has three interfaces. One interface is assigned to **ExternalZone** [1], one interface is assigned to **DMZZone** [2], and one interface is assigned to **InternalZone** [3].
Gateway [5] has two interfaces. One interface is assigned to ExternalZone [1] and one interface is assigned to InternalZone [3].

A Security Gateway interface can belong to only one Security Zone. Interfaces to different networks can be in the same Security Zone.

Workflow
1. Define Security Zone objects. Or, use the predefined Security Zones (on page 57).
3. Use the Security Zone objects in the Source and Destination of a rule. For example:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>InternalZone</td>
<td>ExternalZone</td>
<td>Any Traffic</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

1. Install the Access Control Policy (on page 102).

Creating and Assigning Security Zones
Before you can use Security Zones in the Rule Base, you must assign Gateway interfaces to Security Zones.

To create a Security Zone:
1. In the Objects bar [F11], click New > More > Network Object > Security Zone.
   The Security Zone window opens.
2. Enter a name for the Security Zone.
3. Enter an optional comment or tag.
4. Click OK.

To assign an interface to a Security Zone
1. In the Gateways & Servers view, right-click a Security Gateway object and select Edit.
   The Gateway Properties window opens.
2. In the Network Management pane, right-click an interface and select Edit.
   The Interface window opens. The Topology area of the General pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface Leads To.
3. Click Modify.
   The Topology Settings window opens.
4. In the **Security Zone** area, click **User Defined** and select **Specify Security Zone**.
5. From the drop-down box, select a Security Zone.
   Or click **New** to create a new one.
6. Click **OK**.

**Predefined Security Zones**
These are the predefined security zones, and their intended purposes:

- **WirelessZone** - Networks that can be accessed by users and applications with a wireless connection.

- **ExternalZone** - Networks that are not secure, such as the Internet and other external networks.

- **DMZZone** - A DMZ (demilitarized zone) is sometimes referred to as a *perimeter* network. It contains company servers that can be accessed from external sources.

  A DMZ lets external users and applications access specific internal servers, but prevents the external users accessing secure company networks. Add rules to the firewall Rule Base that allow traffic to the company DMZ. For example, a rule that allows HTTP and HTTPS traffic to your web server in the DMZ.

- **InternalZone** - Company networks with sensitive data that must be protected and used only by authenticated users.

**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 the R80.10 VoIP Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54844.

**Logical Servers**

A Logical Server is a group of machines that provides the same services. The workload of this group is distributed between all its members.

When a Server group is stipulated in the Servers group field, the client is bound to this physical server. In Persistent server mode the client and the physical server are bound for the duration of the session.

- Persistency by Service — once a client is connected to a physical server for a specified service, subsequent connection to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.

- Persistency by Server — once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

**Balance Method**

The load balancing algorithm stipulates how the traffic is balanced between the servers. There are several types of balancing methods:

- **Server Load** — The Security Gateway determines which 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.

**Open Security Extension (OSE) Devices**

The Open Security Extension features let you manage third-party devices with the Check Point SmartConsole. The number of managed devices, both hardware and software packets, depends on your license. OSE devices commonly include hardware security devices for routing or dedicated Network Address Translation and Authentication appliances. Security devices are managed in the Security Policy as Embedded Devices.

The Security Management Server generates Access Lists from the Security Policy and downloads them to selected routers and open security device. Check Point supports these devices:

<table>
<thead>
<tr>
<th>OSE Device</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Systems</td>
<td>9.x, 10.x, 11.x, 12.x</td>
</tr>
</tbody>
</table>

The Check Point Rule Base must not have these objects. If it does, the Security Management Server will not generate Access Lists.

- Drop (in the Action column)
- Encrypt (Action)
• Alert (Action)
• RPC (Service)
• ACE (Service)
• Authentication Rules
• Negate Cell

Defining OSE Device Interfaces
OSE devices report their network interfaces and setup at boot time. Each OSE device has a
different command to list its configuration. You must define at least one interface for each device,
or Install Policy will fail.

To define an OSE Device:
1. From the Object Explorer, click New > More.
2. Click Network Object > More > OSE Device.
3. Enter the general properties (on page 59).
   We recommend that you also add the OSE device to the host lists on other servers: hosts
   (Linus) and lmhosts (Windows).
4. Open the Topology tab and add the interfaces of the device.
   You can enable Anti-Spoofing on the external interfaces of the device. Double-click the
   interface. In the Interface Properties window > Topology tab, select External and Perform
   Anti-Spoofing.
5. Open the Setup tab and define the OSE device and its administrator credentials (on page 59).

OSE Device Properties Window — General Tab
• Name — The name of the OSE device, as it appears in the system database on the server.
• IP Address — The device’s IP address.
• Get Address — Click this button to resolve the name to an address.
• Comment — Text to show on the bottom of the Network Object window when this object is
   selected.
• Color — Select a color from the drop-down list. The OSE device will be represented in the
   selected color in SmartConsole, for easier tracking and management.
• Type — Select from the list of supported vendors.

Anti-Spoofing Parameters and OSE Devices Setup (Cisco)
For Cisco (Version 10.x and higher) devices, you must specify the direction of the filter rules
generated from anti-spoofing parameters. The direction of enforcement is specified in the Setup
tab of each router.

For Cisco routers, the direction of enforcement is defined by the Spoof Rules Interface Direction
property.

Access List No — The number of Cisco access lists enforced. Cisco routers Version 12x and below
support an ACL number range from 101-200. Cisco routers Version 12x and above support an ACL
range number from 101-200 and also an ACL number range from 2000-2699. Inputting this ACL
number range enables the support of more interfaces.

For each credential, select an option:
• None — Credential is not needed.
- **Known** — The administrator must enter the credentials.
- **Prompt** — The administrator will be prompted for the credentials.

**Username** — The name required to logon to the OSE device.

**Password** — The Administrator password (Read only) as defined on the router.

**Enable Username** — The user name required to install Access Lists.

**Enable Password** — The password required to install Access Lists.

**Version** — The Cisco OSE device version (9.x, 10.x, 11.x, 12.x).

**OSE Device Interface Direction** — Installed rules are enforced on data packets traveling in this direction on all interfaces.

**Spoof Rules Interface Direction** — The spoof tracking rules are enforced on data packets traveling in this direction on all interfaces.
Managing Policies

In This Section:

Working with Policy Packages ................................................................. 61
Viewing Rule Logs ...................................................................................... 65
Policy Installation History ........................................................................... 66

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 & URL Filtering
  - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **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
  - Threat Extraction - Extracts potentially malicious content from e-mail attachments before they enter the corporate network
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 & URL Filtering, and Content Awareness Software 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 and layers*. The *Manage policies and layers* window opens.
2. Click *New*. The *New 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**
   - **Threat Prevention**
   - **QoS**, select *Recommended* or *Express*
   - **Desktop Security**
   To see the **QoS**, and **Desktop Security** policy types, enable them on one or more Gateways:
   Go to gateway editor > General Properties > Network Security tab:
   - For QoS, select **QoS**
   - For Desktop Security, select **IPSec VPN** and **Policy Server**
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*.
7. Click *Close*.
   The new policy shows on the *Security Policies* page.

### Adding a Policy Type to an Existing Policy Package

1. From the Menu, select *Manage policies and layers*. The *Manage policies and layers* window opens.
2. Select a policy package and click the *Edit* button.
3. The *New Policy* package window opens.
4. On the *General* > *Policy types* page, select the policy type to add:
   - **Access Control**
   - **Threat Prevention**
   - **QoS**, select *Recommended* or *Express*
   - **Desktop Security**
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 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 (on page 64), 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`.

**Warning -**
- The `fw unloadlocal` command prevents all traffic from passing through the Security Gateway, because it disables the IP Forwarding in the Linux kernel.
- The `fw unloadlocal` command removes all policies from the Security Gateway. This means that the Security Gateway accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Viewing Rule Logs

You can search for the logs that are generated by a specific 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** - By default, shows the logs for the Current Rule. You can filter them by 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 and press Enter:
     ```
     layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10
     ```
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. From the Access Tools or the Threat Prevention Tools, select Installation History.
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.
Creating an Access Control Policy

In This Section:

Introducing the Unified Access Control Policy ............................................................ 67
Creating a Basic Access Control Policy ....................................................................... 68
Creating Application Control and URL Filtering Rules ............................................. 71
Ordered Layers and Inline Layers ............................................................................... 76
The Columns of the Access Control Rule Base .......................................................... 85
Unified Rule Base Use Cases ..................................................................................... 93
Rule Matching in the Access Control Policy ............................................................... 98
Best Practices for Access Control Rules .................................................................... 101
Installing the Access Control Policy ......................................................................... 102
Analyzing the Rule Base Hit Count ........................................................................... 102
Preventing IP Spoofing .............................................................................................. 104
Multicast Access Control ............................................................................................ 107
Managing Pre-R80.10 Security Gateways ................................................................. 108
Configuring the NAT Policy ....................................................................................... 109
Site-to-Site VPN .......................................................................................................... 128
Remote Access VPN ................................................................................................... 133
Mobile Access to the Network ..................................................................................... 135

Introducing the Unified Access Control Policy

Define one, unified Access Control Policy. The Access Control Policy lets you create a simple and granular Rule Base that combines all these Access Control features:

- Firewall - Control access to and from the internal network.
- Application & URL Filtering - Block applications and sites.
- Content Awareness - Restrict the Data Types that users can upload or download.
- IPsec VPN and Mobile Access - Configure secure communication with Site-to-Site and Remote Access VPNs.
- Identity Awareness - Identify users, computers, and networks.

There is no need to manage separate Rule Bases. For example, you can define one, intuitive rule that: Allows users in specified networks, to use a specified application, but prevents downloading files larger than a specified size. You can use all these objects in one rule:

- Security Zones
- Services
- Applications and URLs
- Data Types
- Access Roles
Creating an Access Control Policy

Information about these features is collected in one log:

- Network
- Protocol
- Application
- User
- Accessed resources
- Data Types

Creating a Basic Access Control Policy

A firewall controls access to computers, clients, servers, and applications using a set of rules that make up an Access Control Rule Base. You need to configure a Rule Base with secure Access Control and optimized network performance.

A strong Access Control Rule Base:

- Allows only authorized connections and prevents vulnerabilities in a network.
- Gives authorized users access to the correct internal resources.
- Efficiently inspects connections.

Basic Rules

**Best Practice** - 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 matched by the earlier rules in the policy

Note - If you delete the cleanup rule, there will still be an **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**.

Use Case - Basic Access Control

This use case shows a Rule Base for a simple Access Control security policy. (The **Hits**, **VPN** and **Content** columns are not shown.)

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Admin Access to Gateways</td>
<td>Admins (Access Role)</td>
<td>Gateways-group</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>2</td>
<td>Stealth</td>
<td>Any</td>
<td>Gateways-group</td>
<td>Any</td>
<td>Drop</td>
<td>Alert</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>3</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>4</td>
<td>Tech support</td>
<td>TechSupport</td>
<td>Remote1-web</td>
<td>HTTP</td>
<td>Accept</td>
<td>Alert</td>
<td>Remote1GW</td>
</tr>
<tr>
<td>5</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>
</tbody>
</table>
Creating an Access Control Policy

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</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>7</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>8</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>9</td>
<td>Cleanup rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Admin Access to Gateways</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Stealth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Critical subnet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Tech support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>DNS server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mail and Web servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SMTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>DMZ and Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Cleanup rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use Case - Inline Layer for Each Department

This use case shows a basic Access Control Policy with a sub-policy for each department. The rules for each department are in an Inline Layer. An Inline Layer is independent of the rest of the Rule Base. You can delegate ownership of different Layers to different administrators.

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical subnet</td>
<td>Internal</td>
<td>Finance</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
</tr>
</tbody>
</table>
### Rules

<table>
<thead>
<tr>
<th></th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General rules for the whole organization.</td>
</tr>
<tr>
<td>2</td>
<td>An Inline Layer for the R&amp;D department.</td>
</tr>
<tr>
<td>3</td>
<td>Rule 3 is the parent rules of the Inline Layer. The <strong>Action</strong> is the name of the Inline Layer.</td>
</tr>
<tr>
<td>3.1</td>
<td><strong>If a packet does not match on parent rule 3:</strong></td>
</tr>
<tr>
<td>3.2</td>
<td>Matching continues to the next rule outside the Inline Layer (rule 4).</td>
</tr>
<tr>
<td>3.X</td>
<td><strong>If a packet matches on parent rule 3:</strong></td>
</tr>
<tr>
<td></td>
<td>Matching continues to 3.1, first rule inside the Inline Layer. If a packet matches on this rule, the rule action is done on the packet.</td>
</tr>
<tr>
<td></td>
<td>If a packet does not match on rule 3.1, continue to the next rule inside the Inline Layer, rule 3.2. If there is no match, continue to the remaining rules in the Inline Layer. --- means one or more rules.</td>
</tr>
<tr>
<td></td>
<td>The packet is matched only inside the inline layer. It never leaves the inline layer, because the inline layer has an implicit cleanup rule. It is not matched on rules 4, 5 and the other rules in the Ordered Layer.</td>
</tr>
<tr>
<td></td>
<td>Rule 3.X is a <strong>cleanup rule</strong>. It drops all traffic that does not match one of the earlier rules in the Inline Layer. This is a default explicit rule. You can change or delete it.</td>
</tr>
<tr>
<td></td>
<td><strong>Best Practice</strong> - Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.</td>
</tr>
<tr>
<td>4</td>
<td>Another Inline Layer, for the QA department.</td>
</tr>
<tr>
<td>4.1</td>
<td>---</td>
</tr>
<tr>
<td>4.Y</td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td>More general rules for the whole organization.</td>
</tr>
<tr>
<td>--</td>
<td>One or more rules.</td>
</tr>
</tbody>
</table>

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>R&amp;D source control</td>
<td>InternalZone</td>
<td>Source control servers (Group)</td>
<td>ssh, http, https</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3.X</td>
<td>Cleanup rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>QA department</td>
<td>QA network</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>QA Layer</td>
</tr>
<tr>
<td>4.1</td>
<td>Allow access to R&amp;D servers</td>
<td>Any</td>
<td>R&amp;D Servers (Group)</td>
<td>Web Services</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>4.Y</td>
<td>Cleanup rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>5</td>
<td>Allow all users to access employee portal</td>
<td>Any</td>
<td>Employee portal</td>
<td>Web Services</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>9</td>
<td>Cleanup rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
</tbody>
</table>

---

The packet is matched only inside the inline layer. It never leaves the inline layer, because the inline layer has an implicit cleanup rule. It is not matched on rules 4, 5 and the other rules in the Ordered Layer.

Rule 3.X is a **cleanup rule**. It drops all traffic that does not match one of the earlier rules in the Inline Layer. This is a default explicit rule. You can change or delete it.

**Best Practice** - Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.
Creating an Access Control Policy

<table>
<thead>
<tr>
<th>Rules</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| 9     | **Cleanup rule** - Drop all traffic that does not match one of the earlier rules in the Ordered Layer. This is a default explicit rule. You can change or delete it.  
**Best Practice** - Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer. |

Creating Application Control and URL Filtering Rules

Create and manage the Policy for Application Control and URL Filtering in the Access Control Policy, in the **Access Control** view of SmartConsole. Application Control and URL Filtering rules define which users can use specified applications and sites from within your organization and what application and site usage is recorded in the logs.

To learn which applications and categories have a high risk, look through the **Application Wiki** in the **Access Tools** part of the **Security Policies** view. Find ideas for applications and categories to include in your Policy.

To see an overview of your Access Control Policy and traffic, see the **Access Control** view in the **Logs & Monitor > New Tab > Views**.

Monitoring Applications

*Scenario: I want to monitor all Facebook traffic in my organization. How can I do this?*

**To monitor all Facebook application traffic:**

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Click one of the **Add rule** toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
4. Create a rule that includes these components:
   - **Name** - Give the rule a name, such as **Monitor Facebook**.
   - **Source** - Keep it as **Any** so that it applies to all traffic from the organization.
   - **Destination** - Keep it as **Internet** so that it applies to all traffic going to the internet or DMZ.
   - **Services & Applications** - Click the plus sign to open the Application viewer. Add the Facebook application to the rule:
     - Start to type “face” in the Search field. In the Available list, see the Facebook application.
     - Click each item to see more details in the description pane.
     - Select the items to add to the rule.
   - **Action** - Select Accept
   - **Track** - Select Log
   - **Install On** - Keep it as **Policy Targets** for or all gateways, or choose specific Security Gateways on which to install the rule

---

Note: Applications are matched by default on their **Recommended** services. You can change this. (on page 87) Each service runs on a specific port. The recommended **Web Browsing Services** are http, https, HTTP_proxy, and HTTPS_proxy.
The rule allows all Facebook traffic but logs it. You can see the logs in the Logs & Monitor view, in the Logs tab. To monitor how people use Facebook in your organization, see the Access Control view (SmartEvent Server required).

Blocking Applications and Informing Users

Scenario: I want to block pornographic sites in my organization, and tell the user about the violation. How can I do this?

To block an application or category of applications and tell the user about the policy violation:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Choose a Layer with Applications and URL Filtering enabled.
3. Create a rule that includes these components:
   - Services & Applications - Select the Pornography category.
   - Action - Drop, and a UserCheck Blocked Message - Access Control
     The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.
   - Track - Log

Note - This Rule Base example contains only those columns that are applicable to this subject.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Porn</td>
<td>Any</td>
<td>Internet</td>
<td>Pornography (category)</td>
<td>Drop Blocked Message</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

The rule blocks traffic to pornographic sites and logs attempts to access those sites. Users who violate the rule receive a UserCheck message that informs them that the application is blocked according to company security policy. The message can include a link to report if the website is included in an incorrect category.

Important - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Captive Portal.

Limiting Application Traffic

Scenario: I want to limit my employees’ access to streaming media so that it does not impede business tasks.

If you do not want to block an application or category, there are different ways to set limits for employee access:

- Add a Limit object to a rule to limit the bandwidth that is permitted for the rule.
- Add one or more Time objects to a rule to make it active only during specified times.

The example rule below:

- Allows access to streaming media during non-peak business hours only.
- Limits the upload throughput for streaming media in the company to 1 Gbps.
To create a rule that allows streaming media with time and bandwidth limits:

1. In the Security Policies view of SmartConsole, go to the Access Control Policy.
2. Choose a Layer with Applications and URL Filtering enabled.
3. Click one of the Add Rule toolbar buttons to add the rule in the position that you choose in the Rule Base.
4. Create a rule that includes these components:
   - **Services & Applications** - Media Streams category.
     - **Note** - Applications are matched on their Recommended services, where each service runs on a specific port, such as the default Application Control Web browsing Services: http, https, HTTP_proxy, and HTTPS_proxy. To change this, see Services & Applications Column [on page 87].
   - **Action** - Click More and select Action: Accept, and a Limit object.
   - **Time** - Add a Time object that specifies the hours or time period in which the rule is active.
     - **Note** - The Time column is not shown by default in the Rule Base table. To see it, right-click on the table header and select Time.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services and Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Streaming Media</td>
<td>Any</td>
<td>Internet</td>
<td>Media Streams (Category)</td>
<td>Accept Upload_1Gb ps</td>
<td>Log</td>
<td>All</td>
<td>Off-Work</td>
</tr>
</tbody>
</table>

**Note** - In a cluster environment, the specified bandwidth limit is divided between all defined cluster members, whether active or not. For example, if a rule sets 1Gbps limit in a three member cluster, each member has a fixed limit of 333 Mbps.

**Using Identity Awareness Features in Rules**

*Scenario: I want to allow a Remote Access application for a specified group of users and block the same application for other users. I also want to block other Remote Access applications for everyone. How can I do this?*

If you enable Identity Awareness on a Security Gateway, you can use it together with Application Control to make rules that apply to an access role. Use access role objects to define users, machines, and network locations as one object.

In this example:
- You have already created an Access Role **Identified_Users** that represents all identified users in the organization. You can use this to allow access to applications only for users who are identified on the Security Gateway.
- You want to allow access to the Radmin Remote Access tool for all identified users.
- You want to block all other Remote Access tools for everyone within your organization. You also want to block any other application that can establish remote connections or remote control.

**To do this, add two new rules to the Rule Base:**

1. Create a rule and include these components:
   - **Source** - The **Identified_Users** access role
• **Destination** - Internet
• **Services & Applications** - Radmin
• **Action** - Accept

2. Create another rule below and include these components:
• **Source** - Any
• **Destination** - Internet
• **Services & Applications** - The category: Remote Administration
• **Action** - Block

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Radmin to Identified Users</td>
<td>Identified_Users</td>
<td>Internet</td>
<td>Radmin</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
</tr>
<tr>
<td>Block other Remote Admins</td>
<td>Any</td>
<td>Internet</td>
<td>Remote Administration</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

**Notes on these rules:**

• Because the rule that allows Radmin is above the rule that blocks other Remote Administration tools, it is matched first.

• The Source of the first rule is the **Identified_Users** access role. If you use an access role that represents the Technical Support department, then only users from the technical support department are allowed to use Radmin.

• Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing services**: http, https, HTTP_proxy, and HTTPS_proxy. To change this see Changing Services for Applications and Categories.


### Blocking Sites

**Scenario:** I want to block sites that are associated with categories that can cause liability issues. Most of these categories exist in the Application Database but there is also a custom defined site that must be included. How can I do this?

You can do this by creating a **custom group** and adding all applicable categories and the site to it. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an access role. Use access role objects to define users, machines, and network locations as one object.

In this example:

• You have already created
  • An Access Role that represents all identified users in the organization (**Identified_Users**).
  • A custom application for a site named **FreeMovies**.

• You want to block sites that can cause liability issues for everyone within your organization.

• You will create a custom group that includes Application Database categories as well as the previously defined custom site named **FreeMovies**.
To create a custom group:

1. In the Object Explorer, click **New > More > Custom Application/Website > Application/Website Group**.
2. Give the group a name. For example, **Liability_Sites**.
3. Click + to add the group members:
   - Search for and add the custom application **FreeMovies**.
   - Select **Categories**, and add the ones you want to block (for example **Anonymizer**, **Critical Risk**, and **Gambling**)
   - Click **Close**
4. Click **OK**.

You can now use the **Liability_Sites** group in the Access Control Rule Base.

**In the Rule Base, add a rule similar to this:**

In the Security Policies view of SmartConsole, go to the **Access Control** Policy.

- **Source** - The **Identified_Users** access role
- **Destination** - **Internet**
- **Services & Applications** - **Liability_Sites**
- **Action** - **Drop**

**Note** - Applications are matched on their Recommended services, where each service runs on a specific port, such as the default Application Control Web Browsing Services: http, https, HTTP_proxy, and HTTPS_proxy. To change this see Changing Services for Applications and Categories.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block sites that may</td>
<td>Identified_Users</td>
<td>Internet</td>
<td>Liability_Sites</td>
<td>Drop</td>
<td>Log</td>
</tr>
<tr>
<td>cause a liability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Blocking URL Categories**

*Scenario: I want to block pornographic sites. How can I do this?*

You can do this by creating a rule that blocks all sites with pornographic material with the Pornography category. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an access role. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role (**Identified_Users**) that represents all identified users in the organization.
- You want to block sites related to pornography.

The procedure is similar to *Blocking Applications and Informing Users.*

**In the Rule Base, add a rule similar to this:**

- **Source** - The **Identified_Users** access role
- **Destination** - **Internet**
- **Services & Applications** - **Pornography** category
Ordered Layers and Inline Layers

A policy is a set of rules that the gateway enforces on incoming and outgoing traffic. There are different policies for Access Control and for Threat Prevention.

You can organize the Access Control rules in more manageable subsets of rules using Ordered Layers and Inline Layers.

In This Section

- The Need for Ordered Layers and Inline Layers
- Order of Rule Enforcement in Inline Layers
- Order of Rule Enforcement in Ordered Layers
- Creating an Inline Layer
- Creating a Ordered Layer
- Enabling Access Control Features
- Types of Rules in the Rule Base
- Administrators for Access Control Layers
- Sharing Layers
- Visual Division of the Rule Base with Sections
- Exporting Layer Rules to a .CSV File
- Managing Policies and Layers

The Need for Ordered Layers and Inline Layers

Ordered Layers and Inline Layers helps you manage your cyber security more efficiently. You can:

- Simplify the Rule Base, or organize parts of it for specific purposes.
- Organize the Policy into a hierarchy, using Inline Layers, rather than having a flat Rule Base. An Inline Layer is a sub-policy which is independent of the rest of the Rule Base.
- Simplify the management of the Policy by delegating ownership of different Layers to different administrators.
- Improve performance by reducing the number of rules in a Layer.

Order of Rule Enforcement in Inline Layers

This is an example of an Inline Layer:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Drop</td>
</tr>
</tbody>
</table>
The Inline Layer has a parent rule (Rule 2 in the example), and sub rules (Rules 2.1 and 2.2). The Action of the parent rule is the name of the Inline Layer.

If the packet does not match the parent rule of the Inline Layer, the matching continues to the next rule of the Ordered Layer (Rule 3).

If a packet matches the parent rule of the Inline Layer (Rule 2), the Firewall checks it against the sub rules:

- If the packet matches a sub rule in the Inline Layer (Rule 2.1), no more rule matching is done.
- If none of the higher rules in the Ordered Layer match the packet, the explicit Cleanup Rule is applied (Rule 2.2). If this rule is missing, the Implicit Cleanup Rule (on page 81) is applied. No more rule matching is done.

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

**Order of Rule Enforcement in Ordered Layers**

When a packet arrives at the gateway, the gateway checks it against the rules in the first Ordered 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 Ordered Layer.
Creating an Access Control Policy

If none of the rules in the Ordered Layer match the packet, the explicit Default Cleanup Rule is applied. If this rule is missing, the Implicit Cleanup Rule (on page 81) is applied.

Every Ordered Layer has its own implicit cleanup rule. You can configure the rule to Accept or Drop in the Layer settings (on page 82).

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

Creating an Inline Layer

An Inline Layer is a sub-policy which is independent of the rest of the Rule Base.

The workflow for making an Inline Layer is:

1. Create a parent rule for the Inline Layer. Make a rule that has one or more properties that are the same for all the rules in the Inline Layer. For example, rules that have the same source, or service, or group of users.
2. Create sub-rules for the Inline Layer. These are rules that define in more detail what to do if the Firewall matches a connection to the parent rule. For example, each sub-rule can apply to specified hosts, or users, or services, or Data Types.

To create an Inline Layer:

1. Add a rule to the Ordered Layer. This is the parent rule.
2. In the Source, Destination, VPN, and Services & Applications cells, define the match conditions for the Inline Layer.
3. Click the Action cell of the rule. Instead of selecting a standard action, select Inline Layer > New Layer.
4. The Layer Editor window opens.
5. Configure the properties of the Inline Layer:
   a) Enable one or more of these Blades for the rules of Inline Layer:
      ▪ Firewall
      ▪ Application & URL Filtering
      ▪ Content Awareness
      ▪ Mobile Access
   b) Optional: It is a best practice to share Layers with other Policy packages when possible. To enable this select Multiple policies can use this layer.
   c) Click Advanced.
   d) Configure the Implicit Cleanup Rule to Drop or Accept (on page 81).
   e) Click OK.

   The name of the Inline Layer shows in the Action cell of the rule.
6. Under the parent rule of the Inline Layer, add sub-rules.
7. Make sure there is an explicit cleanup rule as the last rule of the Inline Layer (on page 81).

Creating an Ordered Layer

To create an Ordered Layer:

1. In SmartConsole, click Menu > Manage Policies and Layers.
2. In the left pane, click **Layers**.
   You will see a list of the Layers. You can select **Show only shared Layers**.
3. Click the **New** icon in the upper toolbar.
4. Configure the settings in the **Layer Editor** window.
5. Optional: It is a best practice to share Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer**.
6. Click **OK**.
7. Click **Close**.
8. Publish the session.
   This Ordered Layer is not yet assigned to a Policy Package.

**To add an Ordered Layer to the Access Control Policy:**

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the Access Control Policy section and select **Edit Policy**.
   The **Policy** window opens.
3. In the Access Control section, click the plus sign.
   You will see a list of the Layers that you can add. These are Layers that have **Multiple policies can use this layer** enabled.
4. Select the Layer.
5. Click **OK**.
6. **Publish** the session.

**Pre-R80.10 Gateways: To create a Layer for URL Filtering and Application Control:**

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the Access Control Policy section and select **Edit Policy**.
   The **Policy** window opens.
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 & URL Filtering on the Layer.
   a) Enter a name for the Layer.
      We recommend the name **Application**.
   b) In the **Blades** section, select **Applications & URL Filtering**.
   c) Click **OK** and the **Layer Editor** window closes.
   d) Click **OK** and the **Policy** window closes.
6. **Publish** the session.

**Enabling Access Control Features**

Before creating the Access Control Policy, you must enable the Access Control features that you will use in the Policy.

Enable the features on the:

- Security Gateways on which you will install the Policy.
Creating an Access Control Policy

Ordered Layers and Inline Layers of the Policy. Here you can enable:
- Firewall. This includes VPN (on page 86).
- Applications & URL Filtering (on page 87)
- Content Awareness (on page 90)
- Mobile Access (on page 86)

Enabling Access Control Features on a 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 one or more of these Access Control features:
   - IPsec VPN
   - Mobile Access
   - Application Control
   - URL Filtering
   - Content Awareness
   - Identity Awareness
4. Click OK.

Enabling Access Control Features on a Layer

To enable the Access Control features on an Ordered Layer:

1. In SmartConsole, click Security Policies.
2. Under Access Control, right-click Policy and select Edit Policy.
3. Click options for the Layer.
4. Click Edit Layer.
   The Layer Editor window opens and shows the General view.
5. Enable the Blades that you will use in the Ordered Layer:
   - Firewall.
   - Applications & URL Filtering
   - Content Awareness
   - Mobile Access
6. Click OK.

To enable the Access Control features on an Inline Layer:

1. In SmartConsole, click Security Policies.
2. Select the Ordered Layer.
3. In the parent rule of the Inline Layer, right-click the Action column, and select Inline Layer > Edit Layer.
4. Enable the Blades that you will use in the Inline Layer:
   - Firewall.
   - Applications & URL Filtering
   - Content Awareness
• Mobile Access

   **Note** - Do not enable a Blade that is not enabled in the Ordered Layer.

5. Click **OK**.

### 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 **default Cleanup rule** is an explicit rule that is added by default to 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 for the Layer that deals with traffic that does not match any explicit or implied rules in the Layer. It is made automatically when you create a Layer.

Implicit cleanup rules do not show in the Rule Base.

For R80.10 later version Security Gateways, the default implicit cleanup rule action is **Drop**. This is because most Policies have Whitelist rules (the Accept action). If the Layer has Blacklist rules (the Drop action), you can change the action of the implicit cleanup rule to **Accept** in the Layer Editor.

For R77.30 or earlier versions Security Gateways, the action of the implicit rule depends on the Ordered Layer:

- **Drop** - for the **Network** Layer
- **Accept** - for a Layer with **Applications and URL Filtering** enabled

**Note** - If you change the default values, the policy installation will fail on R77.30 or earlier versions Security Gateways.
**Order in which the Firewall Applies the Rules**

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 Rules** - 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 Layer match.

**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, select the Access Control Policy.
2. From the toolbar above the policy, select **Actions** > **Implied Rules**.
   - The **Implied Policy** window opens.
3. In the left pane, click **Configuration**.
4. Select a rule to enable it, or clear a rule to disable it.
5. For the enabled rules, select the position of the rules in the Rule Base: **First**, **Last**, or **Before Last** (on page 81).
6. Click **OK** and install the policy.

**Showing the Implied Rules**

**To see the implied rules:**

In SmartConsole, from the **Security Policies** View, select **Actions** > **Implied Rules**.

The **Implied Policy** window opens.

It shows only the implied rules, not the explicit rules.

**Configuring the Implicit Cleanup Rule**

**To configure the Implicit Cleanup Rule:**

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.
3. Select a Layer and click **Edit**.
   - The **Layer Editor** opens.
4. Click **Advanced**
5. Configure the **Implicit Cleanup Rule** to **Drop** or **Accept**.
6. Click **OK**.
7. Click **Close**.
8. **Publish** the session.

**Administrators for Access Control Layers**

You can create administrator accounts dedicated to the role of Access Control, with their own installation and SmartConsole Read/Write permissions.

You can also delegate ownership of different Layers to different administrators (on page 33).

**Sharing Layers**

You may need to use the same rules in different parts of a Policy, or have the same rules in multiple Policy packages.

There is no need to create the rules multiple times. Define an Ordered Layer or an Inline Layer one time, and mark it as shared. You can then reuse the Inline Layer or Ordered layer in multiple policy packages or use the Inline Layer in multiple places in an Ordered Layer. This is useful, for example, if you are an administrator of a corporation and want to share some of the rules among multiple branches of the corporation:

- It saves time and prevents mistakes.
- To change a shared rule in all of the corporation’s branches, you must only make the change once.

