QUANTUM

01 May 2024

SECURITY MANAGEMENT

R80.40

Administration Guide

CHECK POINT™

Check Point Copyright Notice

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.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R80.40
For more about this release, see the R80.40 home page.

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
01 May 2024	Updated *"Creating an Access Control Policy" on page 227*
13 March 2024	Updated *"Managing Administrator Accounts" on page 48*
15 January 2024	Updated *"Configuring the NAT Policy" on page 287*
06 September 2023	Added the *"Compliance" on page 459* chapter
05 September 2023	Updated *"The Columns of the Access Control Rule Base" on page 228*
22 August 2023	Updated *"Working with Policy Packages " on page 219*
10 August 2023	Updated *"Account Units" on page 147*
08 August 2023	Updated *"Central Deployment of Hotfixes" on page 175*
22 June 2023	Added *"Implied Rules" on page 383*
14 June 2023	Updated *"UserCheck in the Access Control Policy" on page 385*
02 May 2023	Updated *"Central Deployment of Hotfixes" on page 175*
07 April 2023	Updated *"Managing Administrator and User Accounts" on page 48*
02 April 2023	Updated *"Creating Application Control and URL Filtering Rules" on page 246*
05 March 2023	Updated *"Location of 'user.def' Files on the Management Server" on page 183*
14 February 2023	Updated *"cp_log_export" on page 521*

Date	Description
17 January 2023	Updated: ▪ "Configuring Implied Rules or Kernel Tables for Security Gateways" on page 180 - corrected paths for R80.30, R80.20, and R80.10 versions
19 December 2022	Updated: ▪ "Configuring a Secondary Security Management Server in SmartConsole" on page 451
04 December 2022	Updated: ▪ "Configuring Implied Rules or Kernel Tables for Security Gateways" on page 180 - added paths for R75.4x, R75.30, and R75.20 versions
17 November 2022	Updated: ▪ "Configuring the NAT Policy" on page 287 ▪ "Working with Automatic NAT Rules" on page 295 ▪ "Working with Manual NAT Rules" on page 304 ▪ "Working with NAT46 Rules" on page 310 ▪ "Working with NAT64 Rules" on page 325 ▪ " Advanced NAT Settings" on page 345
17 October 2022	Updated: ▪ "cp_log_export" on page 521
24 July 2022	Removed: ▪ "Configuring a SIC Proxy" - supported only for internal Check Point needs
15 June 2022	In the HTML version, added glossary terms in the text
28 December 2021	Updated: ▪ "High Availability Troubleshooting" on page 455.
23 December 2021	Updated: ▪ Values for IKE certificate validity period in "CA Procedures" on page 484 ▪ "Network Security for IoT Devices" on page 443

Date	Description
27 November 2021	Updated: - *"Configuring a Security Gateway to Access the Management Server or Log Server at its NATed IP Address" on page 173*
09 November 2021	Updated: - *"Creating a New Security Gateway" on page 156*
28 October 2021	Added a note in: - *"Network Security for IoT Devices" on page 443*
07 October 2021	Updated: - *"Creating a New Security Gateway" on page 156*
07 October 2021	Updated: - *"Database Revisions" on page 431* - *"SmartTasks" on page 437*
8 September 2021	Updated: - *"Viewing Licenses in SmartConsole" on page 168*
13 August 2021	Updated: - *"Secure Internal Communication (SIC)" on page 161* - *"Creating Application Control and URL Filtering Rules" on page 246* - *"Best Practices for Access Control Rules" on page 276* - *"Database Revisions" on page 431*
26 June 2021	Updated formatting
09 May 2021	Added: - *"Configuring Implied Rules or Kernel Tables for Security Gateways" on page 180*
27 April 2021	Updated: - *"Network Security for IoT Devices" on page 443*
17 April 2021	Updated: - *"migrate" on page 802* - *"migrate_server" on page 806*

Date	Description
09 February 2021	Added: - *"Configuring a Security Gateway to Access the Management Server or Log Server at its NATed IP Address" on page 173* Updated: - *"The Columns of the Access Control Rule Base" on page 228* - *"Creating Application Control and URL Filtering Rules" on page 246* - *"Database Revisions" on page 431*
03 May 2020	Updated: - *"Central Deployment of Hotfixes" on page 175* and *"Database Revisions" on page 431*
27 January 2020	First release of this document

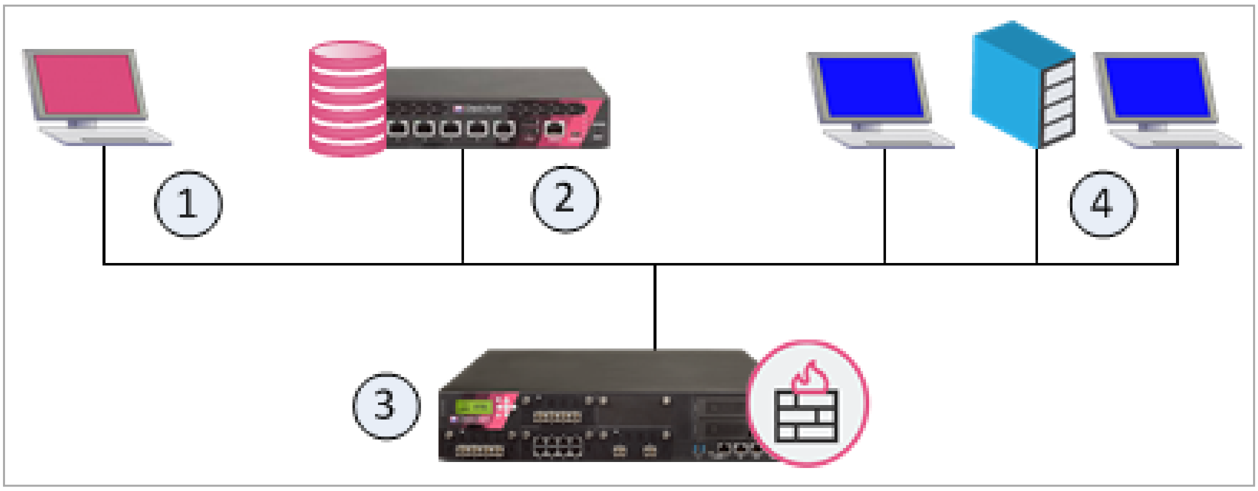
Table of Contents

Introduction to Security Management

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 *R80.40 Multi-Domain Security Management Administration Guide*.

These are the basic components of Check Point security architecture.



Item	Description
1	SmartConsole - Check Point Graphical User Interface for connection to and management of Security Management Servers.
2	Security Management Server - Manages Security Gateways with defined security policies and monitors security events on the network.
3	Security Gateway - Placed at the perimeter of the network topology, to protect your environment through enforcement of the security policies.
4	Your environment to protect.

Getting Started

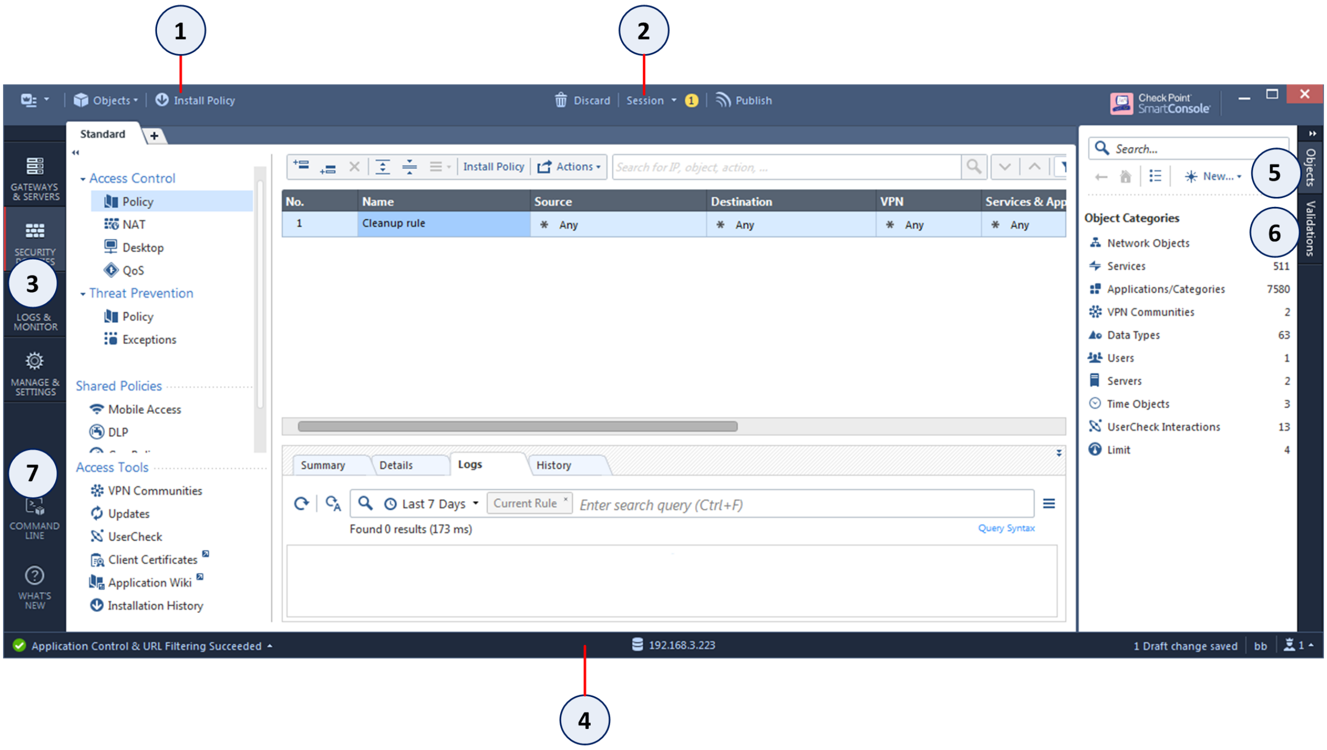
Before you begin deploying a Check Point security solution, familiarize yourself with:

- 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 Window



Item	Description	Item	Description
1	Global Toolbar	5	Objects Bar (F11)

Item	Description	Item	Description
2	Session Management Toolbar	6	Validations pane
3	Navigation Toolbar	7	Command line interface button
4	System Information Area		

SmartConsole Toolbars

Global Toolbar (top of SmartConsole)

	Description
▾	The main SmartConsole Menu. When SmartConsole is connected to a Security Management Server, this includes: ■ Manage policies and layers ■ Open Object Explorer ■ New object (opens menu to create a new object) ■ Publish session ■ Discard session ■ Session details ■ Install policy ■ Verify Access Control Policy ■ Install Database ■ Uninstall Threat Prevention policy ■ Management High Availability ■ Manage Licenses and Packages ■ Global Properties ■ View (opens menu to select a View to open)
📦	Create new objects or open the Object Explorer
⬇	Install policy on managed Security Gateways

Session Management Toolbar (top of SmartConsole)

	Description
🗑	Discard changes made during the session
Session ▾	Enter session details and see the number of changes made in the session.
📡	Publish the SmartConsole session, to make the changes visible to other administrators, and ready to install on Security Gateways. **Note** - When the policy is installed, published changes are installed on the Security Gateways and enforced.

Navigation Toolbar (left side of SmartConsole)

	Keyboard Shortcut	Description
	Ctrl+1	**Gateways & Servers** configuration view: ■ Manage Security Gateways ■ Activate Software Blades ■ Add, edit, or delete Security Gateways and clusters (including virtual clusters) ■ Run scripts ■ Backup and restore Security Gateways ■ Open a command line interface on the Security Gateway ■ View Security 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 Custom Policy 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 Security Gateways ■ See compliance information

	Keyboard Shortcut	Description
⚙	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)

	Keyboard Shortcut	Description
>_	F9	Open a command line interface for management scripting and API

For more SmartConsole shortcuts, see *"Keyboard Shortcuts for SmartConsole" on page 37*.

Objects Bar (right side of SmartConsole)

	Description
Objects	Manage security and network objects

Validations Pane (right side of SmartConsole)

	Description
Validations	See validation errors

System Information Area (bottom of SmartConsole)

	Description
Task List	See management tasks in progress and expand to see recent tasks

	Description
Server Details	See the IP address of the server to which SmartConsole is connected. If Management High Availability is configured, click to see the details.
Session Status	See the number of changes made in the session and the session status.
Connected administrators	See connected administrators: Yourself and others.

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

You can search for an object in the Security Management Server database in two ways:

- Enter the prefix of the object's name. For example, to find *USGlobalHost*, you can enter *USG* in the search box.
- Enter any sequence of characters in the object's name and add an asterisk (*) before such sequence.

  For example, to find *USGlobalHost*, you can enter **oba*, **host*, **SG* and so on in the search box.

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.0.0/16 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 Security 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 Security 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.

If there is...	This is highlighted
A direct match on an object name or on textual columns	Only the specific matched characters
A direct match on object properties	The entire object name
A negated column	The negated label
A match on "Any"	"Any"

Known Limitation:

- Packet search does not support IPv6.

Access and Custom Policy Tools

The **Access Tools** section in the **Security Policies Access Control** view and the **Custom Policy Tools** section in the **Security Policies Threat Prevention** view give you more management and data collection tools.

"Access Tools" in the Security Policies "Access Control" view

Tool	Description
VPN Communities	Create, edit, or delete VPN Communities.
Updates	Update the Application & URL Filtering database, schedule updates, and configure updates.
UserCheck	Configure UserCheck interaction objects for Access Control policy actions.
Client Certificates	Create and distribute client certificates that allow users to authenticate to the Security Gateway from handheld devices.
Application Wiki	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.
Installation History	See the Policy installation history for each Security 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.

"Custom Policy Tools" in the Security Policies "Threat Prevention" view

Tool	Description
Profiles	Create, edit, or delete profiles.
IPS Protections	Edit IPS protections per profile.
Protections	See statistics on different protections
Whitelist Files	Configure Whitelist Files list
Indicators	Configure indicators of malicious activity and how to handle it
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 Security 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.

Software Blade	Description
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.

Software Blade	Description
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 Security Gateways.
Inspection Settings	You can configure Inspection Settings for the Security Gateway (see *"Preferences and Management Settings" on page 431*): ▪ 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 (see *"Managing Security through API" on page 42*).

Keyboard Shortcuts for SmartConsole

From R80.20, there are additional keyboard shortcuts that you can use to navigate between the different SmartConsole fields:

Keyboard shortcut	Description
Ctrl+S	Publish the SmartConsole session
Ctrl+Alt+S	Discard the SmartConsole session.
Shift+Alt+Enter	Install policy.
F10	Show/hide task details.

Keyboard shortcut	Description
F11	Show/hide Object Explorer.
Ctrl+O	Manage policies and layers
Ctrl+E	Open Object Explorer
Ctrl+F3	Switch to high-contrast theme
Alt+Space	System menu
F1	Open the relevant online help
Alt+F4	Close SmartConsole

Shortcuts for the specific views that support them:

Keyboard shortcut	Description
Ctrl+T	Open new tab
Ctrl+W or Ctrl+F4	Close current tab
Ctrl+Tab	Move to the next tab
Ctrl+Shift+Tab	Move to the previous tab
Delete	Delete the currently selected item
Ctrl+A	Select all elements
Esc	Cancel operation to close window
Enter or mouse double-click	Edit item

Shortcuts for views that contain a Rule Base:

Keyboard shortcut	Description
Ctrl+G	Go to rule (in the Access Control Rule Base)
Ctrl+X	Cut rule
Ctrl+C	Copy rule
Ctrl+V	Paste rule below the selected rule

Keyboard shortcut	Description
Delete	Remove a used item from a rule cell
Ctrl+F	Open Rule Base search
F3	Navigate to the next Rule Base search result
Ctrl+arrow up	Go to the first rule in the Rule Base
Ctrl+arrow down	Go to the last rule in the Rule Base
Space or +	Open drop-down menu for the current cell in the Rule Base
Shift+arrow up/down	Move between objects in the Rule Base

Shortcuts for the Logs & Monitor view:

Keyboard shortcut	Description
Ctrl+G	Switch to grid view (in the Logs and Audit Logs views)
Ctrl+L	Switch to table view (in the Logs and Audit Logs views)
Ctrl+R	Resolve objects
F5	Refresh query
F6	Enable auto-refresh
Ctrl+D	Add to favorites
Ctrl+S	Organize favorites

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:*

     a. From the drop-down list, select **Certificate File**.

     b. Browse to the file.

        This is the certificate file you created in the administrator object.

     c. Enter the password of the certificate file.

   - *Logging in with a certificate in the CAPI repository:*

     Prerequisite - You must create a certificate file in the administrator object in SmartConsole, save it, and import it into the Windows Certificate Store on the SmartConsole client computer. See *"Managing Administrator Accounts" on page 48*.

     a. From the drop-down list, select **CAPI Certificate**.

     b. From the drop-down list, select the administrator.

3. Enter the name or the IP address of the Security Management Server / Domain Management Server.
4. Click **Login**.

   The SmartConsole authenticates the Security Management Server / Domain 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 / Domain Management Server are saved to the user settings in Windows.

Setting Up for Security Management

To start setting up your security environment, configure the Security Management Server and the Security Gateways. The Security Gateways enforce the security policy that you define on the Security Management Server.

To configure the Security Management Server in SmartConsole

1. In the **Gateways & Servers** view, find the Security Management Server object.

   In the **Search** box at the top of the view, you can search for it by object name or object IP address.

   When you select the Security Management Server object, the **Summary** tab in the lower pane shows the Software Blades that are enabled on it.

2. Double-click the object to open its properties.

   On the **Management** tab, enable the 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 Endpoint Security Clients on end-user computers and hand-held devices.

     ℹ **Important** - It is not supported to disable this Software Blade after you enable it.
   - **Logging & Status** - Monitor security events and status of Security 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.
   - **Provisioning** - Manage Security Gateway configuration and policies for multiple appliances and open servers in one central SmartConsole.
   - **Compliance** - Optimize your security settings and comply with regulatory requirements
   - **SmartEvent Server** - Manage security events in real-time.
   - **SmartEvent Correlation Unit** - 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 Security Gateway settings in the classic mode (see *"Managing Gateways" on page 156*).

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 (see *"Managing Administrator Accounts" on page 48*) 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

This section describes the API Server on a Management Server and the applicable API Tools.

API

You can configure and control the Management Server through API Requests you send to the API Server that runs on the Management 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.

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

- The API Documentation:
  - Online - *Check Point Management API Reference*
  - Local - `https://<Server IP Address>/api_docs`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`

- Standalone management tool, included with SmartConsole:

  ```
  mgmt_cli.exe
  ```

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.

- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

  These APIs also let other Check Point processes communicate with the Management Server over the HTTPS protocol.

  ```
  https://<IP Address of Management Server>/web_api/<command>
  ```

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

   The **Management API Settings** window opens.
5. Configure the **Startup Settings** and the **Access Settings**.

   Configuring Startup Settings

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

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

Configuring Access Settings

Select one of these options to configure which clients can connect to the API Server:

- **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
- **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
- **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.

6. Publish the SmartConsole session.
7. Restart the API Server on the Management Server with this command:

```
api restart
```

Note - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server.

Creating an Administrator Account with API Key Authentication

An API key is a token that a client provides when making API calls.

API key authentication provides an administrator the ability to use a token for authenticating to the API interface instead of the usual administrator name / password.

You can use SmartConsole to configure an API key for administrators to use the management API.

Note - This administrator can only use the API for executing API commands and cannot use it for SmartConsole authentication.

To configure API authentication for an Administrator using SmartConsole

1. In SmartConsole click **Manage & Settings** > **Permissions & Administrators** > **Administrators**

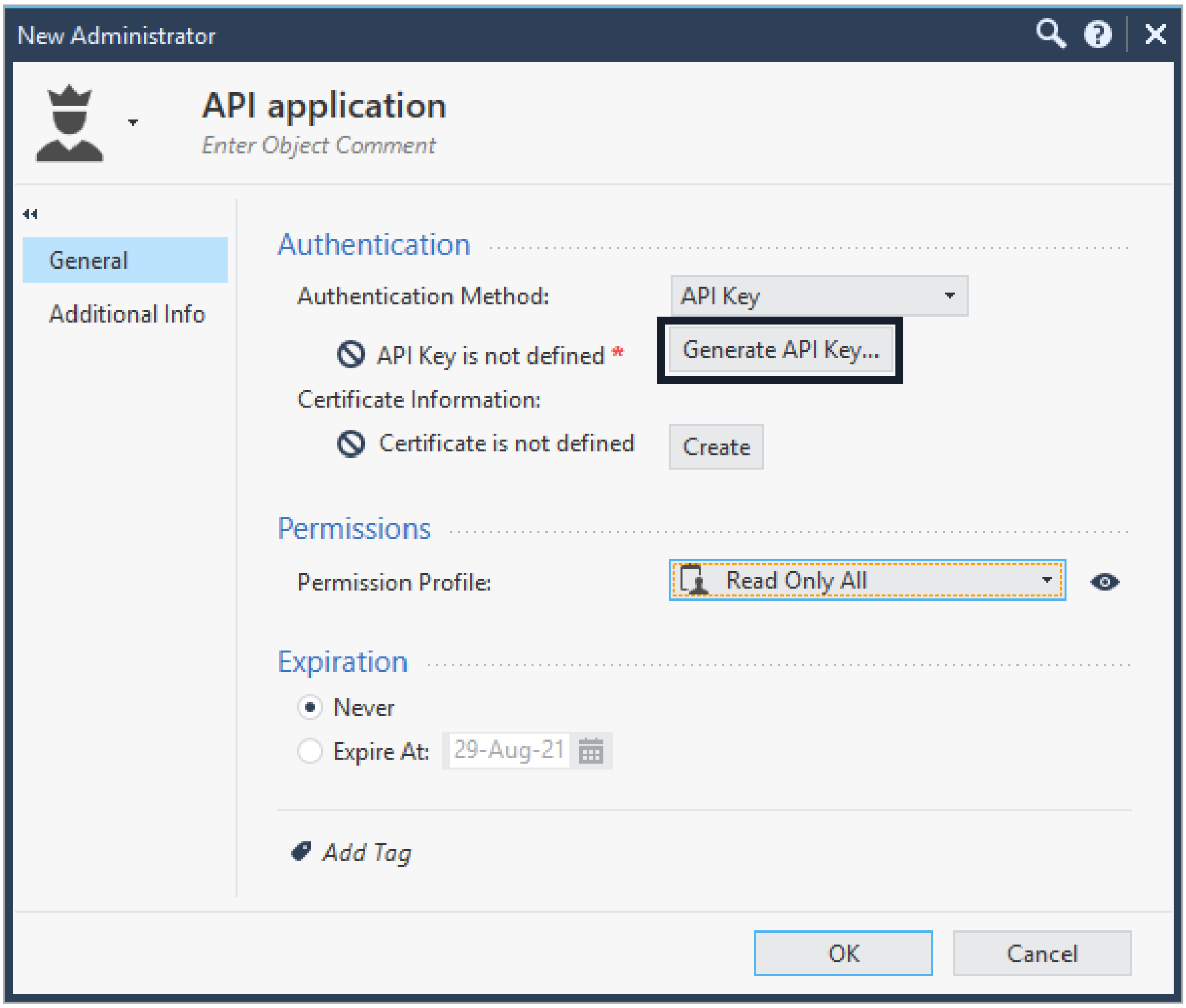
   Click the **New** icon at the top menu.

   The **New Administrator** window opens.

2. Give the administrator a name

3. In the **Authentication Method** field select **API Key**.

4. Click **Generate API key**.



New Administrator

API application

Enter Object Comment

Authentication

Authentication Method: API Key

⊘ API Key is not defined *

Certificate Information:

⊘ Certificate is not defined

Permissions

Permission Profile: Read Only All

Expiration

● Never

○ Expire At: 29-Aug-21

5. A new API key window opens.
   a. Click **Copy key to Clipboard**
   b. Save the key for a later use (provide it to the relevant administrator).

6. Click **OK**

7. Publish the SmartConsole session.

Example

This example demonstrates how to use the API-key for *login* and creating a *simple-gateway* using the API.

1. Log in to the Expert mode.
2. Use the previously generated key for the login, and save the standard output to a file (redirect it to a file using the ">" sign):

   Syntax:

   ```
   mgmt_cli login api-key <api-key> > /<path_to>/<filename>
   ```

   Example:

   ```
   mgmt_cli login api-key mvYSiHVmlJM+J0tu2FqGag12 >
   /var/tmp/token.txt
   ```

3. Run a `mgmt_cli` command with the "**-s**" flag.

   Syntax:

   ```
   mgmt_cli -s /<path_to>/<filename> add simple-gateway name
   <gateway name> ip-address <ip address> one-time-password
   <password> blade <true>
   ```

   Example:

   ```
   mgmt_cli -s /var/tmp/token.txt add simple-gateway name "gw1"
   ip-address 192.168.3.181 one-time-password "aaaa" firewall
   true vpn true
   ```

   For more details, see the *Check Point Management API Reference*.

After you configure API authentication, you can, in addition, configure authentication with a certificate file. The administrator can then authenticate to the Security Management Server with either an API Key or a certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

Planning Security Management

After installing the Security Management Server and Security Gateway, 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 in SmartConsole. See *"Network Object Types" on page 204*.

Define users and user groups that your security environment protects

You can add users and groups to the database manually, through LDAP and User Directory, or with the help of Active Directory.

To add users: see *"User Directory" on page 114*.

To add groups: see *"Managing User Accounts" on page 90*.

To use LDAP, see *"Configuring Administrators and Users on an External LDAP Server" on page 143*.

To use Active Directory, see *"Microsoft Active Directory" on page 144*.

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 based on traffic, applications, Web sites, and data (see *"Managing Policies" on page 219*). 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 and User Accounts

A Check Point administrator is an IT professional who manages and maintains a Check Point security environment with SmartConsole, CLI, or the API. Check Point administrators configure and manage Check Point's security products to protect their organization's networks from cyber attacks, malware, and other security threats. A Check Point administrator typically installs, configures, and maintains the Check Point software, manages network traffic and security policies, monitors system performance, and troubleshoots security issues. Administrators also make sure that the Check Point environment is up to date with the latest Hotfixes and updates to maintain optimal security.

A user account is an object that represents a user that generates traffic in a Check Point environment. The system administrators create, manage and monitor user objects. Administrators can configure Access Control rules for specific users - rules for Remote Access VPN, Identity Awareness, and other features.

Limitation of access to sensitive information and resources only to authorized users secures the organization's network and data.

The Security Management Server authenticates administrators. Security Gateways authenticate individual users.

This chapter explains how to configure, manage and authenticate administrators and users.

Managing Administrator Accounts

A Check Point administrator is an IT professional who manages and maintains a Check Point security environment with SmartConsole, CLI, or the API. Check Point administrators configure and manage Check Point's security products to protect their organizations' networks from cyber attacks, malware, and other security threats. A Check Point administrator typically installs, configures, and maintains the Check Point software, manages network traffic and security policies, monitors system performance, and troubleshoots security issues. Administrators also ensure that the Check Point security environment is up to date with the latest Hotfixes and updates to maintain optimal security.

You can store administrator accounts in the Check Point management database or on an external LDAP server. The Security Management Server authenticates administrators. Check Point supports different authentication methods for administrators.

Creating 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.

When you create an administrator account through SmartConsole, you can select one of these authentication methods:

Authentication Method	Description
Check Point Password	Check Point password is a static password that is configured in SmartConsole. The local database on the Security Management Server stores the password. No additional software is required. See *"Creating an Administrator Account with Check Point Password Authentication" on page 54*.
OS Password	OS password is kept on the operating system of the computer on which the Security Management Server is installed. You can also use passwords that are stored in Windows domain. No additional software is required. See *"Creating an Administrator Account with OS Password Authentication" on page 57*
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. With RADIUS, the Security Management Server forwards the authentication requests to the RADIUS server. The RADIUS server, which stores administrator account information, does the authentication. The RADIUS protocol uses UDP to communicate with the Security Gateway or the Security Management Server. See *"Creating an Administrator Account with RADIUS Server Authentication" on page 59*
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. With TACACS, the Security Management Server forwards authentication requests by remote administrators to the TACACS server. The TACACS server, which stores administrator account information, authenticates administrators. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the administrator name, password, authentication services and accounting information of all authentication requests to secure communication. See *"Creating an Administrator Account with TACACS Server Authentication" on page 63*

Authentication Method	Description
SecurID	SecurID requires administrators to possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices. Software tokens reside on the PC or device from which the administrator wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When an administrator attempts to authenticate to a protected resource, the AM must validate the one-time use code. The Security Management Server forwards SecurID authentication requests by remote administrators to the AM. The AM manages the database of the RSA users and their assigned hard or soft tokens. The Security Management Server act as an AM Agent and directs all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to the RSA Authentication Manager documentation. There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API. See *"Creating an Administrator Account with SecurID Authentication" on page 67*.
API Key	You can use SmartConsole to configure an API key for administrators to use the management API. You can only use the API to execute API commands and not for SmartConsole authentication. For more information, see *"Creating an Administrator Account with API Key Authentication" on page 70*

After you configure authentication with one of the Check Point authentication methods, you can, in addition, configure certificate file authentication. The administrator can then authenticate to SmartConsole with one of the Check Point authentication methods or with a certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

To create an Administrator Account with the "Check Point Configuration Tool" tool (cpconfig)

We do not recommend to create 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 with these commands:

  ```
  cpstop ; cpstart
  ```

- It does not show the other administrators.
- Check Point Password is automatically configured as the authentication method.

Editing an Administrator Account

1. Click **Manage & Settings** > **Permissions & Administrators**.
2. Double-click an administrator account.

   The **Administrators** properties window opens.

Deleting an Administrator Account

To make sure your environment is secure, the best practice is to delete administrator accounts when personnel leave or transfer.

To delete an administrator account

1. Click **Manage & Settings** > **Permissions & Administrators**.

   The **Administrators** pane shows by default.

2. Select an administrator account and click **Delete**.
3. Click **Yes** in the confirmation window that opens.

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 select to show notifications about the approaching expiration date when an administrator logs into SmartConsole or one of the SmartConsole clients. The remaining number of days, during which the account is alive, shows in the status bar.

To configure the default expiration settings

1. Click **Manage & Settings** > **Permissions & 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. Publish the SmartConsole session.

Note - If you configure an expiration date for an administrator, then the administrator is not logged out automatically. Only a new login is blocked.
To improve security, configure the idle timeout. Go to SmartConsole > **Manage & Settings** > **Permissions & Administrators** > **Advanced** > **Idle Timeout**.

Configuring SmartConsole Session Timeout

Use the SmartConsole in a secure manner, and enforce secure usage for all administrators. Configuring a SmartConsole timeout is a basic requirement for secure usage. When an administrator does not use the SmartConsole, it logs out.

To set the SmartConsole session 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.

Revoking an Administrator Certificate

If an administrator that authenticates through a certificate cannot temporarily 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), the administrator can use this method to authenticate to the account.

To revoke an administrator certificate

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

Restricting Administrator Login Attempts

You can configure these login restrictions for administrators who log in to the Security Management Server with a Check Point password:

- The number of login attempts before SmartConsole automatically locks an administrator account.
- 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 who authenticate to the Security Management Server with a Check Point password.

Unlocking Administrator Accounts

An administrator with the **Manage Administrators** permission can unlock another administrator if the locked administrator authenticates to the Security Management Server with 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:

Use the "unlock-administrator" API command.

Note - The **Unlock Administrator** feature does **not** apply to administrators who use other authentication methods.

Creating an Administrator Account with Check Point Password Authentication

Check Point password is a static password that is configured in SmartConsole. The local database on the Security Management Server stores the password. No additional software is required.

After you configure authentication with a Check Point password, you can, in addition, configure certificate file authentication . The administrator can then authenticate to SmartConsole with the Check Point password or the certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

To configure Check Point password authentication for an administrator

1. **Create a new administrator and define Check Point password as the authentication method**

   a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > Click **New**.

      The **New Administrator** window opens.

   b. Give the administrator a name.

   c. In **Authentication method**, select **Check Point Password**.

   d. Click **Set New Password**, type the **Password**, and **Confirm** it.

e. **Optional:** In the **Authentication** section > **Certificate Information**, click **Create**:

   i. Enter a password.

   ii. Click **OK**.

   iii. Save the certificate file to a secure location on the SmartConsole computer:

   Notes:

   - Make sure that the login name is included in the **File name** field.
   - Make sure that Certificate Files (*p12) is selected in the **Save as type** drop-down list. The certificate file is in the PKCS #12 format, and has a `.p12` extension.
   - A password is required to protect the sensitive data in the certificate file. The certificate file contains the private key. After the certificate is issued, save it to a file and give the administrator this file and password. The administrator can then authenticate with the certificate when they log in with SmartConsole to the Security Management Server.

f. Assign a **Permission Profile**.

   See *"Assigning Permission Profiles to Administrators" on page 72*.

g. In the **Expiration** section, select the expiration date and make sure that it is set to a valid future date.

h. Click **OK**.

i. Publish the SmartConsole session.

2. **Optional: Import the certificate file into the Windows Certificate Store**

   Note - This procedure applies if you create a certificate authentication in the administrator object, and you log in to SmartConsole with the CAPI Certificate option.

   a. Right-click the *.p12 file you saved when you created the required administrator, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

d. Enter the same certificate password you used when you created the required administrator certificate.

e. Clear **Enable strong private key protection**.

f. Select **Mark this key as exportable**.

g. Click **Next**.

h. Select **Place all certificates in the following store**, click **Browse** > **Personal** > **OK**.

i. Click **Next**.

j. Click **Finish**.

Creating an Administrator Account with OS Password Authentication

OS password is kept on the operating system of the computer on which the Security Management Server is installed. You can also use passwords that are stored in Windows domain. No additional software is required.

After you configure authentication with an OS password, you can, in addition, configure authentication with a certificate file. The administrator can then authenticate to SmartConsole with either the OS password or the certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

To configure Check Point password authentication for an administrator

1. **Create a new administrator and define OS password as the authentication method**

   a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > Click **New**.

      The **New Administrator** window opens.

   b. Give the administrator a name.

c. In **Authentication method**, select **OS Password**.

d. **Optional:** In the **Authentication** section > **Certificate Information**, click **Create**:

   i. Enter a password.

   ii. Click **OK**.

   iii. Save the certificate file to a secure location on the SmartConsole computer:

   Notes:

   - Make sure that the login name is included in the **File name** field.
   - Make sure that Certificate Files (*p12) is selected in the **Save as type** drop-down list. The certificate file is in the PKCS #12 format, and has a `.p12` extension.
   - A password is required to protect the sensitive data contained in the certificate file. The certificate file contains the private key. After the certificate is issued, save it to a file and give the administrator this file and password. The administrator can then authenticate with the certificate when they log in with SmartConsole to the Security Management Server.

e. Assign a **Permission Profile**.

   See *"Assigning Permission Profiles to Administrators" on page 72*.

f. In the **Expiration** section, select the expiration date and make sure that it is set to a valid future date.

g. Click **OK**.

h. Publish the SmartConsole session.

2. **Optional: Import the certificate file into the Windows Certificate Store**

   Note - This procedure applies if you create a certificate authentication in the administrator object, and you log in to SmartConsole with the CAPI Certificate option.

   a. Right-click the *.p12 file you saved when you created the required administrator, and click **Install PFX**.

   The **Certificate Import Wizard** opens.

b. In the **Store Location** section, select the applicable option:
   - **Current User** (this is the default)
   - **Local Machine**

c. Click **Next**.

d. Enter the same certificate password you used when you created the required administrator certificate.

e. Clear **Enable strong private key protection**.

f. Select **Mark this key as exportable**.

g. Click **Next**.

h. Select **Place all certificates in the following store**, click **Browse** > **Personal** > **OK**.

i. Click **Next**.

j. Click **Finish**.

Creating an Administrator Account with RADIUS Server Authentication

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. With RADIUS, the Security Management Server forwards the authentication requests to the RADIUS server. The RADIUS server, which stores administrator account information, does the authentication. The RADIUS protocol uses UDP to communicate with the Security Gateway or the Security Management Server..

You can perform RADIUS authentication for SmartConsole administrators through a RADIUS server or a RADIUS server group. You define RADIUS servers and RADIUS server group objects in SmartConsole. A RADIUS server group is a high availability group of identical RADIUS servers which includes any or all the RADIUS servers in the system. When you create the group, you define a priority for each server in the group. If the server with the highest priority fails, the one with the next highest priority in the group takes over, and so on. When you define a group of RADIUS servers, all members of the group must use the same protocol.

To learn how to configure a RADIUS server, refer to the vendor documentation.

After you configure RADIUS server authentication, you can, in addition, configure authentication with a certificate file. The administrator can then authenticate to SmartConsole with the RADIUS server or the certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

To configure RADIUS server authentication for an administrator

1. **In SmartConsole, configure a new RADIUS server object**

   a. Go to the Object Explorer and select **New** > **More** > **Server** > **RADIUS**.

   b. Give the server a **Name**. It can be any name.

   c. In the **Host** field, click the drop-down arrow, click **New** and create a **New Host** with the **IP address** of the RADIUS server.

   d. Click **OK**.

      This host now appears in the **Host** field of the **New RADIUS** window.

   e. In the **Shared Secret** field, type the secret key that you defined previously on the RADIUS server.

   f. Click **OK**.

   g. Publish the SmartConsole session.

2. **Create a new administrator and define RADIUS as the authentication method**

a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > Click **New**.

   The **New Administrator** window opens.

b. Give the administrator the name that is defined on the RADIUS server.

c. In **Authentication method**, select **RADIUS**.

d. Select the **RADIUS Server** defined earlier.

e. **Optional:** In the **Authentication** section > **Certificate Information**, click **Create**:

   i. Enter a password.

   ii. Click **OK**.

   iii. Save the certificate file to a secure location on the SmartConsole computer:

   Notes:

   - Make sure that the login name is included in the **File name** field.
   - Make sure that Certificate Files (*p12) is selected in the **Save as type** drop-down list. The certificate file is in the PKCS #12 format, and has a `.p12` extension.
   - A password is required to protect the sensitive data in the certificate file. The certificate file contains the private key. After the certificate is issued, save it to a file and give the administrator this file and password. The administrator can then authenticate with the certificate when they log in with SmartConsole to the Security Management Server.

f. Assign a **Permission Profile**.

   See *"Assigning Permission Profiles to Administrators" on page 72*.

g. In the **Expiration** section, select the expiration date and make sure that it is set to a valid future date.

h. Click **OK**.

i. Publish the SmartConsole session.

3. **Optional: Configure a RADIUS server group for SmartConsole administrator authentication**

a. In SmartConsole, configure all the servers that you want to include in the server group, as explained in *"To configure RADIUS server authentication for an administrator" on page 60*.

   For each server, enter its priority in the group. The lower the number is, the higher the priority.

   For example, if you create a group with 3 servers, with priorities 1,2 and 3, the server with number 1 is approached first, the server with number 2 second, and the server with number 3, third.

b. Create the server group: In SmartConsole, go to **Object Explorer** and click **New** > **Server** > **More** > **RADIUS Group**.

c. Configure the group properties and add servers to the group:

   i. Give the group a **Name**. It can be any name.

   ii. Click the plus (+) for each server you want to add, and select each server from the drop-down list.

   iii. Click **OK**.

   iv. Publish the SmartConsole session.

4. **Optional: Import the certificate file into the Windows Certificate Store**

   Note - This procedure applies if you create a certificate authentication in the administrator object, and you log in to SmartConsole with the CAPI Certificate option.

   a. Right-click the *.p12 file you saved when you created the required administrator, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

   d. Enter the same certificate password you used when you created the required administrator certificate.

   e. Clear **Enable strong private key protection**.

   f. Select **Mark this key as exportable**.

   g. Click **Next**.

h. Select **Place all certificates in the following store**, click **Browse** > **Personal** > **OK**.

i. Click **Next**.

j. Click **Finish**.

Creating an Administrator Account with TACACS Server Authentication

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. With TACACS, the Security Management Server forwards authentication requests by remote administrators to the TACACS server. The TACACS server, which stores administrator account information, authenticates administrators. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the administrator name, password, authentication services and accounting information of all authentication requests to secure communication.

You can perform TACACS authentication for SmartConsole administrators through a TACACS server or a TACACS server group. A TACACS server group is a High Availability group of identical TACACS servers in the system. When you create the group, you define a priority for each server. If the server with the highest priority fails, the one with the next highest priority in the group takes over, and so on. All TACACS servers in the group must use the same protocol.

To learn how to configure a TACACS server, refer to the vendor documentation.

After you configure TACACS server authentication, you can, in addition, configure authentication with a certificate file. The administrator can then authenticate to SmartConsole with the TACACS server or the certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

To configure TACACS server authentication for an administrator

1. **In SmartConsole, add a new TACACS server object**

   a. Go to **Object Explorer** and click **New** > **More** > **Server** > **TACACS**.

   b. Enter the server **Name**.

   c. In the **Host** field, click the drop-down arrow, click **New**, and create a **New Host** with the **IP address** of the TACACS server.

   d. Click **OK**.

      This host now appears in the **Host** field of the **New TACACS** window.

   e. Select a **Server type**.

   f. If your server type is TACACS+, type the **Secret key** that you defined previously on the TACACS+ server.

   g. Click **OK**.

   h. Publish the SmartConsole session.

2. **Add a new administrator and define as the authentication method**

   a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > click **New**.

      The **New Administrator** window opens.

   b. Enter the administrator name that is defined on the TACACS server.

   c. In **Authentication Method**, select **TACACS**.

   d. Select the **TACACS Server** defined earlier from the drop-down list.

e. **Optional:** In the **Authentication** section > **Certificate Information**, click **Create**:

   i. Enter a password.

   ii. Click **OK**.

   iii. Save the certificate file to a secure location on the SmartConsole computer:

   Notes:

   - Make sure that the login name is included in the **File name** field.
   - Make sure that Certificate Files (*p12) is selected in the **Save as type** drop-down list. The certificate file is in the PKCS #12 format, and has a `.p12` extension.
   - A password is required to protect the sensitive data in the certificate file. The certificate file contains the private key. After the certificate is issued, save it to a file and give the administrator this file and password. The administrator can then authenticate with the certificate when they log in with SmartConsole to the Security Management Server.

f. Assign a **Permission Profile**.

   See *"Assigning Permission Profiles to Administrators" on page 72*.

g. In the **Expiration** section, select the expiration date and make sure that it is set to a valid future date.

h. Click **OK**.

i. Publish the SmartConsole session.

3. **Optional: Configure a TACACS Server group for SmartConsole administrator authentication**

   a. In SmartConsole, configure all the servers that you want to include in the server group, as explained in *"To configure TACACS server authentication for an administrator" on the previous page*.

      For each server, enter its priority in the group. The lower the number is, the higher the priority.

      For example, if you create a group with 3 servers, with priorities 1,2 and 3, the server with number 1 is approached first, the server with number 2 second, and the server with number 3, third.

   b. Create the server group: In SmartConsole, go to **Object Explorer** and click **New** > **Server** > **More** > **TACACS Group**.

c. Configure the group properties and add servers to the group:

   i. Enter the group **Name**.

   ii. Click the **+** icon for each server you want to add, and select the server from the drop-down list.

   iii. Click **OK**.

   iv. Publish the SmartConsole session.

4. **Optional: Import the certificate file into the Windows Certificate Store**

   Note - This procedure applies if you create a certificate authentication in the administrator object, and you log in to SmartConsole with the CAPI Certificate option.

   a. Right-click the *.p12 file you saved when you created the required administrator, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

   d. Enter the same certificate password you used when you created the required administrator certificate.

   e. Clear **Enable strong private key protection**.

   f. Select **Mark this key as exportable**.

   g. Click **Next**.

   h. Select **Place all certificates in the following store**, click **Browse** > **Personal** > **OK**.

   i. Click **Next**.

   j. Click **Finish**.

Creating an Administrator Account with SecurID Authentication

SecurID requires administrators to possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices. Software tokens reside on the PC or device from which the administrator wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When an administrator attempts to authenticate to a protected resource, the AM must validate the one-time use code.

The Security Management Server forwards SecurID authentication requests by remote administrators to the AM. The AM manages the database of the RSA users and their assigned hard or soft tokens. The Security Management Server act as an AM Agent and directs all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to the RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API.

To learn how to configure a SecurID server, refer to the vendor documentation.

After you configure SecurID authentication, you can, in addition, configure authentication with a certificate file. The administrator can then authenticate to SmartConsole with SecurID authentication or the certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

To configure SecurID authentication for an administrator

1. **Configure the Security Management Server to use SecurID (this procedure is only relevant if you use an SDK-supported API)**

    a. Connect to the command line on the Security Management Server.

    b. Log in to the Expert mode.

c. Copy the `sdconf.rec` file to the `/var/ace/` directory.

   If the `/var/ace/` directory does not exist, create it with this command:

   ```
   mkdir -v /var/ace/
   ```

d. Assign all permissions to the `sdconf.rec` file:

   ```
   chmod -v 777 /var/ace/sdconf.rec
   ```

2. **Configure the SecurID Server object**

   a. Add a new SecurID server object:

      Go to the Object Explorer and select **New** > **More** > **Server** > **New SecurID**.

   b. Give the server a **Name**. It can be any name.

   c. This step applies only to SDK-supported API:

      Click **Browse** and select the `sdconf.rec` file.

      This must be a copy of the file that is on the Security Management Server

   d. Click **OK**.

3. **Add a new administrator and define SecurID as the authentication method**

   a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > click **New**.

      The **New Administrator** window opens.

   b. Give the administrator a name. A unique, case sensitive character string.

   c. In **Authentication method**, select **SecurID**.

d. **Optional:** In the **Authentication** section > **Certificate Information**, click **Create**:

   i. Enter a password. A password is required to protect the sensitive data contained in the certificate file.

   ii. Click **OK**.

   iii. Save the certificate file to a secure location on the SmartConsole computer:

   Notes:

   - Make sure that the login name is included in the **File name** field.
   - Make sure that Certificate Files (*p12) is selected in the **Save as type** drop-down list. The certificate file is in the PKCS #12 format, and has a `.p12` extension.
   - A password is required to protect the sensitive data in the certificate file. The certificate file contains the private key. After the certificate is issued, save it to a file and give the administrator this file and password. The administrator can then authenticate with the certificate when they log in with SmartConsole to the Security Management Server.

e. Assign a **Permission Profile**.