**To mark a Layer as shared:**

1. In SmartConsole, click **Menu > Manage policies and layers**.
2. In the left pane, click **Layers**.
3. Select a Layer in **Access Control** or in **Threat Prevention**.
4. Right-click and select **Edit Layer**.
5. Configure the settings in the **Layer Editor** window.
6. In **General**, select **Multiple policies and rules can use this layer**.
7. Click **OK**.
8. Click **Close**.
9. **Publish** the session.

**To reuse a Threat Prevention Ordered Layer:**

1. In SmartConsole, go to **Menu > Manage policies and layers > Policies**.
2. Right-click the required policy and click **Edit**. The policy properties window opens.
3. In the Threat Prevention box, click the + sign.
4. Select the layer you want to include in this policy package.
5. Click **OK**.
6. Close the policy properties window.
7. **Install Policy**.
8. Repeat this procedure for all policy packages.

For examples of Inline Layers and Ordered Layer, see Unified Rule Base Use Cases (on page 93).
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.

Exporting Layer Rules to a .CSV File

You can export Layer rules to a .csv file. You can open and change the .csv file in a spreadsheet application such as Microsoft Excel.

To export Layer rules to a .csv file:
1. In SmartConsole, click Menu > Manage Policies and Layers. The Manage Layers window opens.
2. Click Layers.
3. Select a Layer, and then click Actions > Export selected Layer.
4. Enter a path and file name.

Managing Policies and Layers

To work with Ordered Layers and Inline Layers in the Access Control Policy, select Menu > Manage policies and layers in SmartConsole. The Manage policies and layers window shows.

To see the Layer in the policy package and their attributes:

In the Layers pane of the window, you can see:

- Name - Layer name
- Number of Rules - Number of rules in the Layer
- Modifier - The administrator who last changed the Layer configuration.
- Last Modified - Date the Layer was changed.
- Show only Shared Layers - A shared Layer has the Multiple policies and rules can use this Layer option selected (on page 83).
- Layer Details
  - Used in policies - Policy packages that use the Layer
  - Mode:
    - Ordered - An Ordered Layer. In a Multi-Domain Security Management environment, it includes global rules and a placeholder for local, Domain rules.
    - Inline - An Inline Layer, also known as a Sub-Policy.
    - Not in use - A Layer that is not used in a Policy package.

To see the rules in the Layer:
1. Select a Layer.
2. Right-click and select Open layer in policy.
The Columns of the Access Control Rule Base

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

<table>
<thead>
<tr>
<th>Column</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 times that connections match a rule (on page 102).</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network objects [on page 85] that define</td>
</tr>
<tr>
<td>Destination</td>
<td>• Where the traffic starts</td>
</tr>
<tr>
<td></td>
<td>• The destination of the traffic.</td>
</tr>
<tr>
<td>VPN</td>
<td>The VPN Community to which the rule applies [on page 86].</td>
</tr>
<tr>
<td>Services &amp;</td>
<td>Services, Applications, Categories, and Sites [on page 87].</td>
</tr>
<tr>
<td>Applications</td>
<td>If Application &amp; URL Filtering is not enabled, only Services show.</td>
</tr>
<tr>
<td>Content</td>
<td>The data asset to protect, for example, credit card numbers or medical</td>
</tr>
<tr>
<td></td>
<td>records [on page 90]. You can set the direction of the data to Download</td>
</tr>
<tr>
<td>Action</td>
<td>Traffic (into the organization), Upload Traffic (out of the organization),</td>
</tr>
<tr>
<td></td>
<td>or Any Direction.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule [on</td>
</tr>
<tr>
<td></td>
<td>page 92].</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the policy [on page 102].</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>

Source and Destination Column

In the Source and Destination columns of the Access Control Policy Rule Base, you can add Network objects including groups of all types. Here are some of the network objects you can include:

- Network
- Host
- Zones [on page 57]
- Dynamic Objects
- Domain Objects
- Access Roles
Creating an Access Control Policy

To Learn More About Network Objects

You can add network objects (on page 51) to the Source and Destination columns of the Access Control Policy.

VPN Column

You can configure rules for Site-to-Site VPN, Remote Access VPN, and the Mobile Access portal and clients.

To make a rule for a VPN Community, add a Site-to-Site Community or a Remote Access VPN Community object to this column, or select Any to make the rule apply to all VPN Communities.

When you enable Mobile Access on a gateway, the gateway is automatically added to the RemoteAccess VPN Community. Include that Community in the VPN column of the rule or use Any to make the rule apply to Mobile Access gateways. If the gateway was removed from the VPN Community, the VPN column must contain Any.

IPsec VPN

The IPsec VPN solution lets the Security Gateway encrypt and decrypt traffic to and from other gateways and clients. Use SmartConsole to easily configure VPN connections between Security Gateways and remote devices.

For Site to Site Communities, you can configure Star and Mesh topologies for VPN networks, and include third-party gateways.

The VPN tunnel guarantees:

- **Authenticity** - Uses standard authentication methods
- **Privacy** - All VPN data is encrypted
- **Integrity** - Uses industry-standard integrity assurance methods

IKE and IPsec

The Check Point VPN solution uses these secure VPN protocols to manage encryption keys, and send encrypted packets. IKE (Internet Key Exchange) is a standard key management protocol that is used to create the VPN tunnels. IPsec is protocol that supports secure IP communications that are authenticated and encrypted on private or public networks.

Mobile Access to the Network

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the Mobile Application in the Services & Applications column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the Source column of a rule.
Creating an Access Control Policy

To Learn More About VPN

To learn more about Site to Site VPN and Remote Access VPN, see these guides:

- R80.10 Site to Site VPN Administration Guide
  http://downloads.checkpoint.com/dc/download.htm?ID=60371
- R80.10 Remote Access VPN Administration Guide
  http://downloads.checkpoint.com/dc/download.htm?ID=53105
- R80.10 Mobile Access Administration Guide
  http://downloads.checkpoint.com/dc/download.htm?ID=53103

Services & Applications Column

In the Services & Applications column of the Access Control Rule Base, define the applications, sites, and services that are included in the rule. A rule can contain one or more:

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

Service Matching

The Firewall identifies [matches] a service according to IP protocol, TCP and UDP port number, and protocol signature.

To make it possible for the Firewall to match services by protocol signature, you must enable Applications and URL Filtering on the Gateway and on the Ordered Layer [on page 79].

You can configure TCP and UDP services to be matched by source port.

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 in one of these ways:

- On any service
- 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:
   - The default is **Recommended** services. The defaults for Web services are the Application Control **Web Browsing Services**.
   - To match the application with all services, click **Any**.
   - To match the application on specified services, click **Customize**, and add or remove services.
   - To match the application with all services and exclude specified services, click **Customize**, add the services to exclude, and 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 Application Control **Web browsing services**.

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

**To configure matching for blocked applications:**

1. In SmartConsole, go to **Manage & Settings > Blades > Application & URL Filtering > Advanced Settings > Application Port Match**
2. Configure **Match application on ’Any’ port when used in ’Block’ rule**:
   - 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>
</tbody>
</table>
Creating an Access Control Policy

Application - Match Setting | Checkbox: Match web application on ‘Any’ port when used in ‘Block’ rule | Blocked Application is Matched on Service
--- | --- | ---
Customize | Not relevant | Customized
Any | Not relevant | Any

Adding Services, Applications, and Sites to a rule

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

**Note** - Rules with applications or categories do not apply to connections from or to the Security Gateway.

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 a Layer with **Applications and URL Filtering** enabled.
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, which 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 a Layer with **Applications and URL Filtering** enabled.
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 > Application/Site**.
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 a Layer with **Applications and URL Filtering** enabled.
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**.

### Services and Applications on R80 and Lower Gateways, and after Upgrade

For R77.xx and lower Gateways:
- The Firewall matches TCP and UDP services by *port* number. The Firewall cannot match services by protocol signature.
- The Firewall matches applications by the application signature.

When you upgrade the Security Management Server and the Gateway to R80 and higher, this change of behavior occurs:
- Applications that were defined in the Application & URL Filtering Rule Base are accepted on their recommended ports

### Content Column

You can add Data Types to the Content column of rules in the Access Control Policy.

To use the Content column, you must enable **Content Awareness**, in the General Properties page of the Security Gateway, and on the Layer.

A Data Type is a classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

You can set the direction of the data in the Policy to **Download Traffic** (into the organization), **Upload Traffic** (out of the organization), or **Any Direction**.

There are two kinds of Data Types: **Content Types** (classified by analyzing the file content) and **File Types** (classified by analyzing the file ID).

**Content Type examples:**
- PCI - credit card numbers
- HIPAA - Medical Records Number - MRN
- International Bank Account Numbers - IBAN
- Source Code - JAVA
- U.S. Social Security Numbers - According to SSA
- Salary Survey Terms

**File type examples:**
- Viewer File - PDF
- Executable file
- Database file
- Document file
- Presentation file
- Spreadsheet file

Note these limitations:
- Websocket content is not inspected.
- HTTP connections that are not RFC-compliant are not inspected.
To learn more about the Data Types, open the Data Type object in SmartConsole and press the ? button [or F1] to see the Help.

**Note** - Content Awareness and Data Loss Prevention (DLP) both use Data Types. However, they have different features and capabilities. They work independently, and the Security Gateway enforces them separately.

To learn more about DLP, see the *R80.10 Data Loss Prevention Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54805.

### Actions Column

<table>
<thead>
<tr>
<th>Action</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Accepts the traffic</td>
</tr>
<tr>
<td>Drop</td>
<td>Drops the traffic. The Firewall does not send a response to the originating end of the connection and the connection eventually does a time-out. If no UserCheck object is defined for this action, no page is displayed.</td>
</tr>
<tr>
<td>Ask</td>
<td>Asks the user a question and adds a confirmatory check box, or a reason box. Uses a UserCheck object.</td>
</tr>
<tr>
<td>Inform</td>
<td>Sends a message to the user attempting to access the application or the content. Uses a UserCheck object.</td>
</tr>
</tbody>
</table>

**To see these actions, right-click and select More:**

<table>
<thead>
<tr>
<th>Action</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject</td>
<td>Rejects the traffic. The Firewall sends an RST packet to the originating end of the connection and the connection is closed.</td>
</tr>
<tr>
<td>UserCheck Frequency</td>
<td>Configure how often the user sees the configured message when the action is ask, inform, or block.</td>
</tr>
<tr>
<td>Confirm UserCheck</td>
<td>Select the action that triggers a UserCheck message:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Per rule</strong> - UserCheck message shows only once when traffic matches a rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Per category</strong> - UserCheck message shows for each matching category in a rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Per application/Site</strong> - UserCheck message shows for each matching application/site in a rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Per Data type</strong> - UserCheck message shows for each matching data type.</td>
</tr>
<tr>
<td>Limit</td>
<td>Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for uploads and downloads.</td>
</tr>
<tr>
<td>Enable Identity Captive Portal</td>
<td>Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.</td>
</tr>
</tbody>
</table>

**Important** - A rule that drops traffic, with the **Source** and **Destination** parameters defined as **Any**, also drops traffic to and from the Captive Portal.

### UserCheck Actions

UserCheck lets the Security Gateways send messages to users about possible non-compliant or dangerous Internet browsing. In the Access Control Policy, it works with URL Filtering, Application
Creating an Access Control Policy

Control, and Content Awareness. (You can also use UserCheck in the Data Loss Prevention Policy, in SmartConsole). Create UserCheck objects and use them in the Rule Base, to communicate with the users. These actions use UserCheck objects:

- Inform
- Ask
- Drop

UserCheck on a Security Gateway

When UserCheck is enabled, the user’s Internet browser shows the UserCheck messages in a new window.

You can enable UserCheck on Security Gateways that use:

- Access Control features:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention features:
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
  - Threat Extraction
- Data Loss Prevention

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.

To Learn More About UserCheck

To learn more about UserCheck, see the R80.10 Next Generation Security Gateway Guide http://downloads.checkpoint.com/dc/download.htm?ID=54806.

Tracking Column

These are some of the Tracking options:

- None - Do not generate a log.
- Log - This is the default Track option. It shows all the information that the Security Gateway used to match the connection.
- Accounting - Select this to update the log at 10 minute intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.
To Learn More About Tracking

To learn more about Tracking options, see the R80.10 Logging and Monitoring Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54830.

Unified Rule Base Use Cases

Here are some use cases that show examples of rules that you can define for the Access Control Policy.

Use Cases In this section:

- Use Case - Application Control and Content Awareness Ordered Layer .........................................................93
- Use Case - Inline Layer for Web Traffic ..................................................................................................................94
- Use Case - Content Awareness Ordered Layer .......................................................................................................95
- Use Case - Application & URL Filtering Ordered Layer ..........................................................................................97

Use Case - Application Control and Content Awareness Ordered Layer

This use case shows an example unified Access Control Policy. It controls applications and content in one Ordered Layer.

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General compliance (1)</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Anonymizer Critical Risk</td>
<td>Any</td>
<td>Drop Block</td>
<td>Log</td>
</tr>
<tr>
<td>2</td>
<td>Block risky executables [2]</td>
<td>InternalZone</td>
<td>Internet</td>
<td>Any</td>
<td>Uncategorized High Risk</td>
<td>Download Traffic</td>
<td>Drop</td>
<td>Log</td>
</tr>
<tr>
<td>4</td>
<td>Block other credit cards from company Web servers</td>
<td>Any</td>
<td>Web Servers</td>
<td>Any</td>
<td>Any</td>
<td>Any Direction</td>
<td>Drop</td>
<td>Log</td>
</tr>
</tbody>
</table>
Creating an Access Control Policy

<table>
<thead>
<tr>
<th>Rule</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General Compliance section - Block access to unacceptable Web sites and applications.</td>
</tr>
<tr>
<td>2</td>
<td>Block risky executables section - Block downloading of high risk executable files.</td>
</tr>
<tr>
<td>3-4</td>
<td>Credit card data section - Allow uploading of credit cards numbers only by the finance department, and only over HTTPS. Block other credit cards.</td>
</tr>
<tr>
<td>5</td>
<td>Block sensitive data over VPN section - A remote user that connects over the organization’s VPN sees an informational message.</td>
</tr>
<tr>
<td>6</td>
<td>cleanup rule - Accept all traffic that does not match one of the earlier rules.</td>
</tr>
</tbody>
</table>

Use Case - Inline Layer for Web Traffic

This use case shows an example Access Control Policy that controls Web traffic. The Web server rules are in an Inline Layer.

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Headquarter WEB traffic - via proxy</td>
<td>HQ</td>
<td>Proxy</td>
<td>Web Proxy</td>
<td>Any</td>
<td>Ask</td>
<td>Log</td>
</tr>
<tr>
<td>2</td>
<td>Allow Proxy to the Internet</td>
<td>Proxy</td>
<td>Internet</td>
<td>Web</td>
<td>Any</td>
<td>Accept</td>
<td>None</td>
</tr>
<tr>
<td>3</td>
<td>Allow local branch to access the internet directly</td>
<td>Local Branch</td>
<td>Internet</td>
<td>Web</td>
<td>Any</td>
<td>Ask</td>
<td>Log</td>
</tr>
<tr>
<td>4</td>
<td>Web Servers</td>
<td>InternalZone</td>
<td>Web Servers</td>
<td>Web</td>
<td>Any</td>
<td>Web Servers protection</td>
<td>N/A</td>
</tr>
<tr>
<td>4.1</td>
<td>Block browsing with unapproved browsers</td>
<td>Any</td>
<td>Any</td>
<td>NEGATED Google Chrome Internet Explorer 11 Firefox Safari</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
</tr>
<tr>
<td>4.2</td>
<td>Inform user when uploading Credit Cards only over HTTPS</td>
<td>Any</td>
<td>Any</td>
<td>https</td>
<td>Upload Traffic PCI - Credit Card Numbers</td>
<td>Inform Access Noti... once a day per applic...</td>
<td>Log</td>
</tr>
<tr>
<td>4.3</td>
<td>Block Credit Cards</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any Direction PCI - Credit Card Numbers</td>
<td>Drop Block Message</td>
<td>Log</td>
</tr>
<tr>
<td>4.4</td>
<td>Block downloading of sensitive content</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Download Traffic HIPAA - Medical Record Headers</td>
<td>Drop</td>
<td>Log</td>
</tr>
</tbody>
</table>
Creating an Access Control Policy

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5</td>
<td>Cleanup rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>None</td>
</tr>
<tr>
<td>5</td>
<td>Ask user when sending credit cards to PayPal</td>
<td>InternalZone</td>
<td>Internet</td>
<td>PayPal</td>
<td>Any</td>
<td>Ask Company Policy Access Notification once a day per application</td>
<td>Log</td>
</tr>
<tr>
<td>6</td>
<td>Cleanup rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
</tr>
</tbody>
</table>

**Rule Explanation**

4
This is the parent rule of the Inline Layer. The **Action** is the name of the Inline Layer. If a packet matches on the parent rule, the matching continues to rule 4.1 of the Inline Layer. If a packet does not match on the parent rule, the matching continues to rule 5.

4.1-4.4
If a packet matches on rule 4.1, the rule action is done on the packet, and no more rule matching is done. If a packet does not match on rule 4.1, continue to rule 4.2. The same logic applies to the remaining rules in the Inline Layer.

4.5
If none of the higher rules in the Ordered Layer match the packet, the explicit **Cleanup Rule** is applied. The **Cleanup rule** is a default explicit rule. You can change or delete it. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.

**Use Case - Content Awareness Ordered Layer**

This use case shows a Policy that controls the upload and download of data from and to the organization.

There is an explanation of some of the rules below the Rule Base.

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Block the download of executable files</td>
<td>InternalZone</td>
<td>Internet</td>
<td>Any</td>
<td>Download Traffic Executable file</td>
<td>Drop</td>
<td>Log</td>
</tr>
<tr>
<td>2</td>
<td>Allow uploading of credit cards numbers by finance users, only over HTTPS</td>
<td>Finance (Access Role)</td>
<td>Web Servers</td>
<td>https</td>
<td>Upload Traffic PCI - Credit Card Numbers</td>
<td>Accept</td>
<td>Log</td>
</tr>
<tr>
<td>3</td>
<td>Block other credit cards from company Web servers</td>
<td>InternalZone</td>
<td>Web Servers</td>
<td>Any</td>
<td>Any</td>
<td>Drop Block Message</td>
<td>Log</td>
</tr>
</tbody>
</table>

**Personally Identifiable Information**
### Creating an Access Control Policy

#### Human Resources

<table>
<thead>
<tr>
<th>Rule</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Matches U.S. Social Security Numbers (SSN) allocated by the U.S. Social Security Administration (SSA). <strong>Upload Traffic</strong> U.S. Social Security Numbers - According to SSA <strong>Inform</strong> Access Notifier once a day per application <strong>Log</strong></td>
</tr>
<tr>
<td>5</td>
<td>Block downloading of sensitive medical information <strong>Download Traffic</strong> HIPAA – Medical Records Headers <strong>Drop</strong> Block Message <strong>Log</strong></td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td><strong>Ask user when uploading documents containing salary survey reports.</strong> <strong>InternalZone</strong> Internet Any <strong>Upload Traffic</strong> Salary Survey Report <strong>Ask</strong> Company Policy once a day per application <strong>Log</strong></td>
</tr>
<tr>
<td><strong>Intellectual Property</strong></td>
<td><strong>Matches data containing source code</strong> <strong>Any Direction</strong> Source Code <strong>Restrict source code</strong> N/A</td>
</tr>
<tr>
<td>7</td>
<td><strong>Ask user when uploading documents containing salary survey reports.</strong> <strong>InternalZone</strong> Internet Any <strong>Upload Traffic</strong> Salary Survey Report <strong>Ask</strong> Company Policy once a day per application <strong>Log</strong></td>
</tr>
<tr>
<td>7.1</td>
<td><strong>Restrict source code</strong> N/A</td>
</tr>
<tr>
<td>7.2</td>
<td><strong>Ask</strong> Company Policy once a day per application <strong>Log</strong></td>
</tr>
<tr>
<td>7.3</td>
<td><strong>Cleanup Inline Layer</strong> <strong>Any Direction</strong> <strong>Drop</strong> Block Message <strong>Log</strong></td>
</tr>
</tbody>
</table>

#### Rule Explanation

1-3 **Regulatory Compliance** section - Control the upload and download of executable files and credit cards.

You can set the direction of the Content. In rule 1 it is **Download Traffic**, in rule 2 it is **Upload Traffic**, and in rule 3 it is **Any Direction**.

Rule 1 controls executable files, which are File Types. The File Type rule is higher in the Rule Base than rules with Content Types (Rules 2 to 7). This improves the efficiency of the Rule Base, because File Types are matched sooner than Content Types.

4-5 **Personally Identifiable Information** section - Controls the upload and download of social security number and medical records.

The rule Action for rule 4 is **Inform**. When an internal user uploads a file with a social security number, the user sees a message.

6 **Human resources** section - Controls the sending of salary survey information outside of the organization.

The rule action is **Ask**. If sensitive content is detected, the user must confirm that the upload complies with the organization’s policy.
Creating an Access Control Policy

7 Intellectual Property section - A group of rules that control how source code leaves the organization.
Rule 7 is the parent rule of an Inline Layer (on page 76). The Action is the name of the Inline Layer.
If a packet matches on rule 7.1, matching stops.
If a packet does not match on rule 7.1, continue to rule 7.2. In a similar way, if there is no match, continue to 7.3. The matching stops on the last rule of the Inline Layer. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer

Use Case - Application & URL Filtering Ordered Layer

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</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 (group)</td>
<td>Drop 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 iTunes Anonymizer (category)</td>
<td>Drop Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Allow IT department Remote Admin</td>
<td>IT (Access Role)</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(Access Role)</td>
<td>Internet</td>
<td>Facebook</td>
<td>Allow Download_1Gbps</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 Protocols Social Networking P2P File Sharing Remote Administration</td>
<td>Drop Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>6</td>
<td>Log all applications</td>
<td>Any</td>
<td>Internet</td>
<td>Any</td>
<td>Allow</td>
<td>Log</td>
<td>Any</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Explanation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Liability sites - Blocks traffic to sites and applications in the custom Potential Liability group. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>High risk applications - Blocks traffic to sites and applications in the High Risk category and blocks the iTunes application. The UserCheck Block Message is shown to users and explains why their traffic is blocked.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### Rule Matching in the Access Control Policy

The Firewall determines the rule to apply to a connection. This is called *matching* a connection. Understanding how the firewall matches connections will help you:

- Get better performance from the Rule Base.
- Understand the logs that show a matched connection.

### Examples of Rule Matching

These example Rule Bases show how the Firewall matches connections.

Note that these Rule Bases intentionally do not follow *Best Practices for Access Control Rules* (on page 101). This is to make the explanations of rule matching clearer.

#### Rule Base Matching - Example 1

For this Rule Base:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>InternalZone</td>
<td>Internet</td>
<td>ftp-pasv</td>
<td>Download executable file</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Executable file</td>
<td>Accept</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Gambling (Category)</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

This is the matching procedure for an FTP connection:

<table>
<thead>
<tr>
<th>Part of connection</th>
<th>Firewall action</th>
<th>Inspection result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td>Run the Rule Base:</td>
<td>Final match (drop on rule 1). Shows in the log. The Firewall does not turn on the inspection engines for the other rules.</td>
</tr>
<tr>
<td></td>
<td>Look for the first rule that matches:</td>
<td>Final match (drop on rule 1). Shows in the log. The Firewall does not turn on the inspection engines for the other rules.</td>
</tr>
<tr>
<td></td>
<td>• Rule 1 – Match.</td>
<td>Final match (drop on rule 1). Shows in the log. The Firewall does not turn on the inspection engines for the other rules.</td>
</tr>
</tbody>
</table>
**Rule Base Matching - Example 2**

For this Rule Base:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>InternalZone</td>
<td>Internet</td>
<td>Any</td>
<td>Download executable file</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Gambling [category]</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>ftp</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

This is the matching procedure when browsing to a file sharing Web site. Follow the rows from top to bottom. Follow each row from left to right:

<table>
<thead>
<tr>
<th>Part of connection</th>
<th>Firewall action</th>
<th>Inspection result</th>
</tr>
</thead>
</table>
| SYN                | Run the Rule Base. Look for the first rule that matches:  
                    • Rule 1 - Possible match.  
                    • Rule 2 - Possible match.  
                    • Rule 3 - No match.  
                    • Rule 4 - Match.  
                    Possible match (Continue to inspect the connection). |
| HTTP Header        | The Firewall turns on inspection engines to examine the data in the connection. In this example turn on the:  
                    • URL Filtering engine – Is it a gambling site?  
                    • Content Awareness engine - Is it an executable file?  
                    Application: File sharing (category).  
                    Content: Don’t know yet.  
                    Possible match (Continue to inspect the connection). |
| HTTP Body          | Examine the file. Data: PDF file.  
                    Optimize the Rule Base matching. Look for the first rule that matches:  
                    • Rule 1 - No match.  
                    • Rule 2 - No match.  
                    • Rule 3 - No match.  
                    • Rule 4 - Match.  
                    Final match (accept on rule 4).  
                    Shows in the log. |
**Rule Base Matching - Example 3**

For this Rule Base:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>InternalZone</td>
<td>Internet</td>
<td>Any</td>
<td>Download executable file</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Gambling (Category)</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

This is the matching procedure when downloading an executable file from a business Web site. Follow the rows from top to bottom. Follow each row from left to right:

<table>
<thead>
<tr>
<th>Part of connection</th>
<th>Firewall action</th>
<th>Inspection result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td>Run the Rule Base. Look for the first rule that matches:</td>
<td>Possible match (Continue to inspect the connection).</td>
</tr>
<tr>
<td></td>
<td>• Rule 1 – Possible match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule 2 – Possible match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule 3 – Match.</td>
<td></td>
</tr>
<tr>
<td>HTTP Header</td>
<td>The Firewall turns on inspection engines to examine the content in the connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example turn on the:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• URL Filtering engine – Is it a gambling site?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Content Awareness engine - Is it an executable file?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optimize the Rule Base matching. Look for the first rule that matches:</td>
<td>Possible match (Continue to inspect the connection).</td>
</tr>
<tr>
<td></td>
<td>• Rule 1 – Possible match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule 2 – No match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule 3 – Match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optimize the Rule Base matching. Look for the first rule that matches:</td>
<td>Final match (accept on rule 1). Shows in the log.</td>
</tr>
<tr>
<td></td>
<td>• Rule 1 – Match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule 2 – No match.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule 3 – Match.</td>
<td></td>
</tr>
</tbody>
</table>

**The matching examples show that:**

- The Firewall sometimes runs the Rule Base more than one time. Each time it runs, the Firewall optimizes the matching, to find the first rule that applies to the connection.
• If the rule includes an application, or a site, or a service with a protocol signature (in the Application and Services column), or a Data Type (in the Content column), the Firewall:
  • Turns on one or more inspection engines.
  • Postpones making the final match decision until it has inspected the body of the connection.
• The Firewall searches for the first rule that applies to \( \text{matches} \) a connection. If the Firewall does not have all the information it needs to identify the matching rule, it continues to inspect the traffic.

**Best Practices for Access Control Rules**

1. Make sure you have these rules:
   • 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.
2. Use Layers to add structure and hierarchy of rules in the Rule Base.
3. Add all rules that are based only on source and destination IP addresses and ports, in a Firewall/Network Ordered Layer at the top of the Rule Base.
4. Create Firewall/Network rules to explicitly accept safe traffic, and add an explicit cleanup rule at the bottom of the Ordered Layer to drop everything else.
5. Create an Application Control Ordered Layer after the Firewall/Network Ordered Layer. Add rules to explicitly drop unwanted or unsafe traffic. Add an explicit cleanup rule at the bottom of the Ordered Layer to accept everything else.
   Alternatively, put Application Control rules in an Inline Layer as part of the Firewall/Network rules. In the parent rule of the Inline Layer, define the Source and Destination.
6. Share Ordered Layers and Inline Layers when possible.
7. For R80.10 Gateways and higher: If you have one Ordered Layer for Firewall/Network rules, and another Ordered Layer for Application Control - Add all rules that examine applications, Data Type, or Mobile Access elements, to the Application Control Ordered Layer, or to an Ordered Layer after it.
8. Turn off XFF inspection, unless the gateway is behind a proxy server. For more, see: sk92839 http://supportcontent.checkpoint.com/solutions?id=sk92839.
9. Disable a rule when working on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Gateway. To disable a rule, right click in the No. column of the rule and select Disable.

**Best Practices for Efficient rule Matching**

1. Place rules that check the source, destination, and port (network rules) higher in the Rule Base.
   Reason: Network rules are matched sooner, and turn on fewer inspection engines.
2. Place rules that check applications and content (Data Types) below network rules.
3. Do not define a rule with \( \text{Any} \) in the Source and in the Destination, and with an Application or a Data Type. For example these rules are not recommended:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td></td>
<td>Credit Card numbers</td>
</tr>
</tbody>
</table>
Instead, define one of these recommended rules:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Internet</td>
<td>Facebook</td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td>Server</td>
<td></td>
<td>Credit Card numbers</td>
</tr>
</tbody>
</table>

Reason for 2 and 3: Application Control and Content Awareness rules require content inspection. Therefore, they:

- Allow the connection until the Firewall has inspected connection header and body.
- May affect performance.

4. For rules with Data Types (on page 90): Place rules that check File Types higher in the Rule Base than rules that check for Content Types.

Reason: File Types are matched sooner than Content Types.

To see examples of some of these best practices, see the Unified Rule Base Use Cases (on page 93) and Creating a Basic Access Control Policy (on page 68).

### Installing the Access Control Policy

1. On the Global Toolbar, click **Menu > Install Policy**.

   The **Install Policy** window opens showing the Security Gateways.

2. If there is more than one Policy package: From the **Policy** drop-down list, select a policy package.

3. Select **Access Control**. You can also select other Policies.

4. If there is more than one gateway: Select the gateways on which to install the Policy.

5. 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, if installation on a cluster member fails, do not install on that cluster**, 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.

6. Click **Install**.

### Analyzing the Rule Base Hit Count

Use the Hit Count feature to show the number of connections that each rule matches. 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.
• Better understand the behavior of the Access Control Policy

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.

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 3 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
Creating an Access Control Policy

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.

  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**.

**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.
Example:
The diagram shows a Gateway with interfaces 2 and 3, and 4, and some example networks behind the interfaces.

For the Gateway, anti-spoofing makes sure that
- All incoming packets to 2 come from the Internet [1]
- All incoming packets to 3 come from 192.168.33.0
- All incoming packets to 4 come from 192.0.2.0 or 10.10.10.0

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 protection on a Check Point Security Gateway interface, the Anti-Spoofing is done based on the interface topology. The interface topology defines where the interface Leads To (for example, External [Internet] or Internal), and the Security Zone of interface.

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 that the interface **Leads To**:
   - **Internet (External)** or **This Network (Internal)** - This is the default setting. It is automatically calculated from the topology of the gateway. To update the topology of an internal network after changes to static routes, click **Network Management > Get Interfaces** in the General Properties window of the gateway.
   - **Override** - Override the default setting. If you **Override** the default setting:
     - **Internet (External)** - All external/Internet addresses
     - **This Network (Internal)** -
       - **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. Optional: In the Security Zone section, choose the zone of the interface.

10. Configure **Anti-Spoofing** options (on page 106). Make sure that **Perform Anti-Spoofing based on interface topology** is selected.

11. 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.

12. Configure Anti-Spoofing exceptions (optional). For example, configure addresses, from which packets are not inspected by Anti-Spoofing:
   a) Select **Don’t check packets from**.
   b) Select an object from the drop-down list, or click **New** to create a new object.

13. 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

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

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

**Anti-Spoofing Options**

- **Perform Anti-Spoofing based on interface topology** - Select this option to enable spoofing protection on this external interface.

- **Anti-Spoofing action is set to** - Select this option to define if packets will be rejected (the **Prevent** option) or whether the packets will be monitored (the **Detect** option). The Detect option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually preventing packets from passing.
Don't check packets from - Select this option to make sure anti-spoofing does not take place for traffic from internal networks that reaches the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object. The anti-spoofing enforcement mechanism disregards objects selected in the Don't check packets from drop-down menu.

Spoof Tracking - Select a tracking option.

Multicast Access Control

Multicast IP transmits one copy of each datagram (IP packet) to a multicast address, where each recipient in the group takes their copy. The routers in the network forward the datagrams only to routers and hosts with access to receive the multicast packets.