   See *"Assigning Permission Profiles to Administrators" on page 72*.

f. In the **Expiration** section, select the expiration date and make sure that it is set to a valid future date.

g. Click **OK**.

h. Publish the SmartConsole session.

4. **Optional: Import the certificate file into the Windows Certificate Store**

   Note - This procedure applies if you create a certificate authentication in the administrator object, and you log in to SmartConsole with the CAPI Certificate option.

   a. Right-click the *.p12 file you saved when you created the required administrator, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

d. Enter the same certificate password you used when you created the required administrator certificate.

e. Clear **Enable strong private key protection**.

f. Select **Mark this key as exportable**.

g. Click **Next**.

h. Select **Place all certificates in the following store**, click **Browse** > **Personal** > **OK**.

i. Click **Next**.

j. Click **Finish**.

Creating an Administrator Account with API Key Authentication

An API key is a token that a client provides when making API calls.

API key authentication provides an administrator the ability to use a token for authenticating to the API interface instead of the usual administrator name / password.

You can use SmartConsole to configure an API key for administrators to use the management API.

Note - This administrator can only use the API for executing API commands and cannot use it for SmartConsole authentication.

To configure API authentication for an Administrator using SmartConsole

1. In SmartConsole click **Manage & Settings** > **Permissions & Administrators** > **Administrators**

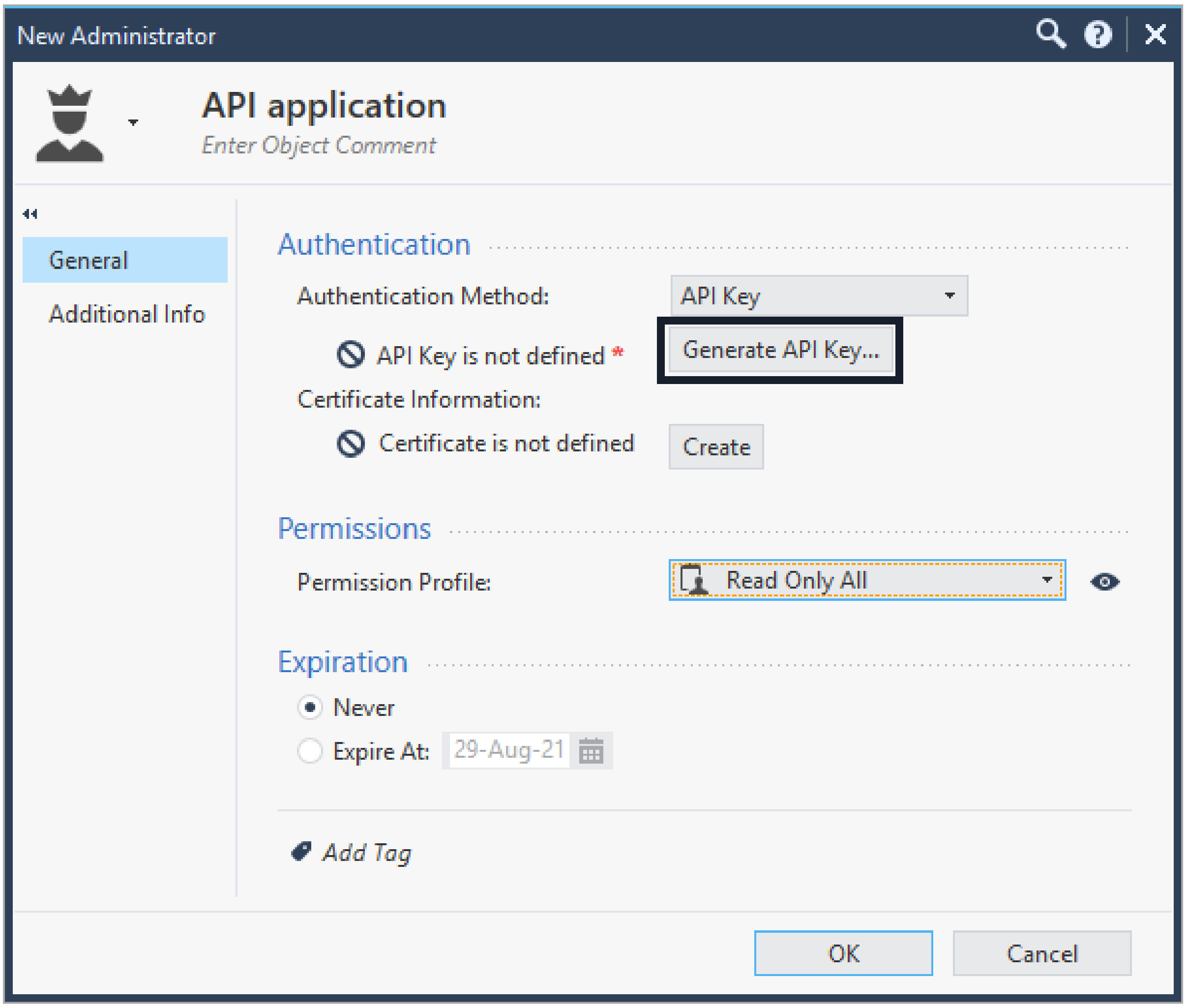
   Click the **New** icon at the top menu.

   The **New Administrator** window opens.

2. Give the administrator a name

3. In the **Authentication Method** field select **API Key**.

4. Click **Generate API key**.



New Administrator

API application

Enter Object Comment

Authentication

Authentication Method: API Key

API Key is not defined *

Certificate Information:

Certificate is not defined

Permissions

Permission Profile: Read Only All

Expiration

● Never

○ Expire At: 29-Aug-21

5. A new API key window opens.
   a. Click **Copy key to Clipboard**
   b. Save the key for a later use (provide it to the relevant administrator).
6. Click **OK**
7. Publish the SmartConsole session.

Example

This example demonstrates how to use the API-key for *login* and creating a *simple-gateway* using the API.

1. Log in to the Expert mode.
2. Use the previously generated key for the login, and save the standard output to a file (redirect it to a file using the ">" sign):

   Syntax:

```
mgmt_cli login api-key <api-key> > /<path_to>/<filename>
```

Example:

```
mgmt_cli login api-key mvYSiHVmlJM+J0tu2FqGag12 >
/var/tmp/token.txt
```

3. Run a `mgmt_cli` command with the "**-s**" flag.

   Syntax:

   ```
   mgmt_cli -s /<path_to>/<filename> add simple-gateway name
   <gateway name> ip-address <ip address> one-time-password
   <password> blade <true>
   ```

   Example:

   ```
   mgmt_cli -s /var/tmp/token.txt add simple-gateway name "gw1"
   ip-address 192.168.3.181 one-time-password "aaaa" firewall
   true vpn true
   ```

   For more details, see the *Check Point Management API Reference*.

After you configure API authentication, you can, in addition, configure authentication with a certificate file. The administrator can then authenticate to the Security Management Server with either an API Key or a certificate file.

You create the certificate file in SmartConsole. The administrator can use the certificate to log in to SmartConsole in two ways:

- Log in to SmartConsole with the **Certificate File** option. The administrator must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole with the CAPI Certificate option. The administrator does not need to provide a password to log in.

The administrator can also give the certificate to other administrators to log in to SmartConsole with no administrator account of their own.

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.

To learn about permission profiles for Multi-Domain Security Management administrators, see the *R81.20 Multi-Domain Security Management Administration Guide*.

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 & 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 & 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 & 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 (see *"Configuring Customized Permissions" on the next page*).
5. Click **OK**.

To delete a permission profile

1. In SmartConsole, go to **Manage & Settings** > **Permissions & 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 (see *"Configuring Permissions for Access Control and Threat Prevention" on page 78*).
   - **Threat Prevention** - Configure Threat Prevention Policy permissions (see *"Configuring Permissions for Access Control and Threat Prevention" on page 78*).
   - **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 (see *"Configuring Permissions for Monitoring, Logging, Events, and Reports" on page 79*).
   - **Events and Reports** - Configure permissions for SmartEvent features (see *"Configuring Permissions for Monitoring, Logging, Events, and Reports" on page 79*).
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)
- **High Availability Operations** -Configure and work with High Availability.
- **Management API Login** -Log in with the management API.
- **Cloud Management Extension (CME) API** - The permission for using CME API.
- **Publish sessions without an approval** - If not selected, any change made to a session requires an approval.
- **Approve/reject other sessions** - If selected, the administrator has permission to approve changes made by other administrators.
- **Manage integration with Cloud Services** - If selected, the administrator has permission to connect to the Infinity Portal through the **Cloud Services** view in SmartConsole.

4. Click **OK**.

Important - In a Permission Profile, if you select the permission **VSX Provisioning** (in the **Gateways** tab), you must also select **Publish sessions without an approval** (in the **Management** tab), because the Management Server must save changes in VSX objects immediately.

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 SmartConsole session.

Configuring Permissions for Access Control and Threat Prevention

In the permission 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.

  In the **Actions** section:

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

- **Threat Prevention**

  In the **Actions** section:

  - **Install Policy** - Install the Threat Prevention Policy on Security Gateways.
  - **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** - **SmartEvent Policy and Settings** on SmartEvent GUI.
    - **Reports** - in SmartConsole > **Logs & Monitor**
  - **SmartEvent Application & URL Filtering reports only**

Defining Trusted Clients

To limit the access to the Security Management Server from a specified list of hosts, you must configure **Trusted Clients**.

You can configure **Trusted Clients** in these ways:

Trusted Client Definition	Description
Any	All hosts
IPv4 Address	A single host with the 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 the specified IPv6 address

Trusted Client Definition	Description
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 hostname
Wild cards (IP only)	Hosts with IP addresses described by the specified regular expression

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

Adding a new trusted client

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

Modifying a trusted client settings

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

Deleting a trusted client

1. In SmartConsole, go to **Manage & Settings > Permissions & Administrators > Trusted Clients**.
2. Select a trusted client and click **Delete**.

   The confirmation window opens.
3. Click **Yes** to confirm.

Note - Administrators can also configure the **GUI Clients** in the Check Point Configuration Tool on the Security Management Server (see *"cpconfig" on page 569*).

Session Flow for Administrators

In SmartConsole, administrators work with sessions. A session is created each time an administrator logs into SmartConsole. Changes made in the session are saved automatically. You can generate a changes report to show you all the changes made in a session. These changes are private and available only to the administrator. To avoid configuration conflicts, other administrators see a lock icon on objects and rules that are being edited in other sessions.

Administrators can publish or discard their private changes. To include private changes in the policy installation, you must publish your changes in the session. This is also true if you want to make your private changes available to other administrators. Unpublished changes from other sessions are not included in the policy installation.

Before you publish a session, we recommend that you give the session a name and add a brief description that documents the work process.

Publishing a Session

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, or the use of objects that are not valid in the Rule Base. Make sure you correct these errors before publishing.

To publish a SmartConsole session

On 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. 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**.

To discard a session

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

Working in SmartConsole Session View

The Session view shows all unpublished sessions in the system. The view shows the sessions of the current administrator, sessions of other administrators and sessions from other applications. The columns in the view can be customized and show the session owner, name, description, connection mode, number of private changes, number of locks, application and other values.

To see session information, click **Manage & Settings** > **Sessions** > **View Sessions**.

Actions available to administrators on private sessions are determined by the **Manage Sessions** permission on their profile.

Administrators without the Manage Session permission can:	Administrators with the Manage Session Permission can:
■ Publish and discard their own sessions ■ See sessions opened by other administrators, the number the locks they have and number of changes they have made ■ Take over sessions created by applications, for example sessions created by the API command line tool	■ Publish and discard their own sessions ■ See sessions opened by other administrators, the number the locks they have and number changes they have made ■ **Publish & Disconnect** the private sessions of other administrators ■ **Disconnect & Discard** the private sessions of other administrators ■ **Disconnect** another administrator's private session ■ **Take over** sessions created by applications, for example sessions created by the API command line tool ■ **Take over** the private sessions of other administrators. **Note** - If you want to keep changes made in your own private session, publish these changes *before* you take over the session of another administrator. If you do not publish your changes, you will lose them. When you take over, you disconnect the other administrator's SmartConsole session. ■ **Publish & Disconnect** the private sessions of other administrators. The action applies to both SmartConsole sessions and command line API sessions. ■ **Disconnect** the private session of other administrators ■ **Discard & Disconnect** the private session of other administrators

Taking over locked objects from administrators with inactive sessions

If there are locked objects in SmartConsole by administrators with inactive sessions, but the relevant administrators are currently unavailable to log back in to SmartConsole and remove the lock, you can take over their sessions.

To take over inactive sessions of other administrators:

1. Log in to SmartConsole with a different administrator account.
2. Go to **Manage & Settings** > **Sessions** > **View Sessions**.
3. Right-click the relevant sessions of the administrator who owns the locked objects and select **Take over**.

You can now open the relevant object and publish or discard changes to remove the lock.

Administrators Working with Multiple Sessions

Administrators working with multiple sessions can open multiple additional private sessions without publishing changes made in the current private session.

Use Case

Suppose you are making changes in a private session and are asked to solve some immediate problem. The task involves making a change and publishing it. You do not wish to publish or discard your current private session.

You open a new private session, make the change required to resolve the issue, publish the change, then return to your previous private session.

To do this, you need to work with multiple sessions. To switch on multiple sessions, you need the **Manage Sessions** permission selected on your administrator profile.

To enable working in multiple sessions

1. Open the relevant permission profile.
2. Make sure the **Manage Sessions** permission is selected on the **Management** page.
3. Open **SmartConsole** > **Manage & Settings** View > **Sessions** > **Advanced**.
4. Select **Each administrator can manage multiple SmartConsole sessions at the same time**.
5. **Publish** the change.

When working with multiple sessions, you can:

- Open and manage multiple sessions to the Security Management Server using the same administrator account
- Switch between the active session and previously saved sessions
- Publish, discard and disconnect other sessions
- Take over other sessions

The SmartConsole Session menu

After multiple sessions are enabled, the SmartConsole Session menu has these new options:

Option	Description
Edit sessions details	Lets you change the session name and description.

Option	Description
Create new session	**In the current window** Opens a new session in the current SmartConsole **In a new window** Opens a new session in a new SmartConsole
Recent	Shows a list of recent sessions. Selecting a session opens the session in the current SmartConsole
More	Opens the **Open Session** window that shows sessions that you previously created and saved. ■ Sessions shown in this window are owned by the current administrator in the current domain. ■ The **Open Session > Actions** menu has options to open a saved session in the current SmartConsole or open the session in a new SmartConsole.

The SmartConsole Session View

When multiple sessions are enabled, you can perform these additional actions:

Action	You can:
For sessions that you own	■ Discard and Disconnect ■ Publish and Disconnect ■ Disconnect ■ Open an older session
For sessions owned by other administrators that have made private changes	■ Publish and Disconnect their changes ■ Discard and Disconnect ■ Disconnect ■ Take over their changes
For sessions owned by other administrators that have not made private sessions	■ Disconnect ■ Take over

Notes:

- When you work in single session, you need to publish or discard your changes before you take over another session. In multiple sessions, you do not have to publish or discard your session before you take over the session of another administrator.
- In multiple sessions, an administrator who connects from another desktop to an already connected session can still take over the connected session by default.

Switching between Multiple and Single Session

If the session management settings switch from multiple SmartConsole sessions to allow only a single SmartConsole session at a time:

- Administrators can still publish, discard and open sessions that they own.
- Cannot create new sessions until they have published or discarded all their unpublished sessions with private sessions
- Cannot take over the sessions of other administrators or applications (for example sessions created with API commands in the *mgmt_cli* utility) until they have published or discarded all their previously saved private sessions.

Approval Cycle for Sessions (SmartWorkflow and Identity Provider)

Lets administrators approve changes in sessions made by other administrators.

Use Case

This feature gives you the option to review and approve configuration changes made by other administrators before publishing them. You can define which administrators must submit their changes for approval and which administrators are authorized to approve changes.

Configuration

1. **Create a new permission profile for the Administrator "A" whose changes require approval**

   a. In SmartConsole, go to **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles** > **New Profile**.

      The **New Profile** window opens.

   b. In the **Overview** page ,select **Read/Write All** or **Customized**.

   c. In the **Management** page, clear the **Publish sessions without an approval** option.

   d. Configure the rest of the profile settings, and click **OK** and publish the changes.

2. **Create a new administrator account for the Administrator "A" whose changes require approval:**

   a. In SmartConsole, go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > **New Administrator**.

      The **New Profile** window opens.

   b. Configure the Administrator name and other properties, and in the **Permission Profile** field, select the profile you created for this administrator.

   c. Click **OK**.

3. **Create a new permission profile for the Administrator "B" who approves the changes"**

   a. In SmartConsole, go to **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles** > **New Profile**.

      The **New Profile** window opens.

   b. In the **Overview** page ,select **Read/Write All** or **Customized**.

   c. In the **Management** page, select **Approve/reject other sessions**.

   d. Configure the rest of the profile settings, and click **OK**.

4. **Create a new administrator account for the Administrator "B" who approves the changes:**

   a. In SmartConsole, go to **Manage & Settings** > **Permissions & Administrators** > **Administrators** > **New Administrator**.

      The **New Profile** window opens.

   b. Configure the Administrator name and other properties, and in the **Permission Profile** field, select the profile you created for this administrator.

   c. Click **OK** and publish your changes.

5. **To submit your changes for approval, in SmartConsole's top toolbar, click Submit Request**

   Note - If Administrator "A" tries to install policy before his changes are approved, a message shows up indicating the changes must be submitted for approval first.

   Each time Administrator "A" makes changes in the SmartConsole configuration:

   After Administrator "A" modifies a rule in the Rule Base and clicks **Submit**, SmartConsole locks this rule for further changes and shows a padlock icon.

   After Administrator "A" modifies an object and clicks **Submit**, SmartConsole locks this object for further changes. You can only view the object properties (right-click the object > **View**).

   Note - To see the status of all sessions, go to **Manage & Settings** > **Sessions** > **View Sessions**.

6. **Administrator "B" to reviews and approves the changes**

   Note - If you have sessions which are pending approval, a notification with the number of sessions pending approval appears next to the **Manage & Settings** tab and next to the **View Sessions** tab.

   a. In SmartConsole, go to **Manage & Settings** > **Sessions** > **View Sessions**.

   b. Right-click a session that is pending approval.

   c. To review the changes, select **Review change report** from the drop-down menu.

d. After you reviewed the changes, right-click the sessions and select one of these options from the drop-down menu:

- To publish the session, select **Approve**. After the session is published, Administrator "A" can install policy.
- To return the session to the submitter to fix, select **Reject**. If you select this option, you return the session to Administrator "A". A window opens and you must provide the return justification.

7. **Administrator "A" sees the notifications of the reviewed sessions in the Manage & Settings tab and the View Sessions tab.**

   To fix a session, click a session and select **open session** from the drop-down menu.

Notes:

- To get email notifications about session updates, go to **Manage & Settings** > **SmartTasks**, and configure the applicable SmartTask (see *"SmartTasks" on page 437*).
- To be able to save changes in the Database Tool or in SmartProvisioning , you must have permission to publish your changes without an approval. If the **Publish sessions without an approval**, option is cleared, you cannot save changes in the Database Tool or in SmartProvisioning.

Managing User Accounts

A user account is an object that represents a user that generates traffic in a Check Point environment. The Management Server administrators create, manage and monitor user accounts. The Security Gateway lets you control access privileges for authenticated users. The administrator uses the Security Rule Base to restrict or give users access to specified resources. Users are unaware of the groups to which they belong. Limitation of access to sensitive information and resources only to authorized users ensures the security of the organization's network and data.

Users authenticate to Security Gateways. Check Point supports different Authentication Methods for users.

All users are configured directly in SmartConsole (in contrast to users configured on external servers, such as Active Directory), and are stored on the Management Server in the management database.

When an administrator installs a policy, the Management Server copies the applicable user data to the managed Security Gateway.

When an administrator installs a database (**Menu** > **Install Database**), the Management Server copies the applicable user data to the managed servers (for example, the Log Server).

Creating a User Account

When you create a user account through SmartConsole, you can select one of these authentication methods:

Authentication Method	Description
Check Point Password	Check Point password is a static password that is configured in SmartConsole.The local database on the Security Gateway stores the password. No additional software is required. See *"Creating a User Account with Check Point Password Authentication" on page 95*.
OS Password	OS Password is stored on the operating system of the computer on which the Security Gateway is installed. You can also use passwords that are stored in a Windows domain. No additional software is required. See *"Creating a User Account with OS Password Authentication" on page 97*
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. With RADIUS, the Security Gateway lets you control access privileges for authenticated RADIUS 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. The Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, does the authentication. The RADIUS protocol uses UDP to communicate with the Security Gateway. 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. For the Gaiaoperating system, use the attribute "Vendor-Specific" (26) - refer to RFC 2865. See *"Creating a User Account with RADIUS Server Authentication" on page 100*.

Authentication Method	Description
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. With TACACS, the forwards authentication requests by remote users to the TACACS server. 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 make sure communication is secure. See *"Creating a User Account with TACACS Server Authentication" on page 104*.
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 Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices. 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 AM. The Security Gateway forwards authentication requests by remote users to the AM. The AM manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway acts as an AM agent and directs all access requests to the AM for authentication. For more information on agent configuration, refer to RSA Authentication Manager documentation. There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API. See *"Creating a User Account with SecurID Authentication" on page 108*.

Important - If you do not select an authentication method, the user cannot log in or use network resources.

After you configure authentication with one of the Check Point authentication methods, you can, in addition, create a certificate file for the user. The user can authenticate to the Security Gateway with one of the Check Point authentication methods or with a certificate file.

You create the certificate file in SmartConsole, and the user can log in to the Security Gateway with the certificate file in two ways:

- Log in to Security Gateway with the **Certificate File** option. The user must provide the password to use the certificate file.
- You can import the certificate file to the Windows Certificate Store on the Microsoft Windows SmartConsole computer. The user can use this stored certificate to log in to the Security Gateway with the CAPI Certificate option. The user does not need to provide a password to log in.

Changing an Existing User

Procedure

1. In the Object Explorer, click **User/Identity** > **Users**.
2. Double-click a user.

   The **User** window opens.
3. Change the properties as necessary.
4. Click **OK**.

Deleting a User

Procedure

1. n the Object Explorer, click **User/Identity** > **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.

To create a new user group

1. In the Object Explorer (F11), click **New** > **More** > **User/Identity** > **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 Explorer (F11), select **Object Categories** > **Users/Identities** > **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**.

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.

Procedure

1. From the main **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.
   - **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 prevents loss of working time.

Creating a User Account with Check Point Password Authentication

Check Point password is a static password that is configured in SmartConsole.The local database on the Security Gateway stores the password. No additional software is required.

After you configure authentication with a Check Point password, you can, in addition, configure authentication with a certificate file. The user can then authenticate to the Security Gateway with the Check Point password or the certificate file.

To create a new user with Check Point password authentication

1. In the Object Explorer (F11), click **New** > **More** > **User/Identity** > **User**.

   The **New User** window opens.

2. Select a template and Click **OK**.

3. Enter a **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.

4. Configure the user's **General Properties**:

   a. Select an **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 main menu > **Global Properties** > **User Accounts** > **Expiration Date**, shows as the expiration date.

   b. Optional settings: **Comment**, **Email Address**, **Mobile Phone Number**.

5. In **Groups** - Use this window to add users to user groups.

6. Configure the user's **Authentication**:

   a. From the drop-down menu, select **Check Point Password**.

      Important - If you do not select an authentication method, the user cannot log in or use network resources.

   b. Click **Set new password**.

7. In **Location**, select objects from which this user can access or send data and traffic.

   In the **Allowed locations** section:

   - **Sources** - 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.

8. In **Time** - If the user has specific working days or hours, you can configure when the user can be authenticated for access.

   - **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 at a time outside the given range.
   - **Days in week** or **Daily** - Select the days on which the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

9. In **Certificates**:

   You can 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.

   a. Click **New**.

   b. 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.

c. Click **OK**.

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

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

10. In **Encryption**:

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

a. Select an encryption method for the user.

b. Click **Edit**.

The encryption **Properties** window opens.

The next steps are for **IKE Phase 2**. The options can be different for different methods.

c. In the **Authentication** tab, select the authentication schemes:

i. **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.

ii. **Public Key** - The user authenticates with a public key contained in a certificate file.

d. Click **OK**.

11. Click **OK**.

Creating a User Account with OS Password Authentication

OS Password is stored on the operating system of the computer on which the Security Gateway is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

After you configure authentication with an operating system password, you can, in addition, configure authentication with a certificate file. The user can then authenticate to the Security Gateway with the operating system password or the certificate file.

To create a new user with OS password authentication

1. In the Object Explorer (F11), click **New** > **More** > **User/Identity** > **User**.

   The **New User** window opens.

2. Select a template and Click **OK**.

3. Enter a **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]`, then enter `James` as the username. If you use Common Names as user names, they must contain exactly one string with no spaces.

4. Configure the user's **General Properties**:

   a. Select an **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 main menu > **Global Properties** > **User Accounts** > **Expiration Date** shows as the expiration date.

   b. Optional settings: **Comment**, **Email Address**, **Mobile Phone Number**.

5. In **Groups** - Use this window to add users to user groups.

6. Configure the user's **Authentication**:

   a. From the drop-down menu, select **OS Password**.

      Important - If you do not select an authentication method, the user cannot log in or use network resources.

   b. Click **Set new password**.

7. In **Location**, select objects from which this user can access or send data and traffic.

   In the **Allowed locations** section:

   - **Sources** - 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.

8. In **Time** - If the user has specific working days or hours, you can configure when the user can be authenticated for access.

   - **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 on which the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

9. In **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.

   a. Click **New**.

   b. 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.

   c. Click **OK**.

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

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

10. In **Encryption**:

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

    a. Select an encryption method for the user.

    b. Click **Edit**.

       The encryption **Properties** window opens.

       The next steps are for **IKE Phase 2**. The options can be different for different methods.

    c. In the **Authentication** tab, select the authentication schemes:

       i. **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.

ii. **Public Key** - The user authenticates with a public key contained in a certificate file.

d. Click **OK**.

11. Click **OK**.

Creating a User Account with RADIUS Server Authentication

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.

With RADIUS, the Security Gateway lets you control access privileges for authenticated RADIUS 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.

The Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the Security Gateway.

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.

For the Gaiaoperating system, use the attribute "Vendor-Specific" (26) - refer to RFC 2865.

To learn how to configure a RADIUS server, refer to the vendor documentation.

Users can perform RADIUS authentication through a RADIUS server or a RADIUS server group. A RADIUS server group is a high availability group of identical RADIUS servers which includes any or all the RADIUS servers in the system. When you create the group, you define a priority for each server in the group. If the server with the highest priority fails, the one with the next highest priority in the group takes over, and so on.

After you configure authentication with a RADIUS server, you can, in addition, configure authentication with a certificate file. The user can then authenticate to the Security Gateway with the RADIUS server or the certificate file.

To configure RADIUS server authentication for a user

1. **In SmartConsole, configure a new RADIUS Server object**

   a. Go to the Object Explorer and select **New** > **More** > **Server** > **RADIUS**.

   a. Give the server a **Name**. It can be any name.

   b. In the **Host** field, click the drop-down arrow, 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 **New Radius** window.

   e. In the **Shared Secret** field, type the secret key that you defined previously on the RADIUS server.

   f. Click **OK**.

   g. Publish the SmartConsole session.

2. **Create a new user and define RADIUS as the authentication method**

   a. In the Object Explorer (F11), click **New** > **More** > **User/Identity** > **User**.

      The **New User** window opens.

   b. Select a template and Click **OK**.

   c. Enter a **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]`, then enter `James` as the username. If you use Common Names as user names, they must contain exactly one string with no spaces.

   d. Configure the user's **General Properties**:

      i. Select an **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 main menu > **Global Properties** > **User Accounts** > **Expiration Date** shows as the expiration date.

      ii. Optional settings: **Comment**, **Email Address**, **Mobile Phone Number**.

   e. In **Groups** - Use this window to add users to user groups.

   f. Configure the user's **Authentication**: From the drop-down menu, select **RADIUS**.

      Important - If you do not select an authentication method, the user cannot log in or use network resources.

g. In **Location**, select objects from which this user can access or send data and traffic.

   In the **Allowed locations** section:

   - **Sources** - 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.

h. In **Time** - If the user has specific working days or hours, you can configure when the user can be authenticated for access.

   - **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 on which the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

i. In **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.

   i. Click **New**.

   ii. 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.

   iii. Click **OK**.

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

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

j. In **Encryption**:

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

   i. Select an encryption method for the user.

   ii. Click **Edit**.

      The encryption **Properties** window opens.

      The next steps are for **IKE Phase 2**. The options can be different for different methods.

   iii. Open the **Authentication** tab.

   iv. Select the authentication schemes:

      - **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.

      - **Public Key** - The user authenticates with a public key contained in a certificate file.

   v. Click **OK**.

k. Click **OK**.

3. **Optional: Configure a RADIUS server group for SmartConsole user authentication**

   Note - When defining a group of RADIUS servers, all members of the group must use the same protocol.

   a. In SmartConsole, configure all the servers that you want to include in the server group. For each server, enter its priority in the group. The lower the number is, the higher the priority. For example, if you create a group with 3 servers, with priorities 1,2 and 3, the server with number 1 is approached first, the server with number 2 second, and the server with number 3, third.

   b. Create the server group:

      In SmartConsole, go to **Object Explorer** and click **New** > **Server** > **More** > **RADIUS Group**.

c. Configure the group properties and add servers to the group:

   i. Give the group a **Name**. It can be any name.

   ii. Click the plus (+) for each server you want to add, and select each server from the drop-down list.

   iii. Click **OK**.

   iv. Publish the SmartConsole session.

d. Add a new user.

e. Publish the SmartConsole session.

Creating a User Account with TACACS Server Authentication

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. With TACACS, the forwards authentication requests by remote users to the TACACS server. 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 make sure communication is secure.

To configure a Security Gateway to use TACACS authentication, you must set up the server and enable its use on the Security Gateway.

Users can perform TACACS authentication through a TACACS server or a TACACS server group. A TACACS server group is a high availability group of identical TACACS servers which includes any or all the TACACS servers in the system. When you create the group, you define a priority for each server in the group. If the server with the highest priority fails, the one with the next highest priority in the group takes over, and so on.

After you configure authentication with a TACACS server, you can, in addition, configure authentication with a certificate file. The user can then authenticate to the Security Gateway with the TACACS server or the certificate file.

To configure TACACS server authentication for a user

1. **In SmartConsole, configure a new TACACS server object**

   a. In SmartConsole, create a TACACS server:

      Go to the Object Explorer > **New** > **More** > **Server** > **TACACS**.

   b. Give the server a **Name**. It can be any name.

c. In the **Host** field, click the drop-down arrow, click **New** and create a **New Host**. Give it the **IP address** of the **TACACS** server.

d. Click **OK**.

e. Make sure that this host shows in the **Host** field of the **New TACACS** window.

f. Select the **Servers Type**.

Best Practice - The default is **TACACS**, but we recommend **TACACS+**.

g. Enter a **Secret key** (required only if you selected **TACACS+** server type).

h. Click **OK**.

2. **Create a new user and define TACACS as the authentication method**

a. In the Object Explorer (F11), click **New** > **More** > **User/Identity** > **User**.

The **New User** window opens.

b. Select a template and click **OK**.

c. Enter a **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]`, then enter `James` as the username. If you use Common Names as user names, they must contain exactly one string with no spaces.

d. Configure the user's **General Properties**:

i. Select an **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 main menu > **Global Properties** > **User Accounts** > **Expiration Date** shows as the expiration date.

ii. Optional settings: **Comment**, **Email Address**, **Mobile Phone Number**.

e. In **Groups** - Use this window to add users to user groups.

f. Configure the user's **Authentication**: From the drop-down menu, select TACACS.

Important - If you do not select an authentication method, the user cannot log in or use network resources.

g. In **Location**, select objects from which this user can access or send data and traffic.

   In the **Allowed locations** section:

   - **Sources** - 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.

h. In **Time** - If the user has specific working days or hours, you can configure when the user can be authenticated for access.

   - **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 on which the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

i. In **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.

   i. Click **New**.

   ii. 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.

   iii. Click **OK**

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

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

j. In **Encryption**:

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

   i. Select an encryption method for the user.

   ii. Click **Edit**.

      The encryption **Properties** window opens.

      The next steps are for **IKE Phase 2**. The options can be different for different methods.

   iii. Open the **Authentication** tab.

   iv. Select the authentication schemes:

      - **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.

      - **Public Key** - The user authenticates with a public key contained in a certificate file.

k. Click **OK**.

3. **Optional: Configure a TACACS server group for SmartConsole user authentication**

   Note - When defining a group of TACACS servers, all members of the group must use the same protocol.

   a. In SmartConsole, configure all the servers that you want to include in the server group.

      For each server, enter its priority in the group. The lower the number is, the higher the priority.

      For example, if you create a group with 3 servers, with priorities 1,2 and 3, the server with number 1 is approached first, the server with number 2 second, and the server with number 3, third.

   b. Create the server group:

      In SmartConsole, go to **Object Explorer** and click **New** > **Server** > **More** > **TACACS Group**.

c. Configure the group properties and add servers to the group:

   i. Give the group a **Name**. It can be any name.

   ii. Click the plus (+) for each server you want to add, and select each server from the drop-down list.

   iii. Click **OK**.

   iv. Publish the SmartConsole session.

d. Add a new user.

e. Publish the SmartConsole session.

Creating a User Account with SecurID Authentication

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 Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices. 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 AM.

The Security Gateway forwards authentication requests by remote users to the AM. The AM manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway acts as an AM agent and directs all access requests to the AM for authentication. For more information on agent configuration, refer to RSA Authentication Manager documentation. There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API.

After you configure SecurID authentication, you can, in addition, configure authentication with a certificate file. The user can then authenticate to the Security Gateway with the SecurID or the certificate file.

To configure SecurID authentication for users:

1. **Configure the API to send authentication requests**

   You can select to enable one of two API types:

- **SDK-supported API**

  A proprietary API that uses a proprietary communication protocol on UDP port 5500 through SDKs available for selected platforms.

To enable SecurID authentication over SDK-supported API

a. Create the `sdconf.rec` file on an ACE/Server and copy it to your computer.

   For details, refer to the RSA documentation.

   Important - Use the IP address of a Security Gateway interface that connects to the ACE/Server:

   - **For a specific Security Gateway** - Configure the IP address as the authentication agent.
   - **For a Cluster** - Configure these IP addresses as authentication agents: Physical IP address of each Cluster Member and Cluster Virtual IP address.
   - **For a VSX Virtual System on a specific VSX Gateway** - Configure these IP addresses as authentication agents: IP address of the VSX Gateway and IP address of the Virtual System.
   - **For a VSX Virtual System on VSX Cluster** - Configure these IP addresses as authentication agents: Cluster Virtual IP address of the VSX Cluster and Cluster Virtual IP address of the Virtual System.

b. Open the SecurID object in SmartConsole, click **Browse** and import the `sdconf.rec` file into the SecurID object.

c. Install policy.

   Note - During the policy installation, the `sdconf.rec` file is transferred the Security Gateway to `/var/ace/sdconf.rec`.

- **REST API**

To enable SecurID authentication over REST API

a. Connect to the command line on the Security Gateway.

b. Log in to the Expert mode.

c. On a VSX Gateway or VSX Cluster Member, go to the context of VSID 0:

```
vsenv 0
```

d. Back up the current `$CPDIR/conf/RSARestServer.conf` file:

```
cp -v $CPDIR/conf/RSARestServer.conf{,_BKP}
```

e. Edit the `$CPDIR/conf/RSARestServer.conf` file.

Fill in these fields:

- `host` - The configured host name of the RSA server.
- `port`, `client key`, and `accessid` - From the RSA SecurID Authentication API window.
- `certificate` - The name of the certificate file.

f. Save the changes in the file and exit the editor.

Note - If you do not complete the REST API configuration, the authentication is performed through the SDK-supported API.

2. **Configure user groups**

a. In SmartConsole, open the Object Explorer (F11).

b. Click **New** > **More** > **User/Identity** > **User Group**.

The **New User Group** window opens.

c. Enter the name of the group, for example *SecurID_Users*.

Make sure the group is empty.

d. Click **OK**.

e. Publish the SmartConsole session.

f. Install the policy.

3. **Create a new user and define SecurID as the authentication method**

This configuration procedure is different for internal users (that are defined in SmartConsole) and for external users.

To configure SecurID authentication settings for internal users

Internal users are users that you configure in SmartConsole. The Security Management Server keeps these users in the management database.

a. In SmartConsole, open the Object Explorer (F11).

b. Click **New** > **More** > **User/Identity** > **User**.

   The **New User** window opens.

c. Choose a template.

d. Click **OK**.

e. In the **General** page:

   - Enter a default **Name**. This name is used to authenticate users by the Authentication Manager.
   - Set the **Expiration** date.

f. In the **Authentication** page, from the **Authentication Method** drop-down list, select **SecurID**.

g. Click **OK**.

To configure SecurID authentication settings for external users

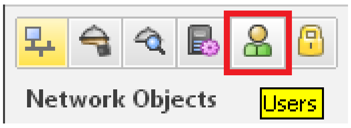
External users are users that are you configure the Legacy SmartDashboard. The Security Management Server does not keep these users in the management database.

a. In SmartConsole, click **Manage & Settings** > **Blades**.

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

   Legacy SmartDashboard opens.

c. In the bottom left **Network Objects** pane, and click **Users**.



d. 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**.

e. Configure the **External User Profile** properties:

   i. **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 is used to authenticate users by the Authentication Manager.
        - In the **Expiration Date** field, set the applicable date.
        - In the **Domain Name matching definitions** section, configure the applicable settings.

   ii. **Authentication** page:

      From the **Authentication Scheme** drop-down list, select **SecurID**.

   iii. Click **OK**.

f. From the top toolbar, click **Update** (or press the **CTRL S** keys).

g. Close the Legacy SmartDashboard.

4. **Complete the SecurID authentication configuration**

   a. Make sure that connections between the Security Gateway and the Authentication Manager are not NATed in the Address Translation Rule Base.

      On a Virtual System, follow the instructions in sk107281.

   b. 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 Authentication Manager, 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 this line:

```
CLIENT_IP=<IP Address>
```

Where *`<IP Address>`* is the primary IP address of the Security Gateway, as defined on the Authentication Manager. This is the IP address of the interface, to which the server is routed.

Example:

```
CLIENT_IP=192.168.20.30
```

Note - On a VSX Gateway and VSX Cluster Members, you must create the same `sdopts.rec` file in the context VSID 0 and in the context of each applicable Virtual System.

Access Roles

Access Role objects let you configure network access according to:

- Networks
- Users and user groups
- Computers and computer groups
- Remote Access VPN clients (supported for Security Gateways R80.10 and higher)

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.

For more information, see the *R81.20 Identity Awareness Administration Guide*.

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.

User Directory

The Check Point User Directory stores user-specific information.

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

The User Directory lets you:

- Configure *High Availability*, to duplicate user data across multiple servers for backup.

  See *"Account Units and High Availability" on page 153*.
- Configure *Multiple Account Units*, for distributed databases.
- *Define LDAP Account Units*, for encrypted User Directory connections.

See *"Modifying the LDAP Server" on page 153*.

- Configure *Profiles*, to support multiple LDAP vendors.

  See *"User Directory Profiles" on page 127*.

User Directory Considerations

Before you begin, plan your use of User Directory.

- Decide whether to use the User Directory servers for user management, CRL retrieval, user authentication, or all of those.

  See *"Working with LDAP Account Units" on page 148*.

- Decide how many Account Units you need.

  You can have one for each User Directory server, or you can divide branches of one User Directory server among different Account Units.

  See *"Account Units" on page 147*.

- Decide whether to use High Availability setup.

  See *"Account Units and High Availability" on page 153*.

- Determine the order of priority among the User Directory servers for High Availability and querying purposes.

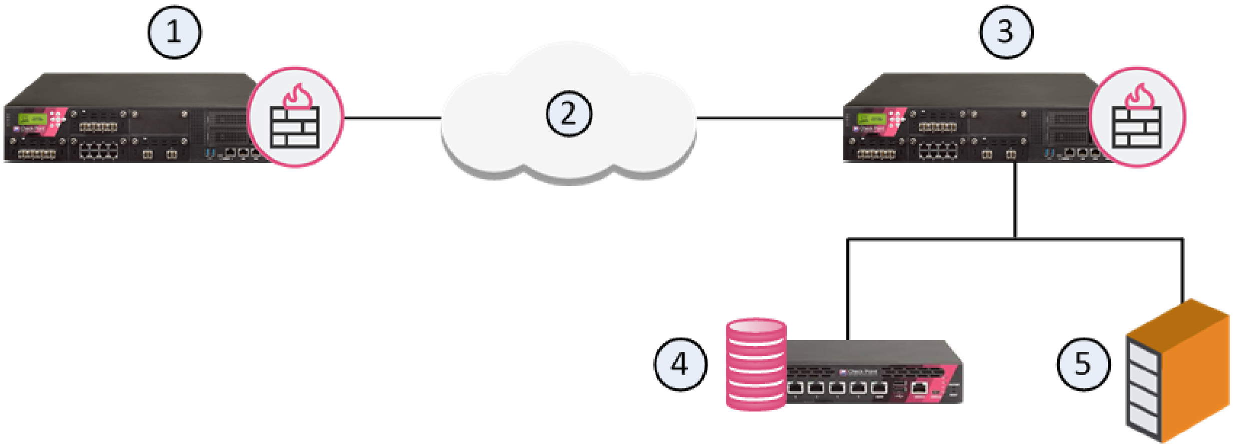
  See *"Setting High Availability Priority" on page 154*.

- Assign users to different Account Units, branches, and sub-branches, so that users with common attributes (such as their role in the organization, permissions, an so on) are grouped together.

  See *"Managing Users on a User Directory Server" on page 139*.

Deploying User Directory

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



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

Enabling User Directory

In SmartConsole, enable the Security Management Server to manage users in the Account Unit. See *"Working with LDAP Account Units" on page 148*.

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

To enable User Directory on the Security Management Server

1. From the Menu, select **Global Properties** > **User Directory**.

   The **User Directory** page opens.

2. Select **Use User Directory for Security Gateways**.
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
6. On **General Properties** page, **Management** tab, select **Network Policy Management** and **User Directory**.
7. Click **OK**.
8. Install the policy.

User Directory Schema for LDAP

The User Directory default schema is a description of the structure of the data in a user directory.

It has user definitions defined for an LDAP server.

This schema does not have Security Management Server or Security Gateway specific data, such as IKE-related attributes, authentication methods, or values for remote users.

You can use the default User Directory schema, if all users have the same authentication method and are defined according to a default template.

But if users in the database have different definitions, it is better to apply a Check Point schema to the LDAP server.

See *"User Directory Schema for LDAP" above*.

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

object class	OID
fw1template	1.3.114.7.4.2.0.1
fw1person	1.3.114.7.4.2.0.2

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 *"User Directory Schema Attributes" below*.

User Directory Schema Attributes

cn

The entry's name.

This is also referred to as "Common Name".

For users this can be different from the uid attribute, the name used to login to the Security Gateway.

This attribute is also used to build the User Directory entry's distinguished name, that is, it is the RDN of the DN.

uid

The user's login name, that is, the name used to login to the Security Gateway.

This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication 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.

The default is "`no value`".

mail

User's email address.

The default is "`no value`".

member

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

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

userPassword

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

```
"{crypt}xxyyyyyyyyyyy"
```

where:

- "`xx`" is the "salt"
- "`yyyyyyyyyyy`" 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

"X" in OID	fw1person	fw1template	default
1	y	y	"undefined"

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:

method	meaning
RADIUS	name of a RADIUS server, a group of RADIUS servers, or "Any"

method	meaning
TACACS	name of a TACACS server

"X" in OID	fw1template
2	y

fw1pwdLastMod

The date on which the password was last modified.

The format is `yyyymmdd` (for example, 20 August 1998 is 19980820).

A password can be modified through the Security Gateway as a part of the authentication process.

"X" in OID	fw1person	fw1template	default
3	y	y	If no value is given, then the password has never been modified.

fw1expiration-date

The last date on which the user can login to a Security Gateway, or "no value" if there is no expiration date.

The format is `yyyymmdd` (for example, 20 August 1998 is 19980820).

The default is "`no value`".

"X" in OID	fw1person	fw1template	default
8	y	y	"no value"

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).

"X" in OID	fw1person	fw1template	default
9	y	y	"00:00"

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).

"X" in OID	fw1person	fw1template	default
10	y	y	"23:59"

fw1day

The days (of week) on which the user can login to a Security Gateway.

Can have the values "`SUN`","`MON`", and so on.

"X" in OID	fw1person	fw1template	default
11	y	y	all days of the week

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.

"X" in OID	fw1person	fw1template	default
12	y	y	"no value"

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.

"X" in OID	fw1person	fw1template	default
13	y	y	"no value"

fw1allowed-vlan

Not currently used.

"X" in OID	fw1person	fw1template	default
14	y	y	"no value"

fw1SR-keym

The algorithm used to encrypt the session key in SecuRemote.

Can be "`CLEAR`", "`FWZ1`", "`DES`", or "`Any`".

"X" in OID	fw1person	fw1template	default
15	y	y	"Any"

fw1SR-datam

The algorithm used to encrypt the data in SecuRemote.

Can be "`CLEAR`", "`FWZ1`", "`DES`", or "`Any`".

"X" in OID	fw1person	fw1template	default
16	y	y	"Any"

fw1SR-mdm

The algorithm used to sign the data in SecuRemote.

Can be "`none`" or "`MD5`".

"X" in OID	fw1person	fw1template	default
17	y	y	"none"

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`".

"X" in OID	fw1person	fw1template	default
25	y	y	"SHA1"

fw1ISAKMP-SharedSecret

The pre-shared secret for SecuRemote users using IKE, (formerly known as ISAMP).

The value can be calculated using the `fw ikecrypt` command line.

"X" in OID	fw1person	fw1template
26	y	y

fw1ISAKMP-DataEncMethod

fw1ISAKMP-DataEncMethod

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

"X" in OID	fw1person	fw1template	default
27	y	y	"DES"

fw1enc-Methods

The encryption method allowed for SecuRemote users.

This can be one or more of: "`FWZ`", "`ISAKMP`" (meaning IKE).