To configure multicast access control:

1. Open a gateway object.
2. On the Network Management page, select an interface and click Edit.
3. On Interface > Advanced, click Drop Multicast packets by the following conditions.
4. Select a multicast policy for the interface:
   - Drop multicast packets whose destination is in the list
   - Drop all multicast packets except those whose destination is in the list
When access is denied to a multicast group on an interface for outbound IGMP packets, inbound packets are also denied.
If you do not define access restrictions for multicast packets, multicast datagrams to one interface of the gateway are allowed out of all other interfaces.
5. Click Add.
   The Add Object window opens, with the Multicast Address Ranges object selected.
6. Click New > Multicast Address Range.
   The Multicast Address Range Properties window opens.
7. Enter a name for this range.
8. Define an IP address Range or a Single IP Address in the range: 224.0.0.0 - 239.255.255.255.
   Class D IP addresses are reserved for multicast traffic and are allocated dynamically. The multicast address range 224.0.0.0 - 239.255.255.255 is used only for the destination address of IP multicast traffic.
   Every IP datagram whose destination address starts with 1110 is an IP multicast datagram. The remaining 28 bits of the multicast address range identify the group to which the datagram is sent.
   The 224.0.0.0 - 224.0.0.255 range is reserved for LAN applications that are never forwarded by a router. These addresses are permanent host groups. For example: an ICMP request to 224.0.0.1 is answered by all multicast capable hosts on the network, 224.0.0.2 is answered by all routers with multicast interfaces, and 224.0.0.13 is answered by all PIM routers. To learn more, see the IANA website [http://www.iana.org/assignments/multicast-addresses].
   The source address for multicast datagrams is always the unicast source address.
9. Click OK.
10. In the Add Object window, click OK.
11. In the **Interface Properties** window, click **OK**.
12. In the gateway window, click **OK**.
13. In the Rule Base, add a rule that allows the multicast address range as the **Destination**.
14. In the **Services** of the rule, add the multicast protocols.
   - **Multicast routing protocols** - For example: Protocol-Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Extensions to OSPF (MOSPF).
   - **Dynamic registration** - Hosts use the Internet Group Management Protocol (IGMP) to let the nearest multicast router know they want to belong to a specified multicast group. Hosts can leave or join the group at any time.
15. Install the policy.

### Managing Pre-R80.10 Security Gateways

When you upgrade a pre-R80 Security Management Server that manages pre-R80.10 Security Gateways to R80 or higher, 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 & 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.
Configuring the NAT Policy

In This Section:

- Translating IP Addresses (NAT) ................................................................. 109
- NAT Rule Base .............................................................................................. 112
- Configuring Static and Hide NAT ................................................................. 113
- Advanced NAT Settings .............................................................................. 119

Translating IP Addresses (NAT)

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. You can enable NAT for all SmartConsole objects to help manage network traffic. NAT protects the identity of a network and does not show internal IP addresses to the Internet. You can also use NAT to supply more IPv4 addresses for the network.

The Firewall can change both the source and destination IP addresses in a packet. For example, when an internal computer sends a packet to an external computer, the Firewall translates the source IP address to a new one. The packet comes back from the external computer; the Firewall translates the new IP address back to the original IP address. The packet from the external computer goes to the correct internal computer.

SmartConsole gives you the flexibility to make necessary configurations for your network:

- Easily enable the Firewall to translate all traffic that goes to the internal network.
- SmartConsole can automatically create Static and Hide NAT rules that translate the applicable traffic.
- You can manually create NAT rules for different configurations and deployments.

How Security Gateways Translate Traffic

A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.
  
  The configuration of static NAT on a range results in the translation of the IP addresses in the range into a range of the same size, starting with the IP address specified.

- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers; external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.

- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules (on page 112) to use Port Translation.
**Using Hide NAT**

For each SmartConsole object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object

Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- `rlogin` [destination port 512]
- `rshell` [destination port 513]
- `rexec` [destination port 514]

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

**Sample NAT Deployments**

**Static NAT**

Firewalls that do Static NAT, translate each internal IP address to a different external IP address.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with Static NAT</td>
</tr>
<tr>
<td>1</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>

**Sample Static NAT Workflow**

An external computer in the Internet sends a packet to 192.0.2.5. The Firewall translates the IP address to 10.10.0.26 and sends the packet to internal computer A. Internal computer A sends back a packet to the external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.5.

Internal computer B (10.10.0.37) sends a packet to an external computer. The Firewall intercepts the packet the translates the source IP address to 192.0.2.16.
Internal computer A (10.10.0.26) sends packet to Internet → Firewall translates this address to 192.0.2.5 → Internet receives packet from 192.0.2.5

Internal computer B (10.10.0.37) sends packet to Internet → Firewall translates this address to 192.0.2.16 → Internet receives packet from 192.0.2.16

**Hide NAT**

Firewalls that do Hide NAT use different port numbers to translate internal IP address to one external IP address. External computers cannot start a connection to an internal computer.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internal computers</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with Hide NAT</td>
</tr>
<tr>
<td>3</td>
<td>External computers and servers in the Internet</td>
</tr>
</tbody>
</table>

**Sample Hide NAT Workflow**

Internal computer A (10.10.0.26) sends a packet to an external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.1 port 11000. The external computer sends back a packet to 192.0.2.1 port 11000. The Firewall translates the packet to 10.10.0.26 and sends it to internal computer A.

Internal computer A (10.10.0.26) sends packet to Internet → Firewall translates this address to 192.0.2.1 port 11000 → Internet receives packet from 192.0.2.1 port 11000

Internet sends back packet to 192.0.2.1 port 11000 → Firewall translates this address to 10.10.0.26 → Internal computer A receives packet
NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

- **Original Packet**
- **Translated Packet**

Each section in the NAT Rule Base is divided into cells that define the **Source**, **Destination**, and **Service** for the traffic.

**Automatic and Manual NAT Rules**

There are two types of NAT rules for network objects:

- Rules that SmartConsole automatically creates and adds to the NAT Rule Base
- Rules that you manually create and then add to the NAT Rule Base

When you create manual NAT rules, it can be necessary to create the translated NAT objects for the rule.

**Using Automatic Rules**

You can enable automatic NAT rules for these SmartConsole objects:

- Security Gateways
- Hosts
- Networks
- Address Ranges

SmartConsole creates two automatic rules for Static NAT, to translate the source and the destination of the packets.

For Hide NAT, one rule is created to translate the source of the packets.

For network and address range objects, SmartConsole creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the NAT automatic rules:

<table>
<thead>
<tr>
<th>Type of Traffic</th>
<th>Static NAT</th>
<th>Hide NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal to external</td>
<td>Rule translates source IP address</td>
<td>Rule translates source IP address</td>
</tr>
<tr>
<td>External to internal</td>
<td>Rule translates destination IP address</td>
<td>N/A [External connections are not allowed]</td>
</tr>
<tr>
<td>Intranet (for network and address range objects)</td>
<td>Rule does not translate IP address</td>
<td>Rule does not translate IP address</td>
</tr>
</tbody>
</table>

**Order of NAT Rule Enforcement**

The Firewall enforces the NAT Rule Base in a sequential manner. Automatic and manual rules are enforced differently. Automatic rules can use bidirectional NAT to let two rules be enforced for a connection.
Manual rules - The first manual NAT rule that matches a connection is enforced. The Firewall does not enforce a different NAT rule that can be more applicable.

Automatic rules - Two automatic NAT rules that match a connection, one rule for the Source and one for the Destination can be enforced. When a connection matches two automatic rules, those rules are enforced.

SmartConsole organizes the automatic NAT rules in this order:
1. Static NAT rules for Firewall, or host (computer or server) objects
2. Hide NAT rules for Firewall, or host objects
3. Static NAT rules for network or address range objects
4. Hide NAT rules for network or address range objects

Sample Automatic Rules

Here are some sample automatic rules.

Static NAT for a Network Object
1. Intranet connections in the HR network are not translated. The Firewall does not translate a connection between two computers that are part of the HR object.
   The Firewall does not apply rules 2 and 3 to traffic that matches rule 1.
2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.
3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.

Hide NAT for Address Range
1. Intranet connections in the Sales address range are not translated. The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.
   The Firewall does not apply rule 2 to traffic that matches rule 1.
2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

Configuring Static and Hide NAT

You can enable and configure NAT for SmartConsole objects.

Configuring Static NAT

When you enable Static NAT, each object is translated to a different IP address. SmartConsole can automatically create the NAT rules, or you can create them manually.

Configuring Hide NAT

Hide NAT uses different port numbers to identify the internal IP addresses. When you enable Hide NAT mode, the Firewall can translates the IP address to:

- The IP address of the external Security Gateway interface
- The IP address for the object

Note - You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
Creating an Access Control Policy

- An external server that uses IP addresses to identify different computers and clients

**Enabling Automatic NAT**

SmartConsole can automatically create and configure the NAT rules for a network. Enable automatic NAT for every object, for which you are translating the IP address. Then configure the Access Control Rule Base to allow traffic to the applicable objects.

**To enable automatic NAT:**

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 **NAT > Advanced**.
3. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
4. Select the **Translation method**: **Hide** or **Static**.
5. Configure the NAT IP address for the object.
   - **Hide behind Gateway** - Use the IP address of the Security Gateway
   - **Hide behind IP address** - Enter the IP address.
6. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
7. Click **OK**.

After you enable and configure NAT on all applicable gateways, install the policy.

**Automatic Hide NAT to External Networks**

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses. An easy alternative is to enable a Firewall to automatically Hide NAT for all traffic with external networks. The Firewall translates all traffic that goes through an external interface to the valid IP address of that interface.

In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of an external interface.
Creating an Access Control Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internal networks</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with automatic Hide NAT.</td>
</tr>
<tr>
<td>2A and 2B</td>
<td>Two external interfaces 192.0.2.1 and 192.0.2.100.</td>
</tr>
<tr>
<td>1 --&gt;3</td>
<td>External computers and servers on the Internet</td>
</tr>
</tbody>
</table>

Source IP addresses are translated to the applicable external interface IP address: **192.0.2.1** or **192.0.2.100**.

**Note** - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.

**To enable automatic Hide NAT:**

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 **NAT**.
3. Select **Hide internal networks behind the Gateway’s external IP**.
4. Click **OK**.
5. Install the policy.

**Enabling Manual NAT**

For some deployments, it is necessary to manually define the NAT rules. Create SmartConsole objects that use the **valid** (NATed) IP addresses. Create NAT rules to translate the original IP addresses of the objects to valid IP addresses. Then configure the Firewall Rule Base to allow traffic to the applicable translated objects with these valid IP addresses.

**Note** - For manual NAT rules, it is necessary to configure Proxy ARP entries to associate the translated IP address (on page 119).

These are some situations that must use manual NAT rules:

- Rules that are restricted to specified destination IP addresses and to specified source IP addresses
- Translate both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translate services (destination ports)
- Rules that only use specified services (ports)
- Translate IP addresses for dynamic objects

This procedure explains how to configure manual Static NAT for a web server. You can also configure manual Hide NAT for SmartConsole objects (on page 117).

To enable manual Static NAT, follow this workflow:

1. Create a clone from the network object, for example, the Web server.
2. Add a NAT rule that maps the original object to the NATed one.
3. Add Access Control rules that allow traffic to the new NATed objects.
To create a clone network object:
1. In SmartConsole, right-click the object and select Clone. The General Properties window of the new object opens.
2. Enter the Name. We recommend that you name the object <name>_valid_address.
3. Enter the NATed IP address.
4. Click OK.

To add a NAT rule to the Rule Base:
1. In SmartConsole, go to Security Policies > Access Control > NAT.
2. Add a manual rule above the automatic NAT rules.
3. Configure the manual rule to translate the IP address. For example:
   - Original Source - WebServer
   - Translated Source - WebServer_valid_address

To add Access Control rules:
1. In SmartConsole, go to Security Policies > Access Control > Policy.
2. Add rules that allow traffic to the applicable NATed objects. These objects are the cloned objects that are called <name>_valid_address.
3. Install the policy.

Sample Deployment (Static and Hide NAT)
The goal for this sample deployment is to configure:

- Static NAT for the SMTP and the HTTP servers on the internal network. These servers can be accessed from the Internet using public addresses.
- Hide NAT for the users on the internal network that gives them Internet access. This network cannot be accessed from the Internet.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internal computers [Alaska_LAN 2001:db8::/64]</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateway [External interface 2001:db8::1]</td>
</tr>
<tr>
<td>5</td>
<td>External computers and servers in the Internet</td>
</tr>
</tbody>
</table>
To configure NAT for the network:

1. Enable automatic Static NAT for the web server.
   a) Double-click the Alaska.Web object and select NAT.
   b) Select Add Automatic Address Translation Rules.
   c) In Translation method, select Static.
   d) Select Hide behind IP Address and enter 2001:db8:0:a::5.
   e) Click OK.

2. Enable automatic Static NAT for the mail server.
   a) Double-click the Alaska.Mail object and select NAT.
   b) Select Add Automatic Address Translation Rules.
   c) In Translation method, select Static.
   d) Select Hide behind IP Address and enter 2001:db8:0:a::6.
   e) Click OK.

3. Enable automatic Hide NAT for the internal computers.
   a) Double-click the Alaska_LAN object and select NAT.
   b) Select Add Automatic Address Translation Rules.
   c) In Translation method, select Hide.
   d) Select Hide behind Gateway.

4. Click OK and then install the policy.

Sample Deployment (Manual Rules for Port Translation)

The goal for this sample configuration is to let external computers access a web and mail server in a DMZ network from one IP address. Configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway [Alaska_GW external interface 2001:db8:0:c::1]</td>
</tr>
<tr>
<td>3</td>
<td>DMZ network [Alaska_DMZ 2001:db8:a::/128]</td>
</tr>
<tr>
<td>4</td>
<td>Web server [Alaska_DMZ_Web 2001:db8:a::35:5 translated to 2001:db8:0:c::1]</td>
</tr>
<tr>
<td>5</td>
<td>Mail server [Alaska_DMZ_Mail 2001:db8:a::35:6 translated to 2001:db8:0:c::1]</td>
</tr>
</tbody>
</table>
To configure NAT for the DMZ servers:

1. Enable automatic Hide NAT for the DMZ network.
   a) Double-click the Alaska_DMZ object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.
   e) Click **OK**.

2. Create a manual NAT rule that translates HTTP traffic from the Security Gateway to the web server.
   a) In SmartConsole, go to **Security Policies > Access Control > NAT**.
   b) Add a rule below the automatic rules.
   c) Right-click the cell and select **Add new items** to configure these settings:
      - **Original Destination** - Alaska_GW
      - **Original Service** - HTTP
      - **Translated Destination** - Alaska_DMZ_Web

3. Create a manual NAT rule that translates SMTP traffic from the Security Gateway to the mail server.
   a) Add a rule below the automatic rules.
   b) Right-click the cell and select **Add new items** to configure these settings:
      - **Original Destination** - Alaska_GW
      - **Original Service** - SMTP
      - **Translated Destination** - Alaska_DMZ_Web

4. Create a rule in the Firewall Rule Base that allows traffic to the servers.
   a) In SmartConsole, go to **Security Policies > Access Control > NAT**.
   b) Add a rule to the Rule Base.
   c) Right-click the cell and select **Add new items** to configure these settings:
      - **Destination** - Alaska_DMZ
      - **Service** - HTTP, SMTP
      - **Action** - Allow

5. Install the policy.

**NAT Rule Base for Manual Rules for Port Translation Sample Deployment**

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Original Packet Destination</th>
<th>Service</th>
<th>Source</th>
<th>Translated Packet Destination</th>
<th>Service</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alaska_DMZ</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Alaska_DMZ</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
<td>Automatic rule</td>
</tr>
<tr>
<td>2</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Any</td>
<td>Alaska_DMZ</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
<td>Automatic rule</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
Advanced NAT Settings
This section includes advanced NAT settings.

Deployment Configurations
This section discusses how to configure NAT in some network deployments.

Automatic and Proxy ARP
Giving a computer in the internal network an external IP address using NAT makes that machine appear to the Internet to be on the external network, or the Internet side of the firewall. When NAT is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP requests from the Internet router for the address of the internal machine.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Computer in the internal network with IP address 10.1.1.3</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway with external interface IP address 192.168.0.2 responds to arp requests on behalf of translated internal objects</td>
</tr>
<tr>
<td>3</td>
<td>Translated IP Address on the external network, or the Internet side of the firewall 192.168.0.3</td>
</tr>
<tr>
<td>4</td>
<td>Internet</td>
</tr>
</tbody>
</table>

If you are using manual rules, you must configure proxy ARPs to associate the translated IP address with the MAC address of the Security Gateway interface that is on the same network as the translated addresses.


NAT and Anti-Spoofing
NAT is performed after Anti-Spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT.
Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is normally not necessary to perform NAT. You can disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule slows down the performance of the VPN.

Connecting Translated Objects on Different Interfaces

The following sections describe how to allow connections in both directions between statically translated objects (hosts, networks or address ranges) on different Security Gateway interfaces. If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

Internal Communication with Overlapping Addresses

If two internal networks have overlapping (or partially overlapping) IP addresses, Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each overlapping internal network.

Network Configuration

For example, assume both Network 2A and Network 2B share the same address space (192.168.1.0/24), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.

Users in Network 2A who want to communicate with users in Network 2B must use the 192.168.30.0/24 network as a destination. Users in Network 2B who want to communicate with users in Network 2A must use the 192.168.20.0/24 network as a destination.

The Security Gateway (4) translates the IP addresses in the following way for each individual interface:

Interface 4A

- Inbound source IP addresses are translated to the virtual network 192.168.20.0/24.
- Outbound destination IP addresses are translated to the network 192.168.1.0/24.

Interface 4B

- Inbound source IP addresses are translated to the network 192.168.30.0/24.
- Outbound destination IP addresses are translated to the network 192.168.1.0/24.
Interface 4C

Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface’s IP address (192.168.4.1).

Communication Examples

This section describes how to enable communication between internal networks, and between an internal network and the Internet.

Communication Between Internal Networks

If user 1A, at IP address 192.168.1.10 in Network 2A, wants to connect to user 1B, at IP address 192.168.1.10 (the same IP address) in Network 2B, user 1A opens a connection to the IP address 192.168.30.10.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface 4A — before NAT</td>
<td>192.168.1.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Interface 4A — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
</tbody>
</table>

Security Gateway enforces the security policy for packets from network 192.168.20.0/24 to network 192.168.30.0/24.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface 4B — before NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Interface 4B — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.1.10</td>
</tr>
</tbody>
</table>

Communication Between an Internal Network and the Internet

If user 1A, at IP address 192.168.1.10 in network 2A, connects to IP address 192.0.2.10 on the Internet (3).

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface 4A — before NAT</td>
<td>192.168.1.10</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>Interface 4A — after NAT</td>
<td>192.168.20.10</td>
<td>192.0.2.10</td>
</tr>
</tbody>
</table>

The Security Gateway (4) enforces the security policy for packets from network 192.168.20.0/24 to the Internet (3).

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface 4C — before NAT</td>
<td>192.168.20.10</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>Interface 4C — after NAT</td>
<td>192.168.4.1</td>
<td>192.0.2.10</td>
</tr>
</tbody>
</table>

Routing Considerations

To allow routing from Network 2A to Network 2B, routing must be configured on the Security Gateway.

These sections contain sample routing commands for Windows and Linux operating systems (for other operating systems, use the equivalent commands).

On Windows

- route add 192.168.30.0 mask 255.255.255.0 192.168.3.2
- route add 192.168.20.0 mask 255.255.255.0 192.168.2.2
On Linux

- `route add -net 192.168.30.0/24 gw 192.168.3.2`
- `route add -net 192.168.20.0/24 gw 192.168.2.2`

**Object Database Configuration**

To activate the overlapping NAT feature, use GuiDBedit Tool [see sk13009](http://supportcontent.checkpoint.com/solutions?id=sk13009), or dbedit [see sk13301](http://supportcontent.checkpoint.com/solutions?id=sk13301). In the sample network configuration, the per interface values for interface 4A and interface 4B are set in the following way:

**Sample Network Configuration: Interface Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_overlapping_nat</td>
<td>true</td>
</tr>
<tr>
<td>overlap_nat_dst_ipaddr</td>
<td>The overlapping IP addresses (before NAT). In the sample network configuration, <strong>192.168.1.0</strong> for both interfaces.</td>
</tr>
<tr>
<td>overlap_nat_src_ipaddr</td>
<td>The IP addresses after NAT. In the sample network configuration, <strong>192.168.20.0</strong> for interface 4A, and <strong>192.168.30.0</strong> for interface 4B.</td>
</tr>
<tr>
<td>overlap_nat_netmask</td>
<td>The net mask of the overlapping IP addresses. In the sample network configuration, <strong>255.255.255.0</strong>.</td>
</tr>
</tbody>
</table>

**Security Management Behind NAT**

The Security Management Server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

NAT (Static or Hide) for the Security Management Server IP address can be configured in one click, while still allowing connectivity with managed gateways. All gateways can be controlled from the Security Management Server, and logs can be sent to the Security Management Server. NAT can also be configured for a Management High Availability server and a Log Server.

**Note** - Security Management behind NAT is not supported for deployments where the Security Management Server also acts as a gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management Server (1) is in a network on which Network Address Translation is performed (the “NATed network”). The Security Management Server can control Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary_Security_Management object with IP address 10.0.0.1. Translated address 192.168.55.1</td>
</tr>
</tbody>
</table>

In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A Security Gateway. However, when using Hide NAT on the Security Management Server, gateways can send logs to the Security Management Server.
When using the Security Management behind NAT feature, the remote gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

**To enable NAT for the Security Management Server:**

- From the NAT page of the Security Management Server object, define NAT and select **Apply for A Security Gateway control connections**.

**Non-Corresponding Gateway Addresses**

Sometimes the gateway contacts the Security Management Server with an address that does not correspond to the deployment of the remote gateway. For example:

- When the automatic selection of the gateway does not conform with the routing of the deployment of the gateway. In this case, define the masters and loggers manually, to allow the remote gateway to contact the Security Management Server using the required address. When an inbound connection from a managed gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management Server.

To define masters and loggers, select **Use local definitions for Log Servers** and **Use local definitions for Masters** and specify the correct IP addresses on the gateway.

This solution encompasses different scenarios:

- The remote gateway addresses the NATed IP when you want it to address the real IP.
- The remote gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management Server in the masters file.

**Notes:**

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management Server or as a Log Server.
- Ensure that you properly define the Topology settings on all gateways. All workarounds required for previous versions still function with no changes in their behavior.

**Configuring the Security Management Server Object**

**To configure the Security Management Server object:**

1. From the NAT page on the Primary_Security_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select **Hide behind IP Address**, for example, **192.168.55.1**. Do not select **Hide behind Gateway** (address 0.0.0.0).
2. Select **Install on Gateway** to protect the NATed objects or network. Do not select **All**.
3. Select **Apply for Security Gateway control connections**.

**Configuring the Security Gateway Object**

**To configure the Security Gateway object:**

1. Open the Security Gateway Network Management page
2. Create the Interface. Click **Actions > New interface**.
3. In the General page of the Interface window, define the IP address and the Net Mask.
4. In the Topology section, click **Modify**.
5. Select **Override**.
6. Select **Network defined by the interface IP and Net Mask**.
**IP Pool NAT**

An IP Pool is a range of IP addresses (an address range, a network or a group of one of these objects) that is routable to the gateway. IP Pool NAT ensures proper routing for encrypted connections for the following two connection scenarios:

- Remote Access Client to MEP (Multiple Entry Point) gateways
- Gateway to MEP gateways

When a connection is opened from a Remote Access Client or a client behind a gateway, to a server behind the MEP Gateways, the packets are routed through one of the MEP gateways. Return packets in the connection must be routed back through the same gateway in order to maintain the connection. To ensure that this occurs, each of the MEP gateways maintains a pool of IP addresses that are routable to the gateway. When a connection is opened to a server, the gateway substitutes an IP address from the IP pool for the source IP address. Reply packets from the server return to the gateway, which restores the original source IP address and forwards the packets to the source.

**IP Pool Per Interface**

You can define a separate IP address pool on one or more of the gateway interfaces instead of defining a single pool of IPs for the gateway.

Defining an IP pool per interface solves routing issues that occur when the gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the gateway through the same gateway interface. This illustration shows one of the MEP Gateways in a Remote Access Client to MEP (Multiple Entry Point) gateway deployment.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1     | Packets from source host:  
|       | Source: Original  
|       | Destination: |
| 2     | VPN tunnel through the Internet |
| 3     | MEP Gateway |
| 3A    | IP Pool 1 packets:  
|       | Source: 10.55.8.x  
|       | Destination: |
| 3B    | IP Pool 2 packets:  
|       | Source: 10.55.10.x  
|       | Destination: |
If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct gateway interface through the use of static IP pool NAT addresses.

The remote client's IP address is NATed to an address in the IP pool on one of the gateway interfaces. The addresses in the IP pool can be routed only through that gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the gateway interface, the gateway restores the remote peer's source IP address.

The routing tables on the routers that lie behind the gateway must be edited so that addresses from a gateway IP pool are returned to the correct gateway interface.

Switching between IP Pool NAT per gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.

**NAT Priorities**

IP Pool NAT can be used both for encrypted (VPN) and non-encrypted (decrypted by the gateway) connections.

**Note** - To enable IP Pool NAT for clear connections through the gateway, configure INSPECT changes in the `user.def` file (see sk98239 http://supportcontent.checkpoint.com/solutions?id=sk98239). Contact Check Point Technical Support.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPsec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

The order of NAT priorities are:

1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

**Reusing IP Pool Addresses For Different Destinations**

IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.
Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers (connections 1 and 2). When reusing addresses from the IP Pool, back connections are supported from the original server only (connection 3). This means that connections back to the client can be opened only from the specific server to which the connection was opened.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Gateway with IP Pool addresses A to Z</td>
</tr>
</tbody>
</table>
| 2    | Clients.  
Source: Original  
Destination: |
| 3A   | NATed packet from connection 3.  
Source: A  
Destination: |
| 4A   | NATed packet from connection 4.  
Source: A  
Destination: |
| 5A   | NATed packet from reply connection 5.  
Source: Original  
Destination: A |
| 6A   | This server cannot open a connection with Destination A back to the client. |

The default **Do not reuse IP Pool NAT** behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in the following illustration). In this mode, if an IP pool contains 20 addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client (connection 3).
Switching between the Reuse and Do not reuse modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

**Configuring IP Pool NAT**

**To configure IP Pool NAT:**

1. From the SmartConsole Menu, select Global Properties.
2. In the Global Properties > NAT page, select Enable IP Pool NAT and the required tracking options.
3. In the gateway General Properties page, ensure the gateway version is specified correctly.
4. For each gateway or gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range. For example, for an address range, do the following:
   a) From the Objects Bar (F11), In the network objects tree, select New > More > Network Object > Address Range > Address Range.
      The Address Range Properties window opens.
   b) In the General tab, enter the first and last IP of the address range.
   c) Click OK. The new address range appears in the Address Ranges branch of the network objects tree.
5. Edit the gateway object, and select NAT > IP Pool NAT.
6. In the IP Pool NAT page, select one of the following:
   a) Allocate IP Addresses from and then select the address range you created to configure IP Pool NAT for the whole gateway, or
   b) Define IP Pool NAT on Gateway interfaces to configure IP Pool NAT per interface.
7. If required, select one or more of the following options:
   a) Use IP Pool NAT for VPN client connections
   b) Use IP Pool NAT for gateway to gateway connections
   c) Prefer IP Pool NAT over Hide NAT to specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.
8. Click Advanced.
   a) **Return unused addresses to IP Pool after**: Addresses in the pool are reserved for 60 minutes (default), even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the time-out to prevent the IP Pool from being depleted.
   b) **Reuse IP addresses from the pool for different destinations**: This is a good option unless you need to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.

9. Click OK.

10. Edit the routing table of each internal router so that packets with an IP address assigned from the NAT pool are routed to the appropriate gateway or, if using IP Pools per interface, the appropriate gateway interface.

**IP Pool NAT for Clusters**

IP Pools for gateway clusters are configured in two places in SmartConsole:

- In the gateway Cluster object **NAT > IP Pool NAT** page, select the connection scenario.
- In the Cluster member object **IP Pool NAT** page, define the IP Pool on the cluster member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each cluster member interface.

**Site-to-Site VPN**

The basis of Site-to-Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

**Sample Site-to-Site VPN Deployment**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, B</td>
<td>Security Gateways</td>
</tr>
<tr>
<td>2</td>
<td>VPN tunnel</td>
</tr>
<tr>
<td>3</td>
<td>Internal network in VPN domain</td>
</tr>
<tr>
<td>4</td>
<td>Host 4</td>
</tr>
</tbody>
</table>
In this sample VPN deployment, Host 4 and Host 5 securely send data to each other. The Security Gateways perform IKE negotiation and create a VPN tunnel. They use the IPsec protocol to encrypt and decrypt data that is sent between Host 4 and Host 5.

**VPN Workflow**

- Host 4 sends packet to Host 5
- Firewalls A & B create VPN tunnel
- Firewall A encrypts data
- Host 5 receives unencrypted data
- Firewall B decrypts data
- Encrypted data is sent through VPN tunnel

**VPN Communities**

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

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

**Note** - Global VPN Communities are not supported in this release.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>Satellite Security Gateways</td>
</tr>
<tr>
<td>3</td>
<td>Central Security Gateway</td>
</tr>
</tbody>
</table>
Sample Star Deployment

This section explains how to configure a VPN star community. This deployment lets the satellite Security Gateways connect to the internal network of the central Security Gateway. The internal network object is named: \textit{Internal-network}.

**To create a new VPN Star Community:**

1. In SmartConsole, go to the \textbf{Security Policies} page.
2. In the \textbf{Access Tools} section, click \textbf{VPN Communities}.
3. Click \textbf{New} and select \textbf{Star Community}.
   
   The \textbf{New Star Community} window opens.
4. Enter the name for the community.
5. From the navigation tree, select \textbf{Encryption}.
6. Configure the VPN encryption methods and algorithms for the VPN community.
7. Click \textbf{OK}.

**To configure star VPN for the Security Gateways:**

For each Security Gateway in the VPN community, follow these configuration steps.

1. In SmartConsole, go to the \textbf{Gateways & Servers} page and double-click the Security Gateway object.
   
   The gateway properties window opens.
2. In the \textbf{Network Security} section of the \textbf{General Properties} page, select \textbf{IPsec VPN}.
3. From the navigation tree, go to \textbf{Network Management > VPN Domain}.
   
   • For the central Security Gateway, click \textbf{Manually defined} and select the \textbf{Internal-network} object.
   
   • For a satellite Security Gateway, select \textbf{All IP addresses}.
4. From the navigation tree, click \textbf{IPsec VPN}.
5. Configure the Security Gateway as a member of a VPN star community.
   
   a) In the \textbf{This Security Gateway participates in the following VPN Communities} section, click \textbf{Add}.
      
      The \textbf{Add this Gateway to Community} window opens.
   
   b) Select the VPN Community and click \textbf{OK}.
6. Click \textbf{OK}.

After you create a community and configure Security Gateways, add those Security Gateways to the community as a center or as a satellite gateway.

**To add a Security Gateway to a new star community:**

1. In SmartConsole, go to the \textbf{Security Policies} page.
2. In the \textbf{Access Tools} section, click \textbf{VPN Communities}.
3. Select the new star community and click \textbf{Edit}.
   
   The \textbf{Star Community} window opens.
4. In the \textbf{Gateways} page, add Security Gateways to the community:
   
   • \textbf{Center Gateways} - Click \textbf{Add} and select center gateways. Select \textbf{Mesh center gateways}, if necessary.
- **Satellite Gateways** - Click **Add** and select satellite gateways.

5. Click **OK**.

### Sample Combination VPN Community

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>New York Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>London - New York Mesh community</td>
</tr>
<tr>
<td>4</td>
<td>London company partner [external network]</td>
</tr>
<tr>
<td>5</td>
<td>London Star community</td>
</tr>
<tr>
<td>6</td>
<td>New York company partner [external network]</td>
</tr>
<tr>
<td>7</td>
<td>New York Star community</td>
</tr>
</tbody>
</table>

This deployment is composed of a Mesh community for London and New York Security Gateways that share internal networks. The Security Gateways for external networks of company partners do not have access to the London and New York internal networks. However, the Star VPN communities let the company partners access the internal networks of the sites that they work with.

### Allowing VPN Connections

To allow VPN connections between Security Gateways in specific VPN communities, add Access Control rules that accept such connections.

To allow all VPN traffic to hosts and clients on the internal networks of a specific VPN community, select these options in the **Encrypted Traffic** section of the properties configuration window for that VPN Community:

- For a meshed community: **Accept all encrypted traffic**
- For a Star Community: **Accept all encrypted traffic on Both center and satellite gateways**, or **Accept all encrypted traffic on Satellite gateways only**.
Sample VPN Access Control Rules

This table shows sample VPN rules for an Access Control Rule Base. [The **Action**, **Track** and **Time** columns are not shown. **Action** is set to **Allow**, **Track** is set to **Log**, and **Time** is set to **Any**.]