"X" in OID	fw1person	fw1template	default
28	y	y	"FWZ"

fw1userPwdPolicy

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

"X" in OID	fw1person
29	y

fw1badPwdCount

Number of allowed wrong passwords entered sequentially.

"X" in OID	fw1person
30	y

fw1lastLoginFailure

Time of the last login failure.

"X" in OID	fw1person
31	4

memberof template

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

"X" in OID	fw1person
33	4

Netscape LDAP Schema

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

ⓘ **Important** - This deletes the object class 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.

Note - 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 the `objects_5_0.C` file.

- 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 the `objects_5_0.C` file to the proper membership setting and start the Security Management Server.

Make sure to install policy/user database on all Security Gateways to enable the new configuration.

Profile Attributes

UserLoginAttr

The unique username User Directory attribute (uid).

In addition, when fetching users by the username, this attribute is used for query.

Default	Other
▪ uid (most servers) ▪ SamAccountName (in Microsoft_AD)	One value allowed

UserPasswordAttr

This user password is User Directory attribute.

Default	Other
▪ userPassword (most servers) ▪ unicodePwd (in Microsoft_AD)	One value allowed

TemplateObjectClass

The object class for Check Point User Directory templates.

If you change the default value with another object-class, make sure to extend that objectclass schema definition with relevant attributes from `fw1template`.

default	Other
fw1template	Multiple values allowed

ExpirationDateAttr

The account expiration date is User Directory attribute.

This could be a Check Point extended attribute or an existing attribute.

Default	Other
▪ fw1expiration-date (most servers) ▪ accountExpires (in Microsoft_AD)	One value allowed

ExpirationDateFormat

Expiration date format.

This format will be applied to the value defined at `ExpirationDateAttr`.

Default	Other
CP format is yyyymmdd	One value allowed

PsswdDateFormat

The format of the password modified date is User Directory attribute.

This formation will be applied to the value defined at `PsswdDateAttr`.

Default	Other
■ CP (most servers) format is yyyymmdd ■ MS (in Microsoft_AD)	One value allowed

PsswdDateAttr

The password last modified date is User Directory attribute.

Default	Other
■ fw1pwdLastMod (most servers) ■ pwdLastSet (in Microsoft_AD)	One value allowed

BadPwdCountAttr

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

Default	Other
fw1BadPwdCount	One value allowed

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.

Default	Other
- 0 for most servers - 1 for Netscape_DS if not using encrypted password, SSL is recommended	One value allowed

DefaultCryptAlgorith

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

Default	Other
- Plain (for most servers) - Crypt (for Netscape_DS) - SHAI1	One value allowed

CryptedPasswordPrefix

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

Default	Other
{Crypt} (for Netscape_DS)	One value allowed

PhoneNumberAttr

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

Default	Other
internationalisednumber	One value allowed

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`").

Default	Other
none	Multiple values allowed

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.

Default	Other
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.	Multiple values allowed

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.

Default	Other
■ Organization OrganizationalUnit Domain (most servers) ■ Container (extra for Microsoft_AD)	Multiple values allowed

BranchOCOperator

If "One" is set, an "OR"ed query will be sent and every object that matches the criteria will be displayed as a branch.

If "All" is set, an "AND"ed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

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.

Default	Other
organization	Multiple values allowed

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.

Default	Other
▪ organizationalUnit (most servers) ▪ Contained (added to Microsoft_AD)	Multiple values allowed

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.

Default	Other
Domain	Multiple values allowed

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.

Default	Other
▪ User (in Microsoft_AD) ▪ Person OrganizationalPerson InertOrgPerson FW1 Person (most servers)	Multiple values allowed

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" is set, an "AND"ed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

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.

Default	Other
■ Groupofnames ■ Groupofuniquenames (most servers) ■ Group ■ Groupofnames (in Microsoft_ AD)	Multiple values allowed

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" is set, an "AND"ed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

GroupMembership

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

Default	Other
■ 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.	One value allowed

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
■ 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)	One value allowed

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
member	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
member	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
o	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
ou	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
cn	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`. Therefore, if the object created is of type `ObjectClass`, additional attributes is included in the created object with name '`name`' and value '`value`'.

Default	Other
user:userAccountControl:66048 For Microsoft_AD This means that when a user object is created an extra attribute is included automatically: userAccountControl with the value 66048	Multiple values allowed

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 ■ groupOfUniqueNames:uniqueMember (All other servers)	Multiple values allowed

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.

Default	Other
■ User (in Microsoft_AD) ■ person ■ organizationalPerson ■ inetOrgPerson ■ fw1Person ■ (All other servers)	Multiple values allowed

DomainObjectClass

Determines which ObjectClass to use when creating and/or modifying a domain context object.

These values can be different from the read counterpart.

Default	Other
Domain	Multiple values allowed

Managing Users on a User Directory Server

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.

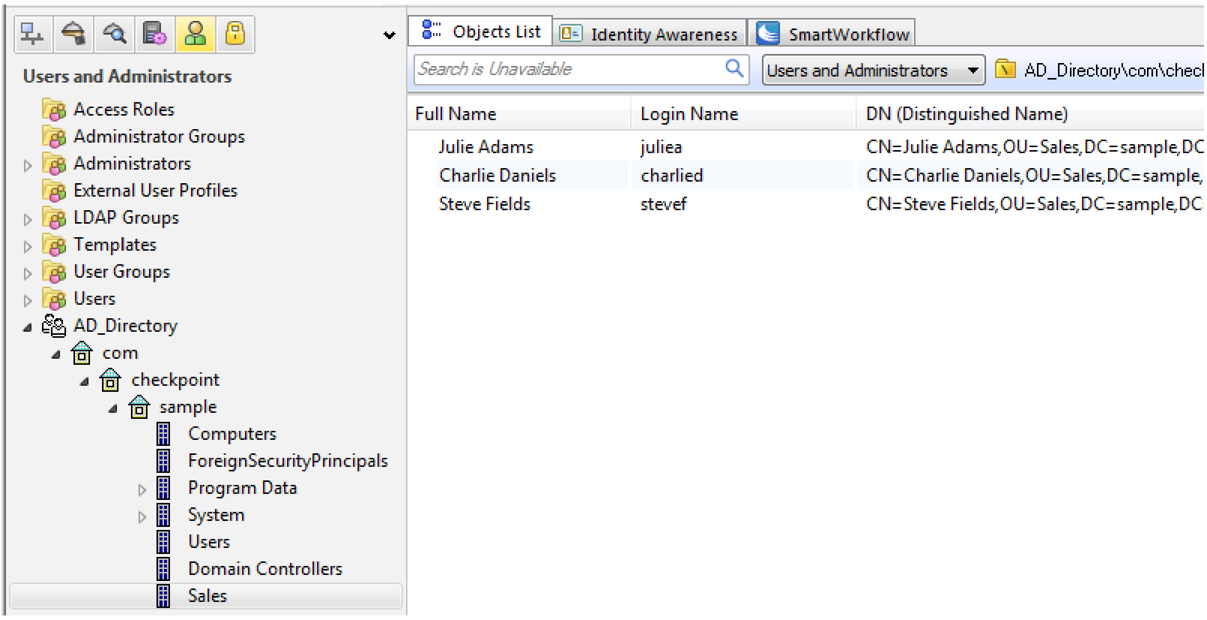
To manage LDAP information from SmartDashboard

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.



Full Name	Login Name	DN (Distinguished Name)
Julie Adams	juliea	CN=Julie Adams,OU=Sales,DC=sample,DC
Charlie Daniels	charlied	CN=Charlie Daniels,OU=Sales,DC=sample,
Steve Fields	stevef	CN=Steve Fields,OU=Sales,DC=sample,DC

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. 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:**
   1. Click **Apply filter for dynamic group**.
   2. 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**

Retrieving Information from a User Directory Server

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

1. The Security Gateway searches for the user in the *internal users database*.
2. If the specified user is not defined in the *internal users database*, the Security 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 Security 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 Security 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 Security 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 **yyyymmdd** syntax.
- **Free Form** - Enter your own query expression. See RFC 1558 for information about the syntax of User Directory (LDAP) query expressions.
- **Add** - Appends the condition to the query (in the text box to the right of **Search Method**).

Example of a Query

If you create a query where:

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

The server queries the User Directory with this filter:

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

Querying Multiple LDAP Servers

The Security Management Server and the Security Gateways can work with multiple LDAP servers concurrently. For example, if a Security 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 Security Gateway can find the location of a user by looking at the user DN, when working with certificates.)

Configuring Administrators and Users on an External LDAP Server

Check Point's environment integrates LDAP and other external management technologies with the Check Point solution.

If you have a large administrator and user count, we recommend that you use an external database such as LDAP for enhanced Security Management Server performance.

- You can manage administrators and users externally by an LDAP server.
- The Security Gateways can retrieve CRLs.

- The Security Management Server can use the LDAP data to authenticate administrators and users.
- Administrator and user data from other applications gathered in the LDAP database can be shared by different applications.

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

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,DCOOT
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` object-class. This information is downloaded to the directory using the `schema_microsoft_ad.ldif` file (see *"Adding New Attributes to the Active Directory" on page 146*).

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 `schmea_microsoft_ad.ldif` to the **C:\** drive in the Active Directory server.
3. From Active Directory server, with a text editor open the schema file.
4. Find the value `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.

   ```
   dn: CN=User,CN-
   Schema,CN=Configuration,DC=sample,DC=checkpoint,DC=com
   changetype: modify
   add: auxiliaryClass
   auxiliaryClass: 1.3.114.7.3.2.0.2
   -
   ```
6. Run:

   ```
   ldifde -i -f c:/schema_microsoft_ad.ldif
   ```

Adding New Attributes to the Active Directory

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

```
dn:CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
changetype: add
adminDisplayName: fw1auth-method
attributeID: 1.3.114.7.4.2.0.1
attributeSyntax: 2.5.5.4
cn: fw1auth-method
distinguishedName:
CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
instanceType: 4
isSingleValued: FALSE
LDAPDisplayName: fw1auth-method
name: fw1auth-method
objectCategory:
CN=Attribute-
Schema,CN=ConfigurationCN=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
```

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 Blade , 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 create a new or to edit an existing Account Unit or to create a new one manually.

To create or edit an existing LDAP Account Unit:

1. - **Create**: In the **Objects** tab, click **New > More > User/Identity > LDAP Account unit**.
   - **Edit**: In SmartConsole, open the **Object Explorer** (press the **CTRL+E** keys) > **Users/Identities** > **LDAP Account Units** > Right-click the LDAP Account Unit and select **Edit**.

   The **LDAP Account Unit Properties** window opens.
2. Edit the settings in these tabs:

- **General**

  Configure how the Security Management Server uses the Account Unit

  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**

- **Servers**

  Manage LDAP servers that are used by this Account Unit. You can add, edit, or delete LDAP server objects.

  To configure an LDAP server for the Account Unit

  a. 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.

  b. From the **Host** drop-down menu, select the server object.

     If necessary, create a new SmartConsole server object:

     i. Click **New**.

     ii. In the **New Host** window opens, enter the settings for the LDAP server.

     iii. Click **OK**.

  c. Enter the login credentials and the **Default priority**.

     Note -If you create the LDAP account unit to submit group queries, no special permissions are needed.
     If you create the LDAP account unit to submit Active Directory queries, you must have the permissions provided in sk93938.

  d. Select access permissions for the Check Point Gateways:

     - **Read data from this server**
     - **Write data to this server**

  e. 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.

  f. Click **OK**.

  To remove an LDAP server from the Account Unit:

  a. Select a server from the table.

  b. 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:

a. Click **Update Account Credentials**.

   The **Update Account to All Servers** window opens.

b. Enter the login credentials.

c. Click **OK**.

- **Objects Management**

  Configure the LDAP server for the Security Management Server to query and the branches to use

  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:

a. From the **Manage objects on** drop-down menu, select the LDAP server object.

b. Click **Fetch branches**.

   The Security Management Server queries and shows the LDAP branches.

c. 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**

d. Select **Prompt for password when opening this Account Unit**, if necessary (optional).

e. Configure the number of **Return entries** that are stored in the LDAP database (the default is 500).

- **Authentication**

  Configure the authentication scheme for the Account Unit. 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

3. Click **OK**.
4. Install the Access Control Policy.

Configuring 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).

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

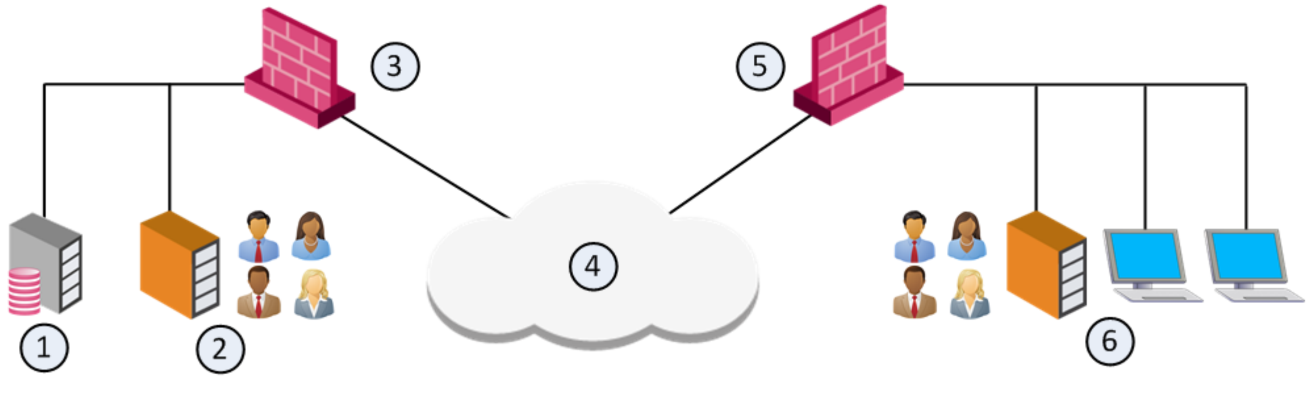
3. On the **Encryption** tab, you can change the encryption settings between Security Management Server / Security Gateways and LDAP server.

   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). To use certificates, the LDAP server must be configured with SSL strong authentication. See *"Authenticating with Certificates" on the next page*.

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.



Item	Description
1	**Security Management Server**. Manages user data in User Directory. It has an Account Unit object, where the two servers are defined.
2	**User Directory server** replication.
3	**Security Gateway**. Queries user data and retrieves CRLs from nearest User Directory server replication (2).
4	Internet
5	**Security Gateway**. Queries user data and retrieves CRLs from nearest User Directory server replication (6).
6	**User Directory server** replication.

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. Close all SmartConsole windows connected to the Management Server.
2. On each Account Unit, to which you want to authenticate with a certificate, set the `ldap_use_cert_auth` attribute to `true`:

   a. Connect with Database Tool (GuiDBEdit Tool) (see sk13009) to the Management Server.

   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 Database Tool (GuiDBEdit Tool).

3. Connect with SmartConsole to the Management Server.

4. Add a CA object:

   a. In the Object Explorer (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.

5. 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.

6. Test connectivity between the Security Management Server and the LDAP Server.

   See *"Managing LDAP Information" on page 140*.

Managing Gateways

This section describes how to create, update, and manage Security Gateways, and to use Secure Internal Communication (SIC) methods for Check Point platforms and products to authenticate each other.

Creating a New Security Gateway

A Security Gateway enforces security policies configured on the Security Management Server.

To install security policies on the Security Gateway, configure the Security Gateway object 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**.

   ⓘ **Important** - Make sure to select the correct Appliance model. Otherwise, policy installation may fail.
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 Security Gateway (see *"Secure Internal Communication (SIC)" on page 161*).

   If trust fails to establish, click **OK** to continue configuring the Security Gateway.
9. Click **OK**.

10. The **Get Topology Results** window that opens, shows interfaces successfully configured on the Security 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 Security Gateway, click **Get** to automatically retrieve the information from the Security 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.

Note - You cannot add additional information fields to the Security Gateway object.

Manually Updating the Gateway Topology

As the network changes, you must update the Security Gateway topology.

To update the Security Gateway topology

1. In SmartConsole, click **Gateways & Servers**.
2. Double-click the Security Gateway object.

   The Security Gateway property window opens.
3. Click **Network Management**.
4. Click **Get Interfaces** and select the applicable option:
   - **Get Interfaces With Topology**

     A warning window asks if you want to overwrite the existing Topology and Anti-Spoofing settings.

     Click **Yes**.

     Note - The physical interfaces that are part of a Bridge interface always appear with the topology "Undefined".
     Workaround: Use the API command "get-interfaces".
   - **Get Interfaces Without Topology**
5. The **Get Topology Results** window opens.
6. Click **Accept**.
7. Configure the applicable Topology and Anti-Spoofing settings for the interfaces.
8. Click **OK**.
9. Install the Access Control Policy.

Get Interfaces API

From R80.40 Jumbo Hotfix Accumulator Take 126, you can use the Check Point API to execute the Get Interfaces command.

The Get Interfaces API:

- Supports a larger number of interfaces compared with SmartConsole.
- Supports interfaces which are not supported by SmartConsole: Bridge and Bond interfaces without IP addresses.
- Configures the default topology for internal networks for R80.20 and higher Security Gateway and ClusterXL to **Network defined by routes**, where applicable (the default in SmartConsole is **This network (Internal)**).
- Does not get unnecessary Bridge and Bond satellite interfaces.

The Get Interfaces API command only supports Security Gateways and ClusterXL that run on Gaia operating system.

For explanations on how to use the API Get Interfaces command, see the *Check Point Management API Reference*

Dynamically Updating the Security Gateway Topology

This feature is supported only for Security Gateways R77.20 and above. Once selected, the range of IP addresses behind the internal interface is automatically calculated every second (default value) without the need for the administrator to click **Get Interfaces** and install a policy.

To configure dynamic topology updates

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Edit**.
3. In the **Topology** section, click **Modify**.
4. In the **Leads To** section, select **Network defined by routes**.
5. Click **OK**.

This default update value is configured in **SmartConsole > Preferences** and set to one second. The value set here applies to all internal interfaces for all gateways in the Domain.

To set the update value for a specific interface

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Actions > Settings**.
3. Select **Use custom update time (seconds)** and set the applicable update time.
4. Click **OK**.

Dynamic Anti-Spoofing

When Anti-Spoofing is selected and you click **Get interfaces**, the Security Gateway generates a list of valid IP addresses based on the IP address and netmask of the interface and the routes assigned to the interface.

Anti-Spoofing drops packets with a source IP address that does not belong to the network behind the packet's interface. For example, packets with an internal IP address that comes from an external interface.

When the **Network defined by routes** option is selected along with **Perform Anti-Spoofing based on interface topology**, you get *Dynamic Anti-Spoofing*. The valid IP addresses range is automatically calculated without the administrator having to do click **Get Interfaces** or install a policy.

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.

  Security Gateways R71 and higher use AES128 for SIC. If one of the Security Gateways is below R71, the Security Gateways use 3DES.

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

Note - From R80.40 Jumbo Hotfix Accumulator Take 119, to see SIC errors, examine the `$CPDIR/log/sic_info.elg` file on the Security Management Server and on the Security Gateway.

Initializing Trust

To establish the initial trust, a Security 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 Security 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 Security Gateway and Security Management Server, go to the **Gaia Portal** > **System Management** > **Time**.

To initialize Trust

1. In SmartConsole, open the Security Gateway network object.
2. In the **General Properties** page of the Security Gateway, click **Communication**.
3. In the **Communication** window, enter the **Activation Key** that you created during installation of the Security Gateway.
4. Click **Initialize**.

   The ICA signs and issues a certificate to the Security Gateway.

   Trust state is **Initialized but not trusted**. The Internal Certificate Authority (ICA) issues a certificate for the Security 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 Security Gateway. The Activation Key is deleted.

The Security Gateway can communicate with Check Point hosts that have a security certificate signed by the same ICA.

SIC Status

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

- **Communicating** - The secure communication is established.
- **Unknown** - There is no connection between the Security Gateway and Security Management Server.
- **Not Communicating** - The Security Management Server can contact the Security 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 Security Gateways during the next SIC connection. If two Security Gateways have different CRLs, they cannot authenticate.

1. In SmartConsole, from the Gateways & Servers view, double-click the Security Gateway object.
2. Click **Communication**.
3. In the **Trusted Communication** window that opens, click **Reset**.
4. Install Policy on the Security Gateways.

   This deploys the updated CRL to all Security Gateways. If you do not have a Rule Base (and therefore cannot install a policy), you can reset Trust on the Security Gateways.

   ⓘ **Important** - Before a new trust can be established in SmartConsole, make sure the same one-time activation password is configured on the Security Gateway.

Troubleshooting SIC

If SIC fails to Initialize:

1. Make sure there is connectivity between the Security Gateway and Security Management Server.
2. Make sure that the Security Management Server and the Security 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 Security 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 Security Gateway.

   If the IP address of the Security Management Server mapped through static NAT by its local Security Gateway, add the public IP address of the Security Management Server to the `/etc/hosts` file on the remote Security Gateway. 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 Security Gateway reside in different time zones, the remote Security Gateway may have to wait for the certificate to become valid.
6. Remove the Security Policy on the Security Gateway to let all the traffic through:
   a. Connect to the command line on the Security Gateway
   b. Log in to the Expert mode.
   c. Run:

      ```
      fw unloadlocal
      ```

      Important - See the *R80.40 CLI Reference Guide* > Chapter *Security Gateway Commands* > Section *fw* > Section *fw unloadlocal*.
7. Try to establish SIC again.

Remote User access to resources and Mobile Access

If you install a certificate on a Security 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.

To establish a new trust state for a Security Gateway

1. Open the command line interface on the Security Gateway.
2. Run:

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

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 Security 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 Tool - This is the `cpconfig` CLI utility. One of the options creates the ICA, which issues a SIC certificate for the Security Management Server.
- SmartConsole - SIC certificates for Security Gateways and administrators, VPN certificates, and user certificates.
- *"The ICA Management Tool" on page 472* - VPN certificates for users and advanced ICA operations.

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 Security Gateway properties window.
- *"The ICA Management Tool" on page 472*.

Certificates have these configurable attributes:

Attributes	Default	Comments
validity	5 years	
key size	2048 bits	
KeyUsage	5	Digital Signature and Key encipherment
ExtendedKeyUsage	0 (no KeyUsage)	VPN certificates only

To learn more about key size values, see RSA key lengths.

To view license information for each Software Blade

Step	Instructions
1	Select a Security Gateway or a Security Management Server.
2	In the **Summary** tab below, click the object's **License Status** (for example: **OK**). The **Device & License 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 and higher. ■ The tooltip of the SKU is the product name.

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

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

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 servers R80.30 and higher.

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 *R80.40 Release Notes* for a list of supported Software Blades

Viewing Licenses in SmartConsole

To view license information

Step	Instructions
1	In SmartConsole, from the left navigation panel, click **Gateways & Servers**.
2	From the **Columns** drop-down list, select **Licenses**.

You can see these columns:

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

To view license information for each Software Blade

Step	Instructions
1	Select a Security Gateway or a Security Management Server.

Step	Instructions
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 and higher. ■ The tooltip of the SKU is the product name.

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

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

Viewing License Information for VSX:

SmartConsole reports an error when viewing VS Licenses.

To see the VS license information:

Select the VSG Gateway or VSX Cluster object (and not objects of Virtual Systems or Virtual Routers).

Monitoring Licenses in SmartConsole

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

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

Step	Instructions
1	View the License Inventory report from the Gateways & Servers view: 1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**. 2. From the top toolbar, click **Actions** > **License Report**. 3. 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	Export the License Inventory report from the Gateways & Servers view: 1. In the top right corner, click the **Options** button. 2. 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.

Step	Instructions
1	View License Status report from the Logs & Monitor view: 1. In SmartConsole, from the left navigation panel, click **Logs & Monitor** 2. At the top, open a new tab by clicking **New Tab**, or **[+]**. 3. In the left section, click **Views**. 4. In the list of reports, double-click **License Status**. 5. 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	Filter the License Status report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button **> View Filter**. The **Edit View Filter** window opens. 2. Select a **Field** to filter results. For example, **Device Name**, **License Status**, **Account ID**. 3. Select the logical operator - **Equals**, **Not Equals**, or **Contains**. 4. Select or enter a filter value. Note - Click the **X** icon to delete a filter. 5. Optional: Click the **+** icon to configure additional filters. 6. Click **OK** to apply the configured filters. The report is filtered based on the configured filters.
3	Export the License Status report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

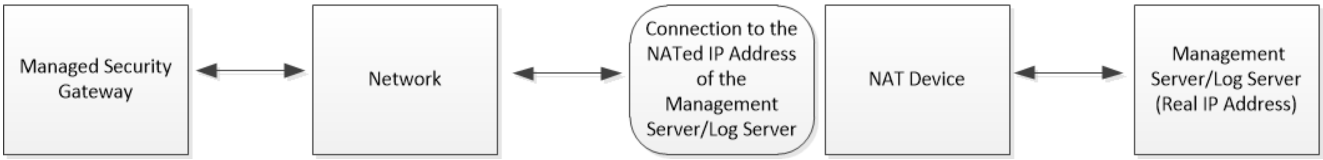
The Logs & Monitor view in SmartConsole lets you see filter and export the *License Inventory* report.

Step	Instructions
1	View the License Inventory report from the Logs & Monitor view: 1. In SmartConsole, from the left navigation panel, click **Logs & Monitor** 2. At the top, open a new tab by clicking **New Tab**, or **[+]**. 3. In the left section, click **Reports**. 4. In the list of reports, double-click **License Inventory**. 5. 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	Filter the License Inventory report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button **> Report Filter**. The **Edit Report Filter** window opens. 2. Select a **Field** to filter results. For example, **Blade Name**, **Device Name**, **License Overall Status**, **Account ID**. 3. Select the logical operator - **Equals**, **Not Equals**, or **Contains**. 4. Select or enter a filter value. Note - Click the **X** icon to delete a filter. 5. Optional: Click the **+** icon to configure additional filters. 6. Click **OK** to apply the configured filters. The report is filtered based on the configured filters.
3	Export the License Inventory report in the Logs & Monitor view: 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

Configuring a Security Gateway to Access the Management Server or Log Server at its NATed IP Address

Starting from R80.40 Jumbo Hotfix Accumulator Take 92, you can configure a Security Gateway to access the Security Management Server or Log Server at the server's NATed IP address for fetching policy or sending logs.

This diagram describes the flow of this process:


Managed Security Gateway
Network
Connection to the NATed IP Address of the Management Server/Log Server
NAT Device
Management Server/Log Server (Real IP Address)

Procedure:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. On a VSX Gateway / each VSX Cluster Member, go to the context of the applicable Virtual System:

   ```
   vsenv <VSID>
   ```

4. Run the applicable command (this change survives reboot):

   a. To force the Security Gateway / Cluster Member to connect only to the **public (NATed)** IP address (this is the default behavior) of the Management Server or Log Server, run:

   ```
   ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 FORCE_NATTED_IP
   -n 1
   ```

   b. To force the Security Gateway / Cluster Member to connect only to the **real** IP address of the Management Server or Log Server, run:

   ```
   ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 FORCE_NATTED_IP
   -n 0
   ```

   Notes:

   - This change survives reboot.
   - In a Cluster, you must configure all the Cluster Members in the same way.

5. Restart the FWD process:

   See the instructions in sk97638 > section *Infrastructure Processes*.

Central Deployment of Hotfixes

Central Deployment allows performing batch deployment of Jumbo Hotfix Accumulators and Hotfixes using SmartConsole.

You can deploy a Recommended Jumbo Hotfix Accumulator or a specific Jumbo Hotfix Accumulator take.

You can find the name of the specific Jumbo Hotfix Accumulator in the relevant SK article for the applicable version.

Notes:

- You can select up to 30 Security Gateways and ClusterXL Cluster Members.
- Up to 10 targets can be deployed concurrently.

Prerequisites

This table shows the Jumbo Hotfix Accumulator takes which are required to install the *recommended* Jumbo Hotfix Accumulator.

Version	Jumbo Hotfix Accumulator
R80.30	Take 76 or higher.
R80.20	A Take higher than Take 118.
R80.10	A Take higher than 245.

To use the Install Hotfix from SmartConsole options:

- The version of the installed Security Management Server must be R80.40 or higher.
- The Security Management Server and target Security Gateways must be able to connect to the Check Point cloud.
- The administrator has the **Manage Licenses and Packages** permissions.
- The latest deployment agent is installed on the targets.
- SIC is already established for the target Security Gateways.
- A policy is installed on the target Security Gateways.
- To upgrade a configured ClusterXL, the Cluster object must be selected.

Limitations

Only *recommended* and on-going Jumbo Hotfix Accumulators Takes made available in the Check Point update servers are supported.

If SmartConsole and the Security Management Server are connected through a proxy server, the GUI for this feature is not supported. In this case, use the applicable API command.

The following are **not** supported with Hotfix Central Deployment:

- ClusterXL in High Availability mode configured as "`Switch to higher priority Cluster Member`" (known as "`Primary Up`").
- ClusterXL in Load Sharing mode, and VRRP Clusters.
- VSX.
- Using Central Deployment from:
  - A Global Domain or in the Multi-Domain Server context.
  - A Standalone server.
  - Standby Multi-Domain Security Management and Security Management Server.
- Log Server
- SmartEvent Server

Installing the Jumbo Hotfix Accumulator

Workflow

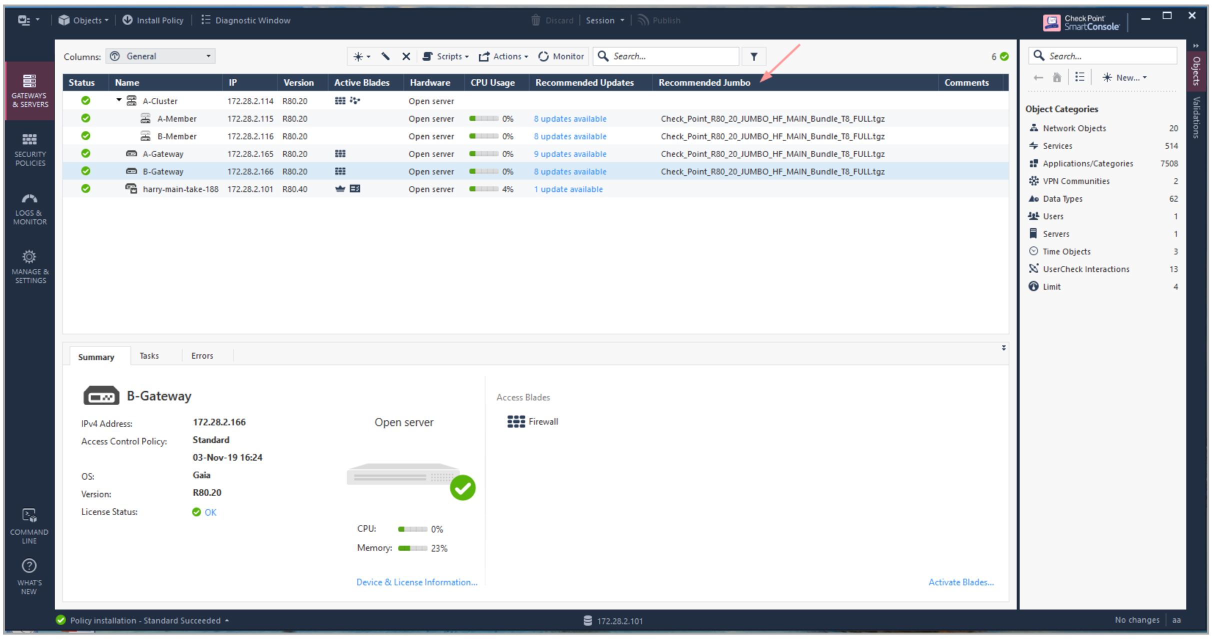
1. Select the target Security Gateways for upgrade.
2. Select the type of Jumbo Hotfix Accumulators to install.
3. **Validate** - This process makes sure that the package is available for download from Check Point servers.
4. **Verify** - the process of verification is making sure that the selected Jumbo Hotfix Accumulator Take can be installed on the target Security Gateways. The verification process checks if other installed Hotfixes are not overridden and that enough free disk space is available for the process to complete.
5. Install the Jumbo Hotfix Accumulator.

To Install a Jumbo Hotfix Accumulator or a Hotfix

Best Practice - Central deployment of Hotfixes on the Security Management Server relies on status reports from the managed Gaia servers. Therefore, we recommend to wait for two minutes after the Gaia server is up and running before you install a Hotfix.

1. In SmartConsole Go to the **GATEWAYS & SERVERS** view.

   The list of available Jumbo Hotfix Accumulators shows in a new column.



Columns: General

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Comments
✓	A-Cluster	172.28.2.114	R80.20		Open server				
✓	A-Member	172.28.2.115	R80.20		Open server	0%	8 updates available	Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz	
✓	B-Member	172.28.2.116	R80.20		Open server	0%	8 updates available	Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz	
✓	A-Gateway	172.28.2.165	R80.20		Open server	0%	9 updates available	Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz	
✓	B-Gateway	172.28.2.166	R80.20		Open server	0%	8 updates available	Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz	
✓	harry-main-take-188	172.28.2.101	R80.40		Open server	4%	1 update available		

Object Categories

Network Objects	20
Services	514
Applications/Categories	7508
VPN Communities	2
Data Types	62
Users	1
Servers	1
Time Objects	3
UserCheck Interactions	13
Limit	4

B-Gateway

IPv4 Address: 172.28.2.166
Access Control Policy: Standard
03-Nov-19 16:24
OS: Gaia
Version: R80.20
License Status: ✓ OK

Open server

CPU: 0%
Memory: 23%

Access Blades

Firewall

✓ Policy installation - Standard Succeeded

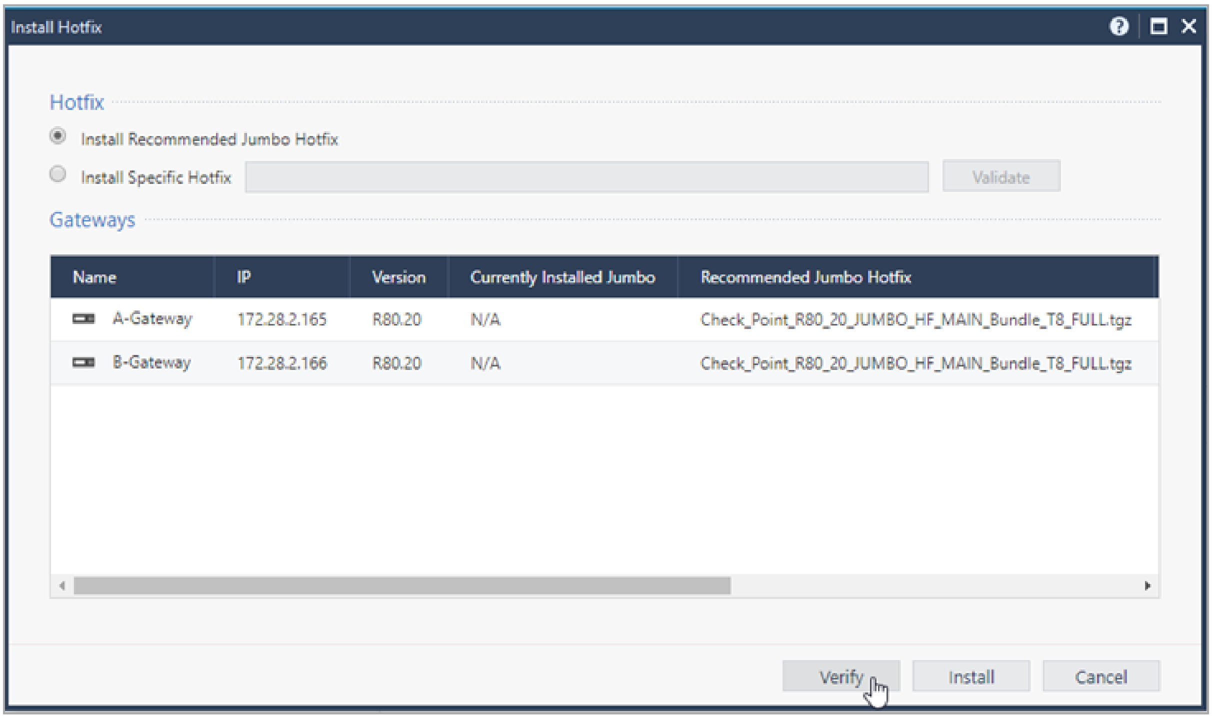
172.28.2.101

2. Select the target Security Gateways for deployment.

3. From the Toolbar menu, select **Actions** > **Install Hotfix**

   Alternatively, right-click the **Gateways & Servers** view > **Actions** > **Install Hotfix**.

   The **Install Hotfix** window opens, and shows Information about the selected targets and their corresponding recommended Jumbo Hotfix Accumulators.



Hotfix

● Install Recommended Jumbo Hotfix

○ Install Specific Hotfix

Gateways

Name	IP	Version	Currently Installed Jumbo	Recommended Jumbo Hotfix
A-Gateway	172.28.2.165	R80.20	N/A	Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz
B-Gateway	172.28.2.166	R80.20	N/A	Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz

4. Select one of the options:

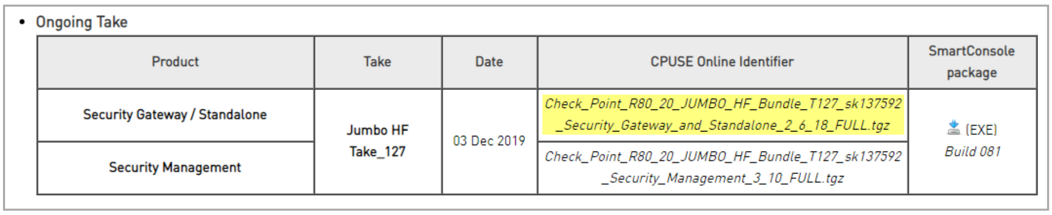
   - Install **Recommended Jumbo Hotfix** (default).

     Note - If there is no recommended Jumbo Hotfix Accumulator for the selected targets, this option is grayed out.
     If a recommended Jumbo Hotfix Accumulator applies only to some of the selected targets, the deployment takes place only for those targets.

   Or

   - **Install Specific Hotfix**

     a. Copy the Jumbo Hotfix Accumulator file name from the applicable SK article and paste it in the **Install Specific Hotfix** text box.



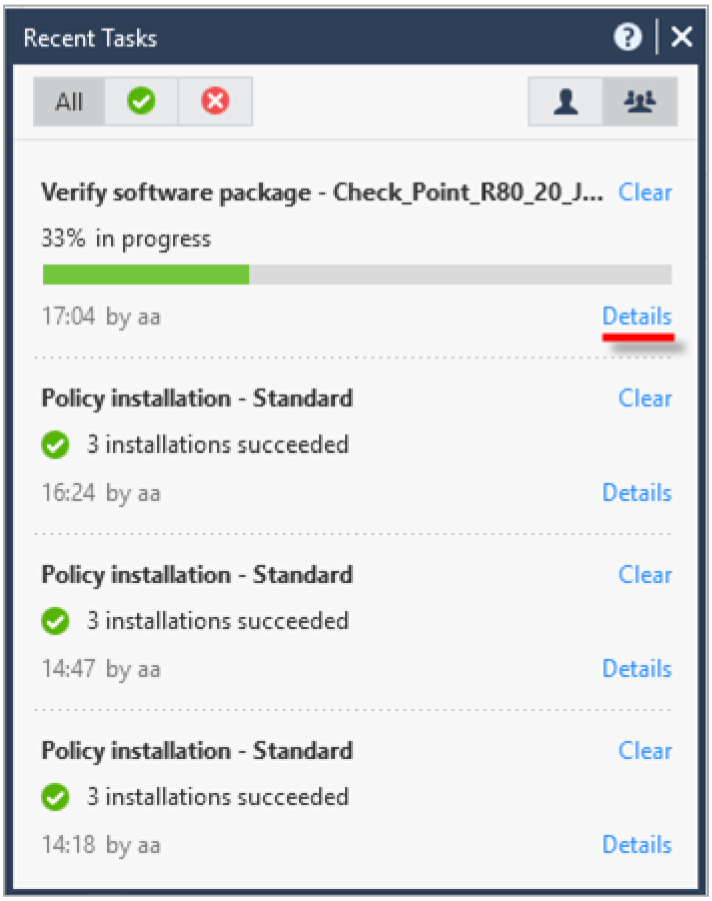
- Ongoing Take

Product	Take	Date	CPUSE Online Identifier	SmartConsole package
Security Gateway / Standalone	Jumbo HF Take_127	03 Dec 2019	Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592 _Security_Gateway_and_Standalone_2_6_18_FULL.tgz	(EXE) Build 081
Security Management			Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592 _Security_Management_3_10_FULL.tgz	

     b. Click **Validate**

5. Click **Verify** - The **Install Hotfix** window is minimized and the verification process starts.

a. To see the progress of the verification process open the **Tasks** view at the bottom left corner of SmartConsole and click **Details**:



Recent Tasks

Verify software package - Check_Point_R80_20_J... Clear
33% in progress
17:04 by aa Details

Policy installation - Standard Clear
✓ 3 installations succeeded
16:24 by aa Details

Policy installation - Standard Clear
✓ 3 installations succeeded
14:47 by aa Details

Policy installation - Standard Clear
✓ 3 installations succeeded
14:18 by aa Details

6. Click **Install**.

Configuring Implied Rules or Kernel Tables for Security Gateways

Introduction

An administrator configures Security Policy and other inspection settings in SmartConsole.

During a policy installation, the Management Server creates the applicable files and transfers them to the target Security Gateways.

The Management Server creates these files based on:

- Security Policy in SmartConsole
- Global properties in SmartConsole
- Security Gateway properties
- Multiple configuration files on the Management Server that control the inspection of various network protocols

It is possible to modify these configuration files on the Management Server to fine-tune the inspection in your network (in Check Point INSPECT language).

There are two main categories of these configuration files:

- Files for Security Gateways that have the same software version as the Management Server.
- Files for Security Gateways that have the a lower software version than the Management Server. This category is called "Backward Compatibility".

Configuration files

File Name	Controls	Location
`user.def`	User-defined implied rules.	See *"Location of 'user.def' Files on the Management Server" on page 183*
`implied_rules.def`	Default implied rules.	See *"Location of 'implied_rules.def' Files on the Management Server" on page 185*

File Name	Controls	Location
`table.def`	Definitions of various kernel tables.	See *"Location of 'table.def' Files on the Management Server" on page 187*
`crypt.def`	VPN encryption macros.	See *"Location of 'crypt.def' Files on the Management Server" on page 189*
`vpn_table.def`	Definitions for various kernel tables that hold VPN data. For example, VPN timeouts, number of VPN tunnels, whether a specific kernel table should be synchronized between cluster members, and others.	See *"Location of 'vpn_table.def' Files on the Management Server" on page 191*
`communities.def`	VPN encryption macros for X11 server (X Window System) traffic.	See *"Location of 'communities.def' Files on the Management Server" on page 193*
`base.def`	Definitions of packet inspection for various network protocols.	See *"Location of 'base.def' Files on the Management Server" on page 195*
`dhcp.def`	Definitions of packet inspection for DHCP traffic - DHCP Request, DHCP Reply, and DHCP Relay.	See *"Location of 'dhcp.def' Files on the Management Server" on page 197*
`gtp.def`	Definitions of packet inspection for GTP (GPRS Tunnelling Protocol) traffic.	See *"Location of 'gtp.def' Files on the Management Server" on page 199*

Configuration Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Back up the current file:

   ```
   cp -v /<Full Path to File>/<File Name>{,_BKP}
   ```

   Example:

   ```
   cp -v $FWDIR/conf/user.def.FW1{,_BKP}
   ```

4. Edit the current file:

   ```
   vi /<Full Path to File>/<File Name>
   ```

   Example:

   ```
   vi $FWDIR/conf/user.def.FW1
   ```

5. Make the applicable changes as described in the applicable SK article, or as instructed by Check Point Support.
6. Save the changes in the file and exit the editor.
7. Connect with SmartConsole to the Security Management Server.
8. In SmartConsole, install the Access Control Policy on the applicable Security Gateway or Cluster object.

Location of 'user.def' Files on the Management Server

The '`user.def`' files contain the user-defined implied rules.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`$FWDIR/conf/user.def.FW1`
R80.20SP on Maestro, or Scalable Chassis	`$FWDIR/conf/user.def.FW1`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`$FWDIR/conf/user.def.SFWR80CMP`
R77.30, R77.20, R77.10, R77	`$FWDIR/conf/user.def.R77CMP`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`$FWDIR/conf/user.def.SFWR77CMP`
R76SP.x on Scalable Chassis	`$FWDIR/conf/user.def.R76CMP`
R76	`$FWDIR/conf/user.def.R76CMP`
R75.40VS, R75.40VS for 61000 Scalable Chassis	`$FWDIR/conf/user.def.R7540VSCMP`
R75.47, R75.46, R75.45, R75.40	`$FWDIR/conf/user.def.R7540CMP`
R75.30, R75.20	`$FWDIR/conf/user.def.R7520CMP`
R75.20.x on SMB Appliances 1100	`$FWDIR/conf/user.def.SFWR75CMP`

Important - If the required file does not exist, create a copy of the `$FWDIR/conf/user.def.FW1` file, rename it, and edit it.

Location of 'implied_rules.def' Files on the Management Server

The '`implied_rules.def`' files contain the default implied rules.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/implied_rules.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/implied_rules.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/implied_rules.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/implied_rules.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/implied_rules.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/implied_rules.def`
R76	`/opt/CPR76CMP-R80.40/lib/implied_rules.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/implied_rules.def`

Version of the Target Security Gateway	Location of the File
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/implied_rules.def`
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/implied_rules.def`

Location of 'table.def' Files on the Management Server

The '`table.def`' files contain definitions of various kernel tables for Security Gateways.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/table.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/table.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/table.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/table.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/table.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/table.def`
R76	`/opt/CPR76CMP-R80.40/lib/table.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/table.def`
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/table.def`

Version of the Target Security Gateway	Location of the File
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/table.def`

Location of 'crypt.def' Files on the Management Server

The '`crypt.def`' files contain VPN encryption macros.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/crypt.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/crypt.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/crypt.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/crypt.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/crypt.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/crypt.def`
R76	`/opt/CPR76CMP-R80.40/lib/crypt.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/crypt.def`
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/crypt.def`

Version of the Target Security Gateway	Location of the File
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/crypt.def`

Location of 'vpn_table.def' Files on the Management Server

The '`vpn_table.def`' files contain definitions for various kernel tables that hold VPN data.

For example, VPN timeouts, number of VPN tunnels, whether a specific kernel table should be synchronized between cluster members, and others.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/vpn_table.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/vpn_table.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/vpn_table.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/vpn_table.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/vpn_table.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/vpn_table.def`
R76	`/opt/CPR76CMP-R80.40/lib/vpn_table.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/vpn_table.def`

Version of the Target Security Gateway	Location of the File
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/vpn_table.def`
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/vpn_table.def`

Location of 'communities.def' Files on the Management Server

The '`communities.def`' files contain VPN encryption macros for X11 server (X Window System) traffic.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/communities.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/communities.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/communities.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/communities.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/communities.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/communities.def`
R76	`/opt/CPR76CMP-R80.40/lib/communities.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/communities.def`

Version of the Target Security Gateway	Location of the File
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/communities.def`
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/communities.def`

Location of 'base.def' Files on the Management Server

The '`base.def`' files contain definitions of packet inspection for various network protocols.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/base.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/base.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/base.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/base.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/base.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/base.def`
R76	`/opt/CPR76CMP-R80.40/lib/base.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/base.def`
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/base.def`

Version of the Target Security Gateway	Location of the File
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/base.def`

Location of 'dhcp.def' Files on the Management Server

The '`dhcp.def`' files contain definitions of packet inspection for DHCP traffic - DHCP Request, DHCP Reply, and DHCP Relay.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/dhcp.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/dhcp.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/dhcp.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/dhcp.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/dhcp.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/dhcp.def`
R76	`/opt/CPR76CMP-R80.40/lib/dhcp.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/dhcp.def`
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/dhcp.def`

Version of the Target Security Gateway	Location of the File
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/dhcp.def`

Location of 'gtp.def' Files on the Management Server

The '`gtp.def`' files contain definitions of packet inspection for GTP (GPRS Tunnelling Protocol) traffic.

Important - To edit the file, go to the context of the applicable Domain Management Server. To go to the required context, use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Location of files on an R80.40 Security Management Server:

Version of the Target Security Gateway	Location of the File
R80.40, R80.30, R80.20, R80.10	`/opt/CPsuite-R80.40/lib/gtp.def`
R80.20SP on Maestro, or Scalable Chassis	`/opt/CPsuite-R80.40/lib/gtp.def`
R80.20.x on Quantum Spark Appliances 1530 / 1550 / 1570 / 1570R / 1590	`/opt/CPSFWR80CMP-R80.40/lib/gtp.def`
R77.30, R77.20, R77.10, R77	`/opt/CPR77CMP-R80.40/lib/gtp.def`
R77.20.x on SMB Appliances 1100 / 1200R / 1400	`/opt/CPSFWR77CMP-R80.40/lib/gtp.def`
R76SP.x on Scalable Chassis	`/opt/CPR76CMP-R80.40/lib/gtp.def`
R76	`/opt/CPR76CMP-R80.40/lib/gtp.def`
R75.47, R75.46, R75.45, R75.40VS, R75.40VS for 61000 Scalable Chassis, R75.40	`/opt/CPR7540CMP-R80.40/lib/gtp.def`
R75.30, R75.20	`/opt/CPR7520CMP-R80.40/lib/gtp.def`

Version of the Target Security Gateway	Location of the File
R75.20.x on SMB Appliances 1100	`/opt/CPSG80R75CMP-R80.40/lib/gtp.def`

Managing Objects

Network Objects, defined in SmartConsole and stored in the proprietary Check Point object database, represent physical and virtual network components (such as Security 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, Security 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?

Note - In SmartConsole, when you configure properties of an object and create a new object from the original object, the new object is not available in the original Object Editor.

To resolve this issue:

1. After you close the second Object Editor, click OK in the original Object Editor.
2. Edit the original object again. The new object is now available.

Object Categories

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

Icon	Object Type	Examples
🖧	Network Objects	Security Gateways, hosts, networks, address ranges, dynamic objects, security zones
⇄	Services	Services, Service groups
▦	Custom Applications/Sites	Applications, Categories, Mobile applications
✳	VPN Communities	Site to Site or Remote Access communities
👥	Users	Users, user groups, and user templates

Icon	Object Type	Examples
▲●	Data Types	International Bank Account Number - IBAN, HIPAA - Medical Record Number - MRN, Source Code.
▮	Servers	Trusted Certificate Authorities, RADIUS, TACACS
🕒	Time Objects	Time, Time groups
✕	UserCheck Interactions	Message windows: Ask, Cancel, Certificate Template, Inform, and Drop
⏲	Limit	Download and upload bandwidth

Actions with 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.

ℹ **Note** - Do not create two objects with the same name. A validation error shows when you try to publish the SmartConsole session. 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**.

Note - In SmartConsole, you can only search or filter for objects whose name contain two or more characters.

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.

Adding a Tag to an Object

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

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 can be used to facilitate and simplify network management. When you have the same set of objects which you want to use in different places in the Rule Base, you can create a group to include such set of objects and reuse it. Modifications are applied to the group instead of to each member of the group.

Groups are also used where SmartConsole lets you select only one object, but you need to work with more than one. For example, in the Security Gateway object > **Network Management** > **VPN Domain** > **Manually defined**, you can only select on object from the drop-down menu. If you want to select more than one object for your VPN Domain, you can create a group, add the required objects to the group, and select the group from the drop-down menu.

Grouping Network Objects

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 you want to add, click the [**+**] sign and select it from the list that shows.

5. Click **OK**.

From version R80.20.M2, you can also associate groups to a network object directly from the object editor.

To associate groups to a network object

1. Open the object editor, and go to **Groups** in the navigation tree.
2. For each group you want to add, click the [**+**] sign and select it from the list that shows.

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 enabled on the Check Point Host, it cannot function as a Security Gateway. The Host requires SIC and other features provided by the actual Security Gateway.

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 a Management Server from R77.30 or earlier versions, Node objects are converted to Host objects.

Gateway Cluster

A cluster is a group of Security Gateways defined as one logical object. Clustered gateways add redundancy through High Availability or Load Sharing.

Updatable Objects

An updatable object is a network object which represents an external service, such as Office 365, AWS, GEO locations and more. External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically on the Security Gateway each time the provider changes a list. There is no need to install policy for the updates to take effect. You can use updatable objects in all three types of policies: Access Control, Threat Prevention and HTTPS Inspection. You can use an updatable object in the Access Control, Threat Prevention or the HTTPS Inspection policy as a source or a destination. In the Threat Prevention policy, you can also use an updatable object as the protected scope.

Note - For Access Control, this feature is supported for R80.20 and above gateways. For Threat Prevention and HTTPS Inspection, this feature is supported for R80.40 and above gateways.

Adding an Updatable Object to the Security Policy

A customer uses Office365 and wants to allow access to Microsoft Exchange services.

To add the Microsoft Exchange Updatable Object to the Security Gateway

1. Make sure the Security Management Server and the Security Gateway have access to the Check Point cloud.
2. Go to SmartConsole > Security Policies > **Access Control** > **Policy**.
3. Create a new rule.
4. In the Destination column, click the + sign and select **Import** > **Updatable Objects**.

   The **Updatable Objects** window opens.
5. Select the objects to add. For this use case, select the **Exchange Services** object.

   Note - You can also add objects to the **Source** column.
6. Click **OK**.
7. Install policy.

The Exchange Services object is added to the Rule Base.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Accept Exchange	WirelessZone	Exchange Services	Any	Any	Accept	Log
2	Accept Exchange	Exchange Services	WirelessZone	Any	Any	Accept	Log

You can monitor the updates in the **Logs & Monitor > Logs** view.

To monitor the updates

1. Go to SmartConsole > **Logs & Monitor**.
2. From the search bar, enter Updatable Objects.

3. Double-click the relevant log.

   The **Log Details** window shows.

4. `Succeeded` shows in the **Status** field when the update is successful.

More Network Object Types

This section includes explanations of additional network objects 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.

Wildcard Objects

Wildcard objects let you define IP address objects that share a common pattern that can be permitted or denied access in a security policy.

Note - This feature is only supported for R80.20 and above gateways.

To create a new wildcard object

1. Open **Object Explorer** > **New** > **More** > **Network Object** > **Wildcard object**.
2. Enter the Wildcard IP address and Wildcard Netmask in IPv4 or IPv6 Format.
3. Click **OK**.

Understanding Wildcard Objects

The wildcard object contains a wildcard IP address and a wildcard netmask.

The *wildcard netmask* is the mask of bits that indicate which parts of the IP address must match and which do not have to match. For example:

Wildcard IP:	194.	29.	0.	1
Wildcard Netmask:	0.	0.	3.	0

The third octet represents the mask of bits. If we convert the 3 to binary, we get 00000011.

The 0 parts of the mask must match the equivalent bits of the IP address.

The 1 parts of the mask do not have to match, and can be any value.

0 0 0 0 0 0	1 1

Must match the equivalent bits in the IP address	Do not have to match

The binary netmask produces these possible decimal values:

128	64	32	16	8	4	2	1		
						Binary			**Decimal**
0	0	0	0	0	0	0	0		**0**
0	0	0	0	0	0	0	1		**1**
0	0	0	0	0	0	1	0		**2**
0	0	0	0	0	0	1	1		**3**

The netmask permits only these IP addresses:

- 194.29.0.1
- 194.29.1.1
- 192.29.2.1
- 194.29.3.1

Examples of Use Cases

Scenario One

A supermarket chain has all of its cash registers on subnet 194.29.x.1, where x defines the region. In this use case, all the cash registers in this region must have access to the database server at 194.30.1.1.

Instead of defining 256 hosts (194.29.0.1, 194.29.1.1, 194.29.2.1....194.29.255.1), the administrator creates a wildcard object that represents all the cash registers in the region:

Wildcard IP:	194.	29.	0.	1
Wildcard Mask:	0.	0.	255.	0

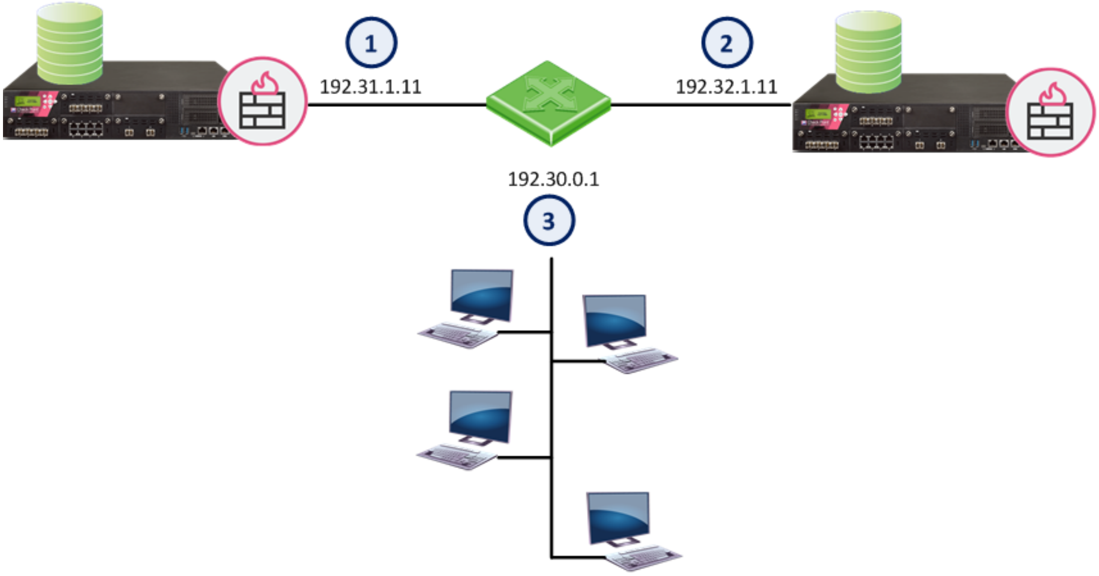
The wildcard object can now be added to the Access Control Policy.

Source	Destination	Action	Track
Wildcard Object	Database server object	Accept	Log

Scenario Two

In this use case, a supermarket chain has stores in Europe and Asia.

The 192.30.0-255.1 network contains both the Asian and European regions, and the stores within those regions.



Item	Description
1	Database Server for Europe
2	Database Server for Asia
3	European and Asia network

The administrator wants stores in the European and Asia regions to access different database servers. In this topology, the third octet of the European and Asia network's IP address will be subject to a wildcard. The first four bits of the wildcard will represent the region and the last four bits will represent the store number.

Bits that represent the region	Bits that represent the store number
0000	0000

In the Wildcard IP:

- The Asia region is represented by **0001xxxx** (Region **1** in decimal)
- The European region is represented by **0010xxxx** (Region **2** in decimal)

In binary:

Binary		Decimal
Region	**Store**	
0001	0000	16 - Asia Region

0010	0000	32 - European Region

To include all the stores of a particular region, the last four bits of the wildcard mask must be set to 1 (15 in Decimal):

Binary		**Decimal**
Region	**Store**	
xxxx	1111	15 - all Asian stores
xxxx	1111	15 - all European stores

A wildcard object that represents all the Asian stores will look like this:

Wildcard IP address	192.30.16.1	(The region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30.**16-31**.1

A wildcard object that represents all the European stores will look like this:

Wildcard IP address	192.30.32.1	(the region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30.**32-47**.1

The administrator can now use these wildcard objects in the Access Control Policy:

Source	Destination	Action	Track
Asian Stores Wildcard	Database Server for Asia	Accept	Log
European Stores Wildcard	Database Server for Europe	Accept	Log

Scenario Three

In this scenario, the netmask bits are not consecutive.

Wildcard IP	1	1	0	1
Wildcard mask	0	0	5	0

Wildcard IP	00000001.00000001.00000000.00000001
Wildcard Mask	00000000.00000000.00000101.00000000

Mask:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0

Which will match only these IP addresses:

IP Address	Binary	Comment
1.1.0.1	00000001.00000001.00000000.00000001	The IP address itself
1.1.1.1	00000001.00000001.00000001.00000001	The equivalent bit at position 23 does not matter
1.1.4.1	00000001.00000001.00000100.00000001	The equivalent bit at position 21 does not matter
1.1.5.1	00000001.00000001.00000101.00000001	The equivalent bits at positions 21 and 23 do not matter

IPv6

The same principles apply to IPv6 addresses. For example, if the wildcard object has these values:

IPv6 Address	2001::1:10:0:1:41
Wildcard netmask	0::ff:0:0

The wildcard will match: 2001::1:10:0-255:1:41

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.

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 Security Gateways R80.10 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.

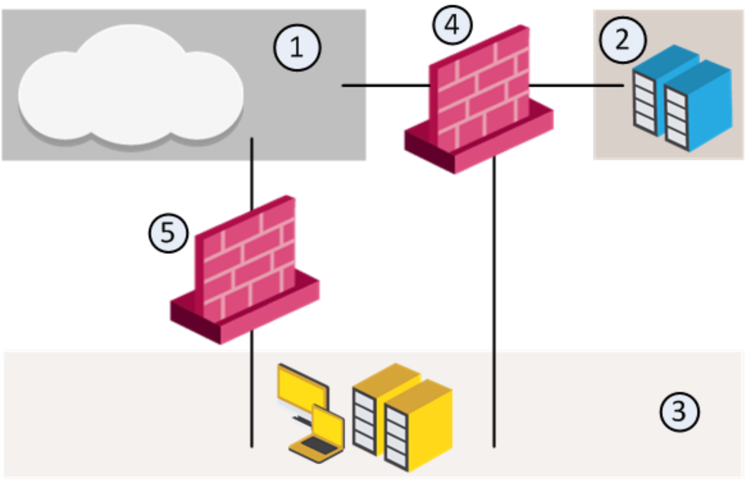
A Security Zone object represents a part of the network (for example, the internal network or the external network). You assign a network interface of a Security Gateway to a Security Zone. You can then use the Security Zone objects in the Source and Destination columns of the Rule Base.

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 (see *"Predefined Security Zones" on the next page*).
2. Assign Gateway interfaces to Security Zones (see *"Creating and Assigning Security Zones " below*).
3. Use the Security Zone objects in the Source and Destination of a rule. For example:

Source	Destination	VPN	Service	Action
InternalZone	ExternalZone	Any Traffic	Any	Accept

4. Install the Access Control Policy (see *"Installing the Access Control Policy" on page 277*).

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 Security Gateway 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.

Limitations

- NAT policy supports Security Zones only for R81 Security Gateways and higher.
- The Threat Prevention Policy supports Security Zones only for R81 Security Gateways and higher.
- If the clean-up rule contains Security Zones, it might prevent the creation of Drop templates for that rule.

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 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, see the *R80.40 VoIP Administration Guide*.

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:

OSE Device	Supported Versions
Cisco Systems	9.x, 10.x, 11.x, 12.x

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 (see *"OSE Device Properties Window - "General" Tab" below*).

   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 (see *"Anti-Spoofing Parameters and OSE Devices Setup (Cisco)" on the next page*).

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

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

- **HTTPS Inspection** - Consists of rules to inspect traffic encrypted by the Transport Layer Security (TLS) protocol between internal browser clients and web servers.

The installation process:

- Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

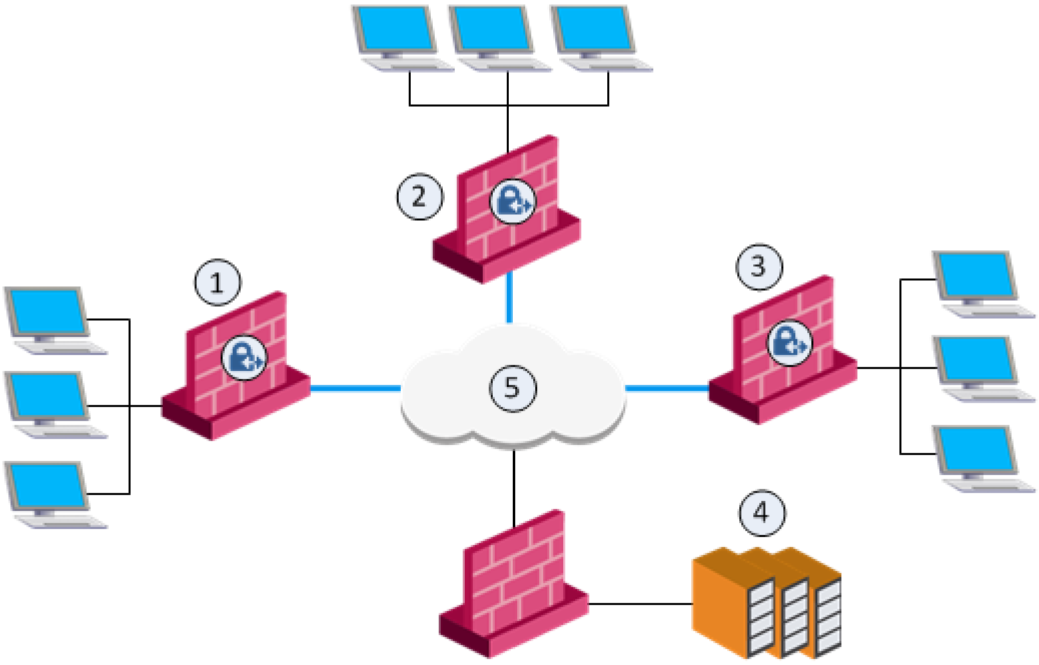
  If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

- 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:



Item	Security Gateway	Installed Software Blades
1	Sales California	Firewall, VPN
2	Sales Alaska	Firewall, VPN, IPS, DLP
3	Executive management	Firewall, VPN, QoS, and Mobile Access
4	Server farm	Firewall
5	Internet	

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 Security 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 Security Gateway that manages bandwidth.

  Install this policy package on the *executive management* Security Gateway.

- A policy package that includes the Desktop Security Policy type for the Security Gateway that handles Mobile Access.

  Install this policy package on the *executive management* Security 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 & HTTPS Inspection**
   - **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 Pol**

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 & HTTPS Inspection**
   - **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 and shows 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, 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 in the Expert mode:

```
fwm dbload <Main IP address of Name of Security Gateway Object>
```

For more information, see the R80.40 CLI Reference Guide - Chapter *Security Management Server Commands* - Section *fwm* - Sub-section *fwm dbload*.

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

Uninstalling the Access Control Policy

You can uninstall the Access Control policy using the command line interface on the Security Gateway.

To uninstall the Access Control policy

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Run:

```
fw unloadlocal
```

Warning

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

For more information, see the R80.40 CLI Reference Guide - Chapter *Security Gateway Commands* - Section *fw* - Sub-section *fw unloadlocal*.

For uninstalling other Security Policies, check the relevant Administration Guide.

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:
   - **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 (Audit logs) related to the rule 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

How to work with the policy installation history

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

- See the revisions that were installed on the Security 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 Security Gateway.
4. In the **Policy Installation History** section, select an installation date.
5. Perform the applicable action:
   - **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

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 VPN.
- 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

Information about these features is collected in one log:

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

The Columns of the Access Control Rule Base

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.

Column	Description
No	Rule number in the Rule Base Layer.
Hits	Number of times that connections match a rule. See *"Analyzing the Rule Base Hit Count" on page 279*.
Name	Name that the system administrator gives this rule.
Source **Destination**	Network objects that define: ■ Where the traffic starts ■ The destination of the traffic See *"Source and Destination Column" on the next page*.
VPN	The VPN Community to which the rule applies. See *"VPN Column" on the next page*.
Services & Applications	Services, Applications, Categories, and Sites. If Application & URL Filtering is not enabled, only Services show. See *"Services & Applications Column" on page 231*.
Content	The data asset to protect, for example, credit card numbers or medical records. You can set the direction of the data to Download Traffic (into the organization), Upload Traffic (out of the organization), or Any Direction. See *"Content Column" on page 234*.
Action	Action that is done when traffic matches the rule. Options include: Accept, Drop, Ask, Inform (UserCheck message), Inline Layer, and Reject. See *"Actions" on page 236*.
Track	Tracking and logging action that is done when traffic matches the rule. See *"Tracking Column" on page 237*.
Install On	Network objects that will get the rule(s) of the policy. See *"Installing the Access Control Policy" on page 277*.

Column	Description
Time	Time period that this rule is enforced.
Comment	An optional field that lets you summarize the rule.

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 (see *"More Network Object Types" on page 207*):

- Network
- Host
- Zones
- Dynamic Objects
- Domain Objects
- Access Roles
- Updatable Objects

To Learn More About Network Objects

You can add network objects to the **Source** and **Destination** columns of the Access Control Policy. See *"Managing Objects" on page 201*.

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 Security Gateway, the Security 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 Security Gateways. If the Security 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 Security Gateways and clients. Use SmartConsole 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.

To Learn More About VPN

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

- *R80.40 Site to Site VPN Administration Guide*
- *R81 Remote Access VPN Administration Guide*
- *R80.40 Mobile Access Administration Guide*

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 Security Gateway identifies (*matches*) a service according to *IP protocol*, TCP and UDP *port number*, and *protocol signature*.

To make it possible for the Security Gateway to match services by protocol signature, you must enable **Application & URL Filtering** on the Security Gateway and on the Ordered Layer.

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

Application - Match Setting	Checkbox: Match web application on 'Any' port when used in 'Block' rule	Blocked Application is Matched on Service
Recommended services (default)	Selected (default)	Any
Recommended services (default)	Not selected	Recommended services
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. See 165094.

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 R77.30 and Lower Security Gateways, and after Upgrade

For Security Gateways R77.30 and lower:

- The Security Gateway matches TCP and UDP services by *port* number. The Security Gateway cannot match services by protocol signature.
- The Security Gateway matches applications by the application signature.

When you upgrade the Security Management Server to R80 and higher and the Security Gateways to R80.10 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 Security Gateway 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

Notes:

- Websocket content is not inspected.
- HTTP connections that are not RFC-compliant are not inspected.
- If an inline layer has **Archive File** in the content column of the parent rule, and another value in the content column in one of the sub-rules (for example: Presentation File), then if the matched archive includes the other value (in this example: a presentation file), the rule is not matched. Use a regular rule for both content types.
- If a content column of a rule includes the **Compound Data Type Group** or **Traditional Data Type Group** with an **Archive File** Data Type and another Data Type (for example: **PCI - Credit Card Numbers**), then if an archive file which contains a file with credit cards is uploaded or downloaded, the rule is not matched.
- If a rule with **Archive File** in the content column is matched, and a lower rule in the Rule Base has a Data Type which is contained in the archive file, then the lower rule in the Rule Base is matched as well.

Limitations:

- Content Awareness supports more than 60 character sets (charsets) for text files, including Japanese, Korean, Greek, and Arabic. If the inspected traffic does not include a supported charset, uses UTF-8 for decoding. To see the list of supported charsets, and to learn how to change the default charset, see sk116155.
- Content Awareness supports Data Types based on file name. For specific HTTP traffic where the file name is not part of the URL or content-disposition header, the file name may be incorrect.

To learn more about the Data Types, open the Data Type object in SmartConsole and press the **?** button (or **F1** key) 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 *R80.40 Data Loss Prevention Administration Guide*.

Actions

Action	Meaning
Accept	Accepts the traffic
Drop	Drops the traffic. The Security Gateway 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.
Ask	Asks the user a question and adds a confirmatory check box, or a reason box. Uses a UserCheck object.
Inform	Sends a message to the user attempting to access the application or the content. Uses a UserCheck object.
To see these actions, right-click and select **More**:	
Reject	Rejects the traffic. The Security Gateway sends an RST packet to the originating end of the connection and the connection is closed.
UserCheck Frequency	Configure how often the user sees the configured message when the action is ask, inform, or block.

Action	Meaning
Confirm UserCheck	Select the action that triggers a UserCheck message: ▪ **Per rule** - UserCheck message shows only once when traffic matches a rule. ▪ **Per category** - UserCheck message shows for each matching category in a rule. ▪ **Per application/Site** - UserCheck message shows for each matching application/site in a rule. ▪ **Per Data type** - UserCheck message shows for each matching data type.
Limit	Limits the bandwidth that is permitted for a rule. Add a **Limit** object to configure a maximum throughput for uploads and downloads.
Enable Identity Captive Portal	Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.
	Important - A rule that drops traffic, with the **Source** and **Destination** parameters defined as **Any**, also drops traffic to and from the Captive Portal.

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 *R80.40 Logging and Monitoring Administration Guide*.

Rule Matching in the Access Control Policy

The Security Gateway determines the rule to apply to a connection. This is called *matching* a connection. Understanding how the Security Gateway 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 Security Gateway matches connections.

Note that these Rule Bases intentionally do not follow the best practices for Access Control Rules (see *"Best Practices for Access Control Rules" on page 276*). This is to make the explanations of rule matching clearer.

Rule Base Matching - Example 1

For this Rule Base:

No	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	ftp-pasv	Download executable file	Drop
2	Any	Any	Any	Executable file	Accept
3	Any	Any	Gambling (Category)	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure for an FTP connection:

Part of connection	Security Gateway action	Inspection result
SYN	Run the Rule Base: Look for the first rule that matches: ▪ Rule 1 - Match.	Final match (drop on rule 1). Shows in the log. The Security Gateway does not turn on the inspection engines for the other rules.

Rule Base Matching - Example 2

For this Rule Base:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (category)	Any	Drop
3	Any	Any	ftp	Any	Drop
4	Any	Any	Any	Any	Accept

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:

Part of connection	Security Gateway action	Inspection result
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 Security Gateway 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.
	Optimize the Rule Base matching. Look for the first rule that matches: ▪ Rule 1 - Possible match. ▪ Rule 2 - No match. ▪ Rule 3 - No match. ▪ Rule 4 - Match.	Possible match (Continue to inspect the connection).

Part of connection	Security Gateway action	Inspection result
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:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (Category)	Any	Drop
3	Any	Any	Any	Any	Accept

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:

Part of connection	Security Gateway action	Inspection result
SYN	Run the Rule Base. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - Possible match. ■ Rule 3 - Match.	Possible match (Continue to inspect the connection).

Part of connection	Security Gateway action	Inspection result
HTTP Header	The Security Gateway turns on inspection engines to examine the content 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: Business (Category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - No match. ■ Rule 3 - Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Content: Executable file.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Match. ■ Rule 2 - No match. ■ Rule 3 - Match.	Final match (drop on rule 1). Shows in the log.

The matching examples show that:

- The Security Gateway sometimes runs the Rule Base more than one time. Each time it runs, the Security Gateway 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 Security Gateway:
  - Turns on one or more inspection engines.
  - Postpones making the final match decision until it has inspected the body of the connection.

- The Security Gateway searches for the first rule that applies to (*matches*) a connection. If the Security Gateway does not have all the information it needs to identify the matching rule, it continues to inspect the traffic.

Creating a Basic Access Control Policy

A Security Gateway 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

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.)

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Admin Access to Security Gateways	Admins (Access Role)	Group of Security Gateways	Any	Accept	Log	Policy Targets
2	Stealth	Any	Group of Security Gateways	Any	Drop	Alert	Policy Targets

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
3	Critical subnet	Internal	Finance HR R&D	Any	Accept	Log	CorpGW
4	Tech support	TechSupport	Remote1-web	HTTP	Accept	Alert	Remote1GW
5	DNS server	Any	DNS	Domain UDP	Accept	None	Policy Targets
6	Mail and Web servers	Any	DMZ	HTTP HTTPS SMTP	Accept	Log	Policy Targets
7	SMTP	Mail	NOT Internal net group	SMTP	Accept	Log	Policy Targets
8	DMZ & Internet	IntGroup	Any	Any	Accept	Log	Policy Targets
9	Cleanup rule	Any	Any	Any	Drop	Log	Policy Targets

Explanations for rules:

Rule	Explanation
1	**Admin Access to Gateways** - SmartConsole administrators are allowed to connect to the Security Gateways.
2	**Stealth** - All internal traffic that is NOT from the SmartConsole administrators to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.
3	**Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and R&D.
4	**Tech support** - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.

Rule	Explanation
5	**DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.
6	**Mail and Web servers** - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.
7	**SMTP** - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.
8	**DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.
9	**Cleanup rule** - Drops all traffic that does not match one of the earlier rules.

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.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Critical subnet	Internal	Finance HR	Any	Any	Accept	Log
2	SMTP	Mail	NOT internal network (Group)	smtp	Any	Accept	Log
3	R&D department	R&D Roles	Any	Any	Any	TechSupport Layer	N/A
3.1	R&D servers	Any	R&D servers (Group) QA network	Any	Any	Accept	Log

No	Name	Source	Destination	Services & Applications	Content	Action	Track
3.2	R&D source control	InternalZone	Source control servers (Group)	ssh http https	Any	Accept	Log
---	---	---	---	---	---	---	---
3.X	Cleanup rule	Any	Any	Any	Any	Drop	Log
4	QA department	QA network	Any	Any	Any	QA Layer	N/A
4.1	Allow access to R&D servers	Any	R&D Servers (Group)	Web Services	Any	Accept	Log
---	---	---	---	---	---	---	---
4.Y	Cleanup rule	Any	Any	Any	Any	Drop	Log
5	Allow all users to access employee portal	Any	Employee portal	Web Services	Any	Accept	None
---	---	---	---	---	---	---	---
9	Cleanup rule	Any	Any	Any	Any	Drop	Log

Explanations for rules:

Rules	Explanation
1 2	General rules for the whole organization.

Rules	Explanation
3 3.1 3.2 --- 3.X	An Inline Layer for the R&D department. Rule 3 is the parent rules of the Inline Layer. The **Action** is the name of the Inline Layer. **If a packet does not match on parent rule 3:** Matching continues to the next rule outside the Inline Layer (rule 4). **If a packet matches on parent rule 3:** 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. 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. 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.
4 4.1 --- 4.Y	Another Inline Layer, for the QA department.
5	More general rules for the whole organization.
--	One or more rules.
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 **Logs & Monitor** > **New Tab** > **Views**.

Best Practice - Do not use Application Control and URL Filtering in the same rule, this may lead to wrong rule matching. Use Application Control and URL Filtering in separate rules. This makes sure that the URL Filtering rule is used as soon as the category is identified. For more information, see sk174045.

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:
     a. Start to type "face" in the Search field. In the Available list, see the **Facebook** application.
     b. Click each item to see more details in the description pane.
     c. Select the items to add to the rule.

     Note - Applications are matched by default on their **Recommended** services. You can change this (see *"Configuring Matching for an Allowed Application" on page 231*). Each service runs on a specific port. The recommended **Web Browsing Services** are `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.
   - **Action** - Select **Accept**

- **Track** - Select **Log**
- **Install On** - Keep it as **Policy Targets** for or all Security Gateways, or choose specific Security Gateways, on which to install the rule

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.

Name	Source	Destination	Services & Applications	Action	Track	Install On
Block Porn	Any	Internet	Pornography (category)	Drop Blocked Message	Log	Policy Targets

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 231*.
   - **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**.

Name	Source	Destination	Services and Applications	Action	Track	Install On	Time
Limit Streaming Media	Any	Internet	Media Streams (Category)	Accept Upload_ 1Gbps	Log	All	Off-Work

Important:

- In ClusterXL Load Sharing modes, the specified bandwidth limit is divided between all configured Cluster Members, regardless of the cluster state. For example, if a maximum limit requirement is 30 Gbps, and there are three Cluster Members, you must configure the Limit object in the rule to 30 Gbps / 3 = 10 Gbps.
- In a Scalable PlatformSecurity Group, the specified bandwidth limit is divided between all Security Group Members, regardless of their state. For example, if a maximum limit requirement is 30 Gbps, and there are three Security Group Members, you must configure the Limit object in the rule to 30 Gbps / 3 = 10 Gbps.

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**

Name	Source	Destination	Services & Applications	Action	Track	Install On
Allow Radmin to Identified Users	Identified_ Users	Internet	Radmin	Allow	Log	All
Block other Remote Admins	Any	Internet	Remote Administration	Block	Log	All

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.

For more about Access Roles and Identity Awareness, see the *R80.40 Identity Awareness Administration Guide*.

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/Site > Application/Site 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.

Name	Source	Destination	Services & Applications	Action	Track
Block sites that may cause a liability	Identified_ Users	Internet	Liability_Sites	Drop	Log

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" on page 248*.

Ordered Layers and Inline Layers

A policy is a set of rules that the Security 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.

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.
- Reuse Ordered Layers in multiple Policy packages, and reuse Inline Layers in multiple Layers.
- 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

The Ordered Layer can contain Inline Layers.

This is an example of an Inline Layer:

No.	Source	Destination	VPN	Services	Action
1					
2	Lab_network	Any	Any	Any	Lab_rules
2.1	Any	Any	Any	https http	Allow
2.2	Any	Any	Any	Any	Drop
3					

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 Security Gateway 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.

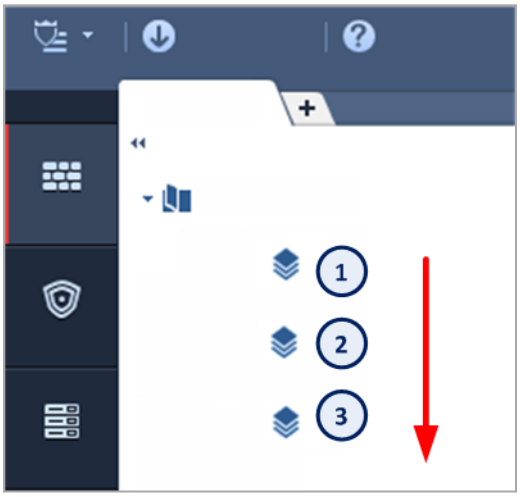
- If none of the higher rules in the Ordered Layer match the packet, the explicit **Cleanup Rule** is applied (Rule 2.2). If this rule is missing, the **Implicit Cleanup Rule** is applied (see *"Types of Rules in the Rule Base" on page 260*). No more rule matching is done.

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 Security Gateway, the Security 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 Security Gateway stops matching against later rules in the Policy Rule Base and drops the packet. If the **Action** is **Accept**, the Security Gateway continues to check rules in the next Ordered Layer.



Item	Description
1	Ordered Layer 1
2	Ordered Layer 2
3	Ordered Layer 3

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** is applied (see *"Types of Rules in the Rule Base" on page 260*).

Every Ordered Layer has its own implicit cleanup rule. You can configure the rule to *Accept* or *Drop* in the **Layer settings**. (see *"Configuring the Implicit Cleanup Rule" on page 262*).

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 Security Gateway 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* (see *"Types of Rules in the Rule Base" on page 260*).

   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. (see *"Types of Rules in the Rule Base" on page 260*).

Creating a 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 SmartConsole 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 SmartConsole session.

Security Gateways R77.30 or lower: 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 **Application & URL Filtering**.

   c. Click **OK** and the **Layer Editor** window closes.

   d. Click **OK** and the **Policy** window closes.

6. Publish the SmartConsole 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.
- Ordered Layers and Inline Layers of the Policy. Here you can enable:
  - Firewall. This includes VPN (see *"VPN Column" on page 229*).
  - Application & URL Filtering (see *"Services & Applications Column" on page 231*).
  - Content Awareness (see *"Content Column" on page 234*).
  - Mobile Access (see *"Mobile Access to the Network" on page 363*).

Enabling Access Control Features on a Security Gateway

1. In SmartConsole, from the left navigation panel, click **Gateways & Servers** and double-click the Security Gateway object.

   The **General Properties** window of the Security 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.
   - Application & 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
   - Application & 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 Security Gateways R80.10 and higher, 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 Security Gateways R77.30 and lower, 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 fails on Security Gateway R77.30 or lower.

Order in which the Security Gateway 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** (see *"Types of Rules in the Rule Base" on the previous page*).
6. Click **OK** and install the policy.

Showing 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 SmartConsole 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.

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 SmartConsole 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. In SmartConsole, install the policy.
8. Repeat this procedure for all policy packages.

For examples of Inline Layers and Ordered Layer, see *"Use Cases for the Unified Rule Base" on the next page*.

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. (see *"Sharing Layers" on page 262*).
- **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**.

Use Cases for the Unified Rule Base

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

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.

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
General compliance (1)								
1	Block categories	Any	Internet	Any	Anonymizer Critical Risk	Any	Drop Block Message	Log
Block risky executables (2)								
2	Block download of executable files from uncategorized and high risk sites	Internal Zone	Internet	Any	Uncategorized High Risk	Download Traffic Executable File	Drop	Log
Credit card data (3-4)								
3	Allow uploading of credit cards numbers, by finance, and only over HTTPS	Finance (Access Role)	Web Servers	Any	https	Upload Traffic PCI - Credit Card Numbers	Accept	Log

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
4	Block other credit cards from company Web servers	Any	Web Servers	Any	Any	Any Direction PCI - Credit Card Numbers	Drop	Log
Inform about sensitive data over VPN (5)								
5	Inform the user about sensitive data from VPN sites	Any	Any	RemoteAccess	Any	Any Direction Salary Survey Report	Inform	Log
Cleanup (6)								
6	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Explanations for rules:

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

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.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Headquarter WEB traffic - via proxy	HQ	Proxy	Web Proxy	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
2	Allow Proxy to the Internet	Proxy	Internet	Web	Any	Accept	None
3	Allow local branch to access the internet directly	Local Branch	Internet	Web	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
4	Web Servers	InternalZone	Web Servers	Web	Any	Web Servers protection	N/A

No	Name	Source	Destination	Services & Applications	Content	Action	Track
4.1	Block browsing with unapproved browsers	Any	Any	NEGATED Google Chrome Internet Explorer 11 Firefox Safari	Any	Drop	Log
4.2	Inform user when uploading Credit Cards only over HTTPS	Any	Any	https	Upload Traffic PCI - Credit Card Numbers	Inform Access Noti... once a day per applic...	Log
4.3	Block Credit Cards	Any	Any	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
4.4	Block downloading of sensitive content	Any	Any	Any	Download Traffic HIPAA - Medical Record Headers	Drop	Log
4.5	Cleanup rule	Any	Any	Any	Any	Accept	None

No	Name	Source	Destination	Services & Applications	Content	Action	Track
5	Ask user when sending credit cards to PayPal	InternalZone	Internet	PayPal	Any Direction PCI - Credit Card Numbers	Ask Company Policy Access Noti... once a day per applic...	Log
6	Cleanup rule	Any	Any	Any	Any	Drop	Log

Explanations for rules:

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.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
Regulatory compliance							
1	Block the download of executable files	InternalZone	Internet	Any	Download Traffic Executable file	Drop	Log
2	Allow uploading of credit cards numbers by finance users, only over HTTPS	Finance (Access Role)	Web Servers	https	Upload Traffic PCI - Credit Card Numbers	Accept	Log
3	Block other credit cards from company Web servers	InternalZone	Web Servers	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
Personally Identifiable Information							
4	Matches U.S. Social Security Numbers (SSN) allocated by the U.S. Social Security Administration (SSA).	InternalZone	Internet	Any	Upload Traffic U.S. Social Security Numbers - According to SSA	Inform Access Notifi... once a day per applicati...	Log

No	Name	Source	Destination	Services & Applications	Content	Action	Track
5	Block downloading of sensitive medical information	InternalZone	Internet	Any	Download Traffic HIPAA - Medical Records Headers	Drop Block Message	Log
Human Resources							
6	Ask user when uploading documents containing salary survey reports.	InternalZone	Internet	Any	Upload Traffic Salary Survey Report	Ask Company Policy once a day per applicati...	Log
Intellectual Property							
7	Matches data containing source code	InternalZone	Internet	Any	Any Direction Source Code	Restrict source code	N/A
7.1		Any	Any	Any	Download Traffic Source Code	Accept	Log
7.2		Any	Any	Any	Upload Traffic Source Code	Ask Company Policy once a day per applicati...	Log

No	Name	Source	Destination	Services & Applications	Content	Action	Track
7.3	Cleanup Inline Layer	Any	Any	Any	Any	Drop Block Message	Log

Explanations for rules:

Rule	Explanation
1-3	**Regulatory Compliance** section - Controls 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.
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 (see *"Ordered Layers and Inline Layers" on page 253*). 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.)

No.	Name	Source	Destination	Services & Applications	Action	Track	Time
1	Liability sites	Any	Internet	Potential liability (group)	Drop Blocked Message	Log	Any
2	High risk applications	Any	Internet	High Risk iTunes Anonymizer (category)	Drop Blocked Message	Log	Any
3	Allow IT department Remote Admin	IT (Access Role)	Any	Radmin	Allow	Log	Work-Hours
4	Allow Facebook for HR	HR (Access Role)	Internet	Facebook	Allow Download_1Gbps	Log	Any
5	Block these categories	Any	Internet	Streaming Media Protocols Social Networking P2P File Sharing Remote Administration	Drop Blocked Message	Log	Any
6	Log all applications	Any	Internet	Any	Allow	Log	Any

Explanations for rules:

Rule	Explanation
1	**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. See *"Blocking Sites" on page 252*. *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/Site > Application/Site 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**

<table>
<tr><th>Rule</th><th>Explanation</th></tr>
<tr><td></td><td>

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>
<tr><th>Name</th><th>Source</th><th>Destination</th><th>Services & Applications</th><th>Action</th><th>Track</th></tr>
<tr><td>Block sites that may cause a liability</td><td>Identified_ Users</td><td>Internet</td><td>Liability_Sites</td><td>Drop</td><td>Log</td></tr>
</table>

</td></tr>
<tr><td>2</td><td><b>High risk applications</b> - Blocks traffic to sites and applications in the <i>High Risk</i> category and blocks the <i>iTunes</i> application. The UserCheck <i>Block Message</i> is shown to users and explains why their traffic is blocked.</td></tr>
<tr><td>3</td><td><b>Allow IT department Remote Admin</b> - Allows the computers in the <code>IT</code> department network to use the <i>Radmin</i> application. Traffic that uses <i>Radmin</i> is allowed only during the <i>Work-Hours</i> (set to 8:00 through 18:30, for example).</td></tr>
<tr><td>4</td><td><b>Allow Facebook for HR</b> - Allows computers in the <code>HR</code> network to use <i>Facebook</i>. The total traffic downloaded from <i>Facebook</i> is limited to 1 Gbps, there is no upload limit.</td></tr>
<tr><td>5</td><td><b>Block these categories</b> - Blocks traffic to these categories: <i>Streaming Media</i>, <i>Social Networking</i>, <i>P2P File Sharing</i>, and <i>Remote Administration</i>. The UserCheck <i>Blocked Message</i> is shown to users and explains why their traffic is blocked.
<b>Note</b> - The <i>Remote Administration</i> category blocks traffic that uses the <code>Radmin</code> application. If this rule is placed before rule 3, then this rule can also block <i>Radmin</i> for the IT department.</td></tr>
<tr><td>6</td><td><b>Log all applications</b> - Logs all traffic that matches any of the URL Filtering and Application Control categories.</td></tr>
</table>

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 Security Gateways R80.10 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 the XFF inspection, unless the Security Gateway is behind a proxy server. For more, see 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 Security 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 *Any* in the Source and in the Destination, and with an Application or a Data Type. For example these rules are not recommended:

Source	Destination	Services & Applications	Content
Any	Any	Facebook	
Any	Any		Credit Card numbers

Instead, define one of these recommended rules:

Source	Destination	Services & Applications	Content
Any	Internet	Facebook	
Any	Server		Credit Card numbers

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

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

4. For rules with Data Types: Place rules that check File Types higher in the Rule Base than rules that check for Content Types. See *"Content Column" on page 234*.

   Reason: File Types are matched sooner than Content Types.

5. Do not use Application Control and URL Filtering in the same rule, this may lead to wrong rule matching. Use Application Control and URL Filtering in separate rules. This makes sure that the URL Filtering rule is used as soon as the category is identified. For more information, see sk174045.

To see examples of some of these best practices, see the *"Use Cases for the Unified Rule Base" on page 264* and *"Creating a Basic Access Control Policy" on page 242*.

Installing the Access Control Policy

1. On the Global Toolbar, click **Menu** > **Publish session**.
2. On the Global Toolbar, click **Menu** > **Verify Access Control Policy** > select the required policy > click **Verify**.
3. Alternatively, click the left **Security Policies** view > **Access Control** > from the top toolbar, click **Actions** > **Verify Access Policy**

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

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

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

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

7. If there is more than one Security Gateway: Select the Security Gateways, on which to install the policy.

8. Select the **Install Mode**:

   - **Install on each selected gateway independently** - Install the policy on each target Security 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 Security 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 Security Gateways. If the policy fails to install on one of the Security Gateways, the policy is not installed on other target Security Gateways.