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>Any</td>
<td>NEGATED Member Gateways</td>
<td>BranchOffices LondonOffices</td>
<td>Any</td>
<td>BranchOffices LondonOffices</td>
</tr>
<tr>
<td>2</td>
<td>Site-to-site VPN</td>
<td>Any</td>
<td>Any</td>
<td>All_GwToGw</td>
<td>FTP-port HTTP HTTPS SMTP</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>3</td>
<td>Remote access</td>
<td>Any</td>
<td>Any</td>
<td>RemoteAccess</td>
<td>HTTP HTTPS IMAP</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

1. **Automatic rule** that SmartConsole adds to the top of the **Implied Rules** when the **Accept All Encrypted Traffic** configuration option is selected for the **BranchOffices VPN community** and the **LondonOffices VPN community**. This rule is installed on all the Security Gateways in these communities. It allows all VPN traffic to hosts and clients on the internal networks of these communities. Traffic that is sent to the Security Gateways in these VPN communities is dropped.

**Note** - This automatic rule can apply to more than one VPN community.

2. **Site-to-site VPN** - Connections between hosts in the VPN Domains of all Site-to-Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

3. **Remote access** - Connections between hosts in the VPN Domains of Remote Access VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

To Learn More About Site to Site VPN

To learn more about Site to Site VPN, see the *R80.10 Site to Site VPN Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=60371.
Remote Access VPN

If employees remotely access sensitive information from different locations and devices, system administrators must make sure that this access does not become a security vulnerability. Check Point’s Remote Access VPN solutions let you create a VPN tunnel between a remote user and the internal network. The Mobile Access Software Blade extends the functionality of Remote Access solutions to include many clients and deployments.

VPN Connectivity Modes

The IPsec VPN Software Blade lets the Firewall overcome connectivity challenges for remote clients. Use VPN connectivity modes to make sure that remote users can connect to the VPN tunnels. These are some examples of connectivity challenges:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a hotel LAN with internal IP addresses
- It is necessary for the remote client to use protocols that are not supported

Office Mode

Remote users can be assigned the same or non-routable IP addresses from the local ISP. Office Mode solves these routing problems and encapsulates the IP packets with an available IP address from the internal network. Remote users can send traffic as if they are in the office and do not have VPN routing problems.

Visitor Mode

Remote users can be restricted to use HTTP and HTTPS traffic only. Visitor Mode lets these users tunnel all protocols with a regular TCP connection on port 443.
Sample Remote Access VPN Workflow

Use SmartConsole to enable and configure the Security Gateway for remote access VPN connections. Then add the remote user information to the Security Management Server: create and configure an LDAP Account Unit or enter the information in the SmartConsole user database. You can also configure the Firewall to authenticate the remote users. Define the Firewall access control and encryption rules. Create the LDAP group or user group object that is used for the Firewall rules. Then create and configure the encryption settings for the VPN community object. Add the access rules to the Firewall Rule Base to allow VPN traffic to the internal networks.

Configuring the Security Gateway for a Remote Access Community

Make sure that the VPN Software Blade is enabled before you configure the Remote Access community.

To configure the Security Gateway for Remote Access:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **IPsec VPN**. The page shows the VPN communities that the Security Gateway is participating.
3. To add the Security Gateway to a Remote Access community:
   a) Click **Add**.
   b) Select the community.
   c) Click **OK**.
4. From the navigation tree, click **Network Management > VPN Domain**.
5. Configure the VPN Domain.
6. Configure the settings for Visitor Mode.
7. From the navigation tree, click **VPN Clients > Office Mode**.
8. Configure the settings for Office Mode.
   **Note** - Office Mode support is mandatory on the Security Gateway side.
9. Click **OK** and publish the changes.

**To Learn More About Remote Access VPN**

To learn more about Remote Access VPN, see the *R80.10 VPN Remote Access Administration Guide* [http://downloads.checkpoint.com/dc/download.htm?ID=53105].

**Mobile Access to the Network**

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the **Mobile Application** in the **Services & Applications** column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the **Source** column of a rule.

**Check Point Mobile Access Solutions**

Check Point Mobile Access has a range of flexible clients and features that let users access internal resources from remote locations. All these solutions include these features:

- Enterprise-grade, secure connectivity to corporate resources
- Strong user authentication
- Granular access control

For more information about the newest versions of Mobile Access solutions and clients, go to [sk67820](http://supportcontent.checkpoint.com/solutions?id=sk67820).

**Client-Based vs. Clientless**

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. The client supplies access to most types of corporate resources according to the access privileges of the user.
Creating an Access Control Policy

- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

**Mobile Access Clients**

- 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 - A full L3 tunnel app that gives users network access to all mobile applications.
- Check Point Mobile for Windows - A Windows IPsec VPN client that supplies secure IPsec VPN connectivity and authentication.

**Mobile Access Web Portal**

The Mobile Access Portal is a clientless SSL VPN solution that supplies secure access to web-based resources. After users authenticate to the portal, they can access Mobile Access applications such as Outlook Web App and a corporate wiki.

**SSL Network Extender**

SSL Network Extender is an on-demand SSL VPN client and is installed on the computer or mobile device from an Internet browser. It supplies secure access to internal network resources.

**Configuring Mobile Access to Network Resources**

**Sample Mobile Access Workflow**

This is a high-level workflow to configure remote access to Mobile Access applications and resources.

1. Use SmartConsole to enable the Mobile Access Software Blade on the gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
   a) Select mobile clients.
   b) Define the Mobile Access portal.
   c) Define applications, for example Outlook Web App.
   d) Connect to the AD server for user information.
3. Select the policy type:
   - The default is to use the Legacy Policy, configured in the **Mobile Access** tab in SmartConsole.
   - To include Mobile Access in the **Unified Access Control Policy**, select this in **Gateway Properties > Mobile Access**.
4. Add rules to the Policy:
Creating an Access Control Policy


5. Configure the authentication settings in Gateway Properties > Mobile Access > Authentication.

Users can access mobile applications through the configured Mobile Access portal with the defined authentication method.

7. Optional: Give secure access to users through the Capsule Workspace app with certificate authentication.
   a) In the gateway Mobile Access > Authentication, click Settings, and select Require client certificate.
   c) Users download the Capsule Workspace app.
   d) Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.

Sample Mobile Access Deployment
This is a sample deployment of a Mobile Access Security Gateway with an AD and Exchange server in the internal network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>2</td>
<td>Mobile Access tunnels</td>
</tr>
<tr>
<td>3</td>
<td>Internet (external networks)</td>
</tr>
</tbody>
</table>
Creating an Access Control Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Mobile Access Security Gateway</td>
</tr>
<tr>
<td>5</td>
<td>Internal network resources, AD and Exchange servers</td>
</tr>
</tbody>
</table>

In this sample Mobile Access deployment, a mobile device uses a Mobile Access tunnel to connect to the internal network. The Mobile Access Security Gateway decrypts the packets and authenticates the user. The connection is allowed and the mobile device connects to the internal network resources.

**Using the Mobile Access Configuration Wizard**

This procedure describes how to enable and configure the Mobile Access Software Blade on a Security Gateway with the Configuration wizard. For this sample configuration, the AD user group **Mobile_Access** contains all the users that are allowed to connect to the internal network. The deployment is based on the Sample Mobile Access Deployment (on page 137).

This configuration lets these clients connect to internal resources:
- Android and iOS mobile devices
- Windows and Mac computers
- Internet browsers can open a SSL Network Extender connection to the internal network

**To configure Mobile Access:**

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** section, select **Mobile Access**.
   The **Mobile Access** page of the **Mobile Access Configuration Wizard** opens.
3. Configure the Security Gateway to allow connections from the Internet and mobile devices.
   Select these options:
   - Web
   - **Mobile Devices** - Select the required options.
   - **Desktops/Laptops** - Select the required options.
4. Click **Next**.
   The **Web Portal** page opens.
5. Enter the primary URL for the Mobile Access portal. The default is `https://<gw_IPv4>/sslvpn`
6. Click **Next**.
   The **Applications** page opens.
7. Configure the applications to show:
   a) In **Web Applications**, make sure Demo web application (World Clock) is selected.
   b) In **Mail/Calendar/Contacts**, enter the domain for the Exchange server and select:
      - Mobile Mail (including push mail notifications)
      - ActiveSync Applications
      - Outlook Web App

   The Mobile Access portal shows links to the Demo web and Outlook Web App applications. The client on the mobile device shows links to the other applications.
8. Click **Next**.
    The **Active Directory** page opens.
9. Select the AD domain and enter the user name and password.
10. Click **Connect**.
    The Security Gateway makes sure that it can connect to the AD server.
11. Click **Next**.
    The **Users** page opens.
    Click **Add** and then select the group **Mobile_Access**.
12. Click **Next** and then click **Finish**.
    The **Mobile Access Configuration Wizard** closes.
13. Click **OK**.
    The **Gateway Properties** window closes.

### Allowing Mobile Connections

The Mobile Access Configuration Wizard enables and configures the Mobile Access Software Blade. It is necessary to add Firewall rules to allow connections from the VPN clients on the computers and devices. Create a Host Node object for the Exchange server, all of the other objects are predefined.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
<th>Track</th>
</tr>
</thead>
</table>

All connections from the RemoteAccess VPN community to the Exchange server are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and MS Exchange. This rule is installed on Security Gateways in the **MobileAccessGW** group.

### Defining Access to Applications

Use the **Security Policies** page in SmartConsole to define rules that let users access Mobile Access applications. The applications that are selected in the Configuration Wizard are automatically added to this page. You can also create and edit the rules that include these SmartConsole objects:

- Users and user groups
- Mobile Access applications
- Mobile Access Security Gateways

### Activating Single Sign On

Enable the SSO (Single Sign On) feature to let users authenticate one time for applications that they use during Mobile Access sessions. The credentials that users enter to log in to the Mobile Access portal can be re-used automatically to authenticate to different Mobile Access applications. SSO user credentials are securely stored on the Mobile Access Security Gateway for that session and are used again if users log in from different remote devices. After the session is completed, the credentials are stored in a database file.
By default, SSO is enabled on new Mobile Access applications that use HTTP. Most Web applications authenticate users with specified Web forms. You can configure SSO for an application to use the authentication credentials from the Mobile Access portal. It is not necessary for users to log in again to each application.

To configure SSO:

1. In SmartConsole, go to Security Policies > Shared Policies > Mobile Access.
2. Click Open Mobile Access Policy in SmartDashboard.
3. In the Mobile Access tab, select Additional Settings > Single Sign On.
   The Single Sign On page opens.
4. Select an application and click Edit.
   The application properties window opens and shows the Single Sign On page.
5. For Web form applications:
   a) In the Application Single Sign On Method section, select Advanced and click Edit.
      The Advanced window opens.
   b) Select This application reuses the portal credentials. Users are not prompted.
   c) Click OK.
   d) Select This application uses a Web form to accept credentials from users.
   e) Click OK.
6. Install the policy.
Connecting to a Citrix Server

Citrix Services

The Mobile Access Software Blade integrates the Firewall Citrix clients and services. It is not necessary to use STA (Secure Ticketing Authority) servers in a Mobile Access Security Gateway deployment because Mobile Access uses its own STA engine. You can also use Mobile Access in a deployment with STA and CSG (Citrix Secure Gateway) servers.

The Mobile Access server certificate must use a FQDN (Fully Qualified Domain Name) that is issued to the FQDN of the Mobile Access Security Gateway.

Sample Deployment with Citrix Server

This is a sample deployment of a Mobile Access Security Gateway and a Citrix web server in the DMZ. The Citrix XenApp server is connected to the internal network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>2</td>
<td>Mobile Access tunnels</td>
</tr>
<tr>
<td>3</td>
<td>Internet (external networks)</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateway for the internal network</td>
</tr>
<tr>
<td>5</td>
<td>Mobile Access Security Gateway in the DMZ</td>
</tr>
<tr>
<td>6</td>
<td>Citrix web interface</td>
</tr>
<tr>
<td>7</td>
<td>Internal network resources</td>
</tr>
<tr>
<td>8</td>
<td>Citrix XenApp (MetaFrame) server</td>
</tr>
</tbody>
</table>

Configuring Citrix Services for Mobile Access

This procedure describes how to configure Mobile Access to let remote users connect to Citrix applications. The deployment is based on the Sample Deployment with Citrix Server (on page 141).

To configure Citrix services:

1. In SmartConsole, go to Manage & Settings > Blades.
2. In the Mobile Access, click Configure in SmartDashboard.
3. In the **Mobile Access** tab, click **Applications > Citrix Services**.

4. Click **New**.
   The **General Properties** page of the **Citrix Service** window opens.

5. Enter the **Name** for the Citrix server object.

6. From the navigation tree, click **Web Interface**.

7. Create a new object for the Citrix web interface server, in **Servers**, click **Manage > New > Host**.
   The **Host Node** window opens.

8. Enter the settings for the Citrix web interface server and click **OK**.

9. In Services, select one or more of these services that the Citrix web interface server supports:
   - HTTP
   - HTTPS

10. From the navigation tree, click **Link in Portal**.

11. Configure the settings for the link to the Citrix services in the Mobile Access portal:
   - **Link text** - The text that is shown for the Citrix link
   - **URL** - The URL for the directory or subdirectory of the Citrix application
   - **Tooltip** - Text that is shown when the user pauses the mouse pointer above the Citrix link

12. From the navigation tree, select **Additional Settings > Single Sign On**.

13. Enable Single Sign On for Citrix services, select these options:
   - **Turn on single Sign On for this application**
   - **Prompt users for their credentials, and store them for future use**

14. Click **OK**.
   The Citrix server object is added to **Defined Citrix Services**.

15. From the Mobile Access navigation tree, select **Policy**.

16. Add the Citrix services object to the applicable rules.
   a) Right-click on the Applications cell of a rule and select **Add Applications**.
   b) Select the Citrix services object.

17. Install the policy.

**Compliance Check**

The Mobile Access Software Blade lets you use the Endpoint Security on Demand feature to create compliance policies and add more security to the network. Mobile devices and computers are scanned one time to make sure that they are compliant before they can connect to the network.

The compliance scanner is installed on mobile devices and computers with ActiveX (for Internet Explorer on Windows) or Java. The scan starts when the Internet browser tries to open the Mobile Access Portal.

**Compliance Policy Rules**

The compliance policy is composed of different types of rules. You can configure the security and compliance settings for each rule or use the default settings.

These are the rules for a compliance policy:
- Windows security - Microsoft Windows hotfixes, patches and Service Packs.
- Anti-Spyware protection - Anti-Spyware software.
Creating an Access Control Policy

- Anti-Virus protection - Anti-Virus software version and virus signature files.
- Firewall - Personal firewall software.
- Spyware scan - Action that is done for different types of spyware.
- Custom - Compliance rules for your organization, for example: applications, files, and registry keys.
- OR group - A group of the above rules. An endpoint computer is compliant if it meets one of the rules in the group.

Creating a Compliance Policy

By default, Endpoint Security on Demand only allows endpoint computers that are compliant with the compliance policy log in to the Mobile Access portal.

To create a compliance policy:

1. In SmartConsole, go to Manage & Settings > Blades.
2. In the Mobile Access section, click Configure in SmartDashboard.
3. In the Mobile Access tab, select Endpoint Security on Demand > Endpoint Compliance.
4. Click Edit policies.
   The Policies window opens.
5. Click New Policy.
   The Policies > New Policy window opens.
6. Enter the Name and Description for the policy.
7. Click Add.
   The Add Enforcement Rules window opens.
8. Select rules for the policy.
   You can also create new rules - click New Rule, and configure the rule settings.
9. Click OK.
   The Policies > New Policy window shows the rules for the policy.
10. Select Bypass spyware scan if necessary.
    When selected, the scan for endpoint computers that are compliant with the Anti-Virus or Anti-Spyware settings is changed. These computers do not scan for spyware when they connect to a Mobile Access Security Gateway.
11. Click OK.
    The Policies window opens.
12. Click OK.

Configuring Compliance Settings for a Security Gateway

The Firewall on a Mobile Access Security Gateway only allows access to endpoint computers that are compliant with the compliance policy.

This procedure shows how to configure the Laptop Computer policy (on page 142) for a Security Gateway.

To configure the compliance settings:

1. In SmartConsole, go to Manage & Settings > Blades.
2. In the Mobile Access section, click Configure in SmartDashboard.
3. In the **Mobile Access** tab, select **Endpoint Security on Demand > Endpoint Compliance**.

4. Select the Security Gateway and click **Edit**.
   
   The **Endpoint Compliance** page of the Security Gateway properties window opens.

5. Select **Scan endpoint machine when user connects**.

6. Select **Threshold policy** and from the drop-down menu select **Laptop Computer**.

7. Click **OK**.

8. Install the policy on the Mobile Access Security Gateway.

**Secure Workspace**

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the “real” workspace. Users can only send data from this secure environment through the Mobile Access portal. Secure Workspace users can only access permitted applications, files, and other resources from the virtual workspace.

Secure Workspace creates an encrypted folder on the computer called **My Secured Documents** and can be accessed from the virtual desktop. This folder contains temporary user files. When the session terminates, Secure Workspace deletes this folder and all other session data.


**To enable Secure Workspace on a Mobile Access Security Gateway:**

1. In SmartConsole, go to **Manage & Settings > Blades**.

2. In the **Mobile Access** section, click **Configure in SmartDashboard**.

3. In the **Mobile Access** tab, click **Endpoint Security on Demand > Secure Workspace**.

4. Select the Security Gateway and click **Edit**.
   
   The **Check Point Secure Workspace** page of the Security Gateway properties window opens.

5. Select **This gateway supports access to applications from within Check Point Secure Workspace**.

6. Click **OK** and then install the policy.

**To Learn More About Mobile Access**

To learn more about Mobile Access VPN, see the **R80.10 Mobile Access Administration Guide** http://downloads.checkpoint.com/dc/download.htm?ID=53103.
Creating a Threat Prevention Policy

In This Section:

Threat Prevention Components ................................................................. 145
Assigning Administrators for Threat Prevention ...................................... 151
Analyzing Threats ..................................................................................... 151
Out-of-the-Box Protection from Threats .................................................... 152
The Threat Prevention Policy ................................................................. 158
Creating Threat Prevention Rules ............................................................ 161
The Check Point ThreatCloud ................................................................. 172
To Learn More About Threat Prevention ................................................ 174

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 cyber security solution, for comprehensive protection against malicious and unwanted network traffic, which focuses on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers.

- **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.

- **SandBlast** - Protection against infections from undiscovered exploits, zero-day and targeted attacks:
  - **Threat Emulation** - 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.
  - **Threat Extraction** - Protection against incoming malicious content. The Threat Extraction capability removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow. To remove possible threats, the Threat Extraction blade creates a safe copy of the file, while the Threat Emulation Software Blade inspects the original file for potential threats.

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 ThreatCloud for use by the other Threat Prevention blades.

**IPS**

The IPS Software Blade delivers complete and proactive intrusion prevention. It delivers 1,000s of signatures, behavioral and preemptive protections. It gives another layer of security on top of Check Point firewall technology. IPS protects both clients and servers, and lets you control the network usage of certain applications. The hybrid IPS detection engine provides multiple defense layers, which allows it excellent detection and prevention capabilities of known threats and in many cases future attacks as well. It also allows unparalleled deployment and configuration flexibility and excellent performance.

**Elements of Protection**

IPS protection includes:

- Detection and prevention of specific known exploits.
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs.
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP.
- Detection and prevention of outbound malware communications.
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering.
- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications.
- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector.

Check Point constantly updates the library of protections to stay ahead of emerging threats.

**Capabilities of IPS**

The unique capabilities of the Check Point IPS engine include:

- Clear, simple management interface.
- Reduced management overhead by using one management console for all Check Point products.
- Integrated management with SmartConsole.
- Easy navigation from business-level overview to a packet capture for a single attack.
- #1 security coverage for Microsoft and Adobe vulnerabilities.
- Resource throttling so that high IPS activity will not impact other blade functionality.
- Complete integration with Check Point configuration and monitoring tools in SmartConsole, to let you take immediate action based on IPS information.

For example, some malware can be downloaded by a user unknowingly when he browses to a legitimate web site, also known as a drive-by-download. This malware can exploit a browser vulnerability to create a special HTTP response and sending it to the client. IPS can identify and
block this type of attack even though the firewall may be configured to allow the HTTP traffic to pass.

**Anti-Bot**

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.

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.

After the discovery of bot infected machines, the Anti-Bot Software Blade blocks outbound communication to C&C sites based on the Rule Base. This neutralizes the threat and makes sure that no sensitive information is sent out.

**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.

**Preventing Bot Damage**

After the discovery of bot infected machines, the Anti-Bot Software Blade blocks outbound communication to C&C sites based on the Rule Base. This neutralizes the threat and makes sure that no sensitive information is sent out.

**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.

**Anti-Virus**

Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats [combinations of malicious code and vulnerabilities for infection and dissemination] and trojans.

The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API.
The Anti-Virus Software Blade:

- Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository:
  - Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance.
  - Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place.
- Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification.

SandBlast

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. To get ahead, enterprises need a multi-faceted prevention strategy that combines proactive protection that eliminates threats before they reach users. With Check Point’s Threat Emulation and Threat Extraction technologies, SandBlast provides zero-day protection against unknown threats that cannot be identified by signature-based technologies.

**Threat Emulation**

Threat Emulation gives networks the necessary protection against unknown threats in web downloads and e-mail attachments. The Threat Emulation engine picks up malware at the exploit phase, before it enters the network. It quickly quarantines and runs the files in a virtual sandbox, which imitates a standard operating system, to discover malicious behavior before hackers can apply evasion techniques to bypass the sandbox.

Threat Emulation receives files through these methods of delivery:
- E-mail attachments transferred using the SMTP or SMTPS protocols.
- Web downloads.
- Files sent to Threat Extraction through the Threat Prevention API.

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.
- After the threat is caught, a signature is created for the new (previously unknown) malware which turns it into a known and documented malware. The new attack information is
automatically shared with Check Point ThreatCloud to block future occurrences of similar threats at the gateway.

If the file is found not to be malicious, you can download the file after the emulation is complete. Learn more about Threat Emulation.

**Threat Extraction**

Threat Extraction is supported on R77.30 and higher.

The Threat Extraction blade extracts potentially malicious content from files before they enter the corporate network. To remove possible threats, the Threat Extraction does one of these two actions:

- Creates a safe copy of the file by converting it to PDF, or
- Extracts exploitable content out of the file.

Threat Extraction receives files through these methods of delivery:

- E-mail attachments received through the Mail transfer Agent (on page 169).
- Files sent to Threat Extraction through the Threat Prevention API.

Threat Extraction delivers the reconstructed file to users and blocks access to the original suspicious version, while Threat Emulation analyzes the file in the background. This way, users have immediate access to content, and can be confident they are protected from the most advanced malware and zero-day threats.

Threat Emulation runs in parallel to Threat Extraction for version R80.10 and higher.

Here are examples for exploitable content in Microsoft Office Suite Applications and PDF files:

- Queries to databases where the query contains a password in the clear
- Embedded objects
- Macros and JavaScript code that can be exploited to propagate viruses
- Hyperlinks to sensitive information
- Custom properties with sensitive information
- Automatic saves that keep archives of deleted data
- Sensitive document statistics such as owner, creation and modification dates
- Summary properties
- PDF documents with:
  - Actions such as launch, sound, or movie URIs
  - JavaScript actions that run code in the reader’s Java interpreter
  - Submit actions that transmit the values of selected fields in a form to a specified URL
  - Incremental updates that keep earlier versions of the document
  - Document statistics that show creation and modification dates and changes to hyperlinks
  - Summarized lists of properties

Before you enable the Threat Extraction blade, you must deploy the gateway as a Mail Transfer Agent.
Assigning Administrators for Threat Prevention

You can control the administrator Threat Prevention permissions with a customized Permission Profile. The customized profile can have different Read/Write permissions for Threat Prevention policy, settings, profiles and protections.

Analyzing Threats

Networks today are more exposed to cyber-threats than ever. This creates a challenge for organizations in understanding the security threats and assessing damage.

SmartConsole helps the security administrator find the cause of cyber-threats, and remediate the network.

The Logs & Monitor > Logs view presents the threats as logs.

The other views in the Logs & Monitor view combine logs into meaningful security events. For example, malicious activity that occurred on a host in the network in a selected time interval (the last hour, day, week or month). They also show pre- and post-infections statistics.

You can create rich and customizable views and reports for log and event monitoring, which inform key stakeholders about security activities. For each log or event, you can see a lot of useful information from the ThreatWiki and IPS Advisories about the malware, the virus or the attack.
Out-of-the-Box Protection from Threats

In This Section:

Getting Quickly Up and Running with the Threat Prevention Policy ........................ 152
Enabling the Threat Prevention Software Blades .................................................... 152
Installing the Threat Prevention Policy ................................................................. 155
Introducing Profiles ............................................................................................... 155
Optimized Protection Profile Settings ................................................................. 156
Predefined Rule ....................................................................................................... 157

Getting Quickly Up and Running with the Threat Prevention Policy

You can configure Threat Prevention to give the exact level of protection that you need, but you can also configure it to provide protection right out of the box.

To get quickly up and running with Threat Prevention:

1. Enable the Threat Prevention blades on the gateway.
2. Install Policy.

After you enable the blades and install the policy, this rule is generated:

<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</td>
<td>Log Packet Capture</td>
<td>*Policy Targets</td>
</tr>
</tbody>
</table>

Notes:

- The Optimized (on page 156) profile is installed by default.
- The Protection/Site column is used only for protection exceptions.

Enabling the Threat Prevention Software Blades

Enabling the IPS Software Blade

Enable the IPS Software Blade on the Security Gateway.

To enable the IPS Software Blade:

1. In the Gateways & Servers view, double-click the gateway object. The General Properties window opens.
2. In the General Properties > Network Security tab, click IPS.
3. Follow the steps in the wizard that opens.
4. Click OK.
5. Click OK in the General Properties window.
6. Install Policy (on page 155).
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 [on page 155].

Enabling the Anti-Virus Software Blade

Enable the Anti-Virus Software Blade on a Security Gateway.

To enable the Anti-Virus Software Blade:

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, click Anti-Bot.
   The Anti-Bot and Anti-Virus First Time Activation window opens.
3. Select one of the activation mode options:
   • According to the Anti-Bot and Anti-Virus policy - Enable the Anti-Virus Software Blade and use the Anti-Virus 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 [on page 155].

Enabling SandBlast Threat Emulation Software Blade

Use the First Time Configuration Wizard in SmartConsole to enable Threat Emulation in the network. Configure the Security Gateway or Emulation appliance for your deployment.

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.
6. Click OK.
   The Gateway Properties window closes.
7. Install Policy (on page 155).

Sample Workflow - Creating a Threat Emulation Profile
This is a sample workflow to create a Threat Prevention profile that includes Threat Emulation.

To create a Threat Prevention profile for Threat Emulation:
1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Click New.
4. Enter the Name for the Threat Prevention profile.
5. In Blades Activation, select the Threat Prevention Software Blades.
6. Configure the Activation Mode settings for the traffic.
7. From the Threat Emulation Settings page, set the Prevent and Ask UserCheck settings.
8. From the navigation tree, click Threat Emulation > General.
9. Configure the Threat Emulation Protected Scope for this profile, and define how traffic from external and internal networks is sent for emulation.
10. Select one or more Protocols for this profile.
    The Software Blade runs emulation only for files and traffic that match the selected protocols.
11. Configure the File Types for this profile.
    The Software Blade runs emulation only for files that match the selected file types.
12. Click OK and install Policy.

Enabling the SandBlast Threat Extraction Blade

To enable the Threat Extraction Blade:
1. In the Gateways & Servers view, right-click the gateway object and select Edit.
   The Gateway Properties window opens.
   The Threat Extraction First Time Activation Wizard opens.
3. Enable the gateway as a Mail Transfer Agent (MTA).
   From the drop-down box, select a mail server for forwarded emails.
4. Click **Next**.
5. Click **Finish**.
   
   **Note:** In a ClusterXL HA environment, do this once for the cluster object.

### Configuring LDAP

If you use LDAP for user authentication, you must activate User Directory for Security Gateways.

**To activate User Directory:**

1. Open **SmartConsole > Global Properties**.
3. Click **OK**.

### Installing the Threat Prevention Policy

The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction 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.

**To install the Threat Prevention policy:**

1. From the Global toolbar, click **Install Policy**.
   
   The **Install Policy** window opens showing the installation targets (Security Gateways).
2. Select **Threat Prevention**.
3. Select **Install Mode**:
   
   - **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**.

### Introducing Profiles

Check Point Threat Prevention provides instant protection based on pre-defined Threat Prevention **Profiles**. You can also configure a custom Threat Prevention profile to give the exact level of protection that the organization needs.

When you install a Threat Prevention policy on the Security Gateways, they immediately begin to enforce IPS protection on network traffic.

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 the Threat Prevention Software Blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.

A profile is a set of configurations based on:

• Activation settings (prevent, detect, or inactive) for each confidence level of protections that the ThreatSpect engine analyzes
• IPS Settings
• Anti-Bot Settings
• Anti-Virus Settings
• Threat Emulation Settings
• Threat Extraction Settings
• Indicator configuration
• Malware DNS Trap configuration
• Links inside mail configuration

Without profiles, it would be necessary to configure separate rules for different activation settings and confidence levels. With profiles, you get customization and efficiency.

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

### Optimized Protection Profile Settings

The **Optimized** profile is activated by default, because it gives excellent security with good gateway performance.

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 all the Threat Prevention Software Blades</td>
<td><strong>Blades Activation</strong></td>
<td>Activate the profile for IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.</td>
</tr>
<tr>
<td>Do not have a critical effect on performance</td>
<td><strong>Performance impact</strong></td>
<td>Activate protections that have a <em>Medium or lower</em> effect on performance.</td>
</tr>
<tr>
<td>Protect against important threats</td>
<td><strong>Severity</strong></td>
<td>Protect against threats with a severity of <em>Medium or above</em>.</td>
</tr>
<tr>
<td>Goal</td>
<td>Parameter</td>
<td>Setting</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Reduce false-positives | Confidence | Set to *Prevent* the protections with an attack *confidence* of *Medium* or *High*.  
|                      |           | Set to *Detect* the protections with a *confidence* of *Low*.            |

**Predefined Rule**

When you enable 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 Optimized profile. By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

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

- When an attack meets the below criteria, the protections are set to **Prevent** mode:
  - **Confidence Level** - Medium or above  
  - **Performance Impact** - Medium or above  
  - **Severity** - Medium or above
- When an attack meets the below criteria, the protections are set to **Detect** mode:
  - **Confidence Level** - Low  
  - **Performance Impact** - Medium or above  
  - **Severity** - Medium or above

Use the **Logs & Monitor** page to show logs related to 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.
The Threat Prevention Policy

**In This Section:**

- Workflow for Creating a Threat Prevention Policy ................................................... 158
- Threat Prevention Policy Layers ................................................................................ 158
- Threat Prevention Rule Base ..................................................................................... 160

**Workflow for Creating a Threat Prevention Policy**

Threat Prevention lets you customize profiles that meet the needs of your organization.

Ideally, you might want to set all protections to Prevent in order to protect against all potential threats. However, to let your gateway processes focus on handling the most important traffic and report only the most concerning threats, you need to determine the most effective way to apply the Threat Prevention settings.

When you define a new Threat Prevention profile, you can create a Threat Prevention Policy which activates only the protections that you need and prevents only the attacks that most threaten your network.

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

2. Update the IPS database and Malware database with the latest protections.
   
   **Note** - For each Policy Layer, configure a Threat Prevention Rule Base with the Threat Prevention profile as the *Action* of the rule.
5. Install the Threat Prevention policy.

**Threat Prevention Policy Layers**

You can create a Threat Prevention Rule Base with multiple Ordered Layers. Ordered Layers help you organize your Rule Base to best suit your organizational needs. You can divide the Ordered Layers by services or networks. Each Ordered Layer calculates its action separately from the other Layers. In case of one Layer in the policy package, the rule enforced is the first rule matched. In case of multiple Layers:

- If a connection matches a rule in only one Layer, then the action enforced is the action in that rule.
- When a connection matches rules in more than one Layer, the gateway enforces the strictest action and settings.

**Important** - When the Threat Prevention blades run in MTA mode, the gateway enforces the automatic MTA rule, which is created when MTA is enabled on the gateway.
**Action Enforcement in Multiple-Layered Security Policies**

These examples show which action the gateway enforces when a connection matches rules in more than one Ordered Layers.

**Example 1**

<table>
<thead>
<tr>
<th>Rule matched</th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 3</td>
<td>Prevent</td>
<td>Detect</td>
</tr>
</tbody>
</table>

**Enforced action:** Prevent

**Example 2**

<table>
<thead>
<tr>
<th>Rule matched</th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 3</td>
<td>Prevent</td>
<td>Detect</td>
</tr>
</tbody>
</table>

**Exception for protection X:** Inactive

**Enforced action for protection X:** Detect

**Example 3**

<table>
<thead>
<tr>
<th>Rule matched</th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 3</td>
<td>Prevent</td>
<td>Detect</td>
</tr>
</tbody>
</table>

**Override for protection X:** Detect

**Exception for protection X:** Inactive

Exception is prior to override and profile action. Therefore, the action for the Data Center Layer is Inactive.

The action for the Corporate LAN Layer is Detect.