9. Click **Install**.

Pre-R80.10 and the Unified Access Control Policy

When you upgrade an R77.30 or lower Security Management Server, which manages R77.30 or lower Security Gateways, to R80.10 or higher, the existing Access Control policies are converted in this way:

- The pre-R80.10 **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-R80.10 **Application & URL Filtering** policy is converted into the **Application** Policy Layer, which is the second Layer of the R80.x 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 fails.

New Access Control Policy for pre-R80.10 Security Gateways on an R80.x 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.

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 connection.

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 (version R75.40 and higher). 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. 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.

Hit Count Display

Configuring the Hit Count Display

These are the options you can configure for how matched connection data is shown in the **Hits** column:

- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total Hit Count for:

  - Security Gateways that are not supported
  - Security Gateways that have disabled the Hit Count feature

  The values are shown with these letter abbreviations:

  - K = 1,000
  - M = 1,000,000
  - G = 1,000,000,000
  - T = 1,000,000,000,000

  For example, 259K represents 259 thousand connections and 2M represents 2 million connections.

- **Percentage** - Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.
- **Level** - The Hit Count level is a label for the range of hits according to the table.

  The Hit Count range = Maximum hit value - Minimum hit value (does not include zero hits)

Hit Count Level	Icon	Range
Zero	▱▱▱▱▱	0 hits
Low	▰▱▱▱▱	Less than 10 percent of the Hit Count range
Medium	▰▰▱▱▱	Between 10 - 70 percent of the Hit Count range
High	▰▰▰▰▱	Between 70 - 90 percent of the Hit Count range
Very High	▰▰▰▰▰	Above 90 percent of the Hit Count range

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**.

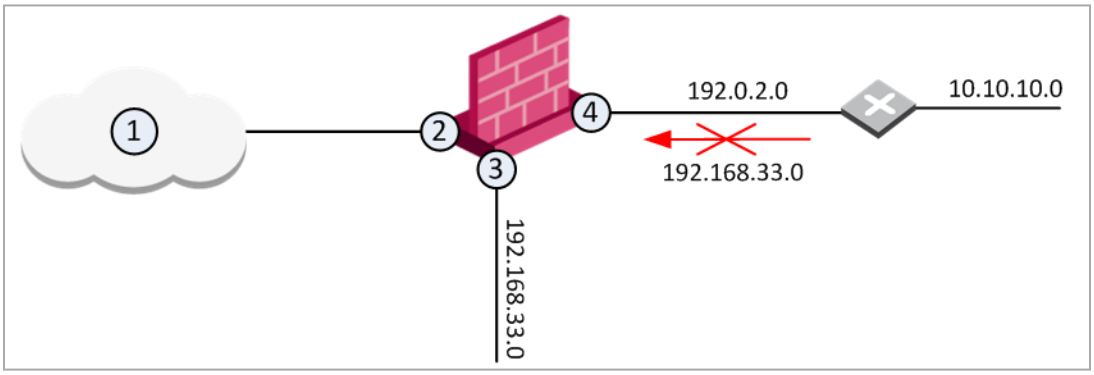
Preventing IP Spoofing

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 Security Gateway with interfaces 2 and 3, and 4, and some example networks behind the interfaces.



For the Security 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, from the left navigation panel, click **Gateways & Servers** and double-click the Security Gateway object.

   The **Gateway Properties** window opens.

2. From the navigation tree, select **Network Management**.
3. Click **Get Interfaces**.
4. Click **Accept**.

   The Security 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, click **General**.
7. In the **Topology** section of the page, click **Modify**.

   The **Topology Settings** window opens.

8. In the **Leads To** section, select the type of network, to which this interface leads:

   - **Internet (External)** - This is the default setting. It is automatically calculated from the topology of the Security Gateway. To update the topology of an internal network after changes to static routes, click **Network Management** > **Get Interfaces** in the **Gateway Properties** window.
   - **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
  - **Network defined by routes** - The Security Gateway dynamically calculates the topology behind this interface. If the network of this interface changes, there is no need to click **Get Interfaces** and install a policy. For more, see the section *Dynamically Updating the Topology*.
  - **Specific** - A specific 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, select **User defined**, check **Specify Security Zone** and choose the zone of the interface.
10. Configure **Anti-Spoofing** options (see *"Anti-Spoofing Options" on the next page*). 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 Access Control 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 Security 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 Security 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 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 Security 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.

Configuring the NAT Policy

This chapter outlines the process of configuring NAT64 (Network Address Translation from IPv6 to IPv4) on a Check Point Security Gateway.

NAT64 is a technology that enables communication between IPv6-only clients and IPv4-only servers. The configuration involves defining rules on a Check Point Security Gateway to translate packet headers using the IPv4/IPv6 Translation Algorithm (RFC 6145). The Security Gateway performs N:M translation, supporting scenarios like Hide NAT behind a single IPv4 address or a range of addresses.

Getting Started with NAT

1. Learn about types of NAT Rules and types of NAT Methods (below in this topic).
2. Follow the applicable procedure:
   - *"Working with Automatic NAT Rules" on page 295* (for IPv4 or IPv6 translation)
   - *"Working with Manual NAT Rules" on page 304* (for IPv4 or IPv6 translation)
   - *"Working with NAT46 Rules" on page 310* (for IPv4-to-IPv6 translation)
   - *"Working with NAT64 Rules" on page 325* (for IPv6-to-IPv4 translation)
3. Configure the applicable NAT advanced settings (see *" Advanced NAT Settings" on page 345*).
4. Install the Access Control Policy.

Introduction

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. NAT protects the identity of a network and does not show internal IP addresses to the Internet.

The Security Gateway can change:

- The source IP address in a packet.
- The destination IP address in a packet.
- The TCP / UDP port in a packet.

Example flow

1. An internal computer sends a packet to an external computer
2. The Security Gateway translates the source IP address to a new one.
3. The packet comes back from the external computer

4. The Security Gateway translates the new IP address back to the original IP address.
5. The packet from the external computer goes to the correct internal computer.

Types of NAT Rules

In SmartConsole, you can create these types of NAT rules:

NAT Rules	How to create these NAT rules?	How to change these NAT rules?
Automatic NAT Rules	Management Server creates these rules automatically based on the NAT settings you configure in objects' properties (on the **NAT** page)	You must change the NAT settings in objects' properties on the **NAT** page.
Manual NAT Rule	You create these rules, select all objects and the NAT method.	You change these rules.

Important - A Security Management Server / Domain Management Server supports a maximum of 16384 NAT rules in one policy. See sk82220.

Types of NAT Methods

You can configure one of these NAT methods for Automatic NAT Rules and in Manual NAT Rules:

Hide

The Security Gateway changes the source IP address of all connections from a source to the same IP address - either that of the Security Gateway's outgoing interface, or an IP address you configure.

Hide > Hide behind gateway

The Security Gateway changes the source IP address of all connections from a source to the same IP address of the Security Gateway's outgoing interface.

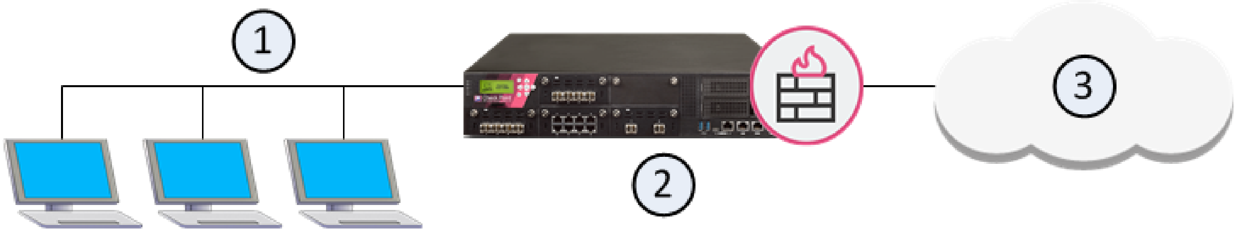
Hide > Hide behind IP address

The Security Gateway changes the source IP address of all connections from a source to the same IP address your configure.

Notes:

- When you configure Hide NAT, connections can only start from internal computers.
  The Security Gateway does **not** allow external traffic to access internal resources.
- If you enable this configuration in an object that represents one IP address (a Host object), then this gives you a one-to-one address translation.
- If you enable this configuration in an object that represents many IP addresses (a Network object, an Address Range object), then this gives you a many-to-one address translation.
- The Security Gateway uses port numbers to translate all specified internal IP addresses to a single external IP address - port numbers from 600 to 1023, and from 10,000 to 60,000.
  The Security Gateway can translate up to 50,000 connections at the same time.
- 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.

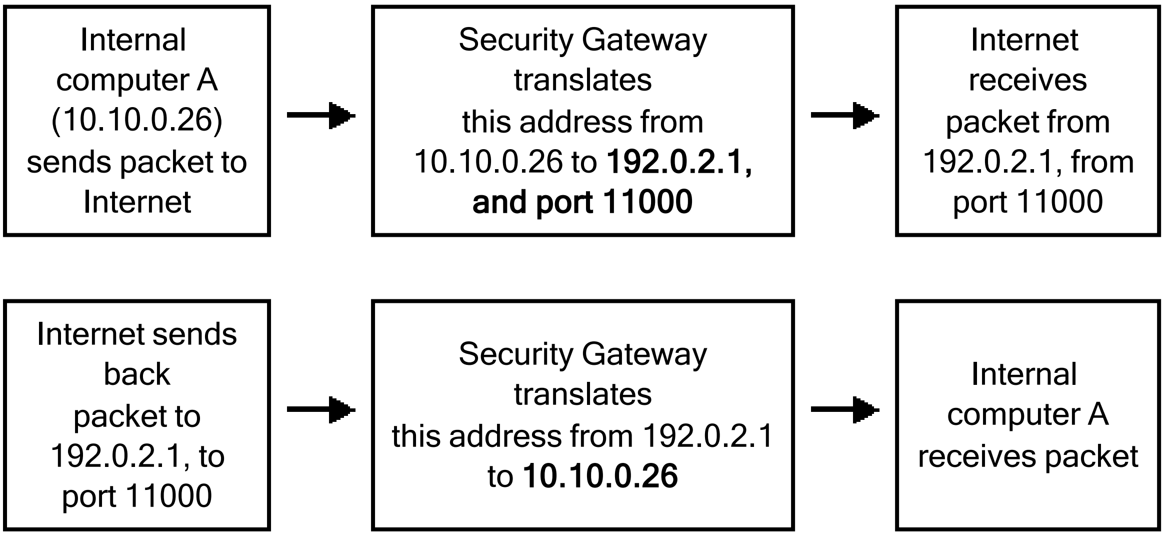
Example diagram



Item	Description
1	Internal computers
2	Security Gateway configured with Hide NAT
3	External computers and servers on the Internet

Sample Hide NAT Workflow

1. Internal computer A (10.10.0.26) sends a packet to an external computer.
2. The Security Gateway intercepts the packet and translates the source IP address from (10.10.0.26) to 192.0.2.1, and port 11000.
3. The external computer sends back a packet to 192.0.2.1, to port 11000.
4. The Security Gateway translates the packet's IP address from 192.0.2.1 to 10.10.0.26 and sends it to internal computer A.



Internal computer A (10.10.0.26) sends packet to Internet

Security Gateway translates this address from 10.10.0.26 to **192.0.2.1, and port 11000**

Internet receives packet from 192.0.2.1, from port 11000

Internet sends back packet to 192.0.2.1, to port 11000

Security Gateway translates this address from 192.0.2.1 to **10.10.0.26**

Internal computer A receives packet

Static

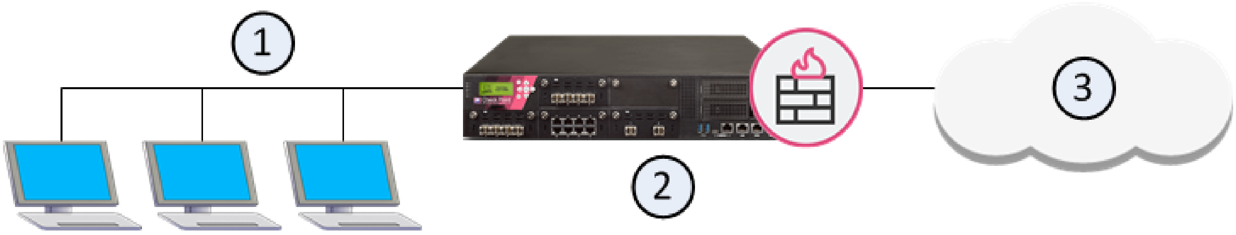
The Security Gateway changes the source IP address of all connections from a source to the IP address your configure.

Notes:

- When you configure Static NAT, the Security Gateway allows external traffic to access internal resources.
- If you enable this configuration in an object that represents one IP address (a Host object), then this gives you a one-to-one address translation.
- If you enable this configuration in an object that represents many IP addresses (a Network object, an Address Range object), then this gives you a many-to-one address translation.
  The Security Gateway translates each internal IP address to a different external IP address.

  Important - The range of the translated IP addresses is the same as the range of the source IP addresses.

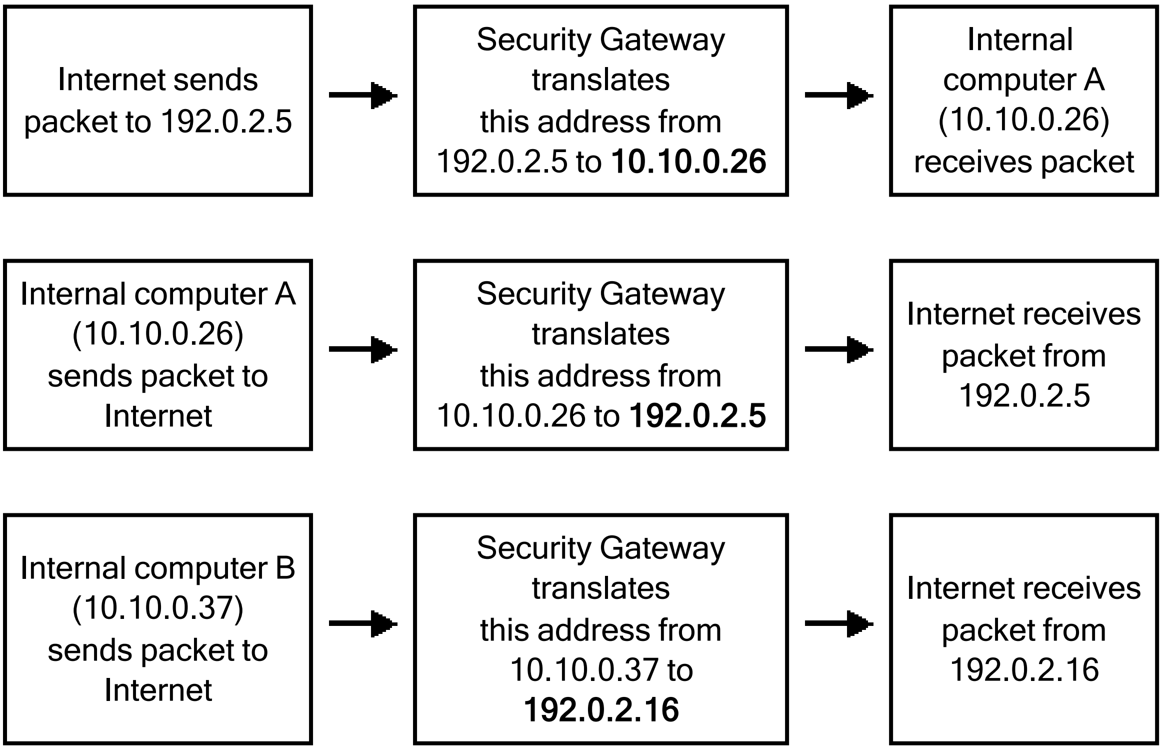
Example diagram



Item	Description
1	Internal computers
2	Security Gateway configured with Static NAT
3	External computers and servers on the Internet

Example traffic flow with Static NAT

1. An external computer on the Internet sends a packet to 192.0.2.5.
2. The Security Gateway translates the IP address from 192.0.2.5 to 10.10.0.26 and sends the packet to internal computer A.
3. Internal computer A (10.10.0.26) sends back a packet to the external computer.
4. The Security Gateway intercepts the packet and translates the source IP address from 10.10.0.26 to 192.0.2.5.
5. Internal computer B (10.10.0.37) sends a packet to an external computer.
6. The Security Gateway intercepts the packet translates the source IP address from 10.10.0.37 to 192.0.2.16.


Internet sends packet to 192.0.2.5
Security Gateway translates this address from 192.0.2.5 to **10.10.0.26**
Internal computer A (10.10.0.26) receives packet
Internal computer A (10.10.0.26) sends packet to Internet
Security Gateway translates this address from 10.10.0.26 to **192.0.2.5**
Internet receives packet from 192.0.2.5
Internal computer B (10.10.0.37) sends packet to Internet
Security Gateway translates this address from 10.10.0.37 to **192.0.2.16**
Internet receives packet from 192.0.2.16

NAT Rules in SmartConsole

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

- **Original** - with columns **Source**, **Destination**, and **Services**
- **Translated** - with columns **Source**, **Destination**, and **Services**

Example of Automatic NAT Rules

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for X (Y-Z)								
1	Object1	Object2	`Any`	`= Original`	`= Original`	`= Original`	`Policy Targets`	
2	Object3	Object4	`Any`	S Object5	S Object6	`= Original`	`Policy Targets`	
3	Object7	Object8	`Any`	H Object9	H Object10	`= Original`	`Policy Targets`	

Example of a Manual NAT rule

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
Manual Lower Rules								
4	Object11	Object12	`Any`	S Object13	`= Original`	`= Original`	`Policy Targets`	
5	Object14	Object15	`Any`	`= Original`	S Object16	`= Original`	`Policy Targets`	

Order of NAT Rule Enforcement

The Security Gateway enforces the NAT Rule Base in a sequential manner - in the order you place the rules in the NAT Policy (see the **No.** column).

The Security Gateway enforces Automatic NAT and Manual NAT rules in different ways.

Explanation

- **Manual NAT rules** - The Security Gateway enforces the first Manual NAT rule that matches a connection. The Security Gateway does not examine other Manual NAT rules.
- **Automatic NAT rules** - The Security Gateway can enforce two Automatic NAT rules that match a connection - one rule for the **Source** and one for the **Destination**. When a connection matches two Automatic NAT rules, the Security Gateway enforces those rules.

  Note - SmartConsole organizes the Automatic NAT rules in this order:
  1. Static NAT rules for the Security Gateway, or Host (computer or server) objects
  2. Hide NAT rules for the Security Gateway, or Host objects
  3. Static NAT rules for Network or Address Range objects
  4. Hide NAT rules for Network or Address Range objects

Working with Automatic NAT Rules

You can create Automatic NAT rules for these objects:

- Security Gateways
- Hosts
- Networks
- Address Ranges

The Management Server creates two Automatic NAT rules for Static NAT, to translate the source and the destination of the packets.

For Hide NAT, one rule translates the source of the packets.

For Network and Address Range objects, the Management Server creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the Automatic NAT rules:

Type of Traffic	Automatic NAT - Static	Automatic NAT - Hide
Internal to external	Rule translates source IP address	Rule translates source IP address
External to internal	Rule translates destination IP address	N/A (External connections are not allowed)
Intranet (for network and address range objects)	Rule does not translate IP address	Rule does not translate IP address

Example of Automatic NAT Rules

Static NAT for a Network object

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for HR (1-3)								

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	HR	HR	Any	= Original	= Original	= Original	Policy Targets	
2	HR	Any	Any	s HR (Valid Address)	= Original	= Original	Policy Targets	
3	Any	HR (Valid Address)	Any	= Original	s HR	= Original	Policy Targets	

1. Intranet connections in the HR network are not translated.

   The Security Gateway does not translate a connection between two computers that are part of the HR object.

   The Security Gateway 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 an Address Range object

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for Sales (1-2)								
1	Sales	Sales	Any	= Original	= Original	= Original	Policy Targets	

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
2	Sales	`Any`	`Any`	H Sales (Hiding Address)	`= Original`	`= Original`	`Policy Targets`	

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 Automatic NAT

Configure the NAT settings in each object, for which you need to create Automatic NAT rules, and configure the Access Control rules to allow traffic to the applicable objects.

Procedure

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.

   The **General Properties** window of the gateway opens.
3. From the navigation tree, select **NAT** > **Advanced**.
4. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
5. Select the **Translation method**: **Hide** or **Static**.
6. Configure the NAT IP address for the object.
   - **Hide behind Gateway** - Uses the IP address of the corresponding Security Gateway's interface
   - **Hide behind IP address** - Enter the IP address.
7. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
8. Click OK.
9. Install the Access Control Policy.

Example Deployment

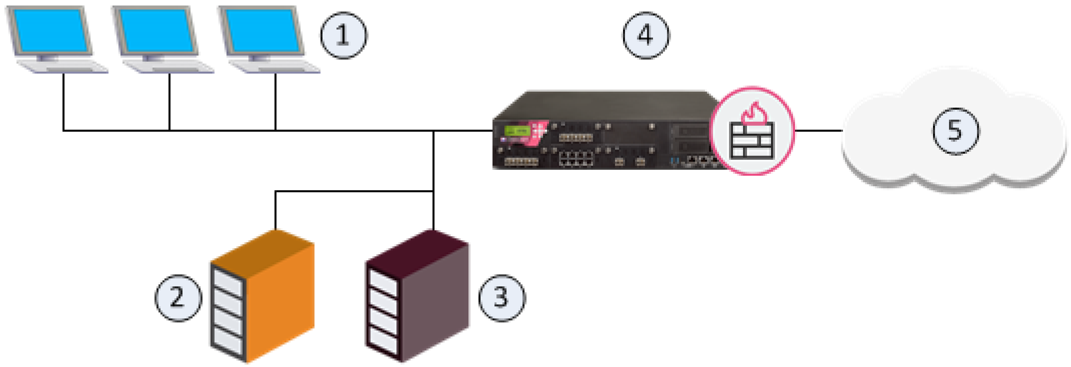
Example

The goal for this sample deployment is to configure:

- Static NAT for the EMail server and the Web server 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.



Item	Description
1	Internal computers (**Alaska_LAN**, IPv6 2001:db8::/64)
2	Web server (**Alaska_Web**, IPv6 2001:db8:0:10::5 is translated to IPv6 2001:db8:0:a::5)
3	Mail server (**Alaska_Mail**, IPv6 2001:db8:0:10::6 is translated to IPv6 2001:db8:0:a::6)
4	Security Gateway (**Alaska_GW**, external IPv6 2001:db8:0:a::1)
5	External computers and servers in the Internet

Configuration Procedure:

1. Configure Automatic Static NAT for the Web server:
   a. Double-click the **Alaska_Web** object.
   b. From the left, click **NAT**.
   c. Select **Add Automatic Address Translation Rules**.
   d. In **Translation method**, select **Static**.
   e. Select **Hide behind IP Address** and enter **2001:db8:0:a::5**.
   f. Click **OK**
2. Enable Automatic Static NAT for the EMail server:
   a. Double-click the **Alaska_Mail** object.
   b. From the left, click **NAT**.
   c. Select **Add Automatic Address Translation Rules**.

   d. In **Translation method**, select **Static**.

   e. Select **Hide behind IP Address** and enter **2001:db8:0:a::6**.

   f. Click **OK**.

3. Enable Automatic Hide NAT for the internal computers:

   a. Double-click the **Alaska_LAN** object.

   b. From the left, click **NAT**.

   c. Select **Add Automatic Address Translation Rules**.

   d. In **Translation method**, select **Hide**.

   e. Select **Hide behind Gateway**.

4. Click **OK**.

5. Install the Access Control Policy.

The Management Server creates these Automatic NAT rules in **Security Policies** view > **Access Control** > **NAT**:

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for Sales (1-2)								
1	Alaska_Web	Alaska_Web	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_Web	Any	Any	S Alaska_Web (Valid Address)	= Original	= Original	Policy Targets	

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
3	Any	Alaska_Web	Any	= Original	S Alaska_Web (Valid Address)	= Original	Policy Targets	
4	Alaska_Mail	Alaska_Mail	Any	= Original	= Original	= Original	Policy Targets	
5	Alaska_Mail	Any	Any	S Alaska_Mail (Valid Address)	= Original	= Original	Policy Targets	
6	Any	Alaska_Mail	Any	= Original	S Alaska_Mail (Valid Address)	= Original	Policy Targets	
7	Alaska_LAN	Alaska_LAN	Any	= Original	= Original	= Original	Policy Targets	
8	Alaska_LAN	Any	Any	H Alaska_LAN (Hiding Address)	= Original	= Original	Policy Targets	

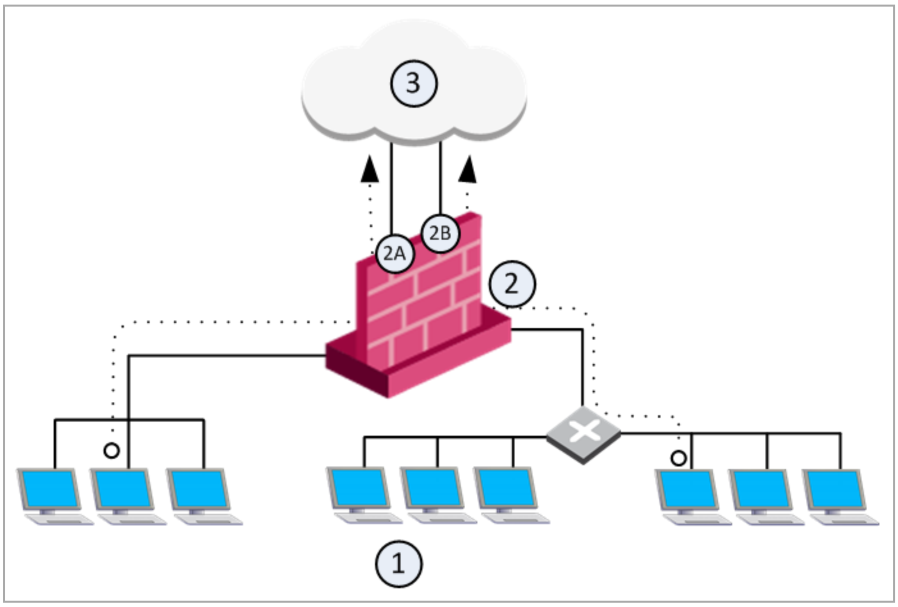
Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses.

Explanation

An easy alternative is to enable a Security Gateway to automatically Hide NAT for all traffic with external networks. The Security Gateway 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.



Item	Description
1	Internal networks
2	Security Gateway is configured with Automatic Hide NAT.
2A and 2B	Two external interfaces 192.0.2.1 and 192.0.2.100.
1 -->3	External computers and servers on the Internet

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. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the navigation tree, click **NAT**.
4. Select **Hide internal networks behind the Gateway's external IP**.
5. Click **OK**.
6. Install the Access Control Policy.

Working with Manual NAT Rules

For some deployments, it is necessary to manually define the NAT rules.

For example:

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

General workflow when working with manual NAT rules:

1. Create SmartConsole objects that use the **valid** (NATed) IP addresses.
2. Create Manual NAT rules to translate the original IP addresses of the objects to valid IP addresses.
3. Configure the Access Control Policy to allow traffic to the applicable translated objects with the valid IP addresses.

Note - For Manual NAT rules, it is necessary to configure Proxy ARP entries to associate the translated IP address. See *"Automatic and Proxy ARP" on page 345*.

Example of a Manual NAT Rule

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	HTTP_ Client	Web_ Server	`http`	`= Original`	S Web_ Server	`= Original`	`Policy Targets`	

Configuring Manual NAT

Procedure

1. From the left navigation panel, click **Security Policies**.
2. Click **Access Control** > **NAT**:
3. Add a new rule in one of these ways:
   - From the top toolbar, click the **Add Rule** icon (the leftmost icon).
   - If there are existing Manual NAT rules, then right-click in the **No.** column of the applicable rule > in the line **New Rule**, click **Above** or **Below**.
4. In the new rule, select the required objects and configure the required translation.

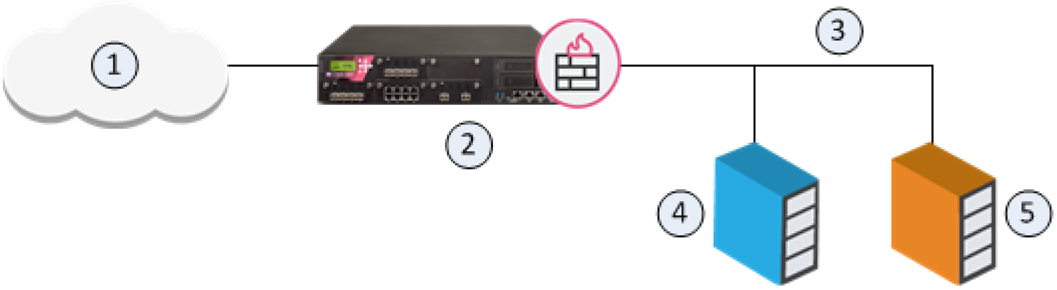
   If the required objects do not exist, you can create them in the selection window (in the top right corner, click ✳).
5. Install the Access Control Policy.

Example Deployment

Example

This example configuration shows how to let external computers access an internal web server and an internal mail server in a DMZ network from one IP address.

To do this, you must configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.



Item	Description
1	External computers and servers on the Internet
2	Security Gateway (**Alaska_GW**, external IPv6 2001:db8:0:c::1)
3	DMZ network (**Alaska_DMZ**, IPv6 2001:db8:a::/128)

Item	Description
4	Web server (**Alaska_DMZ_Web**, IPv6 2001:db8:a::35:5 is translated to IPv6 2001:db8:0:c::1)
5	Mail server (**Alaska_DMZ_Mail**, IPv6 2001:db8:a::35:6 is translated to IPv6 2001:db8:0:c::1)

Configuration Procedure:

1. Configure Automatic Hide NAT for the DMZ network:

   a. Double-click the Network object **Alaska_DMZ**.

   b. From the left, click **NAT**.

   c. Select **Add Automatic Address Translation Rules**.

   d. In **Translation method**, select **Hide**.

   e. Select **Hide behind Gateway**.

   f. Click **OK**.

   The Management Server creates these Automatic NAT rules in **Security Policies** view > **Access Control** > **NAT**:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	`Any`	`= Original`	`= Original`	`= Original`	`Policy Targets`	
2	Alaska_DMZ	`Any`	`Any`	H Alaska_DMZ (Hiding Address)	`= Original`	`= Original`	`Policy Targets`	

2. Create a Manual NAT rule to translate incoming HTTP traffic to the internal Web server:

   a. In SmartConsole, go to **Security Policies** view > **Access Control** > **NAT**.

   b. Add a new rule (#3) below the existing Automatic NAT rules.

   c. Select these objects:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	

3. Create a Manual NAT rule to translate incoming SMTP traffic to the internal Mail server:

a. Add a new rule (#4) below the existing NAT rules.

b. Select these objects:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	
4	Any	Alaska_GW	smtp	= Original	S Alaska_DMZ_Mail	= Original	Policy Targets	

4. Create an Access Control rule to allow the incoming HTTP and SMTP traffic to the internal servers:

a. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.

b. Add a new rule.

c. Select these objects:

No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
...	Incoming HTTP and SMTP traffic to internal servers	`Any`	Alaska_DMZ	`Any`	`http` `smtp`	`Accept`	`Log`	`Policy Targets`

5. Install the Access Control Policy.

Working with NAT46 Rules

Note - NAT46 rules are only supported on Security Gateways and Cluster Members R80.20 and higher.

Overview

NAT46 rules translate IPv4 traffic to IPv6 traffic without maintaining any session information on a Security Gateway.

Properties of Stateless NAT46

- Performs 1:1 IP address mapping.
- The system generates the translated source IPv6 address as a combination of these two parts:
  1. A user-defined Network object with an IPv6 address defined with the 96-bit prefix.
  2. The source IPv4 address, which is added as a 32-bit suffix.

NAT46 use case scenarios

- [IPv4 Network] --- (Internet) --- [Security Gateway] --- [IPv6 Network]

  Common use case for Content Providers.
- [IPv4 Network] --- [Security Gateway] --- (Internet) --- [IPv6 Network]

  Common use case for Enterprises.

Example of NAT46 Translation Flow

Example topology:

[IPv4 Client] --- (internal) [Security Gateway] (external) --- [IPv6 Server]

Where:

Item	Description
IPv4 Client	IPv4 real address is 192.168.2.55 IPv6 NATed address is 2001:DB8:90::192.168.2.55/**96**
Security Gateway internal interface	IPv4 address is 192.168.2.1/24
Security Gateway external interface	IPv6 address is 2001:DB8:5001::1/**96**

Item	Description
IPv6 Server	IPv6 real address is 2001:DB8:5001::30/96 IPv4 NATed address is 1.1.1.66/24
IPv6 NATed network	IPv6 address of the network on the external Security Gateway side is 2001:DB8:90::/96 These IPv6 addresses are used to translate the IPv4 address of the IPv4 Client to IPv6 address
IPv4 NATed network	IPv4 address of the network on the internal Security Gateway side is 1.1.1.0/24 These IPv4 addresses are used to translate the IPv6 address of the IPv6 Server to IPv4 address

Traffic flow:

1. IPv4 Client opens an IPv4 connection to the NATed IPv4 address of the IPv6 Serve

   From IPv4 address 192.168.2.55 to IPv4 address 1.1.1.66
2. Security Gateway performs these NAT translations:
   a. From the source IPv4 address 192.168.2.55 to the source IPv6 address 2001:DB8:90::192.168.2.55/96
   b. From the destination IPv4 address 1.1.1.66 to the destination IPv6 address 2001:DB8:5001::30
3. IPv6 Server receives this request connection as from the IPv6 address 2001:DB8:90::192.168.2.55/96 to the IPv6 address 2001:DB8:5001::30
4. IPv6 Server replies to this connection from the IPv6 address 2001:DB8:5001::30 to the IPv6 address 2001:DB8:90::192.168.2.55/96
5. Security Gateway performs these NAT translations:
   a. From the source IPv6 address 2001:DB8:5001::30 to the source IPv4 address 1.1.1.66
   b. From the destination IPv6 address 2001:DB8:90::192.168.2.55/96 to the destination IPv4 address 192.168.2.55
6. IPv4 Client receives this reply connection as from the IPv4 address 1.1.1.66 to the IPv4 address 192.168.2.55

To summarize:

- Request: [IPv4 Client] ---> [Security Gateway] ---> [IPv6 Server]

Field in packet	Original IPv4 packet	NATed IPv6 packet
Source IP	192.168.2.55 / 24	2001:DB8:90::192.168.2.55 / 96
Destination IP	1.1.1.66 / 24	2001:DB8:5001::30 / 96

- Reply: [IPv4 Client] <--- [Security Gateway] <--- [IPv6 Server]

Field in packet	Original IPv6 packet	NATed IPv4 packet
Source IP	2001:DB8:5001::30 / 96	192.168.2.55 / 24
Destination IP	2001:DB8:90::192.168.2.55 / 96	1.1.1.66 / 24

Known Limitations for NAT46

- NAT46 rules are only supported on Security Gateways and Cluster Members R80.20 and higher.
- NAT46 does not support VoIP traffic.
- NAT46 does not support FTP traffic.
- NAT46 does not support protocols that require state information between Control and Data connections.

Configuring NAT46

Step 1 - Prepare Security Gateway / Cluster Members for NAT46

ⓘ **Note** - In a Cluster, you must configure all the Cluster Members in the same way.

Step	Instructions
1	Make sure that an IPv6 address is assigned to the interface that connects to the destination IPv6 network, and the IPv6 network prefix length is equal to 96. **Note** - This can be any valid IPv6 address with the IPv6 network prefix length equal to **96**. ■ In Gaia Portal: Click **Network Management > Network Interfaces**. ■ In Gaia Clish: Run: `show interface <Name of Interface> ipv6-address` If such IPv6 address is not assigned yet, assign it now. For details, see the *R80.40 Gaia Administration Guide* - Chapter *Network Management* - Section *Network Interfaces* - Section *Physical Interfaces*.

Step	Instructions

2	Make sure that the routing is configured to send the traffic that is destined to the NATed IPv4 addresses (defined in the *Translated Destination* column in the NAT46 rule) through the interface that connects to the destination IPv6 network.
	- In Gaia Portal:
	Click **Advanced Routing > Routing Monitor**.
	- In Gaia Clish:
	Run:
	`show route`
	If such route does not already exist, add it in Gaia Clish.
	For details, see the *R80.40 Gaia Administration Guide*.
	Run these commands in Gaia Clish:
	a. Add the static route:
	`set static route <NATed Destination IPv4 Addresses>/<NATed IPv4 Net Mask> nexthop gateway logical <Name of Interface that connects to the real IPv6 Network> on`
	Example topology:
	[IPv4 Client] --- (NATed IPv4 of IPv6 side are 1.1.1.0/24) [Security Gateway] (eth3) --- [IPv6 Server]
	In such case, configure the IPv4 route using this command:
	`set static route 1.1.1.0/24 nexthop gateway logical eth3 on`
	b. Save the configuration:
	`save config`

Step	Instructions

3	Make sure that the number of IPv6 CoreXL Firewall instances is **equal** to the number of IPv4 CoreXL Firewall instances.
	a. Connect to the command line on the Security Gateway.
	b. Log in to Gaia Clish, or Expert mode.
	c. Show the number of IPv6 CoreXL Firewall instances:
	`fw6 ctl multik stat`
	d. Show the number of IPv4 CoreXL Firewall instances. Run:
	`fw ctl multik stat`
	e. If the number of IPv6 CoreXL Firewall instances is less than the number of IPv4 CoreXL Firewall instances, then do these steps:
	  a. Run:
	  `cpconfig`
	  b. Select **Check Point CoreXL**
	  c. Select **Change the number of IPv6 firewall instances**
	  d. Configure the number of IPv6 CoreXL Firewall instances to be the same as the number of IPv4 CoreXL Firewall instances
	  e. Select **Exit**
	  f. Reboot the Security Gateway
	f. Connect to the command line on the Security Gateway.
	g. Log in to Gaia Clish, or Expert mode.
	h. Show the number of IPv6 CoreXL Firewall instances. Run:
	`fw6 ctl multik stat`
	i. Show the number of IPv4 CoreXL Firewall instances. Run:
	`fw ctl multik stat`
	Example output:

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td></td><td>

```
[Expert@GW:0]# fw6 ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           0 |        0
 1 | Yes     | 2      |           0 |        4
 2 | Yes     | 1      |           0 |        2
[Expert@GW:0]#
[Expert@GW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |          10 |       14
 1 | Yes     | 2      |           6 |       15
 2 | Yes     | 1      |           7 |       15
[Expert@GW:0]#
```

</td></tr>
</table>

Step 2 - Configure NAT46 Rules

Configure NAT46 rules as Manual NAT rules in the Access Control Policy.

Make sure that you add Access Control rules that allow this NAT traffic.

1. Configure an applicable source IPv4 object (IPv4 Host, IPv4 Address Range, or IPv4 Network).

   To configure a source IPv4 Host object

   a. Click **Objects** menu > **New Host**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

   e. In the **IPv4 address** field, enter the source IPv4 address.

   f. In the **IPv6** section:

      Do not enter anything

   g. On the **NAT** page of this object:

      Do not configure anything.

   h. Configure the applicable settings on other pages of this object.

   i. Click **OK**.

To configure a source IPv4 Network object

a. Click **Objects** menu > **New Network**.

b. In the **Object Name** field, enter the applicable name.

c. In the **Comment** field, enter the applicable text.

d. Click the **General** page of this object.

e. In the **IPv4** section:

   i. In the **Network address** field, enter the IPv4 address of your source IPv4 network.

   ii. In the **Net mask** field, enter the net mask of your source IPv4 network.

f. In the **IPv6** section:

   Do not enter anything.

g. On the **NAT** page of this object:

   Do not configure anything.

h. Click **OK**.

To configure a source IPv4 Address Range object

a. Click **Objects** menu > **More object types** > **Network Object** > **Address Range** > **New Address Range**.

b. In the **Object Name** field, enter the applicable name.

c. In the **Comment** field, enter the applicable text.

d. Click the **General** page of this object.

e. In the **IPv4** section:

   i. In the **First IP address** field, enter the first IPv4 address of your IPv4 addresses range.

   ii. In the **Last IP address** field, enter the last IPv4 address of your IPv4 addresses range.

f. In the **IPv6** section:

   Do not enter anything.

g. On the **NAT** page of this object:

   Do not configure anything.

h. Click **OK**.

2. Configure a destination IPv4 Host object.

   This object represents the destination IPv4 address, to which the IPv4 sources connect.

   To configure a translated destination IPv4 Host object

   a. Click **Objects** menu > **New Network**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

   e. In the **IPv4** section:

      i. In the **Network address** field, enter the IPv4 address of your destination IPv4 network.

      ii. In the **Net mask** field, enter the net mask of your destination IPv4 network.

   f. In the **IPv6** section:

      Do not enter anything.

   g. On the **NAT** page of this object:

      Do not configure anything.

   h. Click **OK**.

3. Configure a translated source IPv6 Network object with an IPv6 address defined with the 96-bit prefix.

   This object represents the translated source IPv6 addresses, to which you translate the source IPv4 addresses.

   To configure a translated source IPv6 Network object with an IPv6 address defined with the 96-bit prefix

   a. Click **Objects** menu > **New Network**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

   e. In the **IPv4** section:

      Do not enter anything.

f. In the **IPv6** section:

   i. In the **Network address** field, enter the translated source IPv6 address.

   ii. In the **Prefix** field, enter the number **96**.

g. On the **NAT** page of this object:

   Do not configure anything.

h. Click **OK**.

4. Configure a translated destination IPv6 Host object.

   This object represents the translated destination IPv6 address, to which the translated IPv4 sources connect.

   To configure a translated destination IPv6 Host object

   a. Click **Objects** menu > **New Host**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

   e. In the **IPv4** section:

      Do not enter anything.

   f. In the **IPv6** section:

      In the **Network address** field, enter the destination static IPv6 address.

   g. On the **NAT** page of this object:

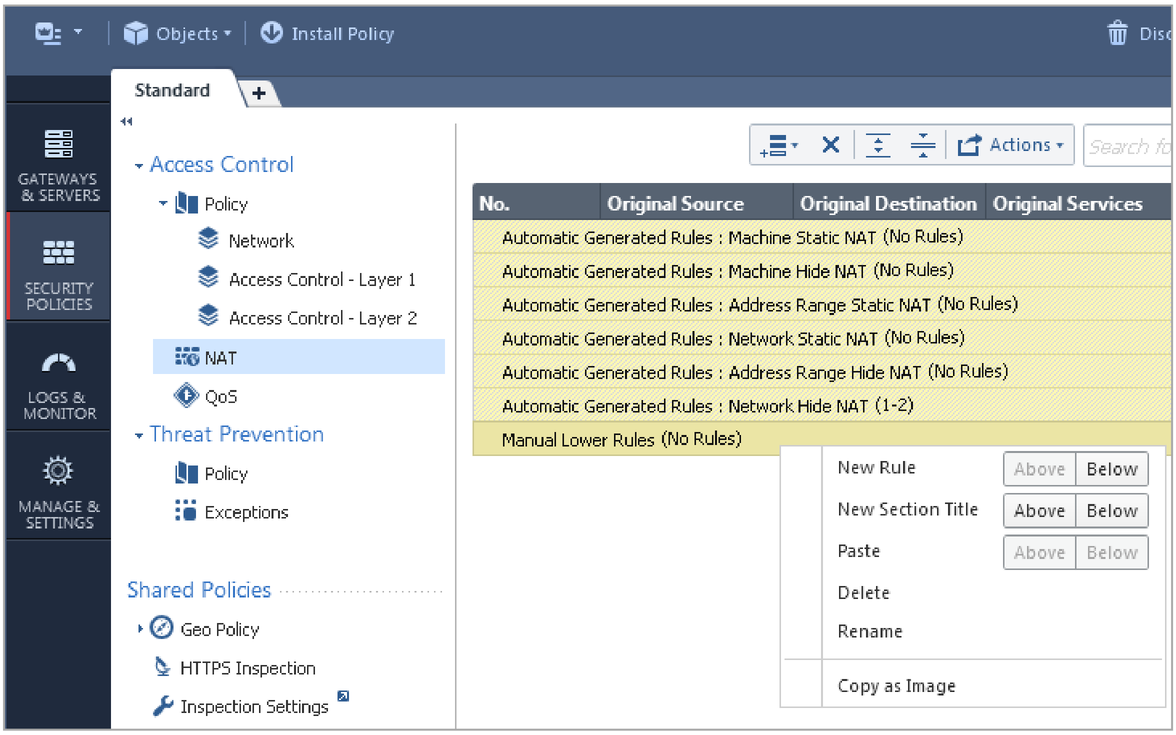
      Do not configure anything.

   h. Configure the applicable settings on other pages of this object.

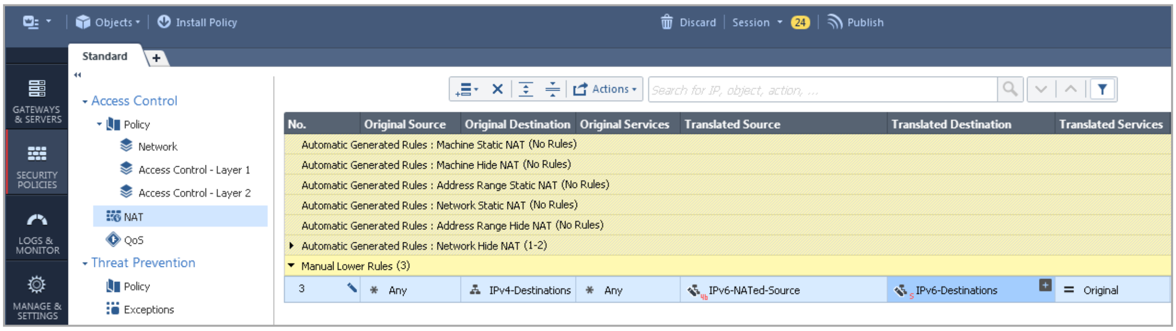
   i. Click **OK**.

5. Create a Manual NAT46 rule.

Procedure



No.	Original Source	Original Destination	Original Services
Automatic Generated Rules : Machine Static NAT (No Rules)			
Automatic Generated Rules : Machine Hide NAT (No Rules)			
Automatic Generated Rules : Address Range Static NAT (No Rules)			
Automatic Generated Rules : Network Static NAT (No Rules)			
Automatic Generated Rules : Address Range Hide NAT (No Rules)			
Automatic Generated Rules : Network Hide NAT (1-2)			
Manual Lower Rules (No Rules)			



No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
Automatic Generated Rules : Machine Static NAT (No Rules)						
Automatic Generated Rules : Machine Hide NAT (No Rules)						
Automatic Generated Rules : Address Range Static NAT (No Rules)						
Automatic Generated Rules : Network Static NAT (No Rules)						
Automatic Generated Rules : Address Range Hide NAT (No Rules)						
Automatic Generated Rules : Network Hide NAT (1-2)						
Manual Lower Rules (3)						
3	Any	IPv4-Destinations	Any	IPv6-NATed-Source	IPv6-Destinations	Original

a. From the left Navigation Toolbar, click **Security Policies**.

b. In the top **Access Control** section, click **NAT**.

c. Right-click on the **Manual Lower Rules** section title, and near the **New Rule**, click **Above** or **Below**.

Configure this NAT46 rule:

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
***Any** or Source IPv4 **Host** object or Source IPv4 **Address Range** object or Source IPv4 **Network** object	IPv4 **Host** object	***Any**	IPv6 **Network** object with an IPv6 address defined with the 96-bit prefix	IPv6 **Host** object	**= Original**

Do these steps:

i. In the **Original Source** column, add the applicable IPv4 object.

In this rule column, NAT46 rules support only these types of objects:

- `*Any`
- Host with a static IPv4 address
- Address Range with IPv4 addresses
- Network with IPv4 address

ii. In the **Original Destination** column, add the IPv4 **Host** object that represents the destination IPv4 address, to which the IPv4 sources connect.

    In this rule column, NAT46 rules support only IPv4 Host objects.

iii. In the **Original Services** column, you must leave the default **Any**.

iv. In the **Translated Source** column, add the IPv6 **Network object** with an IPv6 address defined with the 96-bit prefix.

    In this rule column, NAT64 rules support only IPv6 Network objects with an IPv6 address defined with the 96-bit prefix.

v. In the **Translated Source** column, right-click the IPv6 **Network object** with the 96-bit prefix > click **NAT Method** > click **Stateless NAT46**.

    The **46** icon shows in the **Translated Source** column.

vi. In the **Translated Destination** column, add the IPv6 **Host** object represents the translated destination IPv6 address, to which the translated IPv4 sources connect.

    In this rule column, NAT46 rule supports only an IPv6 Host objects.

vii. In the **Translated Services** column, you must leave the default **= Original**.

To summarize, you must configure only these NAT46 rules (rule numbers are for convenience only):

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	`*Any`	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
2	IPv4 *Host* object with a static IPv4 address	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`
3	IPv4 *Address Range* object	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`
4	IPv4 *Network* object	IPv4 *Host* object	`*Any`	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	`= Original`

6. Install the Access Control Policy.

Logging of NAT46 Traffic

Explanation

In the Security Gateway log for NAT64 connection, the source and destination IPv6 addresses show in their original IPv6 format.

To identify a NAT46 entry, look in the **More** section of the **Log Details** window.

Field in Log	Description
Xlate (NAT) Source IP	Shows the translated source IPv6 address, to which the Security Gateway translated the original source IPv4 address
Xlate (NAT) Destination IP	Shows the translated destination IPv6 address, to which the Security Gateway translated the original destination IPv4 address
More	Identifies the entry as NAT46 traffic (`Nat46 enabled`)

Working with NAT64 Rules

Overview

NAT64 translation (RFC 6146) lets **IPv6-only client** communicate with **IPv4-only server** using **unicast** UDP, TCP, or ICMP.

Definition on an IPv6-only client

One of these:

- A host with a networking stack that implements only IPv6.
- A host with a networking stack that implements both IPv4 and IPv6 protocols, but with only IPv6 connectivity.
- A host that runs an IPv6-only client application.

Definition of an IPv4-only server

One of these:

- A host with a networking stack that implements only IPv4.
- A host with a networking stack that implements both IPv4 and IPv6 protocols, but with only IPv4 connectivity.
- A host that runs an IPv4-only server application.

The translation of IP addresses is done by translating the packet headers according to the IP/ICMP Translation Algorithm defined in RFC 6145. The IPv4 addresses of IPv4 hosts are translated to and from IPv6 addresses using the algorithm defined in RFC 6052, and an IPv6 prefix assigned to the stateful NAT64 for this specific purpose.

Note - For information about DNS64, see RFC 6147.

Properties of Stateful NAT64

- Performs N:M translation:
  - N must be greater than M
  - If M=1, performs a Hide NAT behind a single IPv4 address.
  - If M>1, performs a Hide NAT behind a range of IPv4 addresses.
- Gives good IPv4 address preservation (multiplexed using ports).
- Saves connection states and binding.

- There are no requirements on the assignment of IPv6 addresses to IPv6 clients. Any mode of IPv6 address assignment is legitimate (Manual, DHCP6, SLAAC).
- It is a scalable solution.

NAT64 use case scenarios

- [IPv6 Network] --- (Internet) --- [Security Gateway] --- [internal IPv4 Network]

  Common use case for Content Providers. DNS64 is not needed.
- [internal IPv6 Network] --- [Security Gateway] --- (Internet) --- [IPv4 Network]

  Common use case for Carriers, ISPs, Enterprises. DNS64 is required.
- [IPv6 Network] --- [Security Gateway] --- [IPv4 Network]

  Common use case for Enterprises. DNS64 is required.

Standards supported for NAT64

- RFC 6144 - Framework for IPv4/IPv6 Translation
- RFC 6146 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC 6052 - IPv6 Addressing of IPv4/IPv6 Translators
- RFC 6145 - IP/ICMP Translation Algorithm
- RFC 2428 - FTP Extensions for IPv6 and NATs
- RFC 6384 - An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation

Known Limitations for NAT64

NAT64 rules do **not** support:

- VoIP traffic.
- HTTPS Inspection.
- SSL de-multiplexer.
- Security Gateway in HTTP Proxy mode.
- IPS protection "HTTP Header Spoofing".

Example of NAT64 Translation Flow

Example topology

[IPv6 Client] --- (interface) [Security Gateway] (internal) --- [IPv4 Server]

Where:

Item	Description
IPv6 Client	IPv6 real address is 1111:1111::0100/96
Security Gateway external interface	IPv6 address is 1111:1111::1/96
Security Gateway internal interface	IPv4 address is 10.0.0.1/24 IPv6 address is 3333:4444::1/96
IPv4 Server	IPv4 real address is 10.0.0.100/24 IPv6 NATed address is 1111:2222::0A00:0064/96
IPv6 NATed network	IPv6 address of the network on the external Security Gateway side is 1111:2222::/96 These IPv6 addresses are used to translate the IPv4 address of the IPv4 Server to the IPv6 address
IPv4 NATed network	IPv4 address of the network on the internal Security Gateway side is 1.1.1.0/24 These IPv4 addresses are used to translate the IPv6 address of the IPv6 Client to the IPv4 address

Example traffic flow

1. IPv6 Client opens an IPv6 connection to the NATed IPv6 address of the IPv4 Server:

   From the IPv6 Client's IPv6 real address 1111:1111::0100 to the IPv4 Server's NATed IPv6 address 1111:2222::0A00:0064

   Where:

   The "1111:2222::" part is the NATed IPv6 subnet

   The "0A00:0064" part is 10.0.0.100

2. Security Gateway performs these NAT translations:

   a. Translate the IPv6 Client's *source* address from the real IPv6 address 1111:1111::0100 to the special concatenated *source* IPv6 address 0064:FF9B::0101:01X

      Where:

      The "0064:FF9B::" part is a well-known prefix reserved for NAT64 (as defined by the RFC)

      The "0101:01XX" part is 1.1.1.X

   b. Translate the IPv6 Client's *source* address from the special concatenated *source* IPv6 address 0064:FF9B::0101:01XX to the *source* IPv4 address 1.1.1.X

   c. Translate the IPv6 Client's NATed *destination* address from the IPv6 address 1111:2222::0A00:0064 to the NATed destination IPv4 address 10.0.0.100

3. IPv4 Server receives this request connection as from the *source* IPv4 address 1.1.1.X to the *destination* IPv4 address 10.0.0.100

4. IPv4 Server replies to this connection from the *source* IPv4 address 10.0.0.100 to the *destination* IPv4 address 1.1.1.X

5. Security Gateway performs these NAT translations:

   a. Translate the IPv4 Server's *source* real IPv4 address 10.0.0.100 to the *source* NATed IPv6 address 1111:2222::0A00:0064

   b. Translate the IPv6 Client's NATed *destination* IPv4 address 1.1.1.X to the *destination* special concatenated IPv6 address 0064:FF9B::0101:01X

      Where:

      The "64:FF9B::" part is a well-known prefix reserved for NAT64 (as defined by the RFC)

      The "0101:01XX" part is 1.1.1.X

   c. Translate the IPv6 Client's *destination* special concatenated IPv6 address 0064:FF9B::0101:01XX to the *destination* IPv6 real address 1111:1111::0100

6. IPv6 Client receives this reply connection as from the *source* IPv6 address 1111:2222::0A00:0064 to the *destination* IPv6 address 1111:1111::0100

Example summary

- *Request*: [IPv6 Client] ---> [Security Gateway] ---> [IPv4 Server]

Field in packet	Original IPv6 packet	NATed IPv4 packet
Source IP	1111:1111::0100 / 96	1.1.1.X / 24
Destination IP	1111:2222::0A00:0064 / 96	10.0.0.100 / 24

- *Reply*: [IPv6 Client] <--- [Security Gateway] <--- [IPv4 Server]

Field in packet	Original IPv4 packet	NATed IPv6 packet
Source IP	10.0.0.100 / 24	1111:2222::0A00:0064 / 96
Destination IP	1.1.1.X / 24	1111:1111::0100 / 96

Configuring NAT64

Step 1 - Prepare the Security Gateway for NAT64

Note - In a Cluster, you must configure all the Cluster Members in the same way.

Step	Instructions
1	Make sure that an IPv6 address is assigned to the interface that connects to the destination IPv4 network, and the IPv6 network prefix length is equal to, or less than **96**. **Note** - This can be any valid IPv6 address with the IPv6 network prefix length equal to, or less than **96**. ■ In Gaia Portal: Click **Network Management > Network Interfaces**. ■ In Gaia Clish: Run: `show interface <Name of Interface> ipv6-address` If such IPv6 address is not assigned yet, assign it now. For details, see the [R80.40 Gaia Administration Guide]() - Chapter *Network Management* - Section *Network Interfaces* - Section *Physical Interfaces*.

Step	Instructions

2	Make sure that the IPv6 routing is configured to send the traffic that is destined to the NATed IPv6 addresses (defined in the *Original Destination* column in the NAT64 rule) through the interface that connects to the destination IPv4 network.
	- In Gaia Portal:
	Click **Advanced Routing > Routing Monitor**.
	- In Gaia Clish:
	Run:
	`show ipv6 route`
	If such route does not already exist, add it in Gaia Clish.
	For details, see the *R80.40 Gaia Administration Guide*.
	Run these commands in Gaia Clish:
	a. Add the static route:
	`set ipv6 static-route <NATed Destination IPv6 Addresses>/<96 or less> nexthop gateway <Any IPv6 Address from the IPv6 subnet of the Interface that connects to the destination real IPv4 network> on`
	Example topology:
	[IPv6 Client] --- (NATed IPv6 of IPv4 side are 1111:2222::/96) [Security Gateway] (eth3 with IPv6 3333:4444::1) --- [IPv4 Server]
	In such case, configure the IPv6 route using this command:
	`set ipv6 static-route 1111:2222::/96 nexthop gateway 3333:4444::10 on`
	b. Save the configuration:
	`save config`

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>3</td><td>

Make sure that the number of IPv6 CoreXL Firewall instances is **equal** to the number of IPv4 CoreXL Firewall instances.

a. Connect to the command line on the Security Gateway.
b. Log in to Gaia Clish, or Expert mode.
c. Show the number of IPv6 CoreXL Firewall instances:

```
fw6 ctl multik stat
```

d. Show the number of IPv4 CoreXL Firewall instances:

```
fw ctl multik stat
```

e. If the number of IPv6 CoreXL Firewall instances is less than the number of IPv4 CoreXL Firewall instances, then do these steps:
   i. Run:

   ```
   cpconfig
   ```

   ii. Select **Check Point CoreXL**
   iii. Select **Change the number of IPv6 firewall instances**
   iv. Configure the number of IPv6 CoreXL Firewall instances to be the same as the number of IPv4 CoreXL Firewall instances
   v. Select **Exit**
   vi. Reboot the Security Gateway
f. Connect to the command line on the Security Gateway.
g. Log in to Gaia Clish, or Expert mode.
h. Show the number of IPv6 CoreXL Firewall instances:

```
fw6 ctl multik stat
```

i. Show the number of IPv4 CoreXL Firewall instances:

```
fw ctl multik stat
```

Example output:

```
[Expert@GW:0]# fw ctl multik
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |          10 |       14
 1 | Yes     | 2      |           6 |       15
 2 | Yes     | 1      |           7 |       15
[Expert@GW:0]#
[Expert@GW:0]# fw6 ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           0 |        0
 1 | Yes     | 2      |           0 |        4
 2 | Yes     | 1      |           0 |        2
[Expert@GW:0]#
```

</td></tr>
</table>

Step 2 - Configure NAT64 Rules

Define NAT64 rules as Manual NAT rules in the Access Control Policy.

Make sure that you add access rules that allow this NAT traffic.

1. Define a source IPv6 Network object.

   This object represents the source IPv6 addresses, which you translate to source IPv4 addresses.

   Procedure

   a. Click **Objects** menu > **New Network**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

   e. In the **IPv4** section:

      Do not enter anything.

   f. In the **IPv6** section:

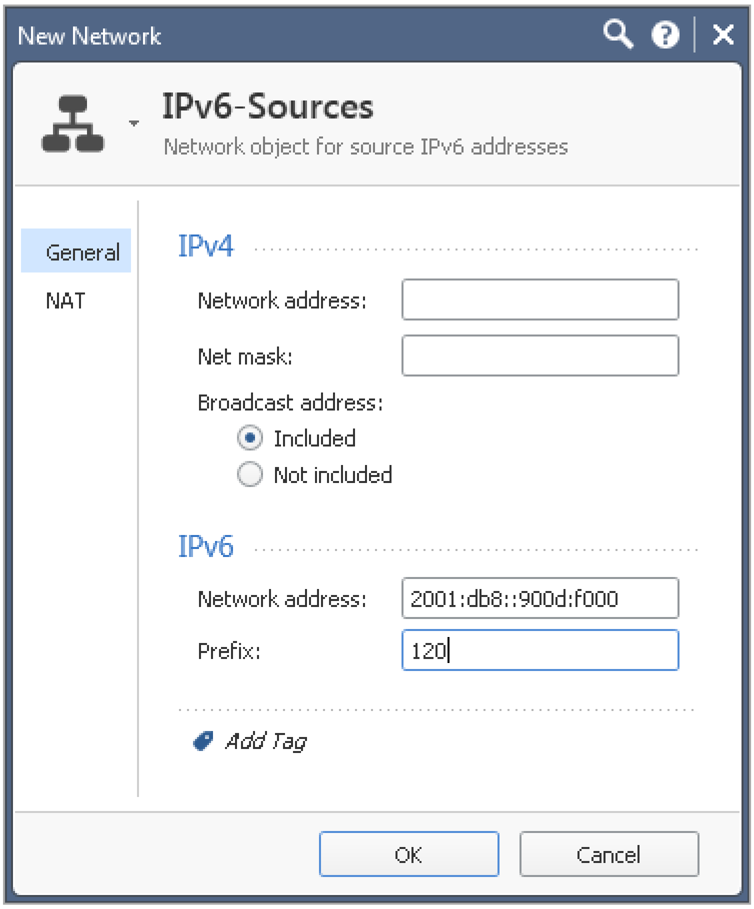
      i. In the **Network address** field, enter the IPv6 address of your IPv6 network, which you translate to source IPv4 addresses.

      ii. In the **Prefix** field, enter the prefix of your IPv6 network.

   g. On the **NAT** page of this object:

      Do not configure anything.

   h. Click **OK**.



New Network

IPv6-Sources

Network object for source IPv6 addresses

IPv4

Network address:

Net mask:

Broadcast address:

● Included

○ Not included

IPv6

Network address: 2001:db8::900d:f000

Prefix: 120

2. Define a translated destination IPv6 Network object with an IPv4-embedded IPv6 address, or a translated destination IPv6 Host object with a static IPv6 address.

   This object represents the translated destination IPv6 address, to which the IPv6 sources connect.

   Procedure

   a. Click **Objects** menu > **New Network**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

   e. In the **IPv4** section:

      Do not enter anything.

f. In the **IPv6** section:

   i. In the **Network address** field, enter the destination *IPv4-embedded* IPv6 address (also called *IPv4-mapped* IPv6 address), to which the IPv6 sources connect.

      Such IPv6 address contains (from left to right) 80 "zero" bits, followed by 16 "one" bits, and then the 32 bits of the IPv4 address - 0:0:0:0:0:FFFF:X.Y.Z.W, where X.Y.Z.W are the four octets of the destination IPv4 address.

      For example, for IPv4 network 192.168.3.0, the IPv4-embedded IPv6 address is 0:0:0:0:0:FFFF:192.168.3.0, or 0:0:0:0:0:FFFF:C0A8:0300. For more information, see RFC 6052.

      These IPv4-embedded IPv6 addresses are published by an external DNS64 server.

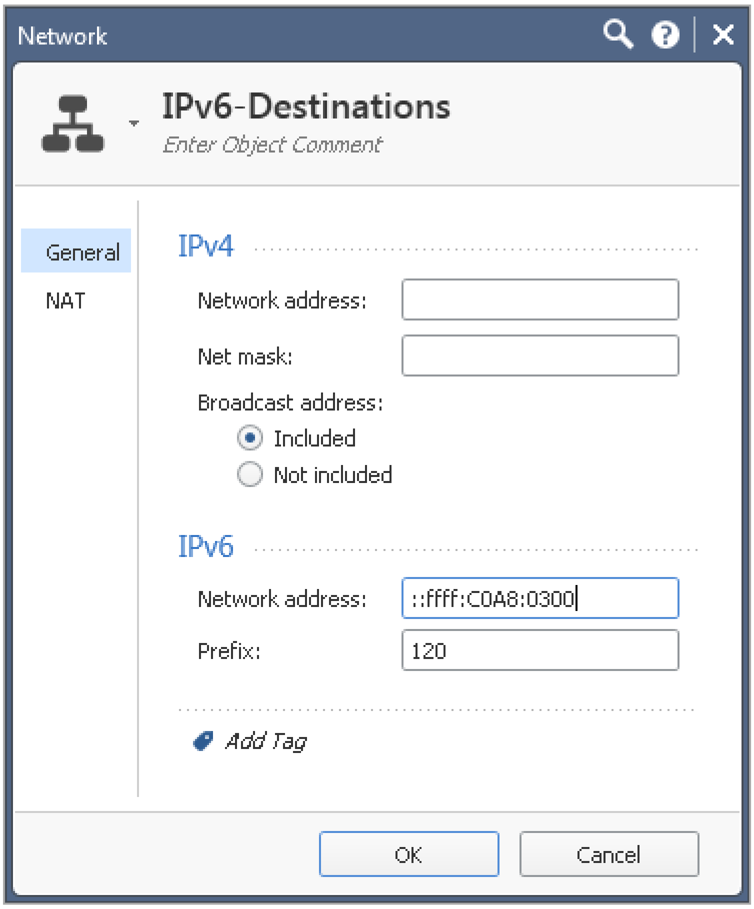
   ii. In the **Prefix** field, enter the applicable IPv6 prefix.

   Note - You can define IPv4-embedded IPv6 addresses only for these object types: Address Range, Network, and Host.

g. On the **NAT** page of this object:

   Do not configure anything.

h. Click **OK**.



Network

IPv6-Destinations

Enter Object Comment

IPv4

Network address:

Net mask:

Broadcast address:

● Included

○ Not included

IPv6

Network address: ::ffff:C0A8:0300

Prefix: 120

3. Define a translated source IPv4 Address Range object.

   This object represents the translated source IPv4 addresses, to which you translate the original source IPv6 addresses.

   Procedure

   a. Click **Objects** menu > **More object types** > **Network Object** > **Address Range** > **New Address Range**.

   b. In the **Object Name** field, enter the applicable name.

   c. In the **Comment** field, enter the applicable text.

   d. Click the **General** page of this object.

e. In the **IPv4** section:

   i. In the **First IP address** field, enter the first IPv4 address of your IPv4 addresses range, to which you translate the source IPv6 addresses.

   ii. In the **Last IP address** field, enter the last IPv4 address of your IPv4 addresses range, to which you translate the source IPv6 addresses.

   Notes:

   - This IPv4 addresses range must not use private IPv4 addresses (see RFC 1918 and **Menu** > **Global properties** > **Non Unique IP Address Range**
   - This IPv4 addresses range must not be used on the IPv4 side of the network.
   - We recommend that you define a large IPv4 addresses range for more concurrent NAT64 connections.

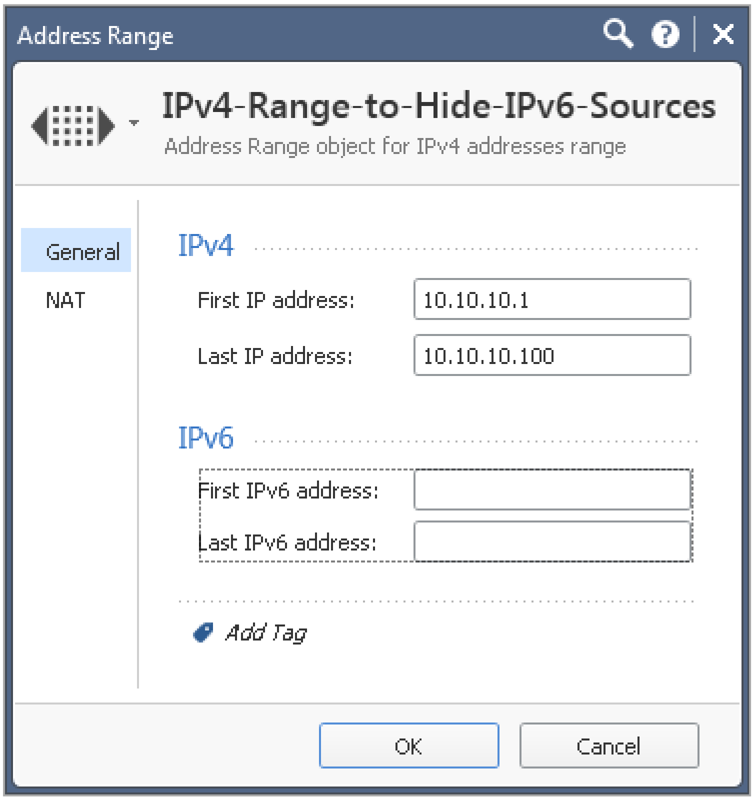
f. In the **IPv6** section:

   Do not enter anything.

g. On the **NAT** page of this object:

   Do not configure anything.

h. Click **OK**.



IPv4-Range-to-Hide-IPv6-Sources

Address Range object for IPv4 addresses range

First IP address: 10.10.10.1

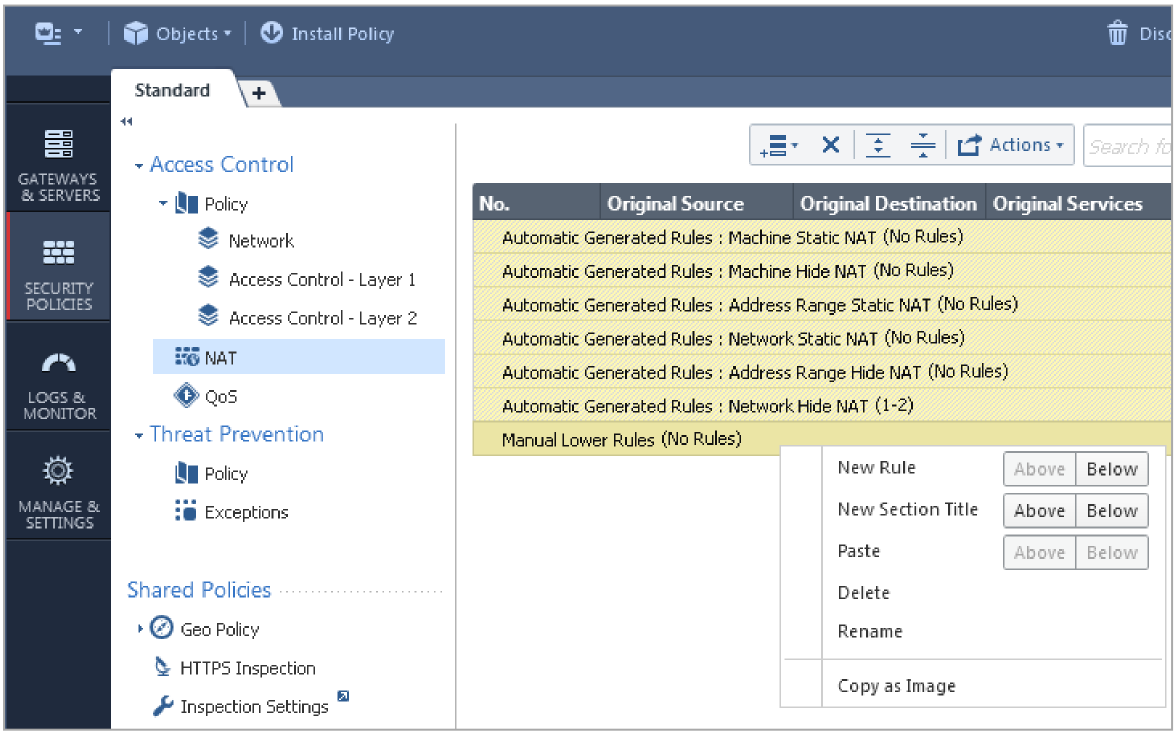
Last IP address: 10.10.10.100

First IPv6 address:

Last IPv6 address:

4. Create a Manual NAT64 rule.

Procedure



No.	Original Source	Original Destination	Original Services
Automatic Generated Rules : Machine Static NAT (No Rules)			
Automatic Generated Rules : Machine Hide NAT (No Rules)			
Automatic Generated Rules : Address Range Static NAT (No Rules)			
Automatic Generated Rules : Network Static NAT (No Rules)			
Automatic Generated Rules : Address Range Hide NAT (No Rules)			
Automatic Generated Rules : Network Hide NAT (1-2)			
Manual Lower Rules (No Rules)			

a. From the left navigation panel, click **Security Policies**.

b. In the top **Access Control** section, click **NAT**.

c. Right-click on the **Manual Lower Rules** section title, and near the **New Rule**, click **Above** or **Below**.

   Configure this Manual NAT64 rule:

   > **Important** - Some combinations of object types are not supported in the *Original Source* and *Original Destination* columns. See the summary table with the supported NAT rules at the bottom of this section.

   i. In the **Original Source** column, add the IPv6 object for your original source IPv6 addresses.

      In this rule column, NAT64 rules support only these types of objects:

      - `*Any`
      - Host with a static IPv6 address
      - Address Range with IPv6 addresses
      - Network with IPv6 address

   ii. In the **Original Destination** column, add a translated destination IPv6 object with an IPv4-embedded IPv6 address.

      In this rule column, NAT64 rules support only these types of objects:

      - Host with a static IPv6 address
      - Address Range with IPv4-embedded IPv6 addresses
      - Network with an IPv4-embedded IPv6 address

   iii. In the **Original Services** column, you must leave the default **Any**.

   iv. In the **Translated Source** column, add the IPv4 **Address Range** object for your translated source IPv4 addresses range.

      In this rule column, NAT64 rules support only these types of objects:

      - Host with a static IPv4 address, only if in the **Original Source** column you selected a Host with a static IPv6 address
      - Address Range with IPv4 addresses

v. In the **Translated Source** column, right-click the IPv4 **Address Range** object > click **NAT Method** > click **Stateful NAT64**:

- The **Translated Packet Destination** column shows **= Embedded IPv4 Address**.
- The **64** icon shows in both the **Translated Source** and **Translated Destination** columns.

In this rule column, NAT64 rule supports only these types of objects:

- Host with a static IPv4 address, only if in the **Original Source** column you selected a Host with a static IPv6 address
- Embedded IPv4 Address

vi. In the **Translated Services** column, you must leave the default **= Original**.

d. Install the Access Control Policy.

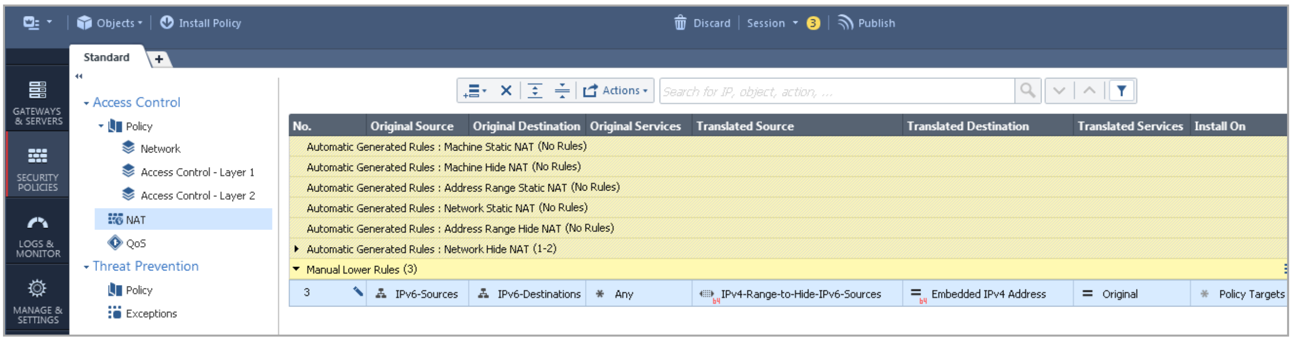
5. Install the Access Control Policy.

To summarize, you must configure only these Manual NAT64 rules (rule numbers are for convenience only):

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	`*Any`	IPv6 *Host* object with a static IPv6 address	`*Any`	IPv4 *Address Range* object	IPv4 *Host* object	`= Original`
2	`*Any`	IPv6 *Address Range* object with an IPv4-embedded IPv6 addresses	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
3	`*Any`	IPv6 *Network* object with an IPv4-embedded IPv6 address	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
4	IPv6 *Host* object with a static IPv6 address	IPv6 *Host* object with a static IPv6 address	`*Any`	IPv4 *Host* object	IPv4 *Host* object	`= Original`
5	IPv6 *Host* object with a static IPv6 address	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
6	IPv6 *Host* object with a static IPv6 address	IPv6 *Network* object with an IPv4-embedded IPv6 address	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
7	IPv6 *Address Range* object	IPv6 *Host* object with a static IPv6 address	`*Any`	IPv4 *Address Range* object	IPv4 *Host* object	`= Original`

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
8	IPv6 *Address Range* object	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
9	IPv6 *Address Range* object	IPv6 *Network* object with an IPv4-embedded IPv6 address	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
10	IPv6 *Network* object	IPv6 *Host* object with a static IPv6 address	`*Any`	IPv4 *Address Range* object	IPv4 *Host* object	`= Original`
11	IPv6 *Network* object	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
12	IPv6 *Network* object	IPv6 *Network* object with an IPv4-embedded IPv6 address	`*Any`	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`



No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
Automatic Generated Rules : Machine Static NAT (No Rules)							
Automatic Generated Rules : Machine Hide NAT (No Rules)							
Automatic Generated Rules : Address Range Static NAT (No Rules)							
Automatic Generated Rules : Network Static NAT (No Rules)							
Automatic Generated Rules : Address Range Hide NAT (No Rules)							
Automatic Generated Rules : Network Hide NAT (1-2)							
Manual Lower Rules (3)							
3	IPv6-Sources	IPv6-Destinations	Any	IPv4-Range-to-Hide-IPv6-Sources	Embedded IPv4 Address	Original	Policy Targets

Step 3 - Configure additional settings for NAT64

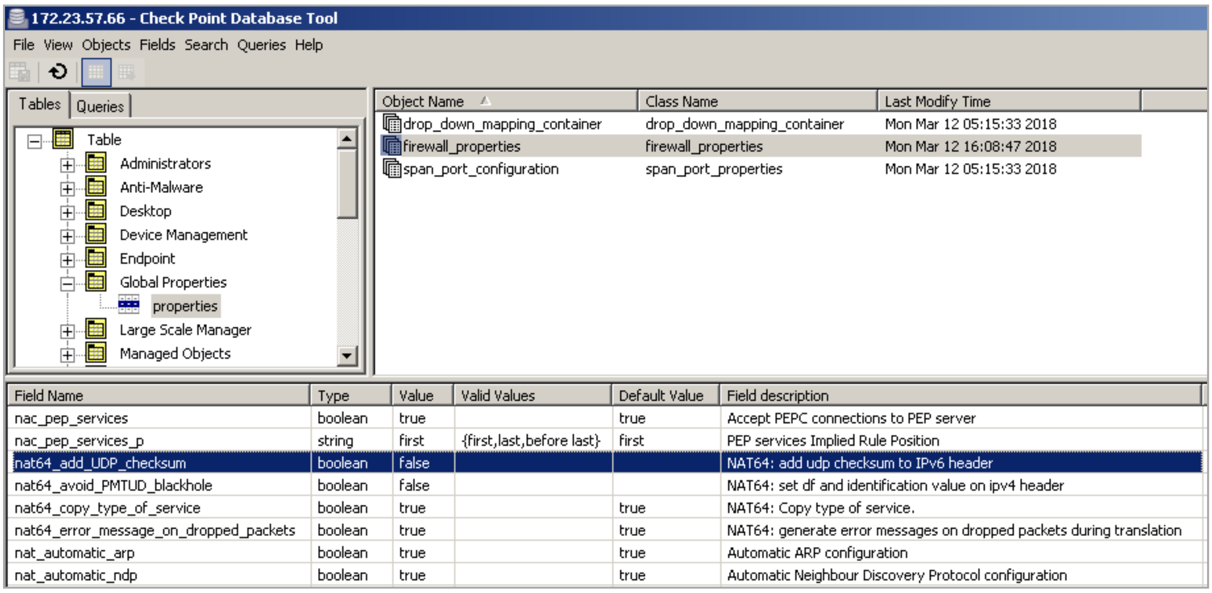
You can configure the additional settings that control the NAT64 translation mechanism.

These settings are compliant with RFC 6145.

Best Practice - We recommend that you change the default settings only if you are familiar with the technology.

Procedure

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with Database Tool (GuiDBEdit Tool) (see sk13009) to the applicable Security Management Server or Domain Management Server.
3. In the top left section, click **Table** > **Global Properties** > **properties**.
4. In the top right section, click **firewall_properties**.
5. In the bottom section, scroll to these **Field Names**:
   - `nat64_add_UDP_checksum`
   - `nat64_avoid_PMTUD_blackhole`
   - `nat64_copy_type_of_service`
   - `nat64_error_message_on_dropped_packets`



Object Name	Class Name	Last Modify Time
drop_down_mapping_container	drop_down_mapping_container	Mon Mar 12 05:15:33 2018
firewall_properties	firewall_properties	Mon Mar 12 16:08:47 2018
span_port_configuration	span_port_properties	Mon Mar 12 05:15:33 2018

Field Name	Type	Value	Valid Values	Default Value	Field description
nac_pep_services	boolean	true		true	Accept PEPC connections to PEP server
nac_pep_services_p	string	first	{first,last,before last}	first	PEP services Implied Rule Position
nat64_add_UDP_checksum	boolean	false			NAT64: add udp checksum to IPv6 header
nat64_avoid_PMTUD_blackhole	boolean	false			NAT64: set df and identification value on ipv4 header
nat64_copy_type_of_service	boolean	true		true	NAT64: Copy type of service.
nat64_error_message_on_dropped_packets	boolean	true		true	NAT64: generate error messages on dropped packets during translation
nat_automatic_arp	boolean	true		true	Automatic ARP configuration
nat_automatic_ndp	boolean	true		true	Automatic Neighbour Discovery Protocol configuration

6. Right-click the applicable parameter in the **Field Name** column and click **Edit**.

7. Select the applicable **Value** (`true`, or `false`) and click **OK**.

Field Name	Description
`nat64_add_UDP_checksum`	This parameter controls whether the translator should calculate and add a valid UDP checksum value to a packet, if the packet checksum value is zero. This is important because, by default, an IPv4 UDP packet with a checksum value of zero is dropped on the IPv6 side. **Default:** `false`
`nat64_avoid_PMTUD_blackhole`	This parameter controls whether to allow packet fragmentation on the IPv4 (destination) side during PMTU discovery. Enable this setting if some equipment combinations cause PMTU discovery to fail. **Default:** `false`
`nat64_copy_type_of_service`	This parameter controls whether to copy the traffic **Class Field** to the **Type Of Service** field, and set the **Type Of Service** field in the translated packet to zero. **Default:** `true`

Field Name	Description
`nat64_error_message_on_dropped_packets`	This parameter controls whether to generate an audit log after a connection is closed. For each closed connection, the log shows: ▪ Connection information (source and destination IP address, source port, and service). ▪ Translated source IP address and source port. ▪ Start time and end time. ▪ If the connection was closed because the connection expired, log shows additional information in the **TCP End Reason** field. If this field does not show in the log, the connection was closed with a TCP RST, or with a TCP FIN, and did not expire. **Default:** `true`

8. Save the changes (click **File > Save All**).
9. Close the Database Tool (GuiDBEdit Tool).
10. Connect with the SmartConsole to the applicable Security Management Server or Domain Management Server.
11. Install the Access Control Policy.

Logging of NAT64 traffic

Explanation

In the Security Gateway log for NAT64 connection, the source and destination IPv6 addresses show in their original IPv6 format.

To identify a NAT64 entry, in the **Log Details** window, look at the **More** section.

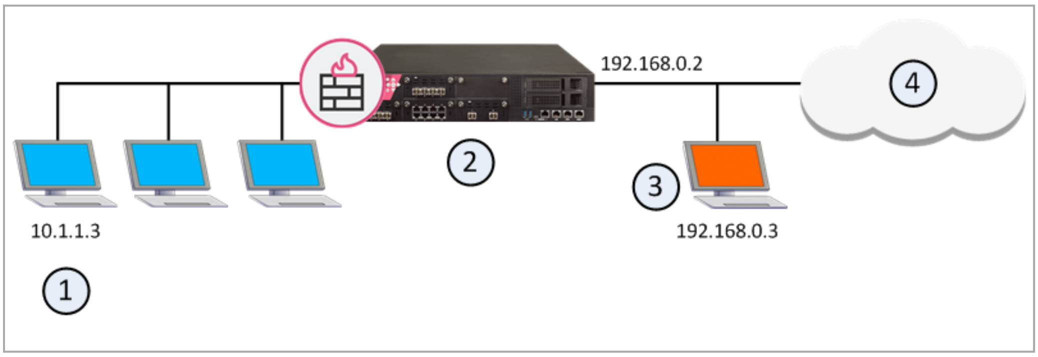
Field in Log	Description
Xlate (NAT) Source IP	Shows the translated source IPv4 address, to which the Security Gateway translated the original source IPv6 address
Xlate (NAT) Destination IP	Shows the translated destination IPv4 address, to which the Security Gateway translated the original destination IPv6 address
More	Identifies the entry as NAT64 traffic (`Nat64 enabled`)

Advanced NAT Settings

This section describes advanced NAT configuration in specific scenarios.

Automatic and Proxy ARP

Giving a computer on the internal network an IP address from an external network using NAT makes that computer appear on the external network. When NAT on the Security Gateway is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP Requests that are sent from the external network for the IP address of the internal computer.



Item	Description
1	Computer on the internal network with IP address 10.1.1.3
2	Security Gateway with external interface IP address 192.168.0.2 responds to ARP Requests on behalf of translated internal objects
3	Translated IP Address 192.168.0.3 on the external network
4	External network

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

See sk30197 for more information about configuring:

- Proxy ARP for IPv4 Manual NAT.
- Proxy ARP for Scalable Platforms.

See sk91905 for more about configuring Proxy NDP for IPv6 Manual NAT.

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.

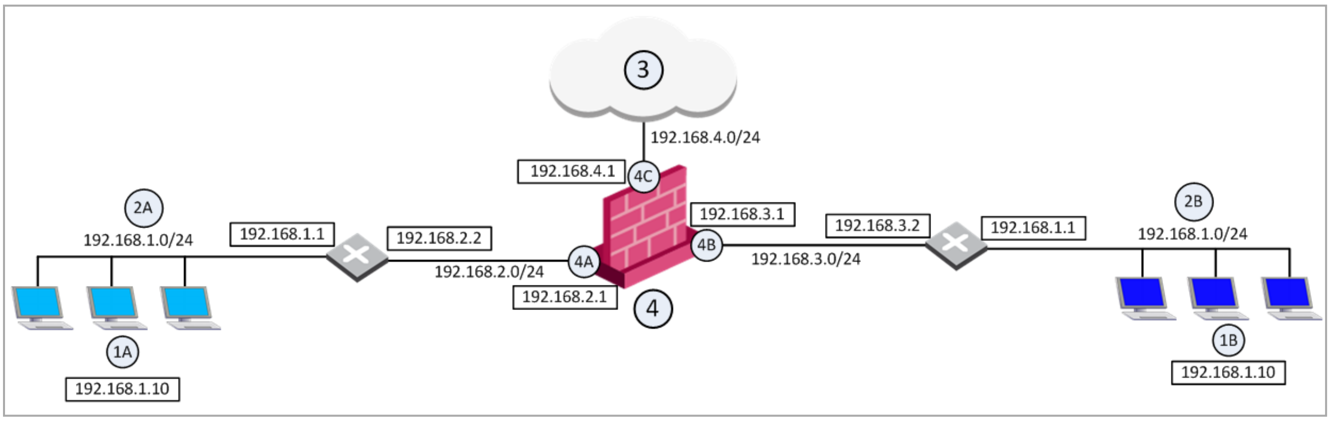
Internal Communication with Overlapping Addresses

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.

Example Network Configuration

Example topology:



For example, assume both Network 2A and Network 2B share the same address space (**192.168.1.0/24**).

Therefore, it is not possible to use standard NAT to enable communication between the two networks.

Instead, it is necessary to perform overlapping NAT 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 this way for each individual interface:

Interface	IP Address Translation on the 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	IP Address Translation on the 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**.
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

Example 1 - 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**.

Communication Between Internal Networks

Step	Source IP address	Destination IP address
Interface 4A - before NAT	**192.168.1.10**	**192.168.30.10**
Interface 4A - after NAT	**192.168.20.10**	**192.168.30.10**
Security Gateway enforces the security policy for packets from network **192.168.20.0/24** to network **192.168.30.0/24**.		
Interface 4B - before NAT	**192.168.20.10**	**192.168.30.10**
Interface 4B - after NAT	**192.168.20.10**	**192.168.1.10**

Example 2 - Communication Between an Internal Network and the Internet

User 1A, at IP address **192.168.1.10** in Network 2A, connects to IP address **192.0.2.10** on the Internet (3).

Communication Between an Internal Network and the Internet

Step	Source IP address	Destination IP address
Interface 4A - before NAT	**192.168.1.10**	**192.0.2.10**

Communication Between an Internal Network and the Internet (continued)

Step	Source IP address	Destination IP address
Interface 4A - after NAT	**192.168.20.10**	**192.0.2.10**
The Security Gateway (4) enforces the security policy for packets from network **192.168.20.0/24** to the Internet (3).		
Interface 4C - before NAT	**192.168.20.10**	**192.0.2.10**
Interface 4C - after NAT Hide	**192.168.4.1**	**192.0.2.10**

Routing Considerations

To allow routing from Network 2A to Network 2B (in our example above), you must configure the required routes on the Security Gateway:

Destination Network Address	Default Gateway
192.168.20.0 / 24	192.168.2.2
192.168.30.0 / 24	192.168.3.2

For configuration instructions, see the *R80.40 Gaia Administration Guide* > Chapter "*Network Management*" > Section "*IPv4 Static Routes*".

Object Database Configuration

To activate the overlapping NAT feature, use Database Tool (GuiDBEdit Tool) (see sk13009), or the `dbedit` command (see skI3301).

In our example network, the per-interface values for the interface 4A and the interface 4B are:

Parameter	Value
enable_overlapping_nat	**true**
overlap_nat_dst_ipaddr	The overlapping IP addresses (before NAT). In our example, **192.168.1.0** for both interfaces.
overlap_nat_src_ipaddr	The IP addresses after NAT. In our example: ▪ **192.168.20.0** for interface 4A. ▪ **192.168.30.0** for interface 4B.

Parameter	Value
overlap_nat_netmask	The net mask of the overlapping IP addresses. In our example, **255.255.255.0**.

Security Management behind NAT

Overview

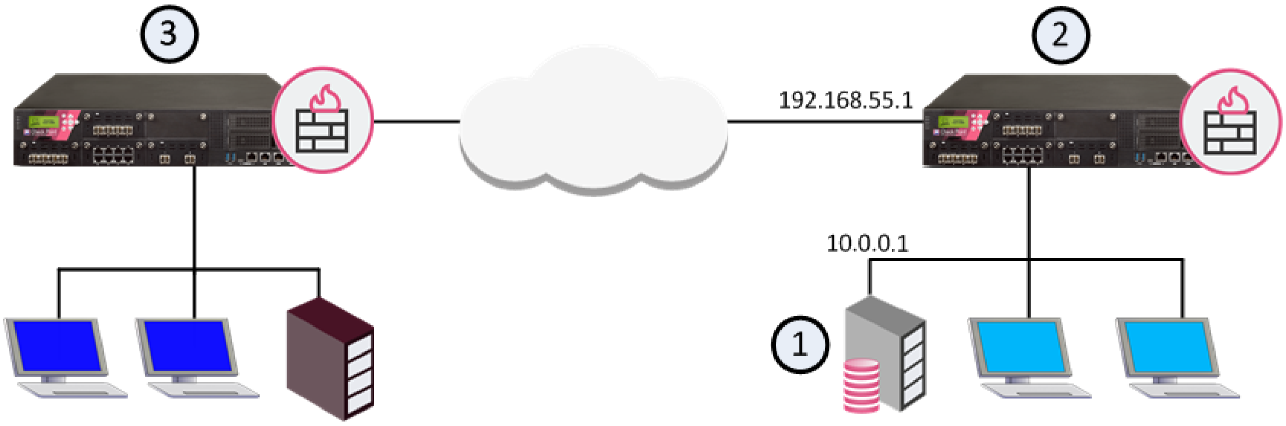
Note - Security Management Server behind NAT is not supported on a Standalone server (where the Security Management Server also acts as a Security Gateway) that receives connections from outside the NATed domain (for example, when it receives SAM commands).