**Enforced action for protection X:** Detect

**Example 4**

<table>
<thead>
<tr>
<th>Rule matched</th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 3</td>
<td>Deep Scan all files</td>
<td>Process specific file type families: Inspect doc files and Drop rtf files.</td>
</tr>
</tbody>
</table>

**Enforced action:** Deep Scan doc files and Drop rtf files.

**Example 5**

MIME nesting level and Maximum archive scanning time

**The strictest action is:**

Block combined with the minimum nesting level/scanning time, or
Allow combined with the maximum nesting level/scanning time, or
If both Block and Allow are matched, the enforced action is Block.

**Example 6**

UserCheck

<table>
<thead>
<tr>
<th>Rule matched</th>
<th>HR Layer</th>
<th>Finance Layer</th>
<th>Data Center Layer 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 3</td>
<td>Rule 1</td>
<td>Rule 4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile action</th>
<th>Detect</th>
<th>Prevent</th>
<th>Prevent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured page</td>
<td>Page A</td>
<td>Page B</td>
<td>Page C</td>
</tr>
</tbody>
</table>

The first Layer with the strictest action is enforced.

**Enforced Action:** Prevent with UserCheck Page B.

**Threat Prevention Layers in Pre-R80 Gateways**

In pre-R80 versions, the IPS Software Blade was not part of the Threat Prevention Policy, and was managed separately. In R80.xx versions, the IPS Software Blade is integrated into the Threat Prevention Policy.

When you upgrade SmartConsole to R80.xx from earlier versions, with some Security Gateways upgraded to R80.xx, and other Security Gateways remaining in previous versions:

- For pre-R80 gateways with IPS and Threat Prevention Software Blades enabled, the policy is split into two parallel layers: IPS and Threat Prevention.
  
  To see which Security Gateway enforces which IPS profile, look at the **Install On** column in the IPS Layer.

- R80.xx gateways are managed separately, based on the R80 or higher Ordered Layers [on page 158].

**Best Practice** - For better performance, we recommend that you use the **Optimized** profile when you upgrade to R80 or higher from earlier versions.

**Threat Prevention Rule Base**

Each Threat Prevention Layer contains a Rule Base. The Rule Base determines how the system inspects connections for malware.

The Threat Prevention 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.

There are no implied rules in this Rule Base, traffic is allowed or not allowed based on how you configure the Rule Base. For example, A rule that is set to the **Prevent** action, blocks activity and communication for that malware.
Creating Threat Prevention Rules

In This Section:

- Configuring IPS Profile Settings ................................................................. 161
- Blocking Viruses .......................................................................................... 162
- Configuring Anti-Bot Settings ....................................................................... 163
- Configuring Threat Emulation Settings ....................................................... 165
- Configuring Threat Extraction Settings ....................................................... 169
- Configuring a Malware DNS Trap ............................................................... 169
- Exception Rules ............................................................................................ 170

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

- The Threat Prevention page shows the rules and exceptions for the Threat Prevention policy. The rules set the Threat profiles for the network objects or locations defined as a protected scope.

Click the Add Rule button to get started.

- You can configure the Threat Prevention settings in the Threat Prevention profile for the specified rule.

- To learn about bots and protections, look through the ThreatWiki.

Best Practice - Disable a rule when you work on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Gateway. To disable a rule, right click in the No. column of the rule and select Disable.

Configuring IPS Profile Settings

To configure 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.
6. From the navigation tree, click IPS > Updates.
7. Configure the settings for newly downloaded IPS protections (on page 162).
8. If you import 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 Policy.
**Updates**

There are numerous protections available in IPS. It takes time to become familiar with those that are relevant to your environment. Some are easily configured for basic security and can be safely activated automatically.

In the Threat Prevention profile, you can configure an updates policy for IPS protections that were newly updated. You can do this with the **IPS > Updates** page in the **Profiles** navigation tree. Select one of these settings for **Newly Updated Protections**:

- **Active - According to profile settings** - Protections are activated according to the settings in the **General** page of the Profile. This option is selected by default.
  - **Set activation as staging mode** - Selected by default. Newly updated protections will remain in staging mode until you change their configuration. The default action for the protections is Detect. You can change the action manually in the **IPS Protections** page. Click **Configure** to exclude protections from the staging mode.

- **Inactive** - Newly updated protections will not be activated

**Best Practice** - Allow IPS to activate protections based on the IPS policy in the beginning. During this time, you can analyze the alerts that IPS generates and how it handles network traffic, while you minimize the impact on the flow of traffic. Then you can manually change the protection settings to suit your needs.

**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.
5. Click **Security Policies > Threat Prevention > Policy > Threat Prevention**.
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.
Configuring Anti-Bot Settings

To configure the Anti-Bot 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 Anti-Bot.
5. Configure the Anti-Bot UserCheck Settings:
   - Prevent - Select the UserCheck message that opens for a Prevent action
   - Ask - Select the UserCheck message that opens for an Ask action
6. Click OK and Install Policy.

Blocking Bots

To block bots in your organization, install this default Threat Policy rule that uses the Optimized profile, 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 with the out-of-the-box Threat Prevention policy rule with the default Optimized Profile.
   - 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.
- **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 the gateway detects malware on this scope.
- **Install On** - Keep it as Policy Targets or select Gateways to install the rule on.

4. Install the Threat Prevention policy (on page 155).

### 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><em>Any</em></td>
<td>A profile that has these changes relative to the Optimized profile: Go to the General Policy pane &gt; Activation Mode section, and set all Confidence levels to 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 (on page 155).

**Disabling a Protection on One Server**

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

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

<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>A profile based on the Optimized profile. Edit this profile &gt; go to the General Policy pane &gt; in the Activation Mode section, set every Confidence to Prevent.</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>Server_1</td>
</tr>
</tbody>
</table>

**To add an exception to a rule:**

1. In SmartConsole, click Threat Prevention > Policy > Layer.
2. Click the rule that contains the scope of Server_1.
3. Click the Add Exception toolbar button to add the exception to the rule. The gateway applies the first exception matched.
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. When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them, if archive scanning is enabled.
   - **Action** - Keep it as Detect.
   - **Track** - Keep it as Log.
   - **Install On** - Keep it as Policy Targets or select specified gateways to install the rule on.
6. Install Policy.

**Configuring Threat Emulation Settings**

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this:

1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway. The gateway window opens and shows the General Properties page.
2. From the navigation tree, click Network Management and then double-click a DMZ interface.
3. In the General page of the Interface window, click Modify.
4. In the **Topology Settings** window, click **Override** and **Interface leads to DMZ**.
5. Click **OK** and close the gateway window.

Do this procedure for each interface that goes to the DMZ.

If there is a conflict between the Threat Emulation settings in the profile and for the Security Gateway, the profile settings are used.

**Note** - The MIME Nesting settings are the same for Anti-Virus, Threat Emulation and Threat Extraction.

**To configure Threat Emulation 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 **Threat Emulation > General**.
5. Select the Threat Emulation **UserCheck Settings** options:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action
   - **Ask** - Select the UserCheck message that opens for an **Ask** action
6. In the **Protected Scope** section, select an interface type and traffic direction option:
7. Select the applicable **Protocols** to be emulated.
8. In the **Protected Scope** section, select an interface type and traffic direction option:
   - **Inspect incoming files from**:
     - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
     - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
     - **All** - Inspect all incoming files from all interface types.
   - **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.
9. **Optional**: Configure how Threat Emulation does emulation for SMTP traffic.
   a) Click **Configure**.
      
The **Threat Prevention Mail Configuration** window opens.
   b) Configure the **MIME Nesting** settings.
      - **Maximum MIME nesting is X levels** - For emails that contain nested MIME content, Set the maximum number of levels that the ThreatSpect engine scans in the email.
      - **When nesting level is exceeded block/allow file** - If there are more nested levels of MIME content than the configured amount, select to **Block** or **Allow** the email file.
10. Select the **File Types** to be emulated.
11. Click **OK** and close the Threat Prevention profile window.
12. Install the Threat Prevention policy.

**Selecting the Threat Emulation Action**

What are the available emulation actions that I can use with a Threat Emulation profile?
• **Prevent** - Files do not go to the destination computer until emulation is completed. If Threat Emulation discovers that a file contains malware, the malicious file does not enter the internal network. Users can notice a delay when downloading a file, because they cannot download and open the file until the emulation is complete.

• **Detect** - The file is sent to the destination and to Threat Emulation. If Threat Emulation discovers that a file contains malware, the appropriate log action is done. Users receive all files without delay.

**Note** - To estimate the system requirements and amount of file emulations for a network, go to sk93598 http://supportcontent.checkpoint.com/solutions?id=sk93598.

**Configuring the Virtual Environment** (Profile)

You can use the **Emulation Environment** window to configure the emulation location and images that are used for this profile.

The **Analysis Locations** section lets you select where the emulation is done.

The **Environments** section lets you select the operating system images on which the emulation is run. If the images defined in the profile and the Security Gateway or Emulation appliance are different, the profile settings are used.

These are the options to select the emulation images:

• Check Point automatically updates images and adds new ones.

• Select the images that are closest to the operating systems for the computers in your organization.

**To configure the virtual environment settings for the profile:**

1. From the Threat Prevention profile navigation tree, select **Threat Emulation > Emulation Environment**.
   The **Emulation Environment** page opens.

2. Set the **Analysis Location** setting:
   - To use the Security Gateway settings for the location of the virtual environment, click **According to the gateway**
   - To configure the profile to use a different location of the virtual environment, click **Specify** and select the applicable option

3. Set the **Environments** setting:
   - To use the emulation environments recommended by Check Point security analysts, click **Use Check Point recommended emulation environments**
   - To select one or more images that are used for emulation, click **Use the following emulation environments**

4. Click **OK** and close the Threat Prevention profile window.

5. Install the Threat Prevention policy.

**Excluding Emails**

You can enter email addresses that are not included in Threat Emulation protection. SMTP traffic that is sent to or from these addresses is not sent for emulation.

**Note** - If you want to do emulation on outgoing emails, make sure that you set the Protected Scope to **Inspect incoming and outgoing files**.
To exclude emails from Threat Emulation:

1. From the Threat Prevention profile navigation tree, select Threat Emulation > Excluded Mail Addresses.

2. In the Recipients section, you can click the Add button and enter one or more emails. Emails and attachments that are sent to these addresses will not be sent for emulation.

3. In the Senders section, you can click the Add button and enter one or more emails. Emails and attachments that are received from these addresses will not be sent for emulation.

   Note - You can also use a wildcard character to exclude more than one email address from a domain.

4. Click OK and close the Threat Prevention profile window.

5. Install the Threat Prevention policy.

Preparing for Local or Remote Emulation

Prepare the network and Emulation appliance for a Local or Remote deployment in the internal network.

1. Open SmartConsole.

2. Create the network object for the Emulation appliance.

3. If you are running emulation on HTTPS traffic, configure the settings for HTTPS Inspection.

4. Make sure that the traffic is sent to the appliance according to the deployment:
   - Local Emulation - The Emulation appliance receives the traffic. The appliance can be configured for traffic the same as a Security Gateway.
   - Remote Emulation - The traffic is routed to the Emulation appliance.

Using Local or Remote Emulation

This section is for deployments that use an Emulation appliance and run emulation in the internal network.

Note - Prepare the network for the Emulation appliance before you run the First Time Configuration Wizard (on page 168).

To enable an Emulation appliance for Local and Remote emulation:

1. In SmartConsole, go to Gateways & Servers and double-click the Emulation appliance. 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.


4. Click Next. The Summary page opens.

5. Click Finish to enable Threat Emulation on the Emulation appliance and close the First Time Configuration Wizard.

6. Click OK. The Gateway Properties window closes.

7. For Local emulation, install the Threat Prevention policy on the Emulation appliance.
To enable Threat Emulation on the Security Gateway for Remote emulation:

1. In SmartConsole, go to Gateways & Servers and double-click the Security Gateway. 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. Configure the Security Gateway for Remote Emulation:
   a) Select Other Emulation appliance.
   b) From the drop-down menu, select the Emulation appliance.

4. Click Next.
   The Summary page opens.

5. Click Finish to enable Threat Emulation on the Security Gateway close the First Time Configuration Wizard.

6. Click OK.
   The Gateway Properties window closes.


Configuring Threat Extraction Settings

To configure Threat Extraction settings for a Threat Prevention profile:

1. In the Security Policies view > Threat Tools section, click Profiles.

2. Right-click a profile and select Edit.
   The Profiles properties window opens.


4. Configure these Threat Extraction Settings:
   • General
   • Exclude/Include Users
   • Advanced.

5. Click OK.

Note - You can configure some of the Threat Extraction features in a configuration file, in addition to the CLI and GUI. See sk114613 http://supportcontent.checkpoint.com/solutions?id=sk114613.

Configuring Threat Extraction on the Security Gateway

1. In the Gateways & Servers view, open the gateway properties > Threat Extraction page.

2. Set the Activation Mode to Active.

3. In the Resource Allocation section, configure the resource settings.

4. Click OK.

5. Install Policy.

Configuring a Malware DNS Trap

The Malware DNS trap works by configuring the Security Gateway to return a false (bogus) IP address for known malicious hosts and domains. You can use the Security Gateways external IP
address as the DNS trap address but:

- Do not use a gateway address that leads to the internal network
- Do not use the gateway internal management address
- If the gateway external IP address is also the management address, select a different address for the DNS trap.

You can also add internal DNS servers to better identify the origin of malicious DNS requests.

Using the Malware DNS Trap you can detect compromised clients by checking logs with connection attempts to the false IP address.

At the Security Gateway level, you can configure the DNS Trap according to the profile settings or as a specific IP address for all profiles on the specific gateway.

**To set the Malware DNS Trap parameters for the 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 Malware DNS Trap.
5. Click Activate DNS Trap.
6. Enter the IP address for the DNS trap.
7. Optional: Add Internal DNS Servers to identify the origin of malicious DNS requests.
8. Click OK and close the Threat Prevention profile window.
9. Install the Threat Prevention policy.

**To set the Malware DNS Trap parameters for a gateway:**

1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
2. From the navigation tree, select Anti-Bot and Anti-Virus.
3. In the Malicious DNS Trap section, select one of these options:
   - According to profile settings - Use the Malware DNS Trap IP address configured for each profile.
   - IPv4 - Enter an IP address to be used in all the profiles assigned to this Security Gateway.
4. Click OK.
5. Install the policy.

**Exception Rules**

If necessary, you can add an exception directly to a rule. An exception sets a different Action to an object in the Protected Scope from the Action specified Threat Prevention rule. In general, exceptions are designed to give you the option to reduce the level of enforcement of a specific protection and not to increase it. For example: The Research and Development (R&D) network protections are included in a profile with the Prevent action. You can define an exception which sets the specific R&D network to Detect. For some Anti-Bot and IPS signatures only, you can define exceptions which are stricter than the profile action.

You can add one or more exceptions to a rule. The exception is added as a shaded row below the rule in the Rule Base. It is identified in the No. column with the rule’s number plus the letter E and
a digit that represents the exception number. For example, if you add two exceptions to rule number 1, two lines will be added and show in the Rule Base as E-1.1 and E-1.2.

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

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

**To add an exception to a rule:**

1. In the **Policy** pane, select the rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. Enter values for the columns. Including these:
   - **Protected Scope** - Change it to reflect the relevant objects.
   - **Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection(s) and click **OK**.
5. **Install Policy**.

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

**Blade Exceptions**

You can also configure an exception for an entire blade.

**To configure a blade exception:**

1. In the **Policy**, select the Layer rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. In the **Protection/Site** column, select **Blades** from the drop-down menu.
5. Select the blade you want to exclude.
6. **Install Policy**.
The Check Point ThreatCloud

In This Section:

- Updating IPS Protections ........................................................................................................ 173
- Scheduling Updates ................................................................................................................. 173
- Updating Threat Emulation ...................................................................................................... 174

Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Customers can send their own threat data to the ThreatCloud and benefit from increased security and protection and enriched threat intelligence. The ThreatCloud distributes attack information, and turns zero-day attacks into known signatures that the Anti-Virus Software Blade can block. The Security Gateway does not collect or send any personal data.

Participation in Check Point information collection is a unique opportunity for Check Point customers to be a part of a strategic community of advanced security research. This research aims to improve coverage, quality, and accuracy of security services and obtain valuable information for organizations.

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.

For the reputation and signature layers of the ThreatSpect engine, each Security Gateway also has:

- A local database, the Malware database that contains commonly used signatures, URLs, and their related reputations. You can configure automatic or scheduled updates for this database.
- A local cache that gives answers to 99% of URL reputation requests. When the cache does not have an answer, it queries the ThreatCloud repository.
  - For Anti-Virus - the signature is sent for file classification.
  - For Anti-Bot - the host name is sent for reputation classification.

Access the ThreatCloud repository from:

- **SmartConsole** - You can add specific malwares to rule exceptions when necessary. From the Threat Prevention Rule Base in SmartConsole, click the plus sign in the Protection column in the rule exceptions, and the Protection viewer opens.
- **ThreatWiki** - A tool to see the entire Malware database. Open ThreatWiki in SmartConsole or access it from the Check Point website.

Data which Check Point Collects

When you enable information collection, the Check Point Security Gateway collects and securely submits event IDs, URLs, and external IPs to the Check Point Lab regarding potential security risks.

For example:

<entry engineType="3" sigID="-1" attackName="CheckPoint - Testing Bot" sourceIP="7a1ec646fe17e2cd" destinationIP="d8c8f142" destinationPort="80" host="www.checkpoint.com" path="/za/images/threatwiki/pages/TestAntiBotBlade.html" numOfAttacks="20" />
This is an example of an event that was detected by a Check Point Security Gateway. It includes the event ID, URL, and external IP addresses. Note that the data does not contain confidential data or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

**Updating IPS Protections**

Check Point constantly develops and improves its protections against the latest threats. You can immediately update IPS with real-time information on attacks and all the latest protections. You can manually update the IPS protections and also set a schedule when updates are automatically downloaded and installed. IPS protections include many protections that can help manage the threats against your network. Make sure that you understand the complexity of the IPS protections before you manually modify the settings.

*Note* - To enforce the IPS updates, you must install policy.

**To update IPS Protections:**

1. In SmartConsole, click **Security Policies > Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the **IPS > Update Now**, from the drop-down menu, select:
   - Download using SmartConsole (if your Security Management Server has no internet access), or
4. **Install 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. Optional, for IPS only:
   - **Select Perform retries on update failure** - lets you configure how many tries the Scheduled Update makes if it does not complete successfully the first time.
• Select **On successful update perform Install Policy** - automatically installs the policy on the devices you select after the IPS update is completed. Click **Configure** to select these devices.

8. Click **OK**.
9. Click **Close**.
10. **Install Policy**.

### Updating Threat Emulation

Threat Emulation connects to the ThreatCloud to update the engine and the operating system images. The default setting for the Threat Emulation appliance is to automatically update the engine and images.

The default setting is to download the package once a day.

**Best Practice** - Configure Threat Emulation to download the package when there is low network activity.

Update packages for the Threat Emulation operating system images are usually more than 2GB. The actual size of the update package is related to your configuration.

**To enable or disable Automatic Updates for Threat Emulation:**

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Updates**.
   
   The **Updates** page opens.
3. Under Threat Emulation, click **Schedule Update**.
4. Select or clear these settings:
   - **Enable Threat Emulation engine scheduled update**
   - **Enable Threat Emulation images scheduled update**
5. Click **Configure** to configure the schedule for Threat Emulation engine or image updates.
6. Configure the automatic update settings to update the database:
   - To update once a day, select **At** and enter the time of day
   - To update multiple times a day, select **Every** and set the time interval
   - To update once or more for each week or month:
     a) **Select At** and enter the time of day.
     b) **Click Days**.
     c) **Click Days of week** or **Days of month**.
     d) **Select the applicable days**.
7. Click **OK** and then install the Threat Prevention policy.

### To Learn More About Threat Prevention

Managing User Accounts

In This Section:

- Authentication Methods for Users and Administrators ........................................... 175
- Configuring Authentication Methods for Users ........................................................ 176
- User Database ............................................................................................................ 180
- Managing User Groups ............................................................................................... 183
- LDAP and User Directory ........................................................................................... 184
- Access Roles ............................................................................................................... 213
- Authentication Rules .................................................................................................. 214

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 180) 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 38).

For background information about the authentication methods, see Authentication Methods for Users and Administrators (on page 175).

**Granting User Access Using RADIUS Server Groups**

The Security Gateway lets you control access privileges for authenticated RADIUS (on page 175) 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 176) 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 User Database on the Security Management Server.

1. In SmartConsole, click **Manage & Settings > Blades.**
2. In the **Mobile Access** section, click **Configure in SmartDashboard.**
   Legacy SmartDashboard opens.
3. In the bottom left Network Objects pane, and click **Users.**
4. Right-click on an empty space and select the applicable option:
   - If you support only one external authentication scheme, select **New > External User Profile > Match all users.**
   - If you support more than one external authentication scheme, select **New > External User Profile > Match by domain.**
5. Configure the **External User Profile** properties:
   a) **General Properties** page:
      - If selected **Match all users,** then configure:
        In the **External User Profile name** field, leave the default name *generic*.
        In the **Expiration Date** field, set the applicable date.
      - If selected **Match by domain,** then configure:
        In the **External User Profile name** field, enter the applicable name. This name will be used to authenticate users on the ACE/Server.
        In the **Expiration Date** field, set the applicable date.
        In the **Domain Name matching definitions** section, configure the applicable settings.
b) **Authentication** page:
   
   From the **Authentication Scheme** drop-down list, select **SecurID**.

c) Click **OK**.

6. From the top toolbar, click **Update** (Ctrl + S).

7. Close the Legacy SmartDashboard.

**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.**
   

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 TACACS+ Authentication**

To configure a Security Gateway to use TACACS+ authentication, you must set up the server and enable its use on the Security Gateway.

**To define a TACACS+ server:**

1. Define a TACACS Host object: **Object Explorer** (Ctrl+E) > **New** > **Host**

2. Enter a name and IP address.

3. Define a TACACS server: **Object Explorer** (Ctrl+E) > **New** > **Server** > **More** > **TACACS**.

4. Enter a name.

5. In **Host**, select the TACACS host.

6. Select the **Type**.
   
   **Best Practice**: The default is **TACACS**, but **TACACS+** is recommended.

7. In **Service**, select the **TACACSpplus** service [or **TACACS** UDP service if you selected **TACACS** type].

8. Enter a **Secret key**. (If you selected **TACACS** type, this is not available. If you selected **TACACS+**, it is required.)

9. Click **OK**.

**To enable TACACS on the Security Gateway:**

1. Right-click the gateway object and select **Edit**.

2. Click **Other** > **Legacy Authentication**.

3. In the **Enabled Authentication Schemes** section, click **TACACS**.

4. Click **OK**.
To enable TACACS authentication for users:
1. In the Object Explorer, click Users > User Templates.
2. Edit the Default user template.
3. In the Authentication page, Authentication method list, select TACACS.
4. When TACACS server shows, select the TACACS server you defined.
5. Click OK.

When you create a new user account, TACACS is the default selected authentication.

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 Bar (F11)tree, click New > More > User > User.
   The New User window opens.
2. Choose a template and click OK.
3. Configure required and optional settings in General Properties (on page 181).
4. Select and configure Authentication (on page 181).
   Important! If you do not select an authentication method, the user cannot log in or use network resources.
5. In Location (on page 181), select objects from which this user can access or send data and traffic.
6. If the user has specified working days or hours, configure when (on page 181) the user can be authenticated for access.
7. 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 (on page 182) 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 > Location**

In the **Allowed locations** section:

**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**

**From** and **To** - 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.

**Days in week** or **Daily** - 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.

**User > 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.

User > 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 when you open the properties of the user in SmartConsole.

To configure the default expiration settings:

1. From the Menu, select Global Properties.
   - The Global Properties window opens.
2. Click User Accounts.
3. Select Expire at or Expire after.
   - Expire at - Select the expiration date from the calendar control.
Managing User Accounts

• **Expire after** - Enter the number of days (from the day the account is made) before user accounts expire.

4. Select **Show accounts expiration indication**, and enter the number of days.
   Expiration warnings in the SmartConsole User object 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 Bar** (F11), click **New > More > User > 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 Bar** (F11), select **Object Categories > User > User Groups**
2. Right click the User group and click **Edit**.
   The **User Group** window opens.
3. Click **+**
4. Select users or user groups.
5. Click **OK**.
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 (on page 210).
- *Multiple Account Units*, for distributed databases.
- *Define LDAP Account Units*, for encrypted User Directory connections (on page 210).
- *Profiles*, to support multiple LDAP vendors (on page 192).

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 (on page 207), 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 207).
- Decide whether you will use High Availability (on page 210) setup.
- Determine the order of priority (on page 211) among the User Directory servers for High Availability and querying purposes.
- Assign users (on page 212) 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 (on page 185).

In This Section

- Schema Checking ................................................................. 185
- OID Proprietary Attributes ................................................... 185
- User Directory Schema Attributes ......................................... 186
- Netscape LDAP Schema ....................................................... 192

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 is 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 (on page 186) for the value of “X”.
### User Directory Schema Attributes

**Attributes:**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>186</td>
</tr>
<tr>
<td>uid</td>
<td>187</td>
</tr>
<tr>
<td>description</td>
<td>187</td>
</tr>
<tr>
<td>mail</td>
<td>187</td>
</tr>
<tr>
<td>member</td>
<td>187</td>
</tr>
<tr>
<td>userPassword</td>
<td>187</td>
</tr>
<tr>
<td>fw1authmethod</td>
<td>187</td>
</tr>
<tr>
<td>fw1authserver</td>
<td>188</td>
</tr>
<tr>
<td>fw1pwdLastMod</td>
<td>188</td>
</tr>
<tr>
<td>fw1expiration-date</td>
<td>188</td>
</tr>
<tr>
<td>fw1hour-range-from</td>
<td>188</td>
</tr>
<tr>
<td>fw1hour-range-to</td>
<td>188</td>
</tr>
<tr>
<td>fw1day</td>
<td>189</td>
</tr>
<tr>
<td>fw1allowed-src</td>
<td>189</td>
</tr>
<tr>
<td>fw1allowed-dst</td>
<td>189</td>
</tr>
<tr>
<td>fw1allowed-vlan</td>
<td>189</td>
</tr>
<tr>
<td>fw1SR-keym</td>
<td>189</td>
</tr>
<tr>
<td>fw1SR-datam</td>
<td>189</td>
</tr>
<tr>
<td>fw1SR-mdm</td>
<td>189</td>
</tr>
<tr>
<td>fw1enc-fwz-expiration</td>
<td>189</td>
</tr>
<tr>
<td>fw1sr-auth-track</td>
<td>190</td>
</tr>
<tr>
<td>fw1groupTemplate</td>
<td>190</td>
</tr>
<tr>
<td>fw1ISAKMP-EncMethod</td>
<td>190</td>
</tr>
<tr>
<td>fw1ISAKMP-AuthMethods</td>
<td>190</td>
</tr>
<tr>
<td>fw1ISAKMP-HashMethods</td>
<td>190</td>
</tr>
<tr>
<td>fw1ISAKMP-Transform</td>
<td>190</td>
</tr>
<tr>
<td>fw1ISAKMP-DataIntegrityMethod</td>
<td>191</td>
</tr>
<tr>
<td>fw1ISAKMP-SharedSecret</td>
<td>191</td>
</tr>
<tr>
<td>fw1ISAKMP-DataEncMethod</td>
<td>191</td>
</tr>
<tr>
<td>fw1enc-Methods</td>
<td>191</td>
</tr>
<tr>
<td>fw1UserPwdPolicy</td>
<td>191</td>
</tr>
<tr>
<td>fw1badPwdCount</td>
<td>191</td>
</tr>
<tr>
<td>fw1lastLoginFailure</td>
<td>191</td>
</tr>
<tr>
<td>memberof template</td>
<td>191</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

mail

User’s email address.

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

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}xxyyyyyyyyyy
```

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 these:

RADIUS, TACACS, SecurID, OS Password, Defender

This default value for this attribute is overridden by Default authentication scheme in the **Authentication** tab of the **Account Unit** window in SmartConsole. 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 authentication 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>&quot;undefined&quot;</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>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

**fw1hour-range-from**

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

<table>
<thead>
<tr>
<th>“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>&quot;00:00&quot;</td>
</tr>
</tbody>
</table>

**fw1hour-range-to**

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

<table>
<thead>
<tr>
<th>“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>&quot;23:59&quot;</td>
</tr>
</tbody>
</table>
**fw1day**

The days on which the user can login to a Security Gateway. Can have the values "SUN", "MON", 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.
"X" in OID | fw1person | fw1template
---|---|---
18 | y | y

**fw1sr-auth-track**

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

| "X" in OID | fw1person | fw1template | default
---|---|---|---
19 | y | y | “none”

**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.

| "X" in OID | fw1person | fw1template | default
---|---|---|---
20 | y | y | “False”

**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.

| "X" in OID | fw1person | fw1template | default
---|---|---|---
21 | y | y | “DES”, “3DES”

**fw1ISAKMP-AuthMethods**

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

| "X" in OID | fw1person | fw1template | default
---|---|---|---
22 | y | y | “signatures”

**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.

| "X" in OID | fw1person | fw1template | default
---|---|---|---
23 | y | y | “MD5”, “SHA1”

**fw1ISAKMP-Transform**

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

| "X" in OID | fw1person | fw1template | default
---|---|---|---
24 | y | y | “ESP”
**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>“SHA1”</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>“DES”</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>“FWZ”</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>

**fw1lastLoginFailure**

Time of the last login failure.

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>4</td>
</tr>
</tbody>
</table>

**memberof template**

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

<table>
<thead>
<tr>
<th>“X” 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:

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

UserLoginAttr

The unique username User Directory attribute [uid]. In addition, when fetching users by the username, this attribute is used for query.
### Managing User Accounts

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<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 is User Directory attribute.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<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></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>fw1template</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**ExpirationDateAttr**

The account expiration date is 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></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<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></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>CP format is yyyymmdd</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**PsswdDateAttr**

The format of the password modified date is 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></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>• CP (most servers) format is yyyymmdd</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 is User Directory attribute.

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

- 0 for most servers
- 1 for Netscape_DS

If not using encrypted password, SSL is recommended

**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></td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

- Plain (for most servers)
- Crypt (for Netscape_DS)
- SHA1

**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}</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

{Crypt} (for Netscape_DS)

**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></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 SmartConsole.

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

**BranchOCOperator**

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

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

**OrganizationObjectClass**

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

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

**OrgUnitObjectClass**

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

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

**DomainObjectClass**

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

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

**UserObjectClass**

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

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

#### UserOCOperator

If ‘one’ is set, an OR'ed query will be sent and every object that matches one of the types will be displayed as a user. If ‘all’ an AND’ed 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 Groupofuniquenames (most servers) Group Groupofnames (in Microsoft_AD)</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

#### GroupOCOperator

If ‘one’ is set an OR'ed query will be sent and every object that matches one of the types will be displayed as a user. If ‘all’ an AND’ed 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>

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) • MemberOf mode defines the group DN in the member object (in Microsoft_AD) • Modes define member DN in Group object and group DN in Member object.</td>
<td>One value allowed</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.
**Default** | **Other**  
---|---  
MemberOf | One value allowed  

**TemplateMembership**

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

| Default | Other |  
|---|---|---  
| | | One value allowed  

- Member mode defines the member DN in the Group object (most servers)  
- MemberOf mode defines the group DN in the member object (in Microsoft_AD)

**TemplateMembershipAttr**

Defines which attribute to use when reading the User members from the template object, as User DNs, if the TemplateMembership mode is Member.

| Default | Other |  
|---|---|---  
| | | Multiple values allowed  

**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.

| Default | Other |  
|---|---|---  
| | | Multiple values allowed  

**OrganizationRDN**

This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when you create a new organizational unit in SmartConsole.

| Default | Other |  
|---|---|---  
| | | One value allowed  

**OrgUnitRDN**

This value is used as the attribute name in the Relatively Distinguished Name (RDN) when you create a new organizational Unit in SmartConsole.

| Default | Other |  
|---|---|---  
| | | One value allowed  

**UserRDN**

This value is used as the attribute name in the Relatively Distinguished Name (RDN), when you create a new User object in SmartConsole.

| Default | Other |  
|---|---|---  
| | | One value allowed  

**GroupRDN**

This value is used as the attribute name for the RDN, when you create a new Group object in SmartConsole.
Default | Other
---|---

cn | One value allowed

**DomainRDN**
This value is used as the attribute name for the RDN, when you create a new Domain object in SmartConsole.

Default | Other
---|---
dc | One value allowed

**AutomaticAttrs**
This field is relevant when you create objects in SmartConsole. The format of this field is `Objectclass:name:value` meaning that if the object created is of type `ObjectClass` then additional attributes will be included in the created object with name `name` and value `value`.

Default | Other
---|---
user:userAccountControl:66048 | Multiple values allowed
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 you modify a group in SmartConsole. 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 is used.

Default | Other
---|---
groupOfNames:member | Multiple values allowed
groupOfUniqueNames:uniqueMember
(All other servers)

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

Default | Other
---|---
OrganizationalUnit | Multiple values allowed

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

Default | Other
---|---
Organization | Multiple values allowed

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

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>User (in Microsoft_AD) person organizationalPerson inetOrgPerson fw1Person (All other servers)</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**DomainObjectClass**

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

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

### 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 204]).

### 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 in 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.