Explanation

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 Security Gateways. All Security 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.

Example:



Item	Description
1	Primary Security Management Server. - Real IP address - 10.0.0.1 - Translated IP address - 192.168.55.1
2	Local Security Gateway that is directly connected to the Security Management Server. The Remote Security Gateway connects to the Security Management Server through this Local Security Gateway.
3	Remote Security Gateway that must connect to the Security Management Server.

Configuring NAT for Control Connections on the Security Management Server

Procedure

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Management Server object.
3. From the left, click **NAT**.
4. Select **Add Automatic Address Translation rules**.
5. In the **Translation method** field, select **Static**.
6. Configure the applicable IP address.

   In our example - 192.168.55.1
7. Select the Security Gateway that must perform this NAT.

   In our example - the local Security Gateway that is directly connected to the Security Management Server.
8. Select **Apply for Security Gateway control connections**.
9. Click **OK**.
10. Install the Access Control Policy on the applicable Security Gateways.

Configuring NAT for Control Connections on a Remote Security Gateway

Possible cases when a Security Management Server is located behind NAT:

- A remote Security Gateway has to connect to the Security Management Server at its real (internal) IP address.
- A remote Security Gateway has to connect to the Security Management Server at its NATed (external) IP address.

To allow such connections from a remote Security Gateway, configure the required IP address in the applicable configuration file on the remote Security Gateway:

Procedure

1. Configure NAT for Control Connections on the Security Management Server as described above.
2. Configure the Security Management Server not to override the `$FWDIR/conf/masters` file on the remote Security Gateway / Cluster Members.

Procedure

a. Close all SmartConsole windows connected to the Security Management Server.

b. Connect with Database Tool (GuiDBEdit Tool) (see sk13009) to the applicable Security Management Server or Domain Management Server.

c. In the top left section, click **Table** > **Network Objects**.

d. In the top right section, click **network_objects**.

e. In the right upper pane, select the object of the remote Security Gateway / Cluster.

f. Press **CTRL+F** (or go to **Search** menu > **Find**) > paste **define_logging_servers** > click **Find Next**.

g. In the lower pane, right-click the **define_logging_servers** > select **Edit** > select "**false**" > click **OK**.

h. Save the changes (click **File > Save All**).

i. Close the Database Tool (GuiDBEdit Tool).

3. Configure the required IP address in the `$FWDIR/conf/masters` file on the remote Security Gateway / Cluster Members.

Procedure

ℹ **Note** - In a Cluster, you must configure all the Cluster Members in the same way.

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Back up the current file:

```
cp -v $FWDIR/conf/masters{,_BKP}
```

d. Edit the current file:

```
vi $FWDIR/conf/masters
```

e. In the **[Policy]** section and in the **[Log Server]** section, add a new line above the current line.

   In the new line, enter the NATed (external) IP address of the Security Management Server.

   > **Important** - If the remote Security Gateway has to connect to the real IP address of the Security Management Server, you must also configure the SIC name of the Security Management Server.
   > Copy it from the existing line:
   > `CN=cp_mgmt,O=<xxx>.checkpoint.com.<yyy>`

f. Save the changes in the file and exit the editor.

4. Install the Security Policy.

   Procedure

   a. Connect with the SmartConsole to the Security Management Server.

   b. Install the Access Control Policy on the remote Security Gateway / Cluster.

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.
- Make sure in objects of all managed Security Gateways, on the **Network Management** page, you configure the correct the **Topology** settings of the applicable interfaces.

IP Pool NAT

Overview

An IP Pool is a range of IP addresses that are routable to the Security Gateway.

IP Pool NAT ensures proper routing for encrypted connections in these VPN connection scenarios:

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

When a connection is opened from a Remote Access Client or a client behind a Security Gateway, to a server behind the MEP Security Gateways, the packets are routed through one of the MEP Security Gateways.

Return packets in the connection must be routed back through the same Security Gateway in order to maintain the connection.

To ensure that this occurs, each of the MEP Security Gateways maintains a pool of IP addresses that are routable to the Security Gateway.

When a connection is opened to a server, the Security Gateway substitutes an IP address from the IP pool for the source IP address.

Reply packets from the server return to the Security Gateway, which restores the original source IP address and forwards the packets to the source.

NAT Priorities

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

Note - To enable IP Pool NAT for **clear** connections through the Security Gateway, it is necessary to configure the required INSPECT settings in the applicable **user.def** file (see *"Location of 'user.def' Files on the Management Server" on page 183*). Contact *Check Point Support* for assistance.

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:

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

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

IP Pool Per Interface

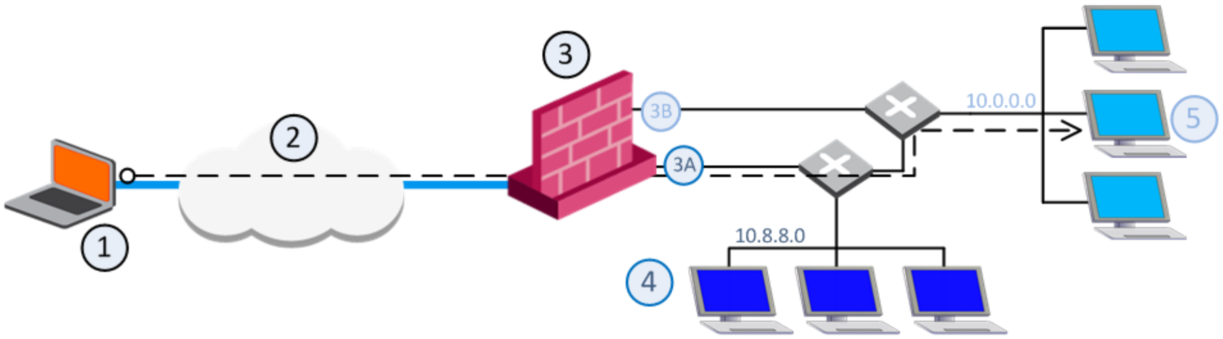
You can define a separate IP address pool on one or more of the Security Gateway interfaces instead of defining a single pool of IP addresses for the Security Gateway.

Defining an IP pool per interface solves routing issues that occur when the Security Gateway has more than two interfaces.

Sometimes it is necessary that reply packets return to the Security Gateway through the same Security Gateway interface.

Example:

This example diagram shows one of the MEP Security Gateways in a Remote Access Client to a MEP Security Gateway deployment:



Item	Description
1	Packets from source host: Source: Original Destination:
2	VPN tunnel through the Internet
3	MEP Security Gateway
3A	IP Pool 1 packets: Source: 10.55.8.x Destination:
3B	IP Pool 2 packets: Source: 10.55.10.x Destination:
4	Internal network 10.8.8.0
5	Target host in internal network 10.10.10.0

If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct Security 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 Security Gateway interfaces. The addresses in the IP pool can be routed only through that Security 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 Security Gateway interface, the Security Gateway restores the remote peer's source IP address.

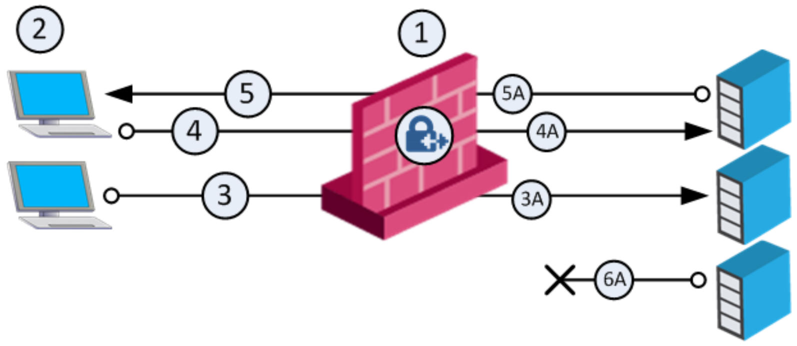
The routing tables on the routers that lie behind the Security Gateway must be edited so that addresses from a Security Gateway IP pool are returned to the correct Security Gateway interface.

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

Reusing IP Pool Addresses For Different Destinations

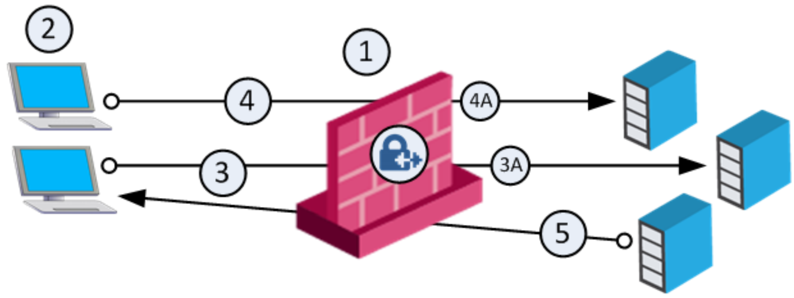
IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

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.



Item	Description
1	Security Gateway with IP Pool addresses A to Z
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).



Item	Description
1	Security Gateway with IP Pool addresses A to Z.
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: Z Destination:
5	Connection. Source: Original Destination: A

Switching between the **Reuse** and **Do not reuse** modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

IP Pool Configuration Procedure

1. **Enable IP Pool NAT in Global Properties**

   a. From the SmartConsole **Menu**, click **Global properties**.

   b. In the **Global properties** > **NAT** page, select **Enable IP Pool NAT** and the required tracking options.

   c. Click **OK**.

2. **For each Security Gateway or Security Gateway interface, create an object that represents its IP pool NAT addresses**

   This object can be a Network, Network Group, or Address Range.

   Important:
   - In a Cluster, you must configure separate IP Pool for each Cluster Member.
   - It is **not** possible to configure a separate IP Pool for each Cluster Member interface.

   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**.

   b. In the **General** tab, enter the first and last IP addresses of the range.

   c. Click **OK**.

3. **Enable and configure IP Pool NAT in the Security Gateway object**

   a. From the left navigation panel, click **Gateways & Servers**.

   b. Double-click the Security Gateway / Cluster object.

   c. From the left, expand **NAT** and click **IP Pool NAT**.

   d. In the **IP Pool NAT** page, select one of these options:

   In a Security Gateway object:

   - **Allocate IP Addresses from** and then select the address range you created to configure IP Pool NAT for the whole Security Gateway.
   - **Define IP Pool NAT on Gateway interfaces** to configure IP Pool NAT per interface.

   In a Cluster object:

   - **Define IP Pool NAT on each cluster member**
   - **Define IP Pool NAT on cluster member interfaces** to configure IP Pool NAT per interface.

e. **Optional:** Select one or more of these options:

   - **Use IP Pool NAT for VPN client connections**
   - **Use IP Pool NAT for gateway to gateway connections**
   - **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 was used up.

f. **Optional:** Configure the applicable advanced settings.

   Click **Advanced** and configure:

   i. **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.

   ii. **Reuse IP addresses from the pool for different destinations**

      This is a good option unless it is necessary 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.

g. Click **OK** to close the **Advanced IP Pool NAT Configuration** window.

h. In a cluster object:

   i. From the left, click **Cluster Members**.

   ii. Double-click each Cluster Member.

   iii. From the top, click the **IP Pool NAT** tab.

   iv. Select **Use IP Pool NAT**.

   v. In the **Allocate IP addresses from** field, select the applicable object for this Cluster Member.

      Important - In a Cluster, you must configure separate IP Pool for each Cluster Member. It is **not** possible to configure a separate IP Pool for each Cluster Member interface.

   vi. Click **OK** to close the Cluster Member Properties window.

i. Click **OK** to close the Security Gateway / Cluster object.

4. **Install the Security Policy**

   a. Connect with the SmartConsole to the Security Management Server.

   b. Install the Access Control Policy on the remote Security Gateway / Cluster.

5. **Edit the routing table of each internal router**

   Configure the applicable routes so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway or, if using IP Pools per interface, the appropriate Security Gateway interface.

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.

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.
- **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 Security 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:

   - For Legacy Policy: Add rules in SmartConsole. Select **Security Policies** > **Shared Policies**> Mobile Access > **Open Mobile Access Policy in SmartConsole**
   - For Unified Access Control Policy: Add rules in SmartConsole > **Security Policies Access Control Policy**.

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

6. Install the Access Control Policy on the Security Gateway.

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

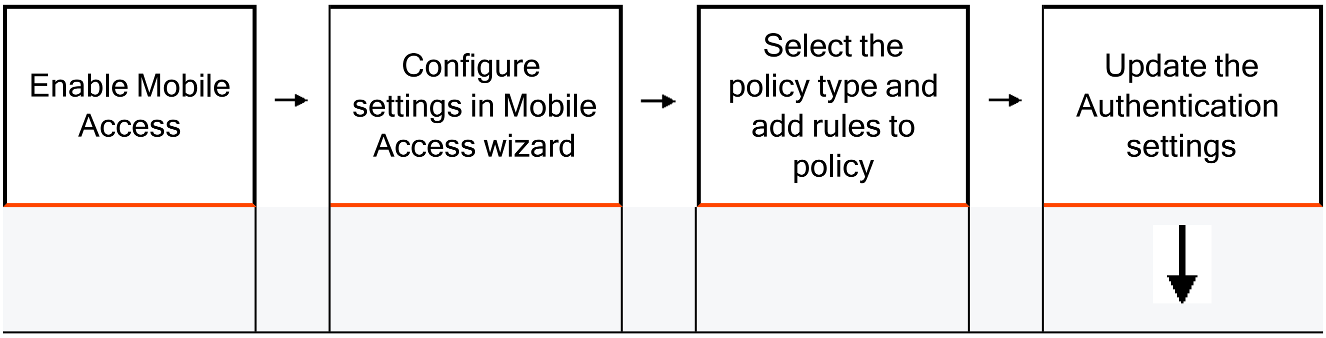
7. Optional: Give secure access to users through the Capsule Workspace app with certificate authentication.

   a. In the Security Gateway object > Mobile Access > **Authentication**, click **Settings**, and select **Require client certificate**.

   b. Use the Certificate Creation and Distribution Wizard (in the **Security Policies** view > **Client Certificates** > **New**).

   c. Users download the Capsule Workspace app.

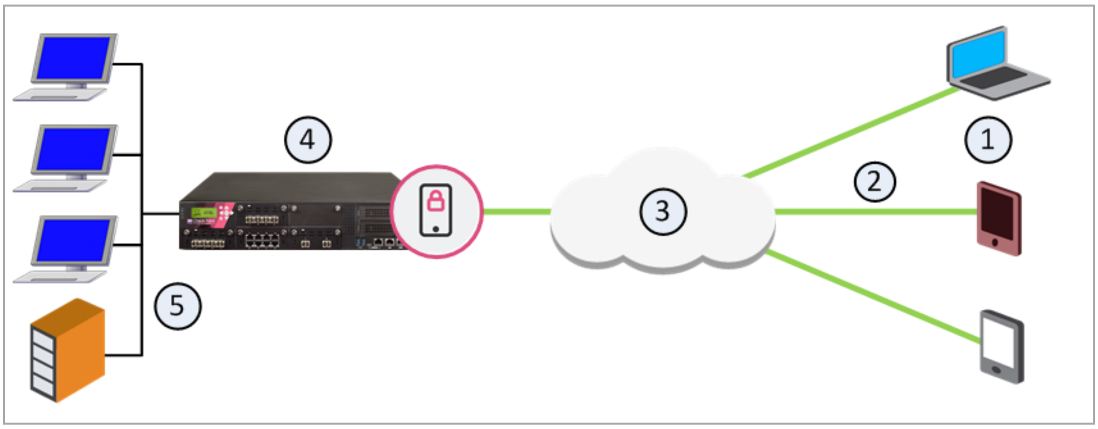
   d. Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.


Enable Mobile Access
Configure settings in Mobile Access wizard
Select the policy type and add rules to policy
Update the Authentication settings

Users can access internal resources	←	Users download app, open it, and enter settings	←	Generate a certificate for the clients	←	Install the Access Control Policy

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.



Item	Description
1	Mobile devices
2	Mobile Access tunnels
3	Internet (external networks)
4	Mobile Access Security Gateway
5	Internal network resources, AD and Exchange servers

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.

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 Security 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://<IPv4 Address of Security Gateway>/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.

Name	Source	Destination	VPN	Service	Action	Install On	Track
Mobile Access Users	Any	ExchngSrvr	RemoteAccess	HTTP HTTPS MSExchange	Accept	Mobile Access GW	Log

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 Gateway 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.

For Web form applications

1. In the **Application Single Sign-On Method** section, select **Advanced** and click **Edit**.

   The **Advanced** window opens.
2. Select **This application reuses the portal credentials. Users are not prompted**.
3. Click **OK**.
4. Select **This application uses a Web form to accept credentials from users**.
5. Click **OK**.
6. Install the policy.

Connecting to a Citrix Server

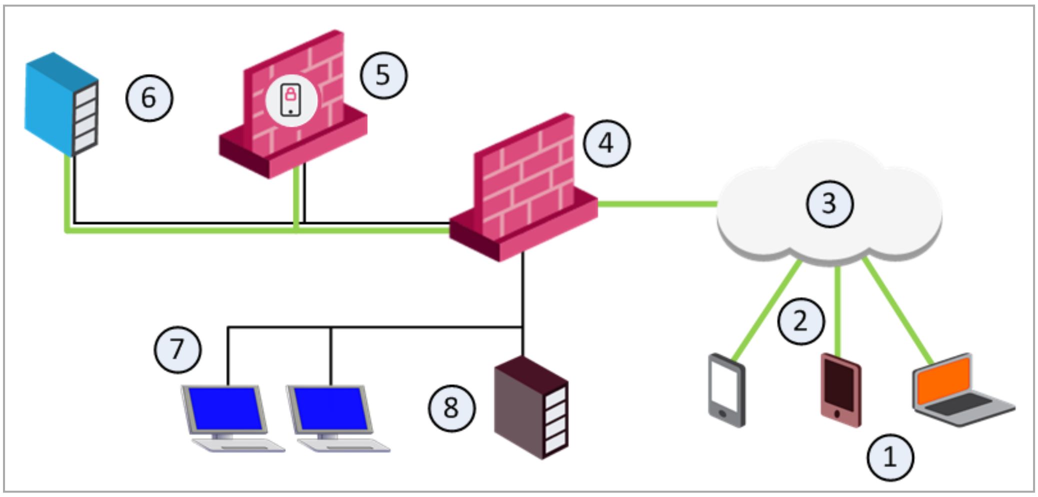
Citrix Services

The Mobile Access Software Blade integrates the Citrix clients and services. It is not necessary to use STA (Secure Ticketing Authority) servers in a Mobile Access Security Gateways 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.



Item	Description
1	Mobile devices
2	Mobile Access tunnels
3	Internet (external networks)
4	Security Gateway for the internal network
5	Mobile Access Security Gateway in the DMZ
6	Citrix web interface
7	Internal network resources
8	Citrix XenApp (MetaFrame) server

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 (see *"Sample Deployment with Citrix Server" on the previous page*).

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.
9. Click **OK**.
10. In Services, select one or more of these services that the Citrix web interface server supports:
    - HTTP
    - HTTPS
11. From the navigation tree, click **Link in Portal**.
12. 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
13. From the navigation tree, select **Additional Settings** > **Single Sign On**.
14. 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**

15. Click **OK**.

    The Citrix server object is added to **Defined Citrix Services**.

16. From the Mobile Access navigation tree, select **Policy**.
17. 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.
18. 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.
- 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. On 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 for a Security Gateway (see *"Compliance Policy Rules" on page 372*).

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 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.

For more about configuring Secure Workspace and Mobile Access VPN, see the *R80.40 Mobile Access Administration Guide*.

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**.

   Legacy SmartDashboard opens.
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**.
7. Install the policy.

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.

For more about configuring Secure Workspace and Mobile Access VPN, see the *R80.40 Mobile Access Administration Guide*.

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**.

   Legacy SmartDashboard opens.
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 *R80.40 Mobile Access Administration Guide*.

Site-to-Site VPN

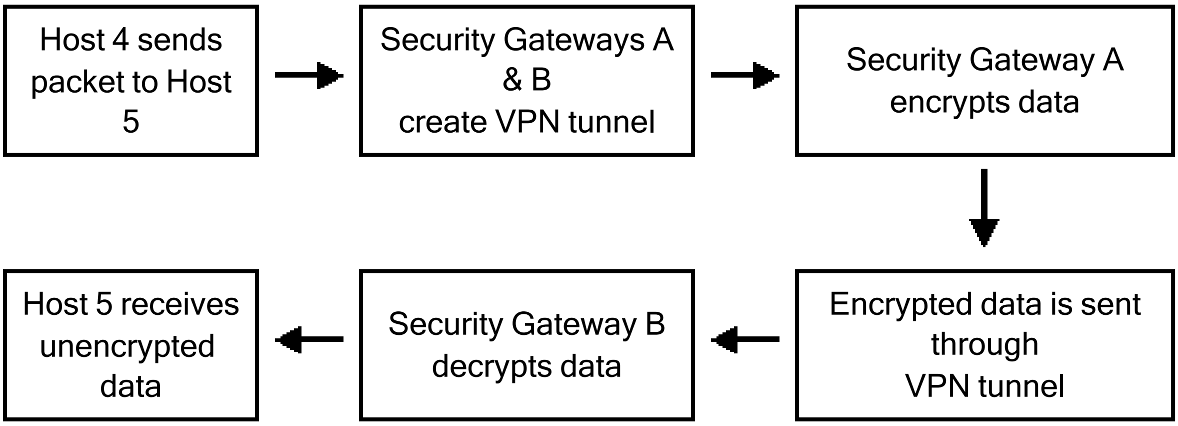
The basis of Site-to-Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

Sample Site-to-Site VPN Deployment

Item	Description
A, B	Security Gateways
2	VPN tunnel
3	Internal network in VPN domain
4	Host 4
5	Host 5

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

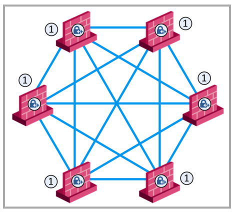

Host 4 sends packet to Host 5
Security Gateways A & B create VPN tunnel
Security Gateway A encrypts data
Encrypted data is sent through VPN tunnel
Security Gateway B decrypts data
Host 5 receives unencrypted data

VPN Communities

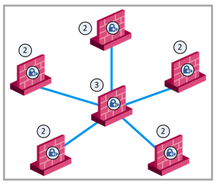
A VPN Domain is a collection of internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community - collection of VPN tunnels and their attributes. Network 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.

Mesh Topology



Star Topology



Item	Description
1	Security Gateway
2	Satellite Security Gateways
3	Central Security Gateway

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: **Internal-network**.

To create a new VPN Star Community:

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Access Tools** section, click **VPN Communities**.
3. Click **New** and select **Star Community**.

   The **New Star Community** window opens.
4. Enter the name for the community.
5. From the navigation tree, select **Encryption**.
6. Configure the VPN encryption methods and algorithms for the VPN community.
7. Click **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 **Gateways & Servers** page and double-click the Security Gateway object.

   The Security Gateway properties window opens.

2. In the **Network Security** section of the **General Properties** page, select **IPsec VPN**.
3. From the navigation tree, go to **Network Management > VPN Domain**.
   - For the central Security Gateway, click **Manually defined** and select the **Internal-network** object
   - For a satellite Security Gateway, select **All IP addresses**
4. From the navigation tree, click **IPsec VPN**.
5. Configure the Security Gateway as a member of a VPN star community.
   a. In the **This Security Gateway participates in the following VPN Communities** section, click **Add**.

      The **Add this Gateway to Community** window opens.

   b. Select the VPN Community.

   c. Click **OK**.
6. Click **OK**.

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

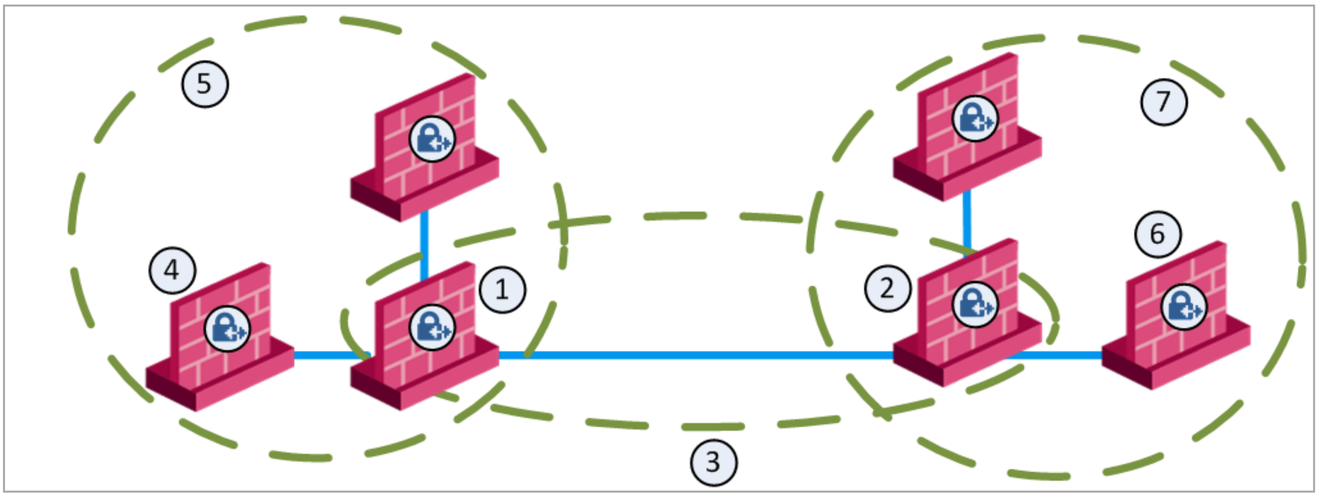
To add a Security Gateway to a new star community

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Access Tools** section, click **VPN Communities**.
3. Select the new star community and click **Edit**.

   The **Star Community** window opens.

4. In the **Gateways** page, add Security Gateways to the community:
   - **Center Gateways** - Click **Add** and select center Security Gateways. Select **Mesh center gateways**, if necessary.
   - **Satellite Gateways** - Click **Add** and select satellite Security Gateways.
5. Click **OK**.

Sample Combination VPN Community



Item	Description
1	London Security Gateway
2	New York Security Gateway
3	London - New York Mesh community
4	London company partner (external network)
5	London Star community
6	New York company partner (external network)
7	New York Star community

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**.)

No.	Name	Source	Destination	VPN	Service	Install On
1	-	Any	**NEGATED** Member Security Gateways	BranchOffices LondonOffices	Any	BranchOffices LondonOffices
2	Site-to-site VPN	Any	Any	All_GwToGw	FTP-port HTTP HTTPS SMTP	Policy Targets
3	Remote access	Any	Any	RemoteAccess	HTTP HTTPS IMAP	Policy Targets

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 *R80.40 Site to Site VPN Administration Guide*.

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

When securely connecting remote clients with the internal resources, organizations face connectivity challenges, such as these:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a LAN with internal IP addresses (such as, at hotels)
- It is necessary for the remote client to use protocols that are not supported

The Check Point IPsec VPN Software Blade provides these VPN connectivity modes to help organizations resolve those challenges:

- **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 avoid VPN routing problems.

- **Visitor Mode**

  Remote users can be restricted to using only HTTP and HTTPS protocols. Visitor Mode lets these users tunnel all protocols through regular TCP connections on port 443.

Sample Remote Access VPN Workflow

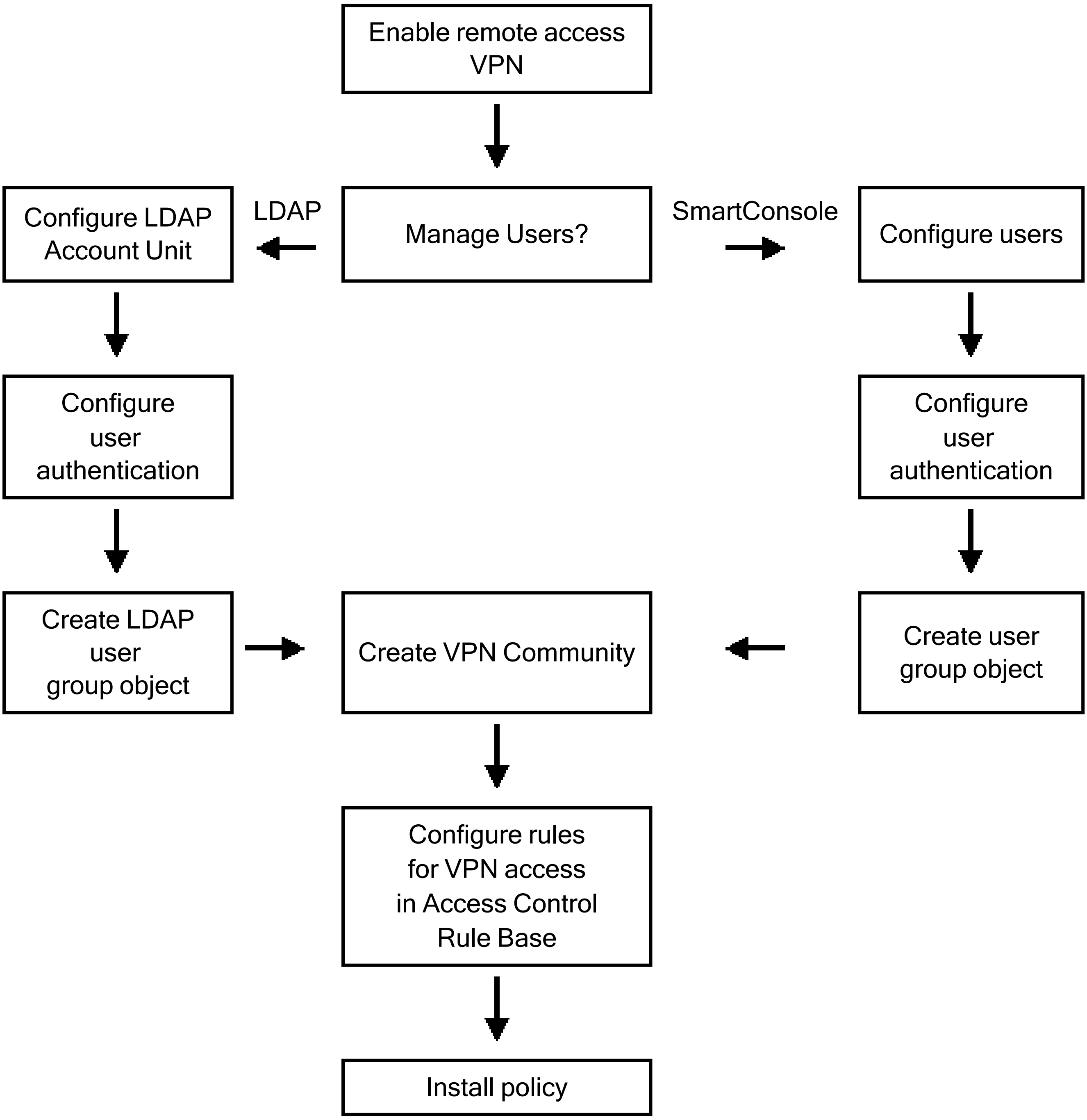
Here is an example of a Remote Access VPN workflow:

1. Use SmartConsole to enable Remote Access VPN on the Security Gateway.
2. Add the remote user information to the Security Management Server:
   - Create and configure an LDAP Account Unit
   - Enter the information in the SmartConsole user database

   Optional: Configure the Security Gateway for remote user authentication.
3. Define the Access Control and encryption rules for the Security Gateway.
4. Create the group objects to use in the Security Gateway rules:

- **LDAP Group** object - for an LDAP Account Unit
- **User Group** object - for users configured in the SmartConsole user database

5. Create and configure the encryption settings for the VPN community object in Menu > **Global properties** > **Remote Access** > **VPN - Authentication and Encryption**.
6. Add Access Control rules to the Access Control Rule Base to allow VPN traffic to the internal networks.


Enable remote access VPN
Manage Users?
LDAP
SmartConsole
Configure LDAP Account Unit
Configure users
Configure user authentication
Configure user authentication
Create LDAP user group object
Create VPN Community
Create user group object
Configure rules for VPN access in Access Control Rule Base
Install policy

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 Security Gateway object 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.

To configure the settings for Visitor Mode

1. From the navigation tree, click **VPN Clients > Office Mode**.

2. Configure the settings for Office Mode.

   Note - Office Mode support is mandatory on the Security Gateway side.

3. Click **OK**.

4. Publish the SmartConsole session.

To Learn More About Remote Access VPN

See the *R81 Remote Access VPN Administration Guide*.

Implied Rules

The Check Point Security Management Server and its managed objects (Security Gateways, Cluster Members, Log Servers, and so on) communicate with each other through the Check Point protocols. By default, each Access Control policy contains predefined implied rules that allow the required internal Check Point communication.

To view the implied rules in SmartConsole:

1. From the left navigation panel, click **Security Policies**.
2. In the top left panel, click **Access Control** > **Policy**.
3. From the top toolbar, click **Actions** > **Implied Rules**.

To configure the implied rules in SmartConsole:

1. In the top left corner, click **Menu** > **Global properties**.
2. In the **Firewall** page, select the applicable options and configure the order of the implied rules.
3. Click **OK**
4. Install the **Access Control** policy on each managed Security Gateway / Cluster / Virtual System.

For more information, see sk179346.

UserCheck in the Access Control Policy

When you enable the UserCheck feature, the Security Gateway sends messages to users about possible non-compliant behavior or dangerous Internet browsing, based on the rules an administrator configured in the Security Policy. This helps users prevent security incidents and learn about the organizational security policy. Create UserCheck objects and use them in the Rule Base, to communicate with the users. You can develop an effective policy based on logged user responses.

These Software Blades support the UserCheck feature:

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

Configuring UserCheck on the Security Gateway

Enable or disable UserCheck directly on the Security Gateway. If users connect to the Security Gateway remotely, set the internal interface of the Security Gateway (on the **Topology** page) to be the same as the **Main URL** for the UserCheck Portal.

To configure UserCheck on a Security Gateway

Step	Instructions
1	Go to the gateway editor, > **UserCheck**, and select **Enable UserCheck for active blades**.

Step	Instructions
2	In the **UserCheck Web Portal** section: The **Main URL** field shows the primary URL for the web portal that shows the UserCheck notifications. You can use the suggested **Main URL** or manually enter a different **Main URL**. **Note** - The **Main URL** field contains an IP address and not a DNS name. Update the **Main URL** field If you change a Security Gateway's IPv4 address to IPv6 address, or the other way around, .
3	Optional: Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**. For example: `Usercheck.mycompany.com` The aliases must be resolved to the portal IP address on the corporate DNS server.
4	In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server. By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority. **Note** - After you download your certificate, you can click **Replace** to replace it with a different certificate, and click **View** to see the certificate information.

Step	Instructions
5	In the **Accessibility** section, click **Edit** to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured for the Security Gateway. The topology must be configured. **Users are sent to the UserCheck Portal if they connect** ■ **Through all interfaces** ■ **Through internal interfaces** (default) • **Including undefined internal interfaces** • **Including DMZ internal interfaces** • **Including VPN encrypted interfaces** (default) - Interfaces used for establishing route-based VPN tunnels (VTIs). ■ **According to the Firewall Policy** - Select this option if there is a rule that states who can access the portal. If the **Main URL** is set to an external interface, you must set the **Accessibility** option to one of these: ■ **Through all interfaces** - Necessary in VSX environment ■ **According to the Firewall Policy**
6	**UserCheck Client** - The UserCheck Client is installed on Endpoint devices to communicate with the Security Gateway and show UserCheck Interaction notifications to users. ■ **Activate UserCheck Client support** - This enables UserCheck through the client. ■ Click **Download Client** to download the installation file for the UserCheck Client. **Note** - The link is not active until the UserCheck Portal is up. For more information about installation and configuration of the UserCheck Client, see .

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>7</td><td>In the <b>Mail Server</b> section, configure a mail server for UserCheck. This server sends notifications to users that the Security Gateway cannot notify using other means, if the server knows the email address of the user. For example, if a user sends an email which matched on a rule, the Security Gateway cannot redirect the user to the UserCheck Portal because the traffic is not HTTP.
<b>If the user does not have a UserCheck Client, UserCheck sends an email notification to the user.</b>
- <b>Use the default settings</b> - Click the link to see which mail server is configured.
- <b>Use specific settings for this gateway</b> - Select this option to override the default mail server settings.
- <b>Send emails using this mail server</b> - Select a mail server from the list, or click <b>New</b> and define a new mail server.</td></tr>
<tr><td>8</td><td>Click <b>OK</b>.</td></tr>
<tr><td>9</td><td>If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy.
<b>This is a sample rule</b>
<table>
<tr><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th></tr>
<tr><td>Any</td><td>Security Gateway on which UserCheck Client is enabled</td><td>Any</td><td>UserCheck</td><td>Accept</td></tr>
</table></td></tr>
<tr><td>10</td><td>Install the Access Control Policy.</td></tr>
</table>

Creating UserCheck Interaction Objects

UserCheck Interaction objects add flexibility and give the Security Gateway a mechanism to communicate with users.

UserCheck Interaction objects:

- Help users with decisions that can be dangerous to the organization security.
- Share the organization's changing internet policy for web applications and sites with users, in real-time.

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

The UserCheck page contains default UserCheck Interaction messages. You can edit, and preview UserCheck Interaction objects and their messages.

To see the default UserCheck Interaction objects:

In SmartConsole, go to **Security Policies** > **Access Control** > **Access Tools** > **UserCheck**.

You can create additional UserCheck Interaction objects based on your needs.

To create a UserCheck Interaction object:

Step	Instructions
1	In the **UserCheck** page, click **New**, and then select the object type: ■ **Ask** Shows a message to users that asks them if they want to continue with the request or not. To continue with the request, the user is expected to supply a reason. ■ **Inform** Shows an informative message to users. Users can continue to the application or cancel the request. ■ **Block** Shows a message to users and blocks the application request. The window opens for the new UserCheck object.
2	**Enter Object Name**.
3	From the menu-bar in the UserCheck object window, click the applicable option: ■ **Source** - Enter HTML code ■ **Design** - Enter text with formatting buttons and options
4	**Optional:** Click **Language** and select one or more languages for the message. The default language for messages is English.

Step	Instructions
5	Enter the text for the title, subtitle, and body of the message. In **Source** mode, in the body of the message, click these options for additional functionality. - **Insert Field** - Dynamic text such as: Original URL, Source IP address, and so on. When the Ask User, Inform User, or Block action occurs, the UserCheck Portal and UserCheck Client replaces these variables with applicable values in the message. **Notes -** To resolve the **Username** variable, you must enable the **Identity Awareness**Software Blade and configure the required settings. See the *R81.20 Identity Awareness Administration Guide*. - **Insert User Input** - To insert special fields for user input, such as: Confirm check box, Report Wrong Category and so on, from the top toolbar, click **Insert User Input** and click the applicable option.
6	**Optional** Click **Add logo** to add a graphic to the message. The size of the graphic must be 176 x 52 pixels.

Step	Instructions
7	You can also click **Settings** from the navigation tree to configure one or more of these options. **Options** ■ **Languages** - Select a language in case the user browser language is not defined. ■ For the Ask and Inform UserCheck Interaction objects, you can select a **Fallback Action** if the user cannot see the message. Select one of these messages: • **Drop** - The connection or traffic is dropped and does not enter the internal network. • **Accept** - The connection or traffic is accepted and enters the internal network. ■ For an Ask UserCheck Interaction object, you can configure **Conditions**: The UserCheck message can contain these items that require user interaction (shown with sample messages). The traffic is allowed only after the user does the necessary actions. Select one or both options: • **User accepted and selected the confirm checkbox** - User is ignoring the warning and wishes to continue. This applies if on the **Message** page from the **Insert User Input** menu you inserted the element **Confirm Checkbox**. • **User entered the required textual input in the user input field** - The user must enter the reason for ignoring the Threat Prevention warning. This applies if on the **Message** page from the **Insert User Input** menu you inserted the element **Textual Input** ⓘ **Important** - The traffic or connection is blocked until the user does the necessary actions. ■ **Redirect the user to an external portal**: You can configure UserCheck to redirect the user to an external UserCheck Portal and the user does not see this UserCheck message. In **External Portal**, enter the URL for the external portal. The URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the Security Gateway. Optional: Select **Add UserCheck Incident ID to the URL query** to add an incident ID to the end of the URL query. **Confirmation sent to the gateway**:

Step	Instructions
	• The URL template field points to an XML file. This file should be placed on the external portal so that it can be sent back to the Security Gateway. • The pre-shared secret authenticates the external portal to the Security Gateway.
8	Click **OK**.
9	Install the Threat Prevention policy.

Send Email Notifications in Plain Text

Not all emails clients can handle emails in rich text or HTML format.

To accommodate such clients, you can configure the Security Gateway to send email notification in plain text without images, in addition to the HTML format. The user's email client decides which format to show.

1. Connect to the command line to the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Back up the configuration file:

   ```
   cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
   ```

4. Edit the configuration file:

   ```
   vi $FWDIR/conf/usrchkd.conf
   ```

5. Change the value of the applicable parameter:

   from

   ```
   :send_emails_with_no_images (false)
   ```

   to

   ```
   :send_emails_with_no_images (true)
   ```

6. Save the changes in the file and exit the editor.

7. Kill the `userchkd` process to load the new configuration:

   ```
   killall userchkd
   ```

   The Security Gateway automatically restarts this process.

UserCheck Client

The UserCheck Client is installed on endpoint computers to communicate with the Security Gateway and show notifications to users.

UserCheck Client sends notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck Client can also work together with the UserCheck Portal to show notifications on the computer itself in these cases:

- It is not possible to show the notification in a web browser.
- The UserCheck engine determines that the notification does not appear correctly in the web browser.

Notifications of incidents are shown in a pop up from the UserCheck Client in the system tray.

Users select an option in the notification message to respond in real-time.

UserCheck Client Requirements

See the *R80.40 Release Notes* > *UserCheck Client Requirements*.

Workflow for installing and configuring UserCheck Clients:

1. Open the Security Gateway object.
2. Enable UserCheck and the UserCheck Client in the Security Gateway object. See *"UserCheck in the Access Control Policy" on page 385* .
3. Configure how the UserCheck Clients communicate with the Security Gateway and create trust with it.

   See *"Client and Gateway Communication" on the next page*.
4. Install the UserCheck Client on the endpoint computers.

   See *"Installing UserCheck Client" on page 400*.
5. Connect the UserCheck Client to the Security Gateway.

   See *"Connecting UserCheck Client to the Security Gateway" on page 404*.
6. Make sure the UserCheck Clients can receive notifications.

Perform a simplest action on the endpoint computers that violates the configured Security Policy.

Client and Gateway Communication

In an environment with UserCheck Clients, the Security Gateway acts as a server for the clients. Each client must be able to *discover* the server and create *trust* with it.

To create trust, the client makes sure that the server is the correct one. It compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the server does not have the expected fingerprint, the client asks the user to manually confirm that the server is correct.

Here is a list of the methods that you can use for clients to discover and trust the server.

Option Comparison

Configuration	Must Have AD	Manual User Trust (one time) Necessary?	Multi-Site	Client Stays Signed?	Still works after Gateway Changes	Level	Recommended for...
File name based	No	Yes	No	Yes	No	Very Simple	Single Security Gateway configurations
AD based	Yes	No	Yes	Yes	Yes	Simple	Configurations with AD that you can modify
DNS based	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Configurations without AD With an AD you cannot change, and a DNS that you can change

Configuration	Must Have AD	Manual User Trust (one time) Necessary?	Multi-Site	Client Stays Signed?	Still works after Gateway Changes	Level	Recommended for...
Remote registry	No	No	Yes	Yes	Yes	Moderate	Where remote registry is used for other purposes

1. **File name based server configuration**

   If no other method is configured (default, out-of-the-box situation), all UserCheck Clients downloaded from the portal are renamed to have the portal machine IP address in the filename. During installation, the client uses this IP address to connect to the Security Gateway. Note that the user has to click **Trust** to manually trust the server.

   Explanation

   This option is the easiest to configure, and works out-of-the-box. It tells users to manually click **Trust** to trust the server the first time they connect. You can use this option if your configuration has only one Security Gateway with the relevant Software Blades.

   ### How does it work?

   When a user downloads the UserCheck Client, the address of the Security Gateway is inserted in the filename. During installation, the client finds if there is a different discovery method configured (AD based, DNS based, or local registry). If no method is configured, and the Security Gateway can be reached, it is used as the server. In the UserCheck Settings window, you can see that the server you connect to is the same as the Security Gateway in the UserCheck Client filename.

   Users must manually make sure that the trust data is valid, because the filename can be easily changed.

   Renaming the MSI

   You can manually change the name of the MSI file before it is installed on a computer.

   This connects the UserCheck Client to a different Security Gateway.

a. Make sure the Security Gateway has a DNS name.

b. Rename the MSI using this format:

UserCheck_~*GWname*.msi

Where *GWname* - is the DNS name of the Security Gateway.

Optional format:

UserCheck_~*GWname-port*.msi

Where *port* is the port number of notifications.

For example:

```
UserCheck_~mygw-18300.msi
```

Notes:

- The prefix does not have to be "UserCheck". The important part of the format is underscore tilde (_~), which indicates that the next string is the DNS of the Security Gateway.
- If you want to add the port number for the notifications to the client from the Security Gateway, the hyphen (-) indicates that the next string is the port number.

2. **Active Directory Based Configuration**

If client computers are members of an Active Directory domain, you can configure the server addresses and trust data using a dedicated tool.