```plaintext
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:

```plaintext
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:

**Note** - A shell script is available for UNIX gateways. The script is at:

```
$FWDIR/lib/ldap/update_schema_microsoft_ad
```

```
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
```
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. In SmartConsole, go to Manage & Settings > Blades.
2. Click Configure in SmartDashboard.

   SmartDashboard opens.
3. In the Objects Tree, click Users.
4. Double-click the Account Unit to open a connection to the LDAP server.
5. 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.
6. Define the query.
7. 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 yyyyymmdd 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:

```
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>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Security Gateway - Queries LDAP user information, retrieves CRLs, and does bind operations for authentication</td>
</tr>
<tr>
<td>4</td>
<td>Security Management Server - Uses User Directory to manage user information</td>
</tr>
<tr>
<td>5</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 (on page 207).

**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**.
Managing User Accounts

The User Directory page opens.

3. Configure login and password settings.
4. Click OK.
5. In the Gateways & Servers view (Ctrl+1), 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 (press the CTRL+E keys).
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 (on page 208) - Configure how the Security Management Server uses the Account Unit
   - Servers (on page 208) - Manage LDAP servers that are used by this Account Unit
   - Objects Management (on page 209) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - Authentication (on page 209) - Configure the authentication scheme for the Account Unit
5. Click OK.
6. Install the Access Control 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** [on page 208] - Configure how the Security Management Server uses the Account Unit
   - **Servers** [on page 208] - Manage LDAP servers that are used by this Account Unit
   - **Objects Management** [on page 209] - Configure the LDAP server for the Security Management Server to query and the branches to use
   - **Authentication** [on page 209] - Configure the authentication scheme for the Account Unit

3. Click **OK**.

4. Install the Access Control 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. To learn about these settings, see the Help. Click ? or press F1 in the **Encryption** tab.

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) (on page 211). 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.
### Managing User Accounts

<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. On each Account Unit, to which you want to authenticate with a certificate, set the `ldap_use_cert_auth` attribute to `true`:
   b) In the left pane, browse to **Table > Managed Objects > servers**.
   c) In the right pane, select the Account Unit object.
   d) In the bottom pane, search for the `ldap_use_cert_auth` attribute, and set it to `true`.
   e) Save the changes and close GuiDBedit.
2. Log in to SmartConsole.
3. Add a CA object:
   a) From the **Objects Bar** (F11), click **New > More > Server > More > Trusted CA**.

The Certificate Authority Properties window opens.
b) In Certificate Authority Type, select **External Check Point CA**.
c) Set the other options of the CA.

4. 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.

5. Test connectivity between the Security Management Server and the LDAP Server (on page 212).

**Managing Users on a User Directory Server**

In SmartConsole, 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 SmartConsole, 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 SmartDashboard to manage information about users and OUs (Organizational Units) that are stored on the LDAP server.

**To manage LDAP information from SmartDashboard:**

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. Click **Configure in SmartDashboard**.
   
   SmartDashboard opens.
3. From the object tree, select **Servers and OPSEC**.
4. Double-click the Account Unit.
   
   The LDAP domain is shown.
5. Double-click the LDAP branch.
   
   The Security Management Server queries the LDAP server and SmartDashboard shows the LDAP objects.
6. Expand the **Objects List** pane.
7. Double-click the LDAP object.
   
   The **Objects List** pane shows the user information.
8. Right-click a user and select **Edit**.  
   The **LDAP User Properties** window opens.
9. 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 **R80.10 Identity Awareness Administration Guide** [http://downloads.checkpoint.com/dc/download.htm?ID=54825](http://downloads.checkpoint.com/dc/download.htm?ID=54825).

Authentication Rules

To make an authentication rule:

1. Add users to user groups.
2. Define an access role (on page 213) 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 ...................................................................................... 215
Creating Client Certificates ........................................................................................ 216
Revoking Certificates ................................................................................................. 216
Creating Templates for Certificate Distribution ....................................................... 217
Cloning a Template ..................................................................................................... 218
Giving Permissions for Client Certificates .............................................................. 218

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 (on page 218).

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 Manage & Settings > Blades > Mobile Access > Configure in 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:**

1. In SmartConsole, select **Security Policies > Access Control > Access Tools > Client Certificates**.
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.
     You can select both QR Code and HTML link to include both in the email.
     The text in Display Text is the text that shows on the link.

a. 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- Select one client type that users will have installed.
     ▪ 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.

b. 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:
1. Define an administrator (on page 28).
2. Create a customized profile for the administrator (on page 31), with permission to handle client certificates. Configure this in the **Others** page of the Administrator Profile. Restrict other permissions.
Database Revisions

The Security Management architecture has built-in revisions. Each revision is a new restore point in the database. It contains only the changes from the previous revision. Revisions therefore need only a small amount of disk space, and are created fast. Other benefits of this architecture are:

- Fast policy verification, based on the difference between installed revisions.
- More efficient Management High Availability.
- Safe recovery from a crisis.

This diagram shows the database revisions over time:

1. Install
2. Upgrade
3. Publish
4. Publish
5. Publish

Working with Database Revisions

To see saved database versions:
In SmartConsole, go to Manage & Settings > Revisions.

To see the changes made during a specific revision:
1. In the Manage & Settings > Revisions window, select revision.
   The bottom pane shows the audit logs of the changes made in the revision.
2. Optional: 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 revision.
2. Click **Purge**.
3. In the confirmation window that opens, click **Yes**.

**Important** - Deletion is irreversible. When you purge, that revision and older revisions are deleted permanently.

## Managing a Crisis Using Database Revisions

<table>
<thead>
<tr>
<th>Case</th>
<th>A connectivity or security problem after making changes to the policy and installing the policy</th>
</tr>
</thead>
</table>
| Solution | 1. Go to **Security Policies > Installation History**.  
2. In the **Policy Installation History**, choose the last known good version and click **Install specific version**.  
After a Gateway is safely installed, the Gateway has the last good revision, and the Security Management Server has the most recent revision.  
3. To see the changes made in the revision, browse the audit logs in the bottom pane of the revision. |

<table>
<thead>
<tr>
<th>Case</th>
<th>Network problem after downloading a Threat Prevention update and installing it on gateways.</th>
</tr>
</thead>
</table>
| Solution | 1. From **Security Policies > Threat Prevention > Threat Tools > Updates**, in the **IPS** section, choose an update that is known to be good.  
2. Click **Switch to Version**.  
3. Install the Threat Prevention Policy.  
The Gateway gets that version of the IPS protections. Other network objects and policies do not change. |

### More Database Revision Scenarios:

- Need a full environment restore to a certain point in time.  
  **Best Practice**: Use **Restore Backup**. All work done after the backup is lost. To learn more, see the **R80.10 Gaia Administration Guide**  
- To revert to a previous state, use **Revert Policy**. This reverts the structure of the Rule Base, but not the objects used in the Rule Base.

## 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.

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. Click Preferences > Login Message.
   The Login Message window opens.
3. Select Show custom message during login.
4. In Customize Message, enter a Header 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, select Add warning sign.
6. If you want the Login window to show your organization’s logo, in Customize Layout, select Add logo and then Browse to an image file.

Testing New SmartConsole Features

You can influence Check Point product development by selecting and testing one or more of the new features listed here.

To test a new SmartConsole feature:

1. Click Manage & Settings.
2. Click Preferences.
3. In the Check Point Lab area, select the feature you want to test:
   • Enable Session pane - Review all changes before you publish
Sync with User Center

You can add information regarding your environment to User Center, such as gateway name, version, and active blades. Check Point uses this additional information for better inventory management, pro-active support, and more efficient ticket resolution.

To learn more, see sk94064 http://supportcontent.checkpoint.com/solutions?id=sk94064.

To sync with User Center:
1. In SmartConsole, click Manage & Settings.
2. Click Sync with User Center
3. Select Synchronize information once a day.

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 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
   - Service - 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.
Management High Availability

In This Section:

- Overview of Management High Availability ............................................................... 225
- The High Availability Environment ............................................................................. 225
- Configuring a Secondary Server in SmartConsole ................................................... 226
- Synchronizing Active and Standby Servers ............................................................... 227
- Changeover Between Active and Standby ................................................................. 228
- Changing a Server to Active or Standby ................................................................. 229
- High Availability Troubleshooting .............................................................................. 229
- Environments with Endpoint Security ....................................................................... 230
- High Availability Disaster Recovery ........................................................................... 230

Overview of Management High Availability

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

Management High Availability uses the built-in revisions technology and allows the High Availability procedure to synchronize only the changes done since the last synchronization. This provides:

- Real-time updates between management peers.
- Minimal effect on the management server resources.

The first management server installed is the primary. If the primary Security Management Server fails, or is off line for maintenance, the administrator can initiate a changeover, so that the secondary server takes over.

Notes:


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 active management server at intervals synchronizes its database with the secondary server or servers.
Active vs. Standby

In a standard High Availability configuration there is one Active server at a time. The administrator uses the Active server to manage the High Availability configuration. The Active server automatically synchronizes the standby server(s) at regular intervals. You can open a Standby server only in Read Only mode. If the Active server fails, you can initiate a changeover to make a Standby server become the Active server. If communication with the Active server fails, there may be more than one Active server. This is called Collision Mode.

Primary Server vs. Secondary Server

The sequence 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 by default.

**Important** - Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Virtual Machine Snapshots, see the vendor documentation.

Configuring a Secondary Server in SmartConsole

In the SmartConsole connected to the Primary server, create a network object to show the Secondary Security Management Server. After you publish, synchronize starts between the primary and secondary servers.

**To configure the secondary server in SmartConsole:**

1. Open SmartConsole.
2. In Object Categories, click **New > More > Network Object > Gateways and Servers > CheckPoint Host**.
3. On the General Properties page, enter a unique name and IP address for the server.
4. In the Software Blades section, select the Management tab.
5. Select Network Policy Management.

---

**Security Management Administration Guide R80.10 (Part of Check Point Infinity) | 226**
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 initialization and synchronization between the servers start.

9. Monitor these tasks in the Task List, in the SmartConsole System Information area. Wait for the Task List 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.

**Synchronizing Active and Standby Servers**

At intervals, the Active server synchronizes with the standby server or servers, and when you publish the session. Sessions that are not published are not synchronized.

**Monitoring High Availability**

The **High Availability Status** window shows the status of each Security Management Server in the High Availability configuration.

**To see the server status 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 **High Availability Status** window shows:

- A Warning or Error message – The message shows if there is a problem between the High Availability peers.

- **Connected To** - The server that SmartConsole is connected to. Also, the High Availability mode of the server (Active or Standby), and the synchronization status and actions of the server (on page 227).

- **Peers** - The servers that the connected server sees. Also, the High Availability mode of each server (Active or Standby), and the synchronization status and actions of each server.

**Monitoring Synchronization Status and Actions**

Status messages can be general, meaning that they apply to the full system, or they can 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>The database of the primary Security Management Server is identical with the database of the secondary.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Some servers could not be synchronized</th>
<th>A communication issue prevents synchronization, or some other synchronization issue exists.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The active and standby servers are not communicating.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communication Problem</th>
<th>Some services are down or cannot be reached.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Collision or HA conflict</th>
<th>More than one management server configured as active. Two active servers cannot sync with each other.</th>
</tr>
</thead>
</table>

When connected to a specified *active* management server:

<table>
<thead>
<tr>
<th>Status window area:</th>
<th>Peer Status</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connected to:</strong></td>
<td>Active</td>
<td>SmartConsole is connected to the active management server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peers</th>
<th>Standby</th>
<th>The peer is in standby. The message can also show:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Sync problem, last time sync</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Synchronized successfully. Last sync time: &lt;time&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No communication</td>
</tr>
</tbody>
</table>

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>Peer Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connected to:</strong></td>
<td>Standby</td>
<td>Also shows: last sync time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peers</th>
<th>Active</th>
<th>The peer is in standby. The message can also show:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• No communication, last sync time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OK., last sync time: &lt;time&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sync problem, last sync time (in any direction)</td>
</tr>
</tbody>
</table>

| Standby or Unknown | Can also show: no communication. |

**Changeover Between Active and Standby**

Changeover 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 this manually. When the management server becomes Standby it becomes Read Only, and gets all changes from the new Active server.
Changing a Server to Active or Standby

The Active server synchronizes with the Standby server or servers at intervals, and when you publish the session. Sessions that are not published are not synchronized.

When the administrator initiates changeover, all public data is synchronized from the new Active to the new Standby server after the Standby becomes Active. Data from the new Active overrides the data on the new Standby. Unpublished changes are not synchronized.

**Best Practice** - We recommend that you publish changes before initiating a changeover to the Standby.

To Interchange the Active and Standby:

1. Open SmartConsole.
2. Connect to the Standby server.
3. On the Menu button, select High Availability.
   
   The High Availability Status window opens.
4. Use the Action buttons to change the Standby server to Active.

This changes the previous Active server to Standby.

Working in Collision Mode

You can make more than one server Active. You may need to do that if there is no connectivity to the primary. When you change the Standby to Active, it becomes Active without telling the current Active server to become Standby. This is known as collision mode. You can later change one of the Active servers to Standby, and return to the standard configuration.

When in collision mode, the Active servers do not sync even if they have network connectivity. When you change one of them to Standby, sync starts and overwrites the data on the Standby server with the remaining Active data.

High Availability Troubleshooting

These error messages show in the High Availability Status window when synchronization fails:

**Not communicating**

Solution:

1. Check connectivity between the servers.
2. Test SIC.

**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.
**Warning** - When this server becomes the Standby, all its data is overwritten by the active server.

**Sync Error**
Solution:
Do a manual sync.

---

**Environments with Endpoint Security**

Environments that include Endpoint Security require additional steps and information.


---

**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 (on page 230)
  
  **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.

---

**Creating a New Primary Management Server**

**To create a new Primary Management Server:**

1. Change the Secondary Management Server from Standby to Active.
2. Promote the Secondary Management Server to be Primary. Follow the procedure of Promoting a Secondary Management Server (on page 230) (no need to do step 5).
3. Install the new Secondary Management Server with the IP of the old Primary Management Server.
4. Reset SIC and connect with SIC to the new Secondary Management Server.

**To set the old Primary Management Server as the new Primary Management Server:**

1. Change the new Secondary Management Server from Standby to Active.
2. Promote the new Secondary Management Server to be the Primary Management Server. Follow the procedure of Promoting a Secondary Management Server (on page 230) (no need to do step 5).
4. Reset SIC and connect with SIC to the Secondary Management Server.

---

**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.

**Note** - This is the disaster recovery method supported for High Availability environments with Endpoint Security.

**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.

For more information, see:

- sk30501: Setting up the ICA Management Tool
- sk102837: Best Practices - ICA Management Tool configuration
- sk39915: Invoking the ICA Management Tool

**In This Appendix**

- Using the ICA Management Tool ................................................................. 233
- Enabling and Connecting to the ICA Management Tool ............................... 233
- The ICA Management Tool GUI ................................................................. 233
- User Certificate Management .................................................................. 234
- Performing Multiple Simultaneous Operations ............................................. 235
- ICA Administrators with Reduced Privileges .............................................. 235
- Management of SIC Certificates .............................................................. 235
- Management of Gateway VPN Certificates ............................................... 235
- Management of User Certificates in SmartConsole .................................... 236
- Notifying Users about Certificate Initialization .......................................... 236
- Retrieving the ICA Certificate .................................................................... 236
- Searching for a Certificate ........................................................................... 236
- Removing and Revoking Certificates and Sending Email Notifications ......... 238
- Submitting a Certificate Request to the CA ................................................ 238
- Initializing Multiple Certificates Simultaneously ....................................... 239
- CRL Management ....................................................................................... 240
- CRL Operations ........................................................................................ 241
- CA Cleanup ................................................................................................ 241
- Configuring the CA .................................................................................... 241
- CA Data Types and Attributes .................................................................. 241
- Certificate Longevity and Statuses ............................................................. 245
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>
</tbody>
</table>
The ICA Management Tool

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Operations Pane</strong>&lt;br&gt;Manage certificates. The window divides into <strong>Search attributes configuration</strong> and <strong>Bulk operation configuration</strong>.&lt;br&gt;<strong>Create Certificates.</strong>&lt;br&gt;<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.&lt;br&gt;<strong>Manage CRLs.</strong> Download, publish, and recreate CRLs.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Search Results Pane.</strong> 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.<br><br>**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>2048 bits</td>
<td>yes</td>
<td>Can be set to 4096 bits</td>
</tr>
<tr>
<td>DN of User certificates managed by the internal database</td>
<td>CN=user name, OU=users</td>
<td>no</td>
<td>This DN is appended to the DN of the ICA</td>
</tr>
<tr>
<td>DN of User certificates managed on an LDAP server</td>
<td></td>
<td>yes</td>
<td>Depends on LDAP branch</td>
</tr>
<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. Go to Advanced, and in the **Advanced Configuration** section, click **configure**.
   
   The **Advanced Configuration** window opens.
3. Go to the **Certificates and PKI properties** page.
4. Set the new key size for this property: `user_certs_key_size`.
5. Click **OK**.

You can also change the key size using the GuiDBedit Tool [see sk13009](http://supportcontent.checkpoint.com/solutions?id=sk13009). 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 in SmartConsole.


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://<Management Server IP address>: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 SmartConsole > **Logs & Monitor** > **Logs**.
- 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**.
2. Search for certificates (on page 236) with set attributes. 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 236).

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 pane, 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 `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:

```
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 (on page 184).

**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 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.
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 (on page 241) 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 (\(<\text{number}\>\) days \(<\text{number}\>\) seconds) or as a number of seconds.

- **Integer** - a regular integer, for example: **SIC Key Size**: 2048
- **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, max-12</td>
<td>6</td>
</tr>
<tr>
<td><strong>CRL Duration</strong></td>
<td>The period of time for which the CRL is valid.</td>
<td>min-5 minutes, max-1 year</td>
<td>1 week</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, max-5 years</td>
<td>1 week</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, max-1 week</td>
<td>1 day</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, max-20 years</td>
<td>5 years</td>
</tr>
<tr>
<td>IKE Certificate Extended Key Usage</td>
<td>Certificate purposes for describing the type of the extended key usage for IKE certificates. Refer to RFC 2459.</td>
<td>means no KeyUsage</td>
<td></td>
</tr>
<tr>
<td>IKE Certificate Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459.</td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
<tr>
<td>Management Tool DN prefix</td>
<td>Determines the DN prefix of a DN that will be created when entering a user name.</td>
<td>possible values CN= UID=</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>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>min-one week</td>
<td>2 years</td>
</tr>
<tr>
<td>Management Tool Mail From Address</td>
<td>When sending mails this is the email address that will appear in the from field. A report of the mail delivery status will be sent to this address.</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Management Tool Mail Subject</td>
<td>The email subject field.</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 | -             |
<p>| 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. |                         | -             |</p>
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Comment</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Certificates Per Distribution Point</td>
<td>The maximum capacity of a CRL in the new CRL mode.</td>
<td>min-3 max-400</td>
<td>400</td>
</tr>
<tr>
<td>New CRL Mode</td>
<td>A Boolean value describing the CRL mode.</td>
<td>0 for old CRL mode 1 for new mode</td>
<td>true</td>
</tr>
<tr>
<td>Number of certificates per search page</td>
<td>The number of certificates that will be displayed in each page of the search window.</td>
<td>min-1 max-approx 700</td>
<td>approx 700</td>
</tr>
<tr>
<td>Number of Digits for Serial Number</td>
<td>The number of digits of certificate serial numbers.</td>
<td>min-5 max-10</td>
<td>5</td>
</tr>
<tr>
<td>Revoke renewed certificates</td>
<td>This flag determines whether to revoke an old certificate after it has been renewed. The reason for not revoking this is to prevent the CRL from growing each time a certificate is renewed. If the certificate is not revoked the user may have two valid certificates.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>SIC Key Size</td>
<td>The key size in bits of keys used in SIC.</td>
<td>possible values: 1024 2048 4096</td>
<td>2048</td>
</tr>
<tr>
<td>SIC Certificate Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459.</td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
<tr>
<td>SIC Certificate Validity Period</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>User Certificate Extended Key Usage</td>
<td>Certificate purposes for describing the type of the extended key usage for User certificates. Refer to RFC 2459.</td>
<td>means no KeyUsage</td>
<td></td>
</tr>
<tr>
<td>User Certificate Key Size</td>
<td>The key size in bits of the user's certificates.</td>
<td>Possible values: 1024 2048 4096</td>
<td>2048</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.

### Attribute Table

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Comment</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Certificate Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459</td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
</tbody>
</table>
Security Management Server
Commands

In This Section:

- cpca_client .................................................................................................................. 246
- cp_conf ........................................................................................................................ 250
- cpconfig ....................................................................................................................... 255
- cpinfo ........................................................................................................................... 256
- cplic ............................................................................................................................. 257
- cppkg ........................................................................................................................... 272
- cprinstall ..................................................................................................................... 275
- cpstart and cpstop ...................................................................................................... 286
- cpstat ........................................................................................................................... 287
- dbedit ........................................................................................................................... 288
- dynamic objects .......................................................................................................... 290
- fw logswitch ................................................................................................................ 291
- fwm .............................................................................................................................. 293
- inet_alert ..................................................................................................................... 295
- ldap .............................................................................................................................. 297
- queryDB_util ............................................................................................................... 303
- rs_db_tool ................................................................................................................... 304

For more information about Security Management Server, see the R80.10 Security Management Administration Guide

cpca_client

Description   Executes operations on the ICA (Internal Certificate Authority).

Syntax:
> cpca_client

cpca_client revoke_cert

Description   Revokes a certificate issued by the ICA.

Syntax:
> cpca_client [-d] revoke_cert [-p <ca_port>] -n "CN=<common name>"

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Runs the command in debug Mode.</td>
</tr>
</tbody>
</table>
### Security Management Server Commands

#### cpca_client lscert

**Description**  Shows all certificates issued by the ICA.

**Syntax:**

```plaintext
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d</code></td>
<td>Runs the command in debug Mode.</td>
</tr>
<tr>
<td><code>-dn substring</code></td>
<td>Filters results to those with a DN that matches this <code>&lt;substring&gt;</code>.</td>
</tr>
<tr>
<td><code>-stat</code></td>
<td>Filters results to the specified certificate status: Pending, Valid, Revoke, Expire, or Renewed</td>
</tr>
<tr>
<td><code>-kind</code></td>
<td>Filters results for specified kind: SIC, IKE, User, or LDAP</td>
</tr>
<tr>
<td><code>-ser &lt;serial&gt;</code></td>
<td>Filters results for this serial number.</td>
</tr>
<tr>
<td><code>-dp &lt;dp&gt;</code></td>
<td>Filters results from this CDP (certificate distribution point).</td>
</tr>
</tbody>
</table>

#### cpca_client init_certs

**Description**  Imports a list of DNs for users and creates a file with registration keys for each user.

**Syntax:**

```plaintext
> cpca_client init certs [-p <ca_port>] -i <input_file> -o <output_file>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-p &lt;ca_port&gt;</code></td>
<td>Specifies the port which is used to connect to the CA. The default port is 18265</td>
</tr>
<tr>
<td><code>-i &lt;input_file&gt;</code></td>
<td>Imports the specified file. Make sure to use the full path. Make sure that there is an empty line between each DN in the file: CN=test1,OU=users &lt;empty line&gt; CN=test2,OU=users</td>
</tr>
<tr>
<td><code>-o &lt;output_file&gt;</code></td>
<td>Saves the registration keys to the specified file.</td>
</tr>
</tbody>
</table>
**cpca_client set_mgmt_tool**

**Description** Starts or stops the ICA Management Tool.

**Syntax:**

```
> cpca_client [-d] set_mgmt_tool {on|off|add|remove|clean|print} [-p <ca_port>] [-no_ssl] [-a <administrator DN>, -u <user DN>, -c <custom user DN>, ...]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Runs the command in debug mode.</td>
</tr>
</tbody>
</table>
| set_mgmt_tool {on|off|add|remove|clean|print} | - on - Starts ICA management tool.  
- off - Stops ICA management tool.  
- add - Adds an administrator, user, or custom user.  
- remove - Removes an administrator, user, or custom user.  
- clean - Removes all the administrators, users, or custom users.  
- print - Shows the administrators, users, or custom users. |
| -p <ca_port> | Specifies the port which is used to connect to the CA. The default port is 18265 |
| -no_ssl | Configures the server to use HTTP instead of HTTPS. |
| -a <administrator DN> | Sets the DNs of the administrators that are permitted to use the ICA management tool. |
| -u <user DN> | Sets the DNs of the users that are permitted to use the ICA management tool. |
| -c <custom user DN> | Sets the DN for custom users that can use the ICA management tool. |

**Notes**

1. If the command is run without -a or -u the list of the permitted users and administrators isn’t changed. The server can be stopped or started with the previously defined permitted users and administrators.

2. If two consecutive start operations are initiated, the ICA management tool will not respond, unless you change the SSL mode. After the SSL Mode has been modified, the server can be stopped and restarted.

**cpca_client set_sign_hash**

**Description** Sets the hash algorithm that the CA uses to sign the file hash. The default algorithm is sha1

**Syntax:**

```
> cpca_client set_sign_hash {sha1|sha256|sha384|sha512}
```
**cpca_client search**

**Description**  
Searches for certificates in the ICA (Internal Certificate Authority).

**Syntax:**

```bash
> cpca_client search <string> [-where {dn|comment|serial}] [-kind [SIC|IKE|User|LDAP]] [-stat [Pending|Valid|Revoked|Expired|Renewed]] [-max <max results>] [-showfp {y|n}]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-where</td>
<td>Where to search for the string, in the <strong>dn</strong>, <strong>serial number</strong>, or <strong>comment</strong> field. The default is all locations.</td>
</tr>
<tr>
<td>-kind</td>
<td>The type of certificate. You can enter multiple values in this format: <code>-kind value1 value2 value3</code>. The default is all values.</td>
</tr>
<tr>
<td>-stat</td>
<td>Filters according to the status of the certificate. You can enter multiple values in this format: <code>-stat value1 value2 value3</code>. The default is all values.</td>
</tr>
<tr>
<td>-max &lt;max results&gt;</td>
<td>Enter the maximum number of results to show. The default setting is 200.</td>
</tr>
<tr>
<td>-showfp {y</td>
<td>n}</td>
</tr>
</tbody>
</table>

**Example:**

```bash
> cpca_client search samplecompany -where comment -kind SIC LDAP -stat Pending Valid Renewed
```

**cpca_client get_crldp**

**Description**  
Defines how to access a CRL file from a distribution point.

**Syntax:**

```bash
> cpca_client get_crldp [-p <ca_port>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA. The default port is 18265s</td>
</tr>
</tbody>
</table>

**cpca_client get_pubkey**

**Description**  
Saves the encoding of the public key for the ICA to a file.

**Syntax:**

```bash
> cpca_client [-p <ca_port>] get_pubkey <output>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA. The default port is 18265</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;output&gt;</td>
<td>Name of the file where the public key is saved.</td>
</tr>
</tbody>
</table>

### cpca_client double_sign

**Description**  
Creates a second signature for a certificate.

**Syntax:**

```bash
> cpca_client [-p <ca_port>] -i <cert file> [-o <output file>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA. The default port is 18265</td>
</tr>
<tr>
<td>-i &lt;cert file&gt;</td>
<td>Imports the specified certificate only in PEM format.</td>
</tr>
<tr>
<td>[-o &lt;output file&gt;]</td>
<td>Saves the certificate to the specified file.</td>
</tr>
</tbody>
</table>

### cp_conf

**Description**  
Configures or reconfigures a Check Point product installation. The configuration options for each machine depend on the configuration and installed products.

**Syntax**

```bash
cp_conf
-h
admin
add [<UserName> <Password> {a | w | r}]
add -gaia [{a | w | r}]
del <UserName1> <UserName2> ...
get
auto
(enable | disable) <Product1> <Product2> ...
get all
ca
fqdn <FQDN Name>
init
client
add <GUI Client>
createlist <GUI Client 1> <GUI Client 2> ...
del <GUI Client 1> <GUI Client 2> ...
get
finger get
lic
add -f <Full Path to License File>
add -m <Host> <Date> <Signature Key> <SKU/Features>
del <Signature Key>
get
sic
cert_pull <Management Server> <DAIP GW object>
init <Activation Key> [norestart]
state
snmp
{activate | deactivate} [norestart]
```
### Parameters

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Shows the entire built-in usage.</td>
</tr>
</tbody>
</table>
| admin {add | del | get} | Configures Check Point system administrators for the Security Management Server:  
|            | • add - Adds a system administrator  
|            | • del - Deletes the specified system administrators  
|            | • get - Shows the list of the configured system administrators  
| Notes:     | • Multi-Domain Server does not support this command.  
|            | • This command corresponds to the option "(2) Administrator" in the cpconfig menu. |
| auto {get all | {enable | disable} ...} | Shows and configures the automatic start of Check Point products during boot:  
|            | • Check Point Security Gateway  
|            | • QoS (former FloodGate-1)  
|            | • SmartEvent Suite  
| Note - This command corresponds to the option "(8) Automatic start of Check Point Products" in the cpconfig menu. |
| ca {fqdn | init} | • Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN).  
|            | • Initializes the Internal Certificate Authority (ICA).  
| Note - This command corresponds to the option "(6) Certificate Authority" in the cpconfig menu. |
| client {add | createlist | del | get} | Configures the GUI clients that can use SmartConsoles to connect to the Security Management Server.  
|            | • add - Adds a GUI client  
|            | • createlist - Deletes all the current GUI clients and adds the new GUI clients  
|            | • del - Deletes the specified GUI clients  
|            | • get - Shows the list of the allowed GUI clients  
| Notes:     | • Multi-Domain Server does not support this command.  
|            | • This command corresponds to the option "(3) GUI Clients" in the cpconfig menu. |
| finger get | Shows the ICA's Fingerprint.  
| Note - This command corresponds to the option "(7) Certificate's Fingerprint" in the cpconfig menu. |
### Security Management Server Commands

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| lic {add | del | get} | Manages Check Point licenses:  
  - add - Adds a license (from a file, or manually)  
  - del - Deletes the specified license  
  - get - Shows the list of the installed local licenses  
  Note - This command corresponds to the option "(1) Licenses and contracts" in the cpconfig menu. |

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| snmp {{activate | deactivate} ... | Do not use these commands anymore.  
To configure SNMP, see the R80.10 Gaia Administration Guide  
http://downloads.checkpoint.com/dc/download.htm?ID=54824 -  
Chapter System Management - Section SNMP. |

### cp_conf admin

**Description**  
Manages Check Point system administrators for the Security Management Server

**Syntax:**

> cp_conf admin get # Get the list of administrators.  
> cp_conf admin add <user> <pass> {a|w|r}  
> cp_conf admin del <admin1> <admin2>...

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows a list of the administrators.</td>
</tr>
<tr>
<td>add &lt;user&gt; &lt;pass&gt;</td>
<td>Adds a new administrator &lt;user&gt; with password &lt;pass&gt;.</td>
</tr>
</tbody>
</table>
| {a|w|r}   | Sets the permissions for the new administrator:  
  a - Read, write and manage administrators  
  w - Read and write  
  r - Read only |
| del <admin1> | Deletes one or more administrators <admin1>, <admin2>, and so on. |

### cp_conf ca

**Description**  
Initializes the Certificate Authority on the Security Management Server

**Syntax:**

> cp_conf ca init  
> cp_conf ca fqdn <name>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>Initializes the internal CA.</td>
</tr>
<tr>
<td>fqdn &lt;name&gt;</td>
<td>Sets the FQDN of the internal CA to &lt;name&gt;.</td>
</tr>
</tbody>
</table>

### cp_conf finger
**Description** Displays the fingerprint which will be used on first-time launch. This verifies the identity of the Security Management Server being accessed by SmartConsole. This fingerprint is a text string derived from the Security Management Server certificate.

**Syntax:**
> cp_conf finger get

**cp_conf lic**

**Description** Shows the installed licenses and lets you manually add new ones.

**Syntax:**
> cp_conf lic get
> cp_conf lic add -f <file>
> cp_conf lic add -m <Host> <Date> <Key> <SKU>
> cp_conf lic del <Signature Key>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows the installed licenses.</td>
</tr>
<tr>
<td>add -f &lt;file&gt;</td>
<td>Adds the license from &lt;file&gt;.</td>
</tr>
<tr>
<td>add -m</td>
<td>Manually adds a license with these parameters:</td>
</tr>
<tr>
<td></td>
<td>&lt;host&gt; - name of the Security Management Server</td>
</tr>
<tr>
<td></td>
<td>&lt;Date&gt; - Date of the license</td>
</tr>
<tr>
<td></td>
<td>&lt;Key&gt; - License key</td>
</tr>
<tr>
<td></td>
<td>&lt;SKU&gt; - License SKU</td>
</tr>
<tr>
<td>del &lt;Key&gt;</td>
<td>Deletes license &lt;key&gt;.</td>
</tr>
</tbody>
</table>

**cp_conf client**

**Description** Manages the GUI clients that can use SmartConsoles to connect to the Security Management Server.

**Syntax:**
> cp_conf client get # Get the GUI clients list
> cp_conf client add <GUI client> # Add one GUI Client
> cp_conf client del <GUI client 1> <GUI client 2>... # Delete GUI Clients
> cp_conf client createlist <GUI client 1> <GUI client 2>... # Create new list.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows the IP addresses of the allowed GUI clients.</td>
</tr>
<tr>
<td>add &lt;GUI client&gt;</td>
<td>Adds the &lt;GUI client&gt; IP address to the list of allowed GUI clients.</td>
</tr>
<tr>
<td>del &lt;GUI client 1&gt; &lt;GUI client 2&gt;</td>
<td>Deletes one or more IP addresses from the list of allowed GUI clients.</td>
</tr>
<tr>
<td>createlist &lt;GUI client 1&gt; &lt;GUI client 2&gt;</td>
<td>Deletes allowed GUI clients and creates a new list. The new list allows &lt;GUI client 1&gt;, &lt;GUI client 2&gt;, and so on.</td>
</tr>
</tbody>
</table>
**cp_conf snmp**

**Description**    Activates or deactivates SNMP.

**Syntax:**

>`cp_conf snmp get` # Get SNMP Extension status.
>`cp_conf snmp {activate|deactivate} [norestart]` # Deactivate SNMP Extension.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows the SNMP status.</td>
</tr>
<tr>
<td>{activate</td>
<td>deactivate}</td>
</tr>
<tr>
<td>[no restart]</td>
<td>By default, the Security Gateway runs <code>cpstop</code> and <code>cpstart</code> when you enable or disable SNMP. Use the <code>norestart</code> parameter to configure SNMP and to not run <code>cpstop</code> and <code>cpstart</code>.</td>
</tr>
</tbody>
</table>

**cp_conf auto**

**Description**    Configures the Security Gateway and Security Management Server products that start automatically when the appliance or server reboots.

**Syntax**

>`cp_conf auto get [fw1] [fg1] [rm] [all]`
>`cp_conf auto {enable|disable} <product1> <product2>...`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Shows which products start automatically</td>
</tr>
<tr>
<td>{enable</td>
<td>disable}</td>
</tr>
<tr>
<td>&lt;product1&gt; &lt;product2&gt;</td>
<td></td>
</tr>
</tbody>
</table>
### cpconfig

**Description**

This command starts the Check Point Configuration Tool. This tool lets you configure specific settings for the installed Check Point products.

The options shown depend on the configuration and installed products:

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses and contracts</td>
<td>Manages Check Point licenses and contracts.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Configures Check Point system administrators for the Security Management Server.</td>
</tr>
<tr>
<td>GUI Clients</td>
<td>Configures the GUI clients that can use SmartConsoles to connect to the Security Management Server.</td>
</tr>
<tr>
<td>SNMP Extension</td>
<td>Do not use this option anymore. To configure SNMP, see the <a href="https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_Gaia_AdminGuide/html_frameset.htm">R80.10 Gaia Administration Guide</a> - Chapter System Management - Section SNMP.</td>
</tr>
<tr>
<td>Random Pool</td>
<td>Configures the RSA keys, to be used by Gaia OS.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Initializes the Internal Certificate Authority (ICA) and configures the Certificate Authority’s (CA) Fully Qualified Domain Name (FQDN).</td>
</tr>
<tr>
<td>Certificate’s Fingerprint</td>
<td>Shows the ICA’s Fingerprint. This fingerprint is a text string derived from the Security Management Server or Domain Management Server ICA certificate. This fingerprint verifies the identity of the Security Management Server or Domain Management Server when you connect to it with a SmartConsole.</td>
</tr>
<tr>
<td>Automatic start of Check Point Products</td>
<td>Shows and controls which of the installed Check Point products start automatically during boot.</td>
</tr>
<tr>
<td>Exit</td>
<td>Exits from the Check Point Configuration Tool.</td>
</tr>
</tbody>
</table>

**Syntax**

```
cpconfig
```

**Note** - On Multi-Domain Server, run the `mdsconfig` command.

**Example - Menu on a Security Management Server**

```
[Expert@MyMGMT:0]# cpconfig
This program will let you re-configure
```
your Check Point Security Management Server configuration.

Configuration Options:
----------------------
(1) Licenses and contracts
(2) Administrator
(3) GUI Clients
(4) SNMP Extension
(5) Random Pool
(6) Certificate Authority
(7) Certificate's Fingerprint
(8) Automatic start of Check Point Products
(9) Exit

Enter your choice (1-9):

**cpinfo**

**Description**  A utility that collects diagnostics data on your machine at the time of execution. You can later analyze the collected data. See sk92739 http://supportcontent.checkpoint.com/solutions?id=sk92739.
The `cplic` command lets you manage Check Point licenses. The `cplic` command can be run in Gaia Clish or in Expert Mode.

**Best Practice** - Manage licenses in the SmartUpdate GUI.

License Management is divided into three types of commands:

- **Local licensing commands** are executed on the Check Point computers.
- **Remote licensing commands** are executed on the Security Management Server, and affect the managed Security Gateways.
- **License Repository commands** are executed on the Security Management Server, and affect the licenses stored in the local license repository.

For more about managing licenses, see the *R80.10 Security Management Administration Guide*

### Syntax for Local Licensing

```
cplic
   -h
   put <options>
   del <options>
   print <options>
   check <options>
   contract <options>
```

### Syntax for Remote Licensing

```
cplic
   -h
   put <Object Name> ...
   del <Object Name> <options>
   get {<IP Address> | <Host Name> | -all}
   upgrade -l <Input File>
```

### Syntax for License Database Operations

```
cplic
   -h
   db_add <options>
   db_rm <options>
   db_print <options>
```

**Note** - For help on commands, add the `-h` option.
cplic check

Description
Confirms that the license includes the feature on the local Security Gateway or Security Management Server.

Syntax
```bash
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;Product&gt;</td>
<td>Product, for which license information is requested.</td>
</tr>
<tr>
<td></td>
<td>Example: fw1, netso</td>
</tr>
<tr>
<td>-v &lt;Version&gt;</td>
<td>Product version, for which license information is requested.</td>
</tr>
<tr>
<td>-c</td>
<td>-count</td>
</tr>
<tr>
<td>-t &lt;Date&gt;</td>
<td>Checks license status on future date.</td>
</tr>
<tr>
<td></td>
<td>Use the format <code>ddmmyyyy</code>.</td>
</tr>
<tr>
<td></td>
<td>A feature can be valid on a given date on one license, but invalid on another.</td>
</tr>
<tr>
<td>-r</td>
<td>-routers</td>
</tr>
<tr>
<td></td>
<td>The <code>&lt;Feature&gt;</code> option is not needed.</td>
</tr>
<tr>
<td>-S</td>
<td>-SRusers</td>
</tr>
<tr>
<td>&lt;Feature&gt;</td>
<td>Feature, for which license information is requested.</td>
</tr>
</tbody>
</table>
**cplic db_add**

**Description**

Adds one or more licenses to the license repository on the Security Management Server. When local licenses are added to the license repository, they are automatically attached to the intended Check Point Security Gateway. Central licenses have to undergo the attachment process. This command is a license repository command and can only be executed on the Security Management Server.

**Syntax**

```
cplic db_add -l <License File> [Host] [Expiration Date] [Signature] [SKU/Features]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l &lt;License File&gt;</td>
<td>Name of the file that contains the license.</td>
</tr>
<tr>
<td>&lt;Host&gt;</td>
<td>Security Management Server hostname or IP address.</td>
</tr>
<tr>
<td>&lt;Expiration Date&gt;</td>
<td>The license expiration date.</td>
</tr>
<tr>
<td>&lt;Signature&gt;</td>
<td>The license signature string. For example:</td>
</tr>
<tr>
<td></td>
<td>aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m</td>
</tr>
<tr>
<td></td>
<td>The string is case sensitive and the hyphens are optional.</td>
</tr>
<tr>
<td>&lt;SKU/Features&gt;</td>
<td>The SKU of the license summarizes the features included in the license.</td>
</tr>
<tr>
<td></td>
<td>For example, CPSUITE-EVAL-3DES-vNG</td>
</tr>
</tbody>
</table>

**Example**

If the file `192.0.2.11.lic` contains one or more licenses, the command `cplic db_add -l 192.0.2.11.lic` produces output similar to:

```
gaia> cplic db_add -l 192.0.2.11.lic
Adding license to database ...  
Operation Done
```
cplic db_print

Description
Displays the details of Check Point licenses stored in the license repository on the Security Management Server.

Syntax
```
cplic db_print <Object Name | -all> [-n | -noheader] [-x] [-t | -type] [-a | -attached]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Object Name&gt;</td>
<td>Prints only the licenses attached to &lt;Object Name&gt;. &lt;Object Name&gt; is the name of the Check Point Security Gateway object as defined in SmartConsole.</td>
</tr>
<tr>
<td>-all</td>
<td>Prints all the licenses in the license repository.</td>
</tr>
<tr>
<td>-n</td>
<td>Prints licenses with no header.</td>
</tr>
<tr>
<td>-noheader</td>
<td>Prints licenses with no header.</td>
</tr>
<tr>
<td>-x</td>
<td>Prints licenses with their signatures.</td>
</tr>
<tr>
<td>-t</td>
<td>Prints licenses with their type: Central or Local.</td>
</tr>
<tr>
<td>-type</td>
<td>Prints licenses with their type: Central or Local.</td>
</tr>
<tr>
<td>-a</td>
<td>Shows to which object the license is attached. Useful, if the -all option is specified.</td>
</tr>
</tbody>
</table>

Note - This command is a license repository command and can only run on the Security Management Server.
cplic db_rm

Description
Removes a license from the license repository on the Security Management Server. It can be executed ONLY after the license was detached using the cplic del command. Once the license is removed from the repository, it can no longer be used.

Syntax
cplic db_rm <Signature>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Signature&gt;</td>
<td>The signature string within the license.</td>
</tr>
</tbody>
</table>

Example
gaiad> cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn

Note - This command is a license repository command and can only run on the Security Management Server.
**cplic del**

**Description**
Deletes a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. Used for both local and remote machines

**Syntax**
```
cplic del [-F <Output File>] <Signature> <Object Name>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-F &lt;Output File&gt;</code></td>
<td>Sends the output to <code>&lt;output file&gt;</code> instead of the screen.</td>
</tr>
<tr>
<td><code>&lt;Signature&gt;</code></td>
<td>The signature string within the license.</td>
</tr>
<tr>
<td></td>
<td>To see the license signature string, run the <code>cplic print -x</code> command.</td>
</tr>
<tr>
<td><code>&lt;Object Name&gt;</code></td>
<td>The name of the Check Point Security Gateway object as defined in SmartConsole.</td>
</tr>
</tbody>
</table>
**cplic del <object name>**

**Description**
Detaches a Central license from a Check Point Security Gateway. When this command is executed, the license repository is automatically updated. The Central license remains in the repository as an unattached license. This command can only run on a Security Management Server.

**Syntax**

```
cplic del <Object Name> [-F <Output File>] [-ip <Dynamic IP Address>] <Signature>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Object Name&gt;</code></td>
<td>The name of the Check Point Security Gateway object as defined in SmartConsole.</td>
</tr>
<tr>
<td><code>-F &lt;Output File&gt;</code></td>
<td>Diverts the output to <code>outputfile</code> rather than to the screen.</td>
</tr>
<tr>
<td><code>-ip &lt;Dynamic IP Address&gt;</code></td>
<td>Deletes the license on the Check Point Security Gateway with the specified IP address. Use this parameter to delete a license on a DAIP Check Point Security Gateway.</td>
</tr>
<tr>
<td><code>&lt;Signature&gt;</code></td>
<td>The signature string within the license.</td>
</tr>
</tbody>
</table>

**Note** - This is a Remote Licensing command, which affects remote managed machines. It is executed on the Security Management Server.
**cplic get**

**Description**
Retrieves all licenses from Security Gateways into the license repository on the Security Management Server. This command helps to synchronize the repository with the Check Point Security Gateways. When the command is run, all local changes are updated.

**Syntax**
```
cplic get {<IP Address> | <Host Name> | -all} [-v41]
```

**Parameters**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP Address&gt;</code></td>
<td>The IP address of the Check Point Security Gateway, from which licenses are to be retrieved.</td>
</tr>
<tr>
<td><code>&lt;Host Name&gt;</code></td>
<td>The name of the Check Point Security Gateway object as defined in SmartConsole, from which licenses are to be retrieved.</td>
</tr>
<tr>
<td><code>-all</code></td>
<td>Retrieves licenses from all Check Point Security Gateways in the managed network.</td>
</tr>
<tr>
<td><code>-v41</code></td>
<td>Retrieves version 4.1 licenses from the NF Check Point Security Gateway. Used to upgrade version 4.1 licenses.</td>
</tr>
</tbody>
</table>

**Example**
If the Check Point Security Gateway with the object name *caruso* contains four Local licenses, and the license repository contains two other Local licenses, the command `cplic get caruso` produces output similar to this:

```
gaia> cplic get caruso
Get retrieved 4 licenses.
Get removed 2 licenses.
```

**Note** - This is a Remote Licensing Command, which affects remote machines. It is executed on the Security Management Server.
cplic print

Description
The cplic print command prints details of Check Point licenses on the local machine.

Syntax

```
cplic print [-n|--noheader][-x][-t|--type][-F <Output File>] [-p|--preatures]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
<td>--noheader</td>
</tr>
<tr>
<td>-x</td>
<td>Prints licenses with their signature.</td>
</tr>
<tr>
<td>-t</td>
<td>--type</td>
</tr>
<tr>
<td>-F &lt;Output File&gt;</td>
<td>Diverts the output to &lt;Output File&gt;.</td>
</tr>
<tr>
<td>-p</td>
<td>--preatures</td>
</tr>
</tbody>
</table>

Note - On a Check Point Security Gateway, this command prints all licenses that are installed on the local machine, both local and central licenses.
cplic put

Description
Installs one or more local licenses on a local machine.

Syntax
```
cplic put [-o|-overwrite] [-c|-check-only] [-s|-select] [-F <Output File>] [-P|-Pre-boot] [-k|-kernel-only] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Features>]
```

Parameters
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-o</td>
<td>-overwrite</td>
</tr>
<tr>
<td>-c</td>
<td>-check-only</td>
</tr>
<tr>
<td>-s</td>
<td>-select</td>
</tr>
<tr>
<td>-F &lt;Output File&gt;</td>
<td>Outputs the result of the command to the designated file rather than to the screen.</td>
</tr>
<tr>
<td>-P</td>
<td>-Pre-boot</td>
</tr>
<tr>
<td>-K</td>
<td>-kernel-only</td>
</tr>
<tr>
<td>-l &lt;License File&gt;</td>
<td>Name of the file that contains the license.</td>
</tr>
<tr>
<td>&lt;Host&gt;</td>
<td>Hostname or IP address of Security Management Server.</td>
</tr>
<tr>
<td>&lt;Expiration Date&gt;</td>
<td>The license expiration date.</td>
</tr>
<tr>
<td>&lt;Signature&gt;</td>
<td>The license signature string. For example: aa6uwknDc-CE6CRTjhv-zipoVWSnm-z98N7Ck3m (The string is case sensitive and the hyphens are optional).</td>
</tr>
<tr>
<td>&lt;SKU/Features&gt;</td>
<td>The SKU of the license summarizes the features included in the license. For example: CPSUITE-EVAL-3DES-vNG</td>
</tr>
</tbody>
</table>

Copy and paste the parameters from the license received from the User Center:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>One of these:</td>
</tr>
<tr>
<td></td>
<td>• All platforms - The IP address of the external interface (in dot notation). The last part cannot be 0 or 255.</td>
</tr>
<tr>
<td></td>
<td>• Solaris2 - The response to the hostid command (beginning with 0x).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>expiration date</td>
<td>The license expiration date. It can be never.</td>
</tr>
<tr>
<td>signature</td>
<td>The license signature string.</td>
</tr>
<tr>
<td></td>
<td>For example: aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m</td>
</tr>
<tr>
<td></td>
<td>[Case sensitive. The hyphens are optional.]</td>
</tr>
<tr>
<td>SKU/features</td>
<td>A string listing the SKU and the Certificate Key of the license. The SKU</td>
</tr>
<tr>
<td></td>
<td>of the license summarizes the features included in the license.</td>
</tr>
<tr>
<td></td>
<td>For example: CPSB-SWB CPSB-ADNC-M CK0123456789ab</td>
</tr>
</tbody>
</table>

**Example**

```
 gaia> cplic put -l License.lic
 Host       Expiration SKU
 192.168.2.3 14Jan2016   CPSB-SWB CPSB-ADNC-M CK0123456789ab
 gaia>
```
**cplic put <object name>**

**Description**
Attaches one or more central or local licenses remotely. When this command is executed, the license repository is also updated.

**Syntax**
```
cplic put <Object Name> [-ip Dynamic IP] [-F <Output File>] [-l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Feature>]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Object Name&gt;</code></td>
<td>The name of the Check Point Security Gateway object, as defined in SmartConsole.</td>
</tr>
<tr>
<td><code>-ip &lt;Dynamic IP&gt;</code></td>
<td>Installs the license on the Check Point Security Gateway with the specified IP address. This parameter is used for installing a license on a DAIP Check Point Security Gateway. <strong>Note</strong> - If this parameter is used, then the object name must be a DAIP Check Point Security Gateway.</td>
</tr>
<tr>
<td><code>-F &lt;Output File&gt;</code></td>
<td>Diverts the output to <code>&lt;outputfile</code> rather than to the screen.</td>
</tr>
<tr>
<td><code>-l &lt;license File&gt;</code></td>
<td>Installs the licenses from <code>&lt;license file</code> .</td>
</tr>
<tr>
<td><code>&lt;Host&gt;</code></td>
<td>Hostname or IP address of Security Management Server.</td>
</tr>
<tr>
<td><code>&lt;Expiration Date&gt;</code></td>
<td>The license expiration date.</td>
</tr>
<tr>
<td><code>&lt;Signature&gt;</code></td>
<td>The license signature string. For example: <code>aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m</code> The string is case sensitive and the hyphens are optional.</td>
</tr>
<tr>
<td><code>&lt;SKU/Features&gt;</code></td>
<td>The SKU of the license summarizes the features included in the license. For example: <code>CPSUITE-EVAL-3DES-vNG</code></td>
</tr>
</tbody>
</table>

**Note** - This is a remote licensing command, which affects remote machines. It is executed on the Security Management Server. More than one license can be attached.

Copy and paste the parameters from the license received from the User Center:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>One of these:</td>
</tr>
<tr>
<td></td>
<td><strong>All platforms</strong> - The IP address of the external interface (in dot notation). The last part cannot be 0 or 255.</td>
</tr>
<tr>
<td></td>
<td><strong>Solaris2</strong> - The response to the <code>hostid</code> command (beginning with <code>0x</code>).</td>
</tr>
<tr>
<td>expiration date</td>
<td>The license expiration date. It can be <code>never</code>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>signature</td>
<td>The license signature string. For example: aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional.)</td>
</tr>
<tr>
<td>SKU/features</td>
<td>A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: CPSB-SWB CPSB-ADNC-M CK0123456789ab</td>
</tr>
</tbody>
</table>
**cplic upgrade**

**Description**

Upgrades licenses in the license repository with licenses in a license file from the user center.

**Syntax**

```plaintext
cplic upgrade -l <Input File>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l &lt;Input File&gt;</td>
<td>Upgrades the licenses in the license repository and Check Point Security Gateways to match the licenses in &lt;Input File&gt;.</td>
</tr>
</tbody>
</table>

**Example**

This example explains the procedure to upgrade the licenses in the license repository. There are two Software Blade licenses in the file. One does not match any license on a remote Security Gateway, the other matches a version NGX license on a Security Gateway that has to be upgraded.

- Upgrade the Security Management Server to the latest version.
  - Ensure that there is connectivity between the Security Management Server and the Security Gateways with the previous product versions.
- Import all licenses into the license repository. This can also be done after upgrading the products on the remote Security Gateways.
- Run this command:
  ```plaintext
cplic get -all
```
  **Example:**
  ```plaintext
[Expert@MyMGMT]# cplic get -all
  Getting licenses from all modules ...
  MyGW:
  Retrieved 1 licenses
  ```
- To see all the licenses in the repository, run this command:
  ```plaintext
cplic db_print -all -a
```
  **Example:**
  ```plaintext
[Expert@MyMGMT]# cplic db_print -all -a
  Retrieving license information from database ...
  The following licenses appear in the database:
  ==============================================================
  Host        Expiration Features                      
  192.0.2.11  Never        CPFW-FIG-25-53              CK49C3A3CC7121 golda
  192.0.2.11  26Nov2017  CPSB-ADNC-M                   CK0123456789ab count
  ```

- In the User Center [https://usercenter.checkpoint.com](https://usercenter.checkpoint.com), view the licenses for the products that were upgraded from version NGX to a Software Blades license. You can also create new upgraded licenses.
- Download a file containing the upgraded licenses. Only download licenses for the products that were upgraded from version NGX to Software Blades.
• If you did not import the version NGX licenses into the repository, import the version NGX licenses now. Use the command `cplic get -all`.

• Run the license upgrade command: `cplic upgrade -l <inputfile>`
  - The licenses in the downloaded license file and in the license repository are compared.
  - If the certificate keys and features match, the old licenses in the repository and in the remote Security Gateways are updated with the new licenses.
  - A report of the results of the license upgrade is printed.

Note - This is a remote licensing command, which affects remote Security Gateways. It is executed on the Security Management Server.

cppkg

**Description**  Manages the product repository. It is always executed on the Security Management Server.

**Important** - This command is not supported for gateways running on Gaia OS.

cppkg add

**Description**  Adds a product package to the product repository. You can only add SmartUpdate packages to the product repository.

Add products to the repository by importing a file downloaded from the Download Center. Add the package file to the repository directly from a DVD or from a local or network drive.

**Syntax:**

```
> cppkg add {<package-full-path>|<CD drive> [product]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>package-full-path</td>
<td>If the package you want to add to the repository is on a local disk or network drive, type the full path to the package.</td>
</tr>
<tr>
<td>CD drive</td>
<td>If the package you want to add to the repository is on a DVD:</td>
</tr>
</tbody>
</table>
|                 | • For Windows machines type the DVD drive letter, for example: d:
|                 | • For UNIX machines, type the DVD root path, for example: /caruso/image/CPsuite-R80.10 |

You are asked to specify the product and appropriate operating system (OS).

**Note** - cppkg add does not overwrite existing packages. To overwrite existing packages, you must first delete existing packages.

**Example:**

```
[d:\winnt\fw\ng\bin]cppkg add l:\CPsuite-R80.10
Enter package name:  
----------------------
(1) SVNfoundation   
(2) firewall        
(3) floodgate       
(4) rtm             
(e) Exit
Enter your choice : 1
Enter package OS :    
----------------------
(1) win32         
(2) linux        
(3) ipso         
(e) Exit
Enter your choice : 1
You choose to add 'SVNfoundation' for 'win32' OS. Is this correct? [y/n] : y
```
cppkg delete

**Description**  Deletes a product package from the repository. To delete a product package you must specify a number of options. To see the format of the options and to view the contents of the product repository, use the `cppkg print` command.

**Syntax:**

```plaintext
> cppkg delete <vendor> <product> <version> <os> [sp]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor</td>
<td>Package vendor. For example, <code>checkpoint</code></td>
</tr>
<tr>
<td>product</td>
<td>Package name.</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>os</td>
<td>Package Operating System. Options are: <code>win32</code>, <code>solaris</code>, <code>ipso</code>, <code>linux</code></td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version.</td>
</tr>
</tbody>
</table>

**Note** - It is not possible to undo the `cppkg del` command.

cppkg get

**Description**  Synchronizes the Package Repository database with the content of the actual package repository under `$SUROOT`

**Syntax:**

```plaintext
> cppkg get
```

cppkg getroot

**Description**  Finds the location of the product repository. The default product repository location on Windows machines is `C:\SUroot`. On UNIX machines it is `/var/SUroot`.

**Syntax:**

```plaintext
> cppkg getroot
```

**Example:**

```plaintext
> cppkg getroot

Current repository root is set to : /var/suroot/
```

cppkg print

**Description**  Lists the contents of the product repository.

Use `cppkg print` to see the product and OS strings required to install a product package using the `cprinstall` command, or to delete a package using the `cppkg delete` command.

**Syntax:**

```plaintext
> cppkg print
```
cppkg setroot

**Description**  Creates a new repository root directory location and moves existing product packages into the new repository.

The default product repository location is created when the Security Management Server is installed. On Windows machines the default location is C:\SUroot and on UNIX machines it is /var/SUroot. Use this command to change the default location.

When changing repository root directory:

- The content of the old repository is copied into the new repository.
- The $SUROOT environment variable gets the value of the new root path.
- A product package in the new location is overwritten by a package in the old location, if the packages are the same (they have the same ID strings).

The repository root directory should have at least 200 Mbyte of free disk space.

**Syntax:**

```
> cppkg setroot <repository>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;repository&gt;</td>
<td>The full path for the desired location for the product repository.</td>
</tr>
</tbody>
</table>

**Note** - It is important to reboot the Security Management Server after using this command. This sets the new $SUROOT environment variable.

**Example:**

cppkg setroot /var/new_suroot
Repository root is set to : /var/new_suroot/

Note: When changing repository root directory :
1. Old repository content will be copied into the new repository.
2. A package in the new location will be overwritten by a package in the old location, if the packages have the same name.

Change the current repository root ? [y/n] : y

The new repository directory does not exist. Create it ? [y/n] : y

Repository root was set to : /var/new_suroot

Notice : To complete the setting of your directory, reboot the machine!
cprinstall

**Description**  Use `cprinstall` commands to perform remote installation of product packages and associated operations.

**Important** - This command is not supported for gateways running on Gaia OS.

On the Security Management Server, `cprinstall` commands require licenses for SmartUpdate.

On the remote Check Point gateways the following are required:

- Trust must be established between the Security Management Server and the Check Point gateway.
- `cpd` must run.
- `cprid` remote installation daemon must run.
cprinstall boot

**Description**  Boot the remote computer.

**Syntax:**

```bash
> cprinstall boot <object name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;object name&gt;</code></td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
> cprinstall boot harlin
```
cprinstall cpstart

Description  Enables cpstart to be run remotely.

All products on the Check Point Security Gateway must be of the same version.

Syntax:

```bash
> cprinstall cpstart <object name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Object name&gt;</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
</tbody>
</table>
cprinstall cpstop

**Description**  Enables `cpstop` to be run remotely.

All products on the Check Point Security Gateway must be the same version.

**Syntax:**

```
> cprinstall cpstop {-proc|-nopolicy} <object name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-proc</td>
<td>Kills Check Point daemons and security servers while it maintains the active Security Policy running in the kernel. Rules with generic allow/reject/drop rules, based on services continue to work.</td>
</tr>
<tr>
<td>-nopolicy</td>
<td></td>
</tr>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
</tbody>
</table>
cprinstall get

**Description**  Gets details of the products and the operating system installed on the specified Check Point Security Gateway. It also updates the database.

**Syntax:**

```
> cprinstall get <object name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;object name&gt;</code></td>
<td>The name of the Check Point Security Gateway object defined in SmartConsole.</td>
</tr>
</tbody>
</table>

**Example:**

```
cprinstall get gw1
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
<table>
<thead>
<tr>
<th>Operating system</th>
<th>Major Version</th>
<th>Minor Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform</td>
<td>R75.20</td>
<td>R75.20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Major Version</th>
<th>Minor Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point</td>
<td>VPN-1 Power/UTM</td>
<td>R75.20</td>
<td>R75.20</td>
</tr>
<tr>
<td>Check Point</td>
<td>SecurePlatform</td>
<td>R75.20</td>
<td>R75.20</td>
</tr>
<tr>
<td>Check Point</td>
<td>SmartPortal</td>
<td>R75.20</td>
<td>R75.20</td>
</tr>
</tbody>
</table>
```
cprinstall install

**Description**  Installs Check Point products on remote Check Point Security Gateways.

To install a product package you must specify a number of options. Use the `cppkg print` command and copy the required options.

**Syntax:**

```
> cprinstall install [-boot] <Object name> <vendor> <product> <version> [sp]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-boot</td>
<td>Boots the remote computer after installing the package. <strong>Note</strong> - Only boot after ALL products have the same version. Boot will be canceled in certain scenarios.</td>
</tr>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor. For example, <code>checkpoint</code></td>
</tr>
<tr>
<td>product</td>
<td>Package name.</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version.</td>
</tr>
</tbody>
</table>

**Note** - Before transferring any files, this command runs the `cprinstall verify` command to verify that the operating system is appropriate and that the product is compatible with previously installed products.

**Example:**

```
# cprinstall install -boot fred checkpoint firewall R70

Installing firewall R75.20 on fred...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
```
cprinstall revert

**Description**  Restores the Check Point Security Gateway from a snapshot.

**Syntax:**

```
cprinstall revert <object name> <filename>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;object name&gt;</code></td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>Name of the snapshot file.</td>
</tr>
</tbody>
</table>

**Note** - Supported on SecurePlatform only.
cprinstall show

**Description**  Displays all snapshot (backup) files on the Check Point Security Gateway.

**Syntax:**

```
> cprinstall show <object name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
</tbody>
</table>

**Note** - Supported on SecurePlatform only.

**Example:**

```
# cprinstall show GW1
SU_backup.tzg
```
**cprinstall snapshot**

**Description**  Creates a snapshot `<filename>` on the Check Point Security Gateway.

**Syntax:**

```
> cprinstall snapshot <object name> <filename>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of the snapshot file</td>
</tr>
</tbody>
</table>

**Note** - Supported on SecurePlatform only.
cprinstall transfer

**Description**  Transfers a package from the repository to a Check Point Security Gateway without installing the package.

**Syntax:**
```
> cprinstall transfer <object name> <vendor> <product> <version> [sp]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor. For example, checkpoint</td>
</tr>
<tr>
<td>product</td>
<td>Package name.</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version. This parameter is optional.</td>
</tr>
</tbody>
</table>
cprinstall uninstall

**Description**  Uninstalls products on remote Check Point Security Gateways.

To uninstall a product package you must specify a number of options. Use the `cppkg print` command and copy the required options.

**Syntax:**

```
> cprinstall uninstall [-boot] <Object name> <vendor> <product> <version> [sp]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-boot</td>
<td>Boots the remote computer after installing the package.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - Only boot after ALL products have the same version. Boot will be canceled in certain scenarios. See the Release Notes for details.</td>
</tr>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor. For example, <code>checkpoint</code></td>
</tr>
<tr>
<td>product</td>
<td>Package name.</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version.</td>
</tr>
</tbody>
</table>

**Note** - Before uninstalling any files, this command runs the `cprinstall verify` command. It verifies that the operating system is appropriate and that the product is installed.

After uninstalling, retrieve the Check Point Security Gateway data by running `cprinstall get`

**Example**

```
# cprinstall uninstall fred checkpoint firewall R75.20

Uninstalling firewall R75.20 from fred...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
```
cprinstall verify

**Description**  Confirm these operations were successful:
- If a specific product can be installed on the remote Check Point Security Gateway.
- That the operating system and currently installed products are appropriate for the package.
- That there is enough disk space to install the product.
- That there is a CPRID connection.

**Syntax:**

```
> cprinstall verify <Object name> <vendor> <product> <version> [sp]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartConsole.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor. For example, checkpoint</td>
</tr>
<tr>
<td>product</td>
<td>Package name. Options are: SVNfoundation, firewall, floodgate</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version. This parameter is optional.</td>
</tr>
</tbody>
</table>

**Example:**

**Successful - Verify succeeds**

```
cprinstall verify harlin checkpoint SVNfoundation R75.20
Verifying installation of SVNfoundation R75.20 on jimmy...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

**Unsuccessful - Verify fails**

```
cprinstall verify harlin checkpoint SVNfoundation R75.20
Verifying installation of SVNfoundation R75.20 on jimmy...
Info : Testing Check Point Gateway.
Info : SVN Foundation R70 is already installed on 192.0.2.134
Operation Success. Product cannot be installed, did not pass dependency check.
```

cpstart and cpstop

**Description**  Starts or stops all Check Point processes and applications.

**Syntax:**

```
> cpstart / cpstop
```

**Note** - This command cannot be used to start cprid. cprid is invoked when the machine is booted and it runs independently.
cpstat

Description
Shows Check Point statistics for applications.

Syntax


Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;port&gt;</td>
<td>Port number of the server. The default is the standard server port (18192).</td>
</tr>
<tr>
<td>-s &lt;SICname&gt;</td>
<td>Secure Internal Communication (SIC) name of the server.</td>
</tr>
<tr>
<td>-f &lt;flavor&gt;</td>
<td>The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file.</td>
</tr>
<tr>
<td>-o &lt;polling&gt;</td>
<td>Polling interval (seconds) specifies the pace of the results. The default is 0, meaning the results are shown only once.</td>
</tr>
<tr>
<td>-c &lt;count&gt;</td>
<td>Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.</td>
</tr>
<tr>
<td>-e &lt;period&gt;</td>
<td>Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds.</td>
</tr>
<tr>
<td>-x</td>
<td>XML output mode</td>
</tr>
<tr>
<td>-j</td>
<td>Json output mode</td>
</tr>
<tr>
<td>-d</td>
<td>Debug mode.</td>
</tr>
<tr>
<td>&lt;flag&gt;</td>
<td>One of these applications is displayed: One of the following: fw — Firewall component of the Security Gateway vpn — VPN component of the Security Gateway fg — QoS (formerly FloodGate-1) ha — ClusterXL (High Availability) os — OS Status mg — for the Security Management Server persistency - for historical status values polsrv uas svr cpsemd cpsead asm ls ca</td>
</tr>
</tbody>
</table>
Return Value
0 on success, 1 on failure

Example

cpstat -c 3 -o 3 fw

Output
Success shows OK. Failure shows an appropriate error message.

The following flavors can be added to the application flags:

- **vpn** — "default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"
- **fg** — "all"
- **ha** — "default", "all"
- **mg** — "default"
- **persistency** — "product", "Tableconfig", "SourceConfig"
- **polsrv** — "default", "all"
- **uas** — "default"
- **svr** — "default"
- **cpsemd** — "default"
- **cpsead** — "default"
- **asm** — "default", "WS"
- **ls** — "default"
- **ca** — "default", "crl", "cert", "user", "all"

**dbedit**

**Description** Edits the objects file on the Security Management Server [see skI3301 http://supportcontent.checkpoint.com/solutions?id=skI3301]. Editing the objects.C file on the gateway is not required or desirable, since it will be overwritten the next time a policy is installed.

Important - Do NOT run this command unless explicitly instructed by Check Point Support or R&D to do so. Otherwise, you can corrupt settings in the management database.

**Syntax**

```bash
```
### Security Management Server Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-s server</code></td>
<td>The Security Management Server on which the <code>objects_5_0.C</code> file to be edited is located. If this is not specified in the command line, the user will be prompted for it. If the server is not <code>localhost</code>, the user will be required to authenticate.</td>
</tr>
<tr>
<td>`-u user</td>
<td>-c certificate`</td>
</tr>
<tr>
<td><code>-p password</code></td>
<td>The user's password (the password used for the SmartConsole).</td>
</tr>
<tr>
<td><code>-f filename</code></td>
<td>The name of the file containing the commands. If <code>filename</code> is not given, then the user will be prompted for commands.</td>
</tr>
<tr>
<td><code>-r db-open-reason</code></td>
<td>A non-mandatory flag used to open the database with a string that states the reason. This reason will be attached to audit logs on database operations.</td>
</tr>
<tr>
<td><code>-help</code></td>
<td>Print usage and short explanation.</td>
</tr>
</tbody>
</table>

**dbedit internal commands:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>create</code></td>
<td>Create an object with its default values. The create command may use an extended (owned) object. Changes are committed to the database only by an <code>update</code> or <code>quit</code> command.</td>
</tr>
<tr>
<td><code>modify</code></td>
<td>Modify fields of an object which is:</td>
</tr>
<tr>
<td></td>
<td>• Stored in the database (the command will lock the object in such case).</td>
</tr>
<tr>
<td></td>
<td>• Newly created by <code>dbedit</code></td>
</tr>
<tr>
<td></td>
<td>Extended formats for owned objects can be used:</td>
</tr>
<tr>
<td></td>
<td>For example, <code>field_name = Field_A:Field_B</code></td>
</tr>
<tr>
<td><code>update</code></td>
<td>Update the database with the object. This command will check the object validity and will issue an error message if appropriate.</td>
</tr>
<tr>
<td><code>delete</code></td>
<td>Delete an object from the database and from the client implicit database.</td>
</tr>
<tr>
<td><code>addelement</code></td>
<td>Add an element [of type string] to a multiple field.</td>
</tr>
<tr>
<td><code>rmelement</code></td>
<td>Remove an element [of type string] from a multiple field.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| rename    | Assign a new name for a given object. The operation also performs an update. **Example:** Rename network object London to Chicago. 
  `rename network_objects london chicago` |
| quit      | Quit `dbedit` and update the database with modified objects not yet committed. |

**Example:**
Replace the owned object with a new null object, where NULL is a reserved word specifying a null object:

`modify network_objects my_obj firewall_setting NULL`

**Example:**
Extended Format

`firewall_properties` **owns** the object `floodgate_preferences`

`floodgate_preferences` **has a Boolean attribute** `turn_on_logging`, which **will be set to true**

`modify properties firewall_properties floodgate_preferences:turn_on_logging true`

`comments` is a field of the owned object contained in the ordered container. The 0 value indicates the first element in the container (zero based index).

`modify network_objects my_networkObj interfaces:0:comments my_comment`

Replace the owned object with a new one with its default values.

`modify network_objects my_net_obj interfaces:0:security interface_security`

dynamic objects

Manages dynamic objects on the appliance. The `dynamic_objects` command specifies an IP address to which the dynamic object is resolved.

First, define the dynamic object in the SmartConsole. Then create the same object with the CLI (-n argument). After the new object is created on the gateway with the CLI, you can use the `dynamic_objects` command to specify an IP address for the object.

Any change you make to dynamic objects’ ranges are applied immediately to the objects. It is not necessary to reinstall the policy.

**Description**
Manages dynamic objects on the appliance.
### Syntax

`dynamic_objects -o <object> [-r <fromIP> <toIP> ...] [-a] [-d] [-l] [-n <object> ] [-c] [-do <object>]`

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-o</td>
<td>Name of the dynamic object that is being configured.</td>
</tr>
<tr>
<td>-r</td>
<td>Defines the range of IP addresses that are being configured for this object.</td>
</tr>
<tr>
<td>-a</td>
<td>Adds range of IP addresses to the dynamic object.</td>
</tr>
<tr>
<td>-d</td>
<td>Deletes range of IP addresses from the dynamic object.</td>
</tr>
<tr>
<td>-l</td>
<td>Lists dynamic objects that are used on the appliance.</td>
</tr>
<tr>
<td>-n</td>
<td>Creates a new dynamic object.</td>
</tr>
<tr>
<td>-c</td>
<td>Compare the objects in the dynamic objects file and in objects.</td>
</tr>
<tr>
<td>-do</td>
<td>Deletes the dynamic object.</td>
</tr>
</tbody>
</table>

**<object>** Name of dynamic object.

**<fromIP>** Starting IPv4 address.

**<toIP>** Ending IPv4 address.

### Example

```
dynamic_objects -n sg80gw -r 190.160.1.1 190.160.1.40 -a
```

### Output

Success shows Operation completed successfully. Failure shows an appropriate error message.

---

### `fw logswitch`

**Description**

Creates a new active log file. The current active log file is closed and renamed by default. `$FWDIR/log/<current_time_stamp>.log` unless you define an alternative name that is unique. The format of the default name is `YYYY-MM-DD_HHmmss.log`. For example, `2003-03-26_041200.log`

**Warning:**

- The Logswitch operation fails if a log file is given a pre-existing file name.
- The rename operation fails on Windows if the active log that is being renamed, is open at the same time that the rename operation is taking place. However, the Logswitch will succeed and the file will be given the default name `$FWDIR/log/current_time_stamp.log`.

The new log file that is created is given the default name `$FWDIR/log/fw.log`. Old log files are located in the same directory.

A Security Management Server can use `fw logswitch` to change a log file on a remote machine and transfer the log file to the Security Management Server. This same operation can be performed for a remote machine using `fw lslogs` and `fw fetchlogs`. 
When a log file is sent to the Security Management Server, the data is compressed.

**Syntax**

```
> fw logswitch [-audit] [<filename>]
> fw logswitch -h <host> [+|-][<filename>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-audit</td>
<td>Logswitch for the Security Management Server audit file is done. This is relevant for local activation.</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>The name of the file to which the log is saved. If no name is specified, a default name is provided.</td>
</tr>
<tr>
<td>-h &lt;host&gt;</td>
<td>The resolvable name or IP address of the remote machine (running either a Security Gateway or &lt;to_sms&gt;) on which the log file is located. The Security Management Server (on which the <code>fw logswitch</code> command is executed) must be defined as one of <code>host</code>'s Security Management Servers. In addition, you must initialize SIC between the Security Management Server and the <code>host</code>.</td>
</tr>
<tr>
<td>+</td>
<td>Change a remote log and copy it to the local machine.</td>
</tr>
<tr>
<td>-</td>
<td>Change a remote log and move it to the local machine thereby deleting the log from the remote machine.</td>
</tr>
</tbody>
</table>

**Note** - Files are created in the `$FWDIR/log` directory on both the `host` and the Security Management Server when the + or - parameters are specified. Note that if - is specified, the log file on the host is deleted rather than renamed.

**host specified:**

- filename specified - On host, the old log file is renamed to `old_log`. On the Security Management Server, the copied file will have the same name, prefixed by `host`s name. For example, the command `fw logswitch -h venus +xyz` creates a file named `venus_xyz.log` on the Security Management Server.

- filename not specified - On host, the new name is the current date. For example, `2003-03-26_041200.log`.

On the Security Management Server, the copied file will have the same name, but prefixed by `host_`. For example, `target_2003-03-26_041200.log`.

**host not specified:**

- filename specified - On the Security Management Server, the old log file is renamed to `old_log`

- filename not specified - On the Security Management Server, the old log file is renamed to the current date.

**Compression**

When log files are transmitted from one machine to another, they are compressed using the `zlib` package, a standard package used in the Unix `gzip` command (see RFC 1950 to RFC 1952 for details). The algorithm is a variation of LZ77 method.

The compression ratio varies with the content of the log records and is difficult to predict. Binary data are not compressed, but string data such as user names and URLs are compressed.
fwm

**Description**  Performs management operations on the Security Gateway. fwm controls fwd and all Check Point daemons.

**Syntax**

>`fwm`

fwm expdate

**Description**  Modifies the expiration date of all users and administrators.

**Syntax**

>`fw expdate dd-mmm-yyyy`

**Comments**  The date can be modified using a filter.

**Example**

>`fw expdate 02-mar-20xx -f 01-mar-20xx`

fwm dbload

**Description**  Downloads the user database and network objects information to selected targets. If no target is specified, then the database is downloaded to localhost.

**Syntax**

>`gw> fwm dbload [-a|-c <conffile>] [<targets>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a &lt;conffile&gt;</td>
<td>Executes commands on all targets specified in the default system configuration file, $FWDIR/conf/sys.conf. This file must be manually created.</td>
</tr>
<tr>
<td>-c &lt;conffile&gt;</td>
<td>Only OPSEC control connections in the file are enabled.</td>
</tr>
<tr>
<td>&lt;targets&gt;</td>
<td>Executes commands on the designated targets.</td>
</tr>
</tbody>
</table>

fwm ikecrypt

**Description**  Encrypts the password of a SecuRemote user using IKE. The resulting string must then be stored in the LDAP database.

**Syntax**

>`fwm ikecrypt <shared-secret> <user-password>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;shared-secret&gt;</td>
<td>The IKE Key is defined in the Encryption tab of the LDAP Account Unit Properties window.</td>
</tr>
<tr>
<td>&lt;user-password&gt;</td>
<td>The password for the SecuRemote user.</td>
</tr>
</tbody>
</table>

**Note**  - An internal CA must be created before implementing IKE encryption. An Internal CA is created during the initial configuration of the Security Management Server, following installation.
fwm getpcap

**Description**  
Fetches the packet capture.

**Syntax**

```
> fwm getpcap -g <gw> -u <cap id> [-p <path>] [-c <domain>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-g &lt;gw&gt;</td>
<td>Host name of the gateway.</td>
</tr>
<tr>
<td>-u &lt;cap id&gt;</td>
<td>Captures UID.</td>
</tr>
<tr>
<td>-p &lt;path&gt;</td>
<td>Outputs pathname.</td>
</tr>
<tr>
<td>-c &lt;domain&gt;</td>
<td>Host name of the Domain Management Server.</td>
</tr>
</tbody>
</table>

fwm logexport

**Description**  
Exports the log file to an ASCII file.

**Syntax**

```
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d &lt;delimiter&gt;</td>
<td>Sets the output delimiter. The default is a semicolon (;).</td>
</tr>
<tr>
<td>-i &lt;filename&gt;</td>
<td>The name of the input log file. The default is the active log file, <code>fw log</code></td>
</tr>
<tr>
<td>-o &lt;outputfile&gt;</td>
<td>The name of the output file. The default prints to the screen.</td>
</tr>
<tr>
<td>-n</td>
<td>Does not perform DNS resolution of the IP addresses in the log file (this option significantly speeds the processing).</td>
</tr>
<tr>
<td>-p</td>
<td>Does not perform service resolution. A service port number is displayed.</td>
</tr>
<tr>
<td>-f</td>
<td>If this is the active log file, <code>fw log</code>, wait for new records and export them to the ASCII output file as they occur.</td>
</tr>
<tr>
<td>-m {initial</td>
<td>semi</td>
</tr>
<tr>
<td>-a</td>
<td>Shows account records only. The default is to show all records.</td>
</tr>
</tbody>
</table>

Use `logexport.ini` to control the output of `fwm logexport`. Put the `logexport.ini` file in the `conf` directory `$FWDIR/conf`

The `logexport.ini` file should be in the following format:

```
[Fields_Info]
included_fields = field1,field2,field3,<REST_OF_FIELDS>,field100
excluded_fields = field10,field11
```
Notes:
- The `num` field will always appear first and cannot be manipulated using `logexport.ini`.
- `<REST_OF_FIELDS>` is a reserved token that refers to a list of fields. It is optional.
  - If `-f` is set, `<REST_OF_FIELDS>` is based on a list of fields taken from the file `logexport_default.C`.
  - If `-f` is not set, `<REST_OF_FIELDS>` is based on the given input log file.
- It is not mandatory to specify both `included_fields` and `excluded_fields`.

Format:
The `fwm logexport` output appears in tabular format. The first row lists the names of all fields included in the next records. Each of the next rows consist of a single log record whose fields are sorted in the same order as the first row. If a record has no information on a specific field, this field remains empty (as indicated by two successive semi-colons).

Example:
```
0; 5Dec2002;9:08:44;jam.checkpoint.com;control; ;daemon;inbound;VPN-1 & FireWall-1;The hme0 interface is not protected by the anti-spoofing feature. Your network may be at risk;;;
1; 5Dec2002;9:08:44;jam.checkpoint.com;control; ;;daemon;inbound;VPN-1 & FireWall-1;;
ftp;23456;1.2.3.4;3.4.5.6;
```

**fwm ver**

**Description**: Shows the build number.

**Syntax**: `> fwm ver [-f <filename>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-f &lt;filename&gt;</code></td>
<td>Exports the build number data to a file.</td>
</tr>
</tbody>
</table>

**fwm verify**

**Description**: Verifies the specified policy package without installing it.

**Syntax**: `> fwm verify <policy>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;policy&gt;</code></td>
<td>The name of an available policy package.</td>
</tr>
</tbody>
</table>

**inet_alert**

**Description**: Notifies an Internet Service Provider (ISP) when a company’s corporate network is under attack. The `inet_alert` utility forwards log messages generated by the alert daemon to an external Management Station. This is usually located at the ISP site. The ISP can then analyze the alert and react accordingly.
inet_alert uses the ELA Protocol to send the alert. The Management Station receiving the alert must be running the ELA Proxy.

If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the Management Station running the ELA Proxy and the Security Gateway generating the alert.

To use this utility, enter it into a script:
1. From Manage & Settings tab > Global Properties > Log and Alert > Alert early versions compatibility > run 4.x alert script.
2. Enter the name of the script.

Syntax

```
# inet_alert -s <ipaddr> [-o] [-a <auth_type>] [-p <port>] [-f <token value>] [-m <alerttype>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s &lt;ipaddr&gt;</td>
<td>The IP address, in dot format, of the ELA Proxy to be contacted.</td>
</tr>
<tr>
<td>-o</td>
<td>Print the alert log received by inet_alert to stdout. Use this option when inet_alert is part of a pipe.</td>
</tr>
<tr>
<td>-a &lt;auth_type&gt;</td>
<td>The type of connection to the ELA Proxy. One of the following values: • ssl_opsec - The connection is authenticated and encrypted, by default. • auth_opsec - The connection is authenticated. • clear - The connection is neither authenticated nor encrypted.</td>
</tr>
<tr>
<td>-p &lt;port&gt;</td>
<td>The ELA proxy port number. Default is 18187.</td>
</tr>
<tr>
<td>-f &lt;token value&gt;</td>
<td>A field to be added to the log, represented by a token-value pair as follows: • token - The name of the field to be added to the log. token cannot contain spaces. • value - The field’s value. value cannot contain spaces. This option can be used multiple times to add multiple token-value pairs to the log.</td>
</tr>
</tbody>
</table>
The alert to be triggered at the ISP site. This alert overrides the alert specified in the log message generated by the alert daemon. The response to the alert is handled according to the actions specified in the ISP Security Policy:

The following alerts execute the OS commands:
- `alert` - Popup alert command
- `mail` - Mail alert command
- `snmptrap` - SNMP trap alert command
- `spoofalert` - Anti-spoof alert command

The following NetQuota and ServerQuota alerts execute the OS commands specified in: `$FWDIR/conf/objects.C: value=clientquotaalert. Parameter=clientquotaalertcmd`

You can configure the alert in the Manage & Settings tab > Global Properties > Log and Alert > Alert

<table>
<thead>
<tr>
<th>Return Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Execution was successful.</td>
</tr>
<tr>
<td>102</td>
<td>Undetermined error.</td>
</tr>
<tr>
<td>103</td>
<td>Unable to allocate memory.</td>
</tr>
<tr>
<td>104</td>
<td>Unable to obtain log information from stdin</td>
</tr>
<tr>
<td>106</td>
<td>Invalid command line arguments.</td>
</tr>
<tr>
<td>107</td>
<td>Failed to invoke the OPSEC API.</td>
</tr>
</tbody>
</table>

**Example**

`# inet_alert -s 10.0.2.4 -a clear -f product cads -m alert`

This command specifies that in the event of an attack, `inet_alert` should take the following actions:

- Establish a clear connection with the ELA Proxy located at IP address 10.0.2.4.
- Send a log message to the specified ELA Proxy. The product field of this log message should be set to `cads`
- Trigger the OS command specified in the Popup Alert Command field of the Log and Alert tab of the Properties Setup window in SmartConsole.

**ldap**

**ldapcmd**

**Description**  Manages processes running on the Security Gateway collectively or individually and includes the following:

- **Cache**
  Cache operations, such as emptying the cache, as well as providing debug information.
• **Statistics**
  Finds statistics such as:
  - All user searches
  - Pending lookups (when two or more lookups are identical)
  - Total lookup time (the total search time for a specific lookup)
  - Cache statistics such as hits and misses

• **Logging**
  View the alert and warning log regarding debug.

**Syntax**

```
# ldapcmd -p {<process_name>|all} <command> [-d debug_level] [command_arg]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>Runs a specified process or all processes.</td>
</tr>
<tr>
<td>&lt;command&gt;</td>
<td>Valid values for the <code>command</code> parameter:</td>
</tr>
<tr>
<td></td>
<td>- <code>cacheclear</code></td>
</tr>
<tr>
<td></td>
<td>`{all</td>
</tr>
<tr>
<td></td>
<td>- <code>cachetrace</code></td>
</tr>
<tr>
<td></td>
<td>`{all</td>
</tr>
<tr>
<td></td>
<td>- `stat {print_interval {&lt;reset interval time in secs&gt;</td>
</tr>
<tr>
<td></td>
<td>- `log {on</td>
</tr>
</tbody>
</table>

**log** Specifies whether or not to create LDAP logs.

**ldapcompare**

**Description** Performs compare queries. Prints a message whether the result returned a match or not. `ldapcompare` opens a connection to an LDAP directory server, and binds and performs the comparison specified on the command line or from a specified file.

**Syntax**

```
# ldapcompare -d [options] dn <attribute> <value>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag.</td>
</tr>
<tr>
<td>&lt;options&gt;</td>
<td>See below.</td>
</tr>
<tr>
<td>dn</td>
<td>The DN object.</td>
</tr>
<tr>
<td>attribute</td>
<td>The attribute of the DN object.</td>
</tr>
<tr>
<td>value</td>
<td>The value of the attribute of the DN object.</td>
</tr>
</tbody>
</table>
The `ldapcompare` options:

- `-u` - Include user-friendly entry names in the output.
- `-d <level>` - Set LDAP debugging level to `level`
- `-F sep` - Print `sep` instead of `=` between attribute names and values.
- `-f <file>` - Perform sequence of compares listed in `file`
- `-D <binddn>` - Bind DN.
- `-w <password>` - Bind password (for simple authentication).
- `-h <host>` - LDAP server.
- `-p <port>` - Port on the LDAP server.
- `-T <timeout>` - Client side timeout for all operations (in milliseconds).
- `-l <time limit>` - Server side time limit (in seconds) for compare.
- `-z <size limit>` - Server side size limit (in entries) for compare.

### ldapconvert

**Description**  
A utility program to port from Member Mode to MemberOf Mode. This is done by searching all specified group/template entries and fetching their Member attribute values.

Each value is the DN of a member entry. The entry identified by this DN is added to the MemberOf attribute value of the group/template DN at hand. In addition, those Member attribute values will be deleted from the group/template unless Both Mode is specified.

When you run the program, a log file, `ldapconvert.log` is generated in the current directory. It logs all modifications done and errors encountered.

**Syntax**

```
> ldapconvert -d -h <host> -p <port> -D user_DN -w <secret> [-g group_DN | -f <file>]
   -m mem_attr -o memberof_attr -c memberobjectclass[<extra options>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d</code></td>
<td>Debug flag.</td>
</tr>
<tr>
<td><code>-h &lt;host&gt;</code></td>
<td>LDAP server IP address.</td>
</tr>
<tr>
<td><code>-p &lt;port&gt;</code></td>
<td>LDAP server port number.</td>
</tr>
<tr>
<td><code>-D user_DN</code></td>
<td>LDAP bind DN.</td>
</tr>
<tr>
<td><code>-w &lt;secret&gt;</code></td>
<td>LDAP bind password.</td>
</tr>
<tr>
<td><code>-g group_DN</code></td>
<td>Group or template DN to perform the conversion on. May appear multiple times for multiple entries.</td>
</tr>
<tr>
<td><code>-f &lt;file&gt;</code></td>
<td>File containing a list of group DNs each separated by a new line.</td>
</tr>
<tr>
<td><code>-m mem_attr</code></td>
<td>LDAP attribute name when fetching and (possibly) deleting a Member attribute value.</td>
</tr>
<tr>
<td><code>-o memberof_attr</code></td>
<td>LDAP attribute name when adding MemberOf attribute value.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>-c</code> memberobjectclass</td>
<td>LDAP objectclass attribute value that filters which type of member entries to modify. May appear multiple times creating a compound filter.</td>
</tr>
</tbody>
</table>

The `ldapconvert` extra options are as follows:

- `-M` - Maximum number of member LDAP updated simultaneously. Default is 20.
- `-B` - Convert to Both Mode.
- `-p <port>` - LDAP port. Default is 389.
- `-T <timeout>` - Client side timeout for LDAP operations, in milliseconds. Default is `never`.
- `-l <time limit>` - Server side time limit for LDAP operations, in seconds. Default is `never`.
- `-s` - Server side size limit for LDAP operations in entries. Default is `none`.
- `-z` - Use SSL.

**Note** - We recommend you make a backup of the LDAP server before running the conversion program in case unrecoverable errors are encountered.

There are two GroupMembership modes. You must keep these modes consistent.

- template-to-groups
- user-to-groups

For example, if you apply conversion on LDAP users to include `MemberOf` attributes for their groups, then this conversion has to be applied on LDAP defined templates for their groups.

**Symptom:**

A command runs with the option `-M` fail. The program stops with an error message stating the connection stopped unexpectedly.

**Solution:**

The LDAP server could not handle that many LDAP requests simultaneously and closed the connection.

Run the program again with a lower value for the `-M` option. The default value should be adequate but can also cause a connection failure in extreme situations. Continue to reduce the value until the program exits normally. Each time you run the program with the same set of groups the program will pick up where it left off.

**Example 1:**

A group is defined with the DN: `cn=cpGroup, ou=groups, ou=cp, c=il` and the following attributes:

```plaintext
...  
cn=cpGroup
uniquemember="cn=member1, ou=people, ou=cp, c=il"
uniquemember=" cn=member2, ou=people, ou=cp, c=il"
...  
```
For the two member entries:

```
...  
 cn=member1
 objectclass=fw1Person
 ...  
```

and:

```
...  
 cn=member2
 objectclass=fw1Person
 ...  
```

Run: `ldapconvert` with the following arguments:

```
ldapconvert -g cn=cpGroup,ou=groups, ou=cp, c=il -h myhost -d cn=admin -w secret \
 -m uniquemember -o memberof -c fw1Person
```

The result for the group DN will be as follows:

```
...  
 cn=cpGroup
 ...  
```

The result for the two member entries will be as follows:

```
...  
 cn=member1
 objectclass=fw1Person
 memberof="cn=cpGroup,ou=groups, ou=cp, c=il"
 ...  
```

and:

```
...  
 cn=member2
 objectclass=fw1Person
 memberof=" cn=cpGroup,ou=groups, ou=cp, c=il"
 ...  
```

If you run the same command with the `-B` options, it will produce the same result but the group entry will not be modified.

**Example 2:**

If there is another member attribute value for the same group entry:

```
uniquemember="cn=template1,ou=people, ou=cp,c=il"
```

and the template is:

```
cn=member1
 objectclass=fw1Template
```

After running the same command line the template entry will stay intact because the command line specified the option `-c fw1Person`, but the object class of template1 is `fw1Template`.
Description  Imports users to an LDAP server. The input file must be in the LDIF format.

Syntax

```bash
# ldapmodify -a -c -d -h <host> -p <port> -D <LDAPadminDN> -p <LDAPadminPassword> -f <exportfilename>.ldif -d
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Adds users.</td>
</tr>
<tr>
<td>-c</td>
<td>Continue on errors.</td>
</tr>
<tr>
<td>-h &lt;host&gt;</td>
<td>LDAP server IP address.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug flag.</td>
</tr>
<tr>
<td>-p &lt;port&gt;</td>
<td>LDAP server port number.</td>
</tr>
<tr>
<td>-D &lt;LDAPadminDN&gt;</td>
<td>LDAP administrator DN.</td>
</tr>
<tr>
<td>-p &lt;LDAPadminPassword&gt;</td>
<td>LDAP administrator password.</td>
</tr>
<tr>
<td>-f &lt;exportfilename&gt;.ldif</td>
<td>Specifies the name of the input file. This file must be in the LDIF format.</td>
</tr>
</tbody>
</table>

Before importing, prepare the LDAP directory as follows:

- Make sure the root branch is defined as an allowed branch on your LDAP server.
- Restart the LDAP server.
- Create the branch into which the users will be imported, either by using **Create Tree Object** in the Account Management Client or with the `ldapmodify` command:

```bash
ldapmodify -a -h <host> -p <port> -D <LDAPadminDN> -w <LDAPadminPassword>
```

```
dn: o=myOrg,c=US
objectclass: organization
o:myOrg
```

**ldapsearch**

Description  Queries an LDAP directory and returns the results.

Syntax

```
ldapsearch [options] filter [attributes] -d
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>options</td>
<td>See the options attributes below.</td>
</tr>
<tr>
<td>filter</td>
<td>RFC-1558 compliant LDAP search filter. For example, objectclass=fw1host.</td>
</tr>
<tr>
<td>attributes</td>
<td>The list of attributes to be retrieved. If no attributes are given, all attributes are retrieved.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug flag.</td>
</tr>
</tbody>
</table>

The following are the attributes for options:

- `-A` –Retrieve attribute names only, without values.
-B  Do not suppress printing of non-ASCII values.
-D bindDN  The DN to be used for binding to the LDAP server.
-F separator  Print separator between attribute name and value instead of =
-h host  The LDAP server identified by IP address or resolvable name.
-l timelimit  The server side time limit for search, in seconds.
-p portnum  The port number. The default is standard LDAP port 389.
-S attribute  Sort the results by the values of attribute
-s scope  One of the following: base, one, sub
-b  Base distinguished name (DN) for search.
-t  Write values to files in /tmp. Each attribute-value pair is written to a separate file, named: /tmp/ldapsearch-<attribute>-<value>.
For example, for the fw1color attribute, the file written is named /tmp/ldapsearch-fw1color-a00188
-T timeout  Client-side timeout in milliseconds, for all operations.
-u  Show user friendly entry names in the output. For example, show cn=Babs Jensen, users, omi instead of cn=Babs Jensen, cn=users,cn=omi
-w password  The password.
-Z  Encrypt using SSL.
-z sizelimit  Server-side size limit for search, in entries.

Example:
ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass
The LDAP directory will be queried for fw1host objects using port number 18185 with DN common name omi. For each object found, the value of its objectclass attribute is printed.

queryDB_util

Description  Enables the search of the object database according to search parameters.

Syntax

```
# queryDB_util [-t <table_name>] [-o <object_name>] [-a]
[-mu <modified_by>] [-mh <modified_from>]
[-ma <modified_after>] [-mb <modified_before>] [-p{m|u|h|t|f}]
[-f <filename>] [-h] [-q]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t &lt;table_name&gt;</td>
<td>The name of the table.</td>
</tr>
<tr>
<td>-o &lt;object_name&gt;</td>
<td>The name of the object.</td>
</tr>
<tr>
<td>[-a]</td>
<td>All objects.</td>
</tr>
<tr>
<td>-mu &lt;modified_by&gt;</td>
<td>The name of the administrator who last modified the object.</td>
</tr>
<tr>
<td>-mh &lt;modified_from&gt;</td>
<td>The host from which the object was last modified.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| -ma <modified_after> | The date after which the object was modified
<[hh:mm:ss][ddmmmyyyy]>. Either or both options may be used.
Omitting hh:mm:ss defaults to today at midnight, omitting
ddmmmyyyy defaults to today's date on the client. |
| -mb <modified_before> | The date before which the object was modified
<[hh:mm:ss][ddmmmyyyy]>. Either or both options may be used.
Omitting hh:mm:ss defaults to today at midnight, omitting
ddmmmyyyy defaults to today's date on the client. |
| -p{m|u|h|t|f} | Short print options:
• c - Creation details.
• m - Last_modification details.
• u - Administrator name (create/modify).
• h - Host name (create/modify).
• t - Time (create/modify).
• f - Field details. |
| -f <filename> | The name of the output file |
| -h | Display command help |
| -q | Quit. |

**Example:**

Print modification details of all objects modified by administrator aa

```
query> -a -mu Bob -pm
Object Name:my_object
Last Modified by:Bob
Last Modified from:london
Last Modification time:Mon Jun 19 11:44:27 2000

Object Name:internal_ca
Last Modified by:Bob
Last Modified from:london
Last Modification time:Tue Jun 20 11:32:58 2000

A total of 2 objects match the query.
```

**rs_db_tool**

**Description**  Manages DAIP gateways in a DAIP database.

**Syntax**

```
# rs_db_tool  [-d]  <-operation <add <name object_name> <ip module_ip>
<TTL Time-To-Live> >
# rs_db_tool  [-d]  <-operation fetch <name object_name> >
# rs_db_tool  [-d]  <-operation <delete <name object_name> >
# rs_db_tool  [-d]  <-operation <list> >
# rs_db_tool  [-d]  <-operation <sync> >
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>debug file.</td>
</tr>
<tr>
<td>-operation add</td>
<td>Add entry to database.</td>
</tr>
<tr>
<td>&lt;name object_name&gt;</td>
<td>Enter the name of the gateway object.</td>
</tr>
<tr>
<td>&lt;ip module_ip&gt;</td>
<td>Enter the IP Address of the gateway.</td>
</tr>
<tr>
<td>&lt;TTL Time-To-Live&gt;</td>
<td>The relative time interval (in seconds) during which the entry is valid. A value of zero specifies unlimited.</td>
</tr>
<tr>
<td>- operation fetch</td>
<td>Get entry from database.</td>
</tr>
<tr>
<td>- operation delete</td>
<td>Delete entry from database.</td>
</tr>
<tr>
<td>- operation list</td>
<td>List all the database entries.</td>
</tr>
<tr>
<td>- operation sync</td>
<td>Synchronize the database.</td>
</tr>
</tbody>
</table>