Explanation

If your client computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- **Welcome** - Describes the tool and lets you enter different credentials that are used to access the AD.
- **Server configuration** - Configure which Security Gateway the client connects to, based on its location.
- **Trusted Security Gateways** - View and change the list of fingerprints that the Security Gateways consider secure.

To enable Active Directory based configuration for clients:

a. Download and install the UserCheck Client MSI on a computer.

   From the command line on that computer, run the client configuration tool with the AD utility.

   For example, on a Windows 7 computer:

```
"C:\Users\%USERNAME%\Local Settings\Application
Data\Checkpoint\UserCheck\UserCheck.exe" -adtool
```

   The **Check Point UserCheck - Distributed Configuration** tool opens.

b. In the **Welcome** page, enter the credentials of an AD administrator.

   By default, your AD username is shown. If you do not have administrator permissions, click **Change user** and enter administrator credentials.

c. In the **Server Configuration** page, click **Add**.

   The **Identity Server Configuration** window opens.

d. Select **Default** and then click **Add**.

e. Enter the IP address or Fully Qualified Domain Name (FQDN) and the port of the Security Gateway.

f. Click **OK**.

   The identity of the AD Server for the UserCheck Client is written in the Active Directory and given to all clients.

Note - The entire configuration is written under a hive named **Check Point** under the **Program Data** branch in the AD database that is added in the first run of the tool. Adding this hive does not affect other AD based applications or features.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure the client to **Automatically discover** the server, the client fetches the rule lists. Each time it must connect to a server, it tries to match itself against a rule, from top to bottom.

When the tool matches a rule, it uses the servers shown in the rule, according to the priority specified.

The configuration in this example means:

a. If the user is coming from `'192.168.0.1 - 192.168.0.255'`, then try to connect to `US-GW1`.

   If it is not available, try `BAK-GS2` (it is only used if `US-GW1` is not available, as its priority is higher).

b. If the user is connected from the Active Directory site `'UK-SITE'`, connect either to `UK-GW1` or `UK-GW2` (select between them randomly, as they both have the same priority). If both of them are not available, connect to `BAK-GS2`.

c. If rules 1 and 2 do not apply, connect to `BAK-GS2` (the default rule is always matched when it is encountered).

Use the **Add**, **Edit** and **Remove** buttons to change the server connectivity rules.

Trusted Gateways

The **Trusted Gateways** window shows the list of servers that are trusted - no messages open when users connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint. Enter its IP address and click **Fetch Fingerprint** in the **Server Trust Configuration** window. If you do not have connectivity to the server, enter the same name and fingerprint that is shown when you connect to that server.

3. **DNS SRV Record Based Server Discovery**

Configure the server addresses in the DNS server. Note that the user has to click **Trust** to manually trust the server.

Explanation

If you configure the client to **Automatic Discovery** (the default), it looks for a server by issuing a DNS SRV query for the address of the Security Gateway (the DNS suffix is added automatically). You can configure the address in your DNS server.

To configure DNS based configuration on the DNS server:

a. Go to **Start** > **All Programs** > **Administrative Tools** > **DNS**.

b. Go to **Forward lookup zones** and select the applicable domain.

c. Go to the **_tcp** subdomain.

d. Right-click and select **Other new record**.

e. Select **Service Location**, **Create Record**.

f. In the **Service** field, enter **CHECKPOINT_DLP**.

g. Set the **Port number** to 443.

h. In **Host offering this server**, enter the IP address of the Security Gateway.

i. Click **OK**.

To configure Load Sharing for the Security Gateway, create multiple SRV records with the same priority.

To configure High Availability, create multiple SRV records with different priorities.

Note - If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting DNS Based Configuration

To troubleshoot issues in DNS based configuration, you can see the SRV records that are stored on the DNS server.

To see SRV records on the DNS server:

Run:

```
C:\> nslookup
 > set type=srv
 > checkpoint_dlp._tcp
```

Example result:

```
C:\> nslookup
 > set type=srv
 > checkpoint_dlp._tcp
Server: dns.company.com
Address: 192.168.0.17
checkpoint_dlp._tcp.ad.company.com SRV service location:
          priority = 0
          weight = 0
          port = 443
          svr hostname = dlpserver.company.com
dlpserver.company.com internet address = 192.168.1.212
>
```

Remote Registry

All of the client configuration, including the server addresses and trust data reside in the registry. You can configure the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration when the client is first installed.

Explanation

If you have a way to configure registry entries to your client computers, for example, Active Directory or GPO updates, you can configure the Security Gateway addresses and trust parameters before you install the clients. Clients can then use the configured settings immediately after installation.

To configure the remote registry option:

1. Install the client on one of your computers. The agent installs itself in the user directory, and saves its configuration to `HKEY_CURRENT_USER`.
2. Connect manually to all of the servers that are configured, verify their fingerprints, and click **Trust** on the fingerprint verification dialog box.
3. Configure the client to manually connect to the requested servers (use the **Settings** window).
4. Export these registry keys:
   a. The entire tree:

      `HKEY_CURRENT_USER\SOFTWARE\CheckPoint\UserCheck\Trusted Gateways`

   b. The branch:

      `HKEY_CURRENT_USER\SOFTWARE\CheckPoint\UserCheck\`

      i. The key:

         `Default Gateway`

      ii. The key:

         `DefaultGatewayEnabled`
5. Import the exported keys to the endpoint computers before you install the UserCheck Client.

Installing UserCheck Client

After configuring the clients to connect to the Security Gateway, install the clients on the user machines.

1. Get the UserCheck Client MSI file from the Security Gateway in **one** of these ways:

   Download the UserCheck Client from the Security Gateway using an SCP client

   Important - The SCP user must have the default shell `/bin/bash` in Gaia OS on the Security Gateway.

a. Go to this directory:

```
/opt/CPUserCheckPortal/htdocs/UserCheck/client/
```

b. Download this file:

```
Check_Point_UserCheck.msi
```

Download the UserCheck Client from the Security Gateway object in SmartConsole

> **Important** - Before you can use this link, you must install an Access Control policy at least one time so that the UserCheck Portal starts.

a. From the left navigation panel, click **Gateways & Servers**.

b. Double-click the Security Gateway object.

c. From the left tree, click **General Properties**.

d. Enable at least one of these Software Blades:

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

e. From the left tree, click **UserCheck**.

f. In the section **UserCheck Client**, click the link **Download Client**.

g. The download opens in your default web browser.

2. Install the UserCheck Client on the user endpoint computers.

   You can use any method of MSI mass configuration and installation that you select.

For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

Notes:

- The installation is silent.
  Reboot is not necessary.
- To install the UserCheck Client for all user accounts on a Windows computer, see sk96107.
- To uninstall the UserCheck Client from a Windows computer, see *"Uninstalling UserCheck Client" below*.

Uninstalling UserCheck Client

Default Uninstall Procedure

1. Go to the **Start** menu > **Check Point** > **UserCheck**.
2. Click the "**Uninstall**" shortcut.
3. Follow the instructions on the screen.
4. Restart the endpoint computer.

Manual Uninstall Procedure

If there is no "**Uninstall**" shortcut in the **Start** menu, follow **one** of these procedures:

Uninstall the UserCheck Client manually using Windows Installer

1. Make sure the **UserCheck.exe** application is not running.

   Use Windows Task Manager, or any similar 3rd-party tool.

   If it is currently running, end / kill it.

2. Get the UserCheck Client GUID from the Windows Registry Editor:

   a. Open the Windows Registry Editor (**regedit**):

      i. Click the **Start** menu.

      ii. Enter **regedit**.

      iii. Click **Registry Editor**.

      Alternatively, press the **Windows + R** keys > type **regedit** > click OK / press the Enter key.

   b. Navigate to:

   ```
   Computer\HKEY_CURRENT_
   USER\Software\CheckPoint\UserCheck\1.0
   ```

   c. Right-click the key **PRODUCT_GUID** > click **Modify**.

   d. Copy the entire string **{<GUID>}** and paste it in a plain-text editor.

   e. Click **Cancel** in the Windows Registry Editor.

   f. Close the Windows Registry Editor.

3. In the plain-text editor, prepare the required syntax:

   ```
   %SystemRoot%\SysWOW64\msiexec.exe /x {<GUID you copied from
   Windows Registry Editor>}
   ```

   Dummy example:

   ```
   C:\Windows\SysWOW64\msiexec.exe /x {AAD3D77A-7476-469F-ADF4-
   04424124E91D}
   ```

   Reference:

   https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec

4. Open Windows Command Prompt:

   a. Click the **Start** menu.

   b. Enter **cmd**.

   c. Click **Command Prompt**.

   Alternatively, press the **Windows + R** keys > type **cmd** > click OK / press the Enter key.

5. Paste the required syntax from the plain-text editor and press the Enter key.

6. Restart the endpoint computer.

Delete the UserCheck client manually from the endpoint computer

1. Make sure the **UserCheck.exe** application is not running.

   Use Windows Task Manager, or any similar 3rd-party tool.

   If it is currently running, end / kill it.

2. Delete the **UserCheck** folder:

Important - You must delete this folder for each user on the computer.

a. In Windows File Manager (or any file manager), go to:

```
C:\Users\%USERNAME%\AppData\Local\CheckPoint\
```

b. Delete this folder:

```
UserCheck
```

3. Delete the **UserCheck** branch in the Windows Registry:

   a. Open the Windows Registry Editor (**regedit**):

      i. Click the **Start** menu.

      ii. Enter **regedit**.

      iii. Click **Registry Editor**.

      Alternatively, press the **Windows + R** keys > type **regedit** > click OK / press the Enter key.

   b. Navigate to:

```
Computer\HKEY_CURRENT_
USER\Software\CheckPoint\UserCheck
```

   c. Back up the Windows Registry.

      Refer to the Microsoft article "Windows registry information for advanced users".

   d. Right-click the **UserCheck** branch > click **Delete** > confirm.

   e. Close the Windows Registry Editor.

4. Restart the endpoint computer.

Connecting UserCheck Client to the Security Gateway

Connecting UserCheck Client

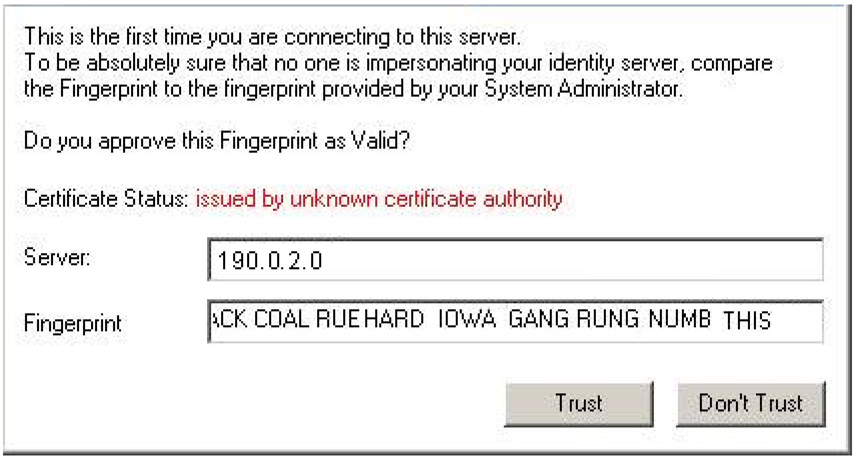
If UserCheck for DLP is enabled on the Security Gateway, users must enter their username and password after the client installs.

When the UserCheck Client is first installed, the UserCheck Client tray icon indicates that it is not connected.

When the UserCheck Client connects to the Security Gateway, the UserCheck Client tray icon shows that the client is active.

The first time that the UserCheck Client connects to the Security Gateway, it asks user to approve of the Security Gateway fingerprint.

Example:



This is the first time you are connecting to this server.
To be absolutely sure that no one is impersonating your identity server, compare the Fingerprint to the fingerprint provided by your System Administrator.

Do you approve this Fingerprint as Valid?

Certificate Status: issued by unknown certificate authority

Server: 190.0.2.0

Fingerprint: ACK COAL RUE HARD IOWA GANG RUNG NUMB THIS

Best Practices:

- Let the users know this happens.
- Use a certificate that is trusted by the certificate authority installed on users' computers.
  Then users do **not** see a message "`Issued by unknown certificate authority`".

Example of message to users about the UserCheck Client installation (for DLP):

```
Dear Users,
Our company has implemented a Data Loss Prevention automation to
protect our confidential data from unintentional leakage. Soon you
will be asked to verify the connection between a small client that
we will install on your computer and the computer that will send
you notifications.
This client will pop up notifications if you try to send a message
that contains protected data. It might let you to send the data
anyway, if you are sure that it does not violate our data-security
guidelines.
When the client is installed, you will see a window that asks if
you trust the DLP server. Check that the server is SERVER NAME and
then click Trust.
In the next window, enter your username and password, and then
click OK.
```

Note - If the UserCheck Client is not connected to the Security Gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Gaia Portal is used for HTTP incidents.

UserCheck and Check Point Password Authentication

To enable Check Point password authentication:

1. SmartConsole Configuration:
    1. From the top, click **Objects** > **Object Explorer**.
    2. In the left pane, select only **Users/Identities**.
    3. Configure the required settings:

        If the required User object already exists

        1. Double-click the applicable **User** object.
        2. From the left, click **General**.
        3. In the **General properties** section, make sure to configure a valid email address.
        4. Click **OK**.

        If the required User object does not exist yet

        1. Make sure the applicable **User Template** object exists.

            If it does not, from the top toolbar, click **New** > **Users/Identity** > **User Template** > configure the required settings > click **OK**.
        2. From the top toolbar, click **New** > **Users/Identity** > **User**.
        3. Select the required **User Template** and click **OK**.
        4. Configure the required settings:
            - At the top, configure the object name
            - On **General** page, in the **General properties** section, make sure to configure a valid email address.
            - On **Authentication** page, in the **Authentication Method** section, select **Check Point Password** > click **Set new password** > enter the password > click **OK**.
        5. Click **OK**.
    4. Close the **Object Explorer** window.
2. UserCheck Client Configuration:

a. On the endpoint computer, right-click the UserCheck Client icon in the Notification Area (next to the system clock).

b. Click **Settings**.

c. Click **Advanced**.

d. Select **Authentication with Check Point user accounts defined internally in SmartConsole**.

Helping Users

If users require assistance to troubleshoot issues with the UserCheck Client, you can ask them to send you the logs.

To configure the UserCheck Client to generate logs:

1. Right-click the UserCheck Client tray icon and select **Settings**.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.
4. Make sure that the UserCheck Clients can connect to the Security Gateway and receive notifications.

   See *"Connecting UserCheck Client to the Security Gateway" on page 404*.

To send UserCheck Client logs from the endpoint computer:

1. Right-click the UserCheck Client tray icon and select **Status**.
2. Click **Advanced**.
3. Click the link **Collect information for technical support**.

   The default email client opens, with an archive of the collected logs attached.

Localizing and Customizing the UserCheck Portal

For more information, see sk83700.

Creating a New Threat Prevention Policy

To learn about configuring a Threat Prevention Policy, see the *R80.40 Threat Prevention Administration Guide*.

HTTPS Inspection

HTTPS Internet traffic uses the TLS (Transport Layer Security) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new TLS connections with the external site or server. The Security Gateways are then able to decrypt and inspect HTTPS traffic that uses the new TLS connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.
- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that arrive from the Internet or an external network.

The Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

For information on what's new in HTTPS Inspection starting from R80.20, see sk163594.

Inspecting HTTPS Connections

Outbound HTTPS Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to an external server.

Outbound connection flow

1. An HTTPS request (from an internal client to an external server) arrives at the Security Gateway.
2. The Security Gateway inspects the HTTPS request.
3. The Security Gateway determines whether the HTTPS request matches an existing HTTPS Inspection rule:
   - If the HTTPS request does **not** match a rule, then the Security Gateway does not inspect the HTTPS payload.
   - If the HTTPS request matches a rule, then the Security Gateway continues to the next step.
4. The Security Gateway validates the HTTPS certificate from the external server.

   The Security Gateway uses the Online Certificate Status Protocol (OCSP) standard.
5. The Security Gateway creates a new certificate for the connection to the external server.
6. The Security Gateway decrypts the HTTPS connection.
7. The Security Gateway inspects the decrypted HTTPS connection.
8. If the Security Policy allows this traffic, the Security Gateway encrypts the HTTPS connection.
9. The Security Gateway sends the HTTPS request to the external server.

Inbound HTTPS Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network.

Inbound connection flow

1. An HTTPS request (from an external client to an internal server) arrives at the Security Gateway.
2. The Security Gateway inspects the HTTPS request.
3. The Security Gateway determines whether the HTTPS request matches an existing HTTPS Inspection rule:
   - If the HTTPS request does **not** match a rule, then the Security Gateway does not inspect the HTTPS payload.
   - If the HTTPS request matches a rule, then the Security Gateway continues to the next step.
4. The Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client.
5. The Security Gateway creates a new HTTPS connection with the internal server.
6. The Security Gateway decrypts the HTTPS connection.
7. The Security Gateway inspects the decrypted HTTPS connection.
8. If the Security Policy allows this traffic, the Security Gateway encrypts the HTTPS connection and sends it to the internal server.

Configuring Gateways to inspect outbound and inbound HTTPS

This section gives an example of how to configure a Gateway to inspect outbound and inbound HTTPS traffic.

Workflow overview

Step	Instructions
1	Enable HTTPS Inspection on the Security Gateway.
2	Configure the Security Gateway to use the certificate. ■ **Outbound Inspection** - Generate a new certificate for the Security Gateway ■ **Inbound Inspection** - Import the certificate for the internal server

Step	Instructions
3	Configure the HTTPS Inspection Rule Base.
4	Install the Access Control Policy.

Enabling HTTPS Inspection

You must enable HTTPS Inspection on each Security Gateway.

To enable HTTPS Inspection on a Security Gateway

Step	Instructions
1	From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2	Click **HTTPS Inspection** > **Step 3**.
3	Select **Enable HTTPS Inspection**.

The first time you enable HTTPS Inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS Inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Creating an Outbound CA Certificate

The outbound CA certificate is saved with a CER file extension and uses a password to encrypt the private key of the file. The Security Gateways use this password to sign certificates for the sites accessed. You must keep the password because it is also used by other Security Management Servers that import the CA certificate to decrypt the file.

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive TLS error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections.

After you create the outbound CA certificate, a certificate object named Outbound Certificate is created. Use this object in rules that inspect outbound HTTPS traffic in the HTTPS Inspection Rule Base.

To create an outbound CA certificate

Step	Instructions
1	In SmartConsole **Gateways & Servers** view, right-click the Security Gateway object and select **Edit**. The **Gateway Properties** window opens.
2	In the navigation tree, select HTTPS Inspection.
3	In **Step 1** of the HTTPS Inspection page, click **Create**. The **Create** window opens.
4	Enter the necessary information: ▪ **Issued by (DN)** - Enter the domain name of your organization. ▪ **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate. ▪ **Retype private key password** - Retype the password. ▪ **Valid from** - Select the date range for which the CA certificate is valid.
5	Click **OK**.
6	Export and deploy the CA certificate (see *"Exporting and Deploying the Generated CA" on page 415*).

Importing an Outbound CA Certificate

You can import a CA certificate that is already deployed in your organization or import a CA certificate created on one Security Management Server to another Security Management Server.

Best Practice - Use *private* CA Certificates.

For each Security Management Server that has Security Gateways enabled with HTTPS Inspection, you must:

- Import the CA certificate.
- Enter the password the Security Management Server uses to decrypt the CA certificate file and sign the certificates for users. Use this password only when you import the certificate to a new Security Management Server.

To import a CA certificate

Step	Instructions
1	If the CA certificate was created on another Security Management Server, export the certificate from the Security Management Server, on which it was created (see *"Exporting a Certificate from the Security Management Server" below*).
2	In the SmartConsole Gateways & Servers view, right-click the Security Gateway object and select **Edit**. The **Gateway Properties** window opens.
3	In the navigation tree, select HTTPS Inspection.
4	In **Step 1** of the HTTPS Inspection page, click **Import**. The **Import Outbound Certificate** window opens.
5	Browse to the certificate file.
6	Enter the **private key password**.
7	Click **OK**.
8	If the CA certificate was created on another Security Management Server, deploy it to clients (see *"Exporting and Deploying the Generated CA" on the next page*).

Exporting a Certificate from the Security Management Server

If you use more than one Security Management Server in your organization, you must *first* export the CA certificate with the `export_https_cert` CLI command from the Security Management Server on which it was created before you can import it to other Security Management Servers.

Command syntax

```
export_https_cert [-local] | [-s server] [-f certificate file
name under FWDIR/tmp][-help]
```

To export the CA certificate

On the Security Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f [certificate file name
under FWDIR/tmp]
```

Example

```
$FWDIR/bin/export_https_cert -local -f mycompany.cer
```

Exporting and Deploying the Generated CA

To prevent users from getting warnings about the generated CA certificates that HTTPS Inspection uses, install the generated CA certificate used by HTTPS Inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.

When users run standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

To distribute a certificate with a GPO

Step	Instructions
1	From the HTTPS Inspection window of the Security Gateway, click **Export certificate**.
2	Save the CA certificate file.
3	Use the Group Policy Management Console to add the certificate to the Trusted Root Certification Authorities certificate store (see *"Deploying Certificates by Using Group Policy" below*).
4	Push the Policy to the client computers in the organization. **Note** - Make sure that the CA certificate is pushed to the client computer organizational unit.
5	Test the distribution by browsing to an HTTPS site from one of the clients. Also, verify that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

Deploying Certificates by Using Group Policy

You can use this procedure to deploy a certificate to multiple client machines with Active Directory Domain Services and a Group Policy Object (GPO). A GPO can contain multiple configuration options, and is applied to all computers in the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.

To deploy a certificate using Group Policy

Step	Instructions
1	On the Microsoft Windows Server, open the **Group Policy Management Console**.
2	Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3	Right-click the GPO and select **Edit**. The **Group Policy Management Editor** opens and shows the contents of the policy object.
4	Open **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Publishers**.
5	Click **Action** > **Import**.
6	Do the instructions in the **Certificate Import Wizard** to find and import the certificate you exported from SmartConsole.
7	In the navigation pane, click **Trusted Root Certification Authorities** and repeat steps 5-6 to install a copy of the certificate to that store.

Configuring Inbound HTTPS Inspection

Configure the Security Gateway for inbound HTTPS Inspection.

Note - By design, the Security Gateway / Cluster is intentionally configured not to perform HTTPS Inspection on traffic directed towards it. To change this behavior, follow sk114574.

To enable inbound HTTPS traffic inspection

Step	Instructions
1	From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2	Click HTTPS Inspection > **Step 3**.
3	Select **Enable HTTPS Inspection**.
4	Import server certificates for servers behind the organization Security Gateway.

Step	Instructions
5	Define an HTTPS Inspection policy: - Create rules - Add a sever certificate to the **Certificate** column of each rule.

The first time you enable HTTPS Inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS Inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Assigning a Server Certificate for Inbound HTTPS Inspection

Add the server certificates to the Security Gateway. This creates a server certificate object.

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the traffic. The Security Gateway inspects the inbound traffic and creates a new HTTPS connection from the gateway to the internal server. To allow HTTPS Inspection, the Security Gateway must use the original server certificate and private key. The Security Gateway uses this certificate and the private key for TLS connections to the internal servers.

After you import a server certificate (with a CER file extension) to the Security Gateway, add the object to the HTTPS Inspection Policy.

Do this procedure for all servers that receive connection requests from clients outside of the organization.

To add a server certificate for inbound HTTPS Inspection

Step	Instructions
1	In SmartConsole, go to **Security Policies** > **HTTPS Inspection** > **HTTPS Tools** > **Additional Settings**.
2	Click **Open HTTPS Inspection Policy In SmartDashboard**. SmartDashboard opens.
3	Click **Server Certificates**.
4	Click **Add**. The **Import Inbound Certificate** window opens.
5	Enter a **Certificate name** and a **Description** (optional).
6	Browse to the certificate file.

Step	Instructions
7	Enter the **Private key password**. Enter the same password that was used to protect the private key of the certificate on the server.
8	Click **OK**.

The **Successful Import** window opens the first time you import a server certificate. It shows you where to add the object in the HTTPS Inspection Rule Base. Click **Don't show this again** if you do not want to see the window each time you import a server certificate and **Close**.

HTTPS Inspection Policy

The HTTPS Inspection rules define how the Security Gateways inspect HTTPS traffic. The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection rules are applied to all the Software Blades that have HTTPS Inspection enabled. These are the Software Blades that support HTTPS Inspection:

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

Starting from R80.40, the HTTPS Inspection policy is in SmartConsole > the **Security Policies** view > **HTTPS Inspection**. Starting from R80.40 you can create different HTTPS Inspection layers per different policy packages. When you create a new policy package, you can use the pre-defined HTTPS Inspection layer, or customize the HTTPS Inspection layer to fit your security needs.

You can share an HTTPS Inspection layer across multiple policy packages.

Note - When you go to the **Security Policies** view > **HTTPS Inspection** > **HTTPS Tools** > **Additional Settings** > **Open HTTPS Inspection Policy In SmartDashboard**, SmartDashboard unexpectedly closes, if there are more than 100,000 network objects configured in the management database of the Management Server.

Fields

These are the fields that manage the rules for the HTTPS Inspection Security Policy.

Field	Description
No.	Rule number in the HTTPS Inspection Rule Base.
Name	Name that the system administrator gives this rule.
Source	Network object that defines where the traffic starts.
Destination	Network object that defines the destination of the traffic.
Services	The network services that are inspected or bypassed. By default, the services `HTTPS` on port 443 and `HTTP_and_HTTPS proxy` on port 8080 are inspected. You can add or delete services from the list.
Site Category	Categories for applications or web sites that are inspected or bypassed.
Action	Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (**Bypass**).
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that will enforce the HTTPS Inspection Policy. You can only select Security Gateways that have HTTPS Inspection enabled (by default, the gateways which appear in the Install On column have HTTPS inspection enabled).
Certificate	The certificate that is used for this rule. ▪ Inbound HTTPS Inspection - Select the certificate that the internal server uses. You can create server certificates from the SmartDashboard > **HTTPS Inspection** > **Server Certificates** > **Add**. ▪ Outbound HTTPS Inspection - Select the Outbound Certificate object that you are using for the computers in the network. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client.
Comment	An optional field that lets you summarize the rule.

Configuring HTTPS Inspection Rules

Create different HTTPS Inspection rules for outbound and inbound traffic.

The outbound rules use the certificate that was generated for the Security Gateway.

The inbound rules use a different certificate for each internal server.

You can also create bypass rules for traffic that is sensitive and should not be inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

After creating the rules, install the Access Control Policy.

Sample HTTPS Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy (The **Track** and **Install On** columns are not shown. **Track** is set to **Log** and **Install On** is set to **HTTPS policy targets**.)

No	Name	Source	Destination	Services	Site Category	Action	Blade	Certificate
1	Inbound traffic	Any	WebCalendar Server	HTTPS	Any	Inspect	Any	WebCalendar Server CA
2	Financial sites	Any	Internet	HTTPS HTTP_HTTPS_proxy	Financial Services	Bypass	Any	Outbound CA
3	Outbound traffic	Any	Internet	HTTPS HTTP_HTTPS_proxy	Any	Inspect	Any	Outbound CA

1. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.

2. **Financial sites** - This is a bypass rule that does not inspect HTTPS traffic to websites that are defined in the Financial Services category.
3. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

HTTPS Inspection Logs

HTTPS Inspection Rule Base enforcement consists of two steps:

1. Matching the connection against the Rule Base.
2. Calculating the action to be performed.

The action is calculated according to the matched rule, the Software Blades defined on the matched rule and the rule exceptions. In certain scenarios, the action in the matched rule is Inspect, but as a result of Step 2, the action is changed to Bypass. In such case, the HTTPS Inspection log is sent with data from the matched rule, but the action in the log is Bypass.

Example 1:

The rule in the HTTPS Inspection policy defines Action: Inspect and Blade: Threat Emulation. The Threat Emulation blade is not enabled on a specific gateway. On that gateway, the traffic is not inspected by Threat Emulation, and the log indicates Action: Bypass.

Example 2:

The administrator defined one rule in the HTTPS Inspection Policy:

Source	Destination	Services	Action	Track	Blade
Any	Any	HTTPS	Inspect	Log	IPS

The administrator also added the 10.1.1.0/24 net to the Global Exceptions for the IPS blade. User with IP 10.1.1.2 surfs to some HTTPS websites.

HTTPS Inspection Rule Base execution:

The connection was matched to the rule with action Inspect.

IPS is the only active blade on the matched rule, but the connection is in exception for the IPS blade. Therefore the updated action is Bypass.

Performed action: SSL is not terminated, HTTPS Inspection log is sent with data from the matched rule, and the action sent is Bypass.

Bypassing HTTPS Inspection for Software Update Services

Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.

To bypass HTTPS Inspection for software updates

Step	Instructions
1	In SmartConsole, go to Security Policies > **HTTPS Inspection**> **HTTPS Tools** > **Additional Settings** > **Open HTTPS Inspection Policy in SmartDashboard**.
2	In SmartDashboard, click the HTTPS Inspection tab.
3	Click **HTTPS Validation**.
4	Go to **Whitelisting** and select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
5	Click **list** to see the list of approved domain names.

Managing Certificates by Gateway

The Gateways pane in the HTTPS Inspection tab in SmartDashboard lists the gateways with HTTPS Inspection enabled.

In the CA Certificate section, in the lower part of the Gateways pane, you can **Renew** the certificate validity date range if necessary and **Export** it for distribution to the organization client machines.

If the Security Management Server which manages the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**.

- You can import a CA certificate already deployed in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export it from the Security Management Server on which it was created (see *"Exporting and Deploying the Generated CA" on page 415*).

Adding Trusted CAs for Outbound HTTPS Inspection

When a client initiates an HTTPS connection to a website server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the Security Gateway to the designated server.

When the Security Gateway establishes a secure connection (a TLS tunnel) to the designated website, it must validate the site server certificate.

HTTPS Inspection comes with a preconfigured list of trusted CAs. This list is updated by Check Point when necessary and is automatically downloaded to the Security Gateway. After you install the update, make sure to install the policy. You can select to disable the automatic update option and manually update the Trusted CA list.

If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates.

Saving a CA Certificate

You can save a selected certificate in the trusted CAs list to the local file system.

To export a CA certificate

Step	Instructions
1	In SmartDashboard, go to the HTTPS Inspection tab > **Trusted CAs**.
2	Click **Actions** > **Export to file**.
3	Browse to a location, enter a file name and click **Save**. A `*.cer` file is created.

HTTPS Validation

On the **HTTPS Validation** page of SmartDashboard you can set options for:

- Fail mode
- HTTPS site categorization mode
- Server validation
- Certificate blacklisting
- Whitelisting
- Troubleshooting

To learn more about these options, see the Help. Click the **?** symbol in the **HTTPS Validation** page.

Showing HTTPS Inspection Logs

The predefined log query for HTTPS Inspection shows all HTTPS traffic that matched the HTTPS Inspection policy, and was configured to be logged.

To see HTTPS Inspection Logs

Step	Description
1	In the SmartConsole Logs & Monitor view, go to the **Logs** tab, and click **Queries**.
2	Select the HTTPS Inspection query.

The **Logs** tab includes an **HTTP Inspection Action** field. The field value can be *inspect* or *bypass*. If HTTPS Inspection was not done on the traffic, this field does not show in the log.

SNI support for Site Categorization

Site Categorization allows the categorization of HTTPS sites before the HTTPS Inspection begins, and prevents connectivity failure if the inspection does not succeed.

SNI support is enabled by default.

SNI is an extension to the TLS protocol, which indicates the hostname at the start of the TLS handshaking process.

The categorization is performed by examining the SNI field in the client hello message at the beginning of the TLS handshaking process. To make sure that you reached the right site, the SNI is verified against the Subject Alternative Name of the host, which appears in the certificate.

After the identity of the host is known and verified, the site is categorized, and it is determined whether the connection should be inspected or not.

The HTTPS Inspection feature decrypts traffic for better protection against advanced threats, bots, and other malware.

Client Certificates for Smartphones and Tablets

To allow your users to access their resources using their handheld devices, make sure they can authenticate to the Security 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 (see *"Giving Permissions for Client Certificates" on page 430*).

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.

Manage client certificates in **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**..

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 Security Gateway, to which users connect.
      - **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. In 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

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
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 inside the E-mail Template body.

9. Click **Insert Link** and select the type of link to add (link or QR code).

   - **Site and Certificate Creation**

     For users who already have a Check Point app installed.

     When users scan the QR 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 Layer 3 tunnel app that gives users network access to all mobile applications.

   - **Download Application**

     Direct users to download a Check Point App for their mobile devices.

     Select the client device operating system:

     - **iOS**

     - **Android**

     Select the client type 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 Layer 3 tunnel app that gives users network access to all mobile applications.

   - **Custom URL**

     Lets you configure your own URL.

For each link type, you can select which elements are added to the mail template

- **Link URL** - Enter the full link address.
- **QR Code** - When enabled, users scan the code with their mobile devices.
- **HTML Link** - When enabled, users tap the link on their mobile devices.

  You can select both **QR Code** and **HTML Link** to include both in the email.
- **Display Text** - Enter the text for the link title.

10. Click **OK**.
11. **Optional:** Click **Preview in Browser** to see a preview of how the email will look.
12. Click **OK**.
13. 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 (see *"Managing Administrator Accounts" on page 48*).
2. Create a customized profile for the administrator, with permission to handle client certificates. Configure this in the **Others** page of the Administrator Profile. Restrict other permissions (see.*"Assigning Permission Profiles to Administrators" on page 72*).

Preferences and Management Settings

Database Revisions

The Security Management architecture has built-in revisions. Each publish operation creates a new revision which contains only the changes from the previous revisions.

Benefits of the revision architecture:

- Safe recovery from a crisis, restore a Domain to a good known revision (see Notes below).
- Fast policy verification, based on the difference between installed versions
- More efficient Management High Availability.

Important - Before using the revision feature consider these limitations:

- Reverting to a previous revision is an irreversible operation, newer revisions than the target revision are lost.
- Changes apply to objects only and not to the file system.
- Tasks, SIC and Licenses are not reverted.
- The revert action disconnects all other connected users and discards all of their private sessions.
- Revision is not supported in these scenarios:
  - The Endpoint Security Management Server is enabled.
  - If SmartConsole and the Security Management Server are connected through a proxy server, the GUI for this feature is not supported. In this case, use the applicable API command.
  - VSX configuration or related networks differ between the source and target revisions.
  - A new Multi-Domain Server, a Security Management Server or a Check Point object was created or deleted after the target revision date.
  - The corresponding revision of the Global Domain, or the IPS or Application Control components was purged.

Best Practices:

1. It is recommended to update the IPS and Application Control signatures and install the policy after the revert. Install policy if changes to log destinations are applied.
2. If it is necessary to restore a full environment to a certain point in time, use **Restore Backup**. All work done after the backup is lost. To learn more, see the: *R80.40 Gaia Administration Guide*
3. We recommend to purge irrelevant revisions. Accumulating too many revisions can create a heavy load on the server, which may cause disk and performance issues.

To see saved database versions:

In SmartConsole, go to **Manage & Settings > Sessions > Revisions**.

To see the changes made during a specific revision:

1. Go to **Manage & Settings > Sessions > Revisions**, and select a 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 revert to an earlier revision

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.
2. In **Actions**, click **Revert to this Revision**.

   The **Revert to Revision** wizard opens.

To delete all versions of the database that are older than the selected version:

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.
2. In **Actions**, click **Purge**.
3. In the confirmation window that opens, click **Yes**.

Important - Purge is irreversible. When you purge, that revision and older revisions are deleted.

Notes:

- When connected with SmartConsole to a Security Management Server, sessions that were published through the Management API in the system Domain are not shown in the **Revisions** view.
- When connecting with the Management API to the Domain of a Security Management Server and running the *show sessions* API command with *view-published-sessions* set to *true*, sessions that were published through SmartConsole are not returned, even if they include changes in the system Domain.

Use Case - Managing a Crisis Using Database Revisions

A network problem occurs after downloading a Threat Prevention update and installing it on gateways.

Solution

1. From Security Policies > Threat Prevention > Custom Policy Tools > **Updates**, in the IPS section, select 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.

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 Default

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.

Synchronization with UserCenter

You can add information regarding your environment to User Center, such as Security 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.

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 Security Gateway:

- Deep packet inspection settings
- Protocol parsing inspection settings
- VoIP packet inspection settings

The Security Management Server comes with two preconfigured inspection profiles for the Security Gateway:

- **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 SmartDashboard R77.30 and lower, **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**.

For advanced configuration of SYN attacks, see sk120476.

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, 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 Security 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 Security Gateway, on which to install the exception
3. Click **OK**.

To enforce the changes, install the Access Control Policy.

SmartTasks

Management SmartTasks let you configure automatic actions according to different triggers in the system. A SmartTask is a combination of trigger and action.

- **Triggers** are events – currently defined in terms of existing management operations, such as installing a policy or publishing a session.

- **Actions** are automatic responses that take place after the trigger event , such as running a script, posting a web request or sending email.

Available Triggers

- **Before Publish** - Fired when an administrator publishes a session. The SmartTask passes the sessions meta-data (publishing administrator, domain information and session name) to the action. If the local Management API server is available, the session changes about to be published are formatted as a response to the "show changes" API.
- **After Publish** - Fired after an administrator successfully publishes a session. The SmartTask passes the same information to the action as the **Before Publish** trigger.
- **After Install Policy** - Fired after a policy has been installed. The SmartTask passes to the action information related to the policy installation task, such as the package installed, the administrator who initiated the installation and the task's result.

Available Actions

- **Run Script** - Runs a pre-defined Repository Script. The script gets the trigger's data as the first parameter. The trigger's data is passed as Base64 encoded JSON data, which can be decoded to implement custom business logic.

  For SmartTasks configured to run with "Before" operation triggers, the repository script can signal whether to abort or continue the operation by printing a JSON object with the "result" and optional "message" fields and then exit with code 0. If the value of the "result" field is "failure" the operation aborts.

  For SmartTasks configured to run with other triggers, exit code 0 is treated as success. Any other exit code is treated as failure.

  Note - By default, Repository Scripts run on the local Security Management Server although this can be customized using the Web API.

- **Web Request** - Executes an HTTPS POST web request to the configured URL. The trigger's data is passed as JSON data to the request's payload.

  Notes:

  - The configured URL must start with HTTPS and the target web server capable of handling such requests.
  - For web servers with self-signed SSL certificates, establish trust by specifying the certificate's fingerprint. You can get the fingerprint by clicking **Get Fingerprint** in the SmartTask editor or by viewing the certificate in a web browser.

  For SmartTasks configured to run with "Before" operation triggers, the repository script can signal whether to abort or continue the operation by responding with JSON object "result" and optional "message" fields and a status of 200 OK. If the value of the "result" field is "failure" the operation aborts.

For SmartTasks configured to run with other triggers, a 200 OK return code is treated as success. Any other exit code is treated as failure.

Configuring SmartTask Properties

1. Enter a unique name for the SmartTask - The name property is required and case sensitive.
2. Switch the SmartTask **ON** or **OFF** using the toggle button.
3. Optional - Enter a description for the SmartTask.
4. Select a trigger for the SmartTask.
5. Select an action that will happen once the trigger is fired.
6. Custom Data – You can add additional information to the JSON data sent with the trigger information by adding a JSON object to the **Custom Data** field. The JSON custom data is concatenated to the trigger's payload and passed to the action.
7. Optional - Add tags for the SmartTask object.

SmartTask Advanced Properties

The available advanced options depend on the action selected on the **General** tab.

Send Web Request

- **Time-out** – Number of seconds before the request times out and the request aborted.
- **If the HTTPS request times out** - Treat the time-out as an error and abort the event or continue normally.
- **X-chkp-shared-secret** – Enter a shared secret that can be used by the target web server to identify the Security Management Server. The value is sent as part of the request in the *X-chkp-shared-secret* header in the out-going web request.

Run script

- **Time-out** – Number of seconds before the request times out and the request aborted.
- **If the script fails to run or times-out** – Treat time-out (or execution failure) as an error and abort the event or continue normally.

Example

Use Case:

A company policy dictates that the publish operation must be used with a service request number as a prefix to the session name before saving any changes to the database, so the administrators can see what the rationale for changing the security policy was.

Procedure:

Add the *Validate Session Name Prefix* to the **Scripts Repository**.

1. Save the script in the repository.

   Instructions

   a. Click **Gateways & Servers** > **Scripts** > **Scripts Repository** > **New** ()

   b. Give the script a name.

   c. In the **Content** text box, paste the script code below.

   d. Click **OK** to save the script in the repository.

Script Code

```
#!/bin/bash
JQ=${CPDIR}/jq/jq
data=`echo $1 | base64 --decode -i`

# Extracting the required session name prefix for the session name based on the input JSON
sessionNamePrefix=`echo $data | $JQ -r  .\"custom-data\".\"session-name-prefix\"`

# If there's no input session name prefix, publish is allowed
if [[ $sessionNamePrefix = "null" ]] || [[ -z "$sessionNamePrefix" ]]; then
    printf '{"result":"success"}\n'
    exit 0
fi

# Extracting the actual session name
sessionName=`echo $data | $JQ -r .session.\"session-name\"`

# Abort the publish if the session doesn't contain a name at all
if [[ $sessionName = "null" ]]; then
    m1="Corporate Policy requires you to use a service request number for the session's name prefix."
    m2="For example: ${sessionNamePrefix}######"
    m3="Session name is missing. Please change your session's name to meet the requirements and try to publish again."
    printf '{"result":"failure","message":"%s %s %s"}\n' "$m1" "$m2" "$m3"
    exit 0
fi
```

```
# Abort the publish if the session name doesn't match the
expected prefix
if [[ ! $sessionName == $sessionNamePrefix* ]]; then
    m1="Corporate Policy requires you to use a ticket number
as the session's name."
    m2="For example: ${sessionNamePrefix}###### "
    m2=${m2//\"/\\\"}
    m3="Please change your session's name to meet the
requirements and publish again."
    printf '{"result":"failure","message":"%s %s
 %s"}\n' "$m1" "$m2" "$m3"
    exit 0
else
    # Session name matches the expected prefix, publish is
allowed
    printf '{"result":"success"}\n'
    exit 0
fi
```

2. Create a SmartTask to run the session validation script.

   Instructions

   a. Go to **Manage & Settings** > **Tasks** > **SmartTasks** > **New** ().

   b. Give the new SmartTask a name (you can call it "`Validate Session Name Before Publish`")

   c. In the **Trigger and Action** section, select from the drop down menu:

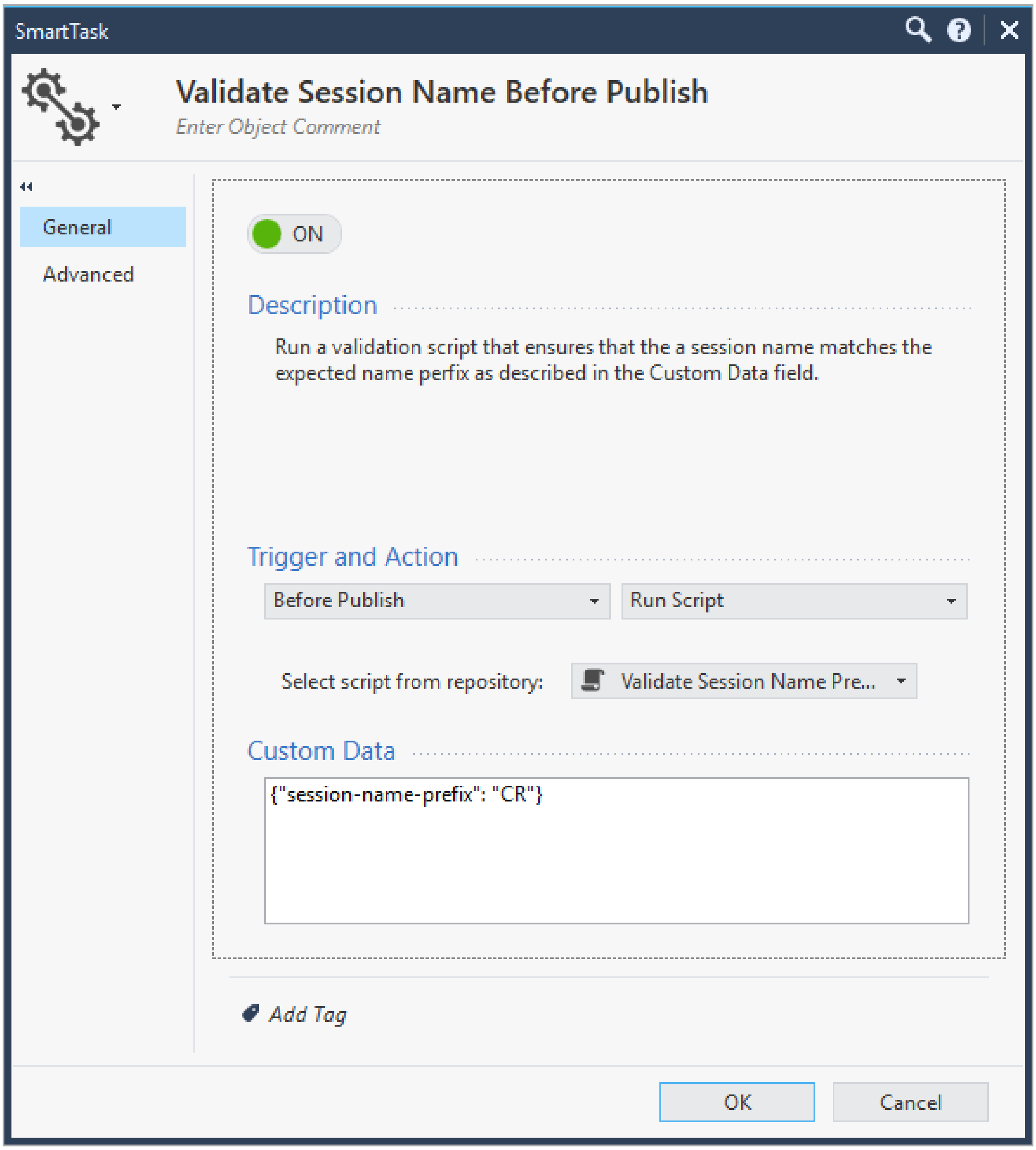
      Before Publish and **Run Script**.

   d. In the **Select script from repository** drop down, select the script saved in Step 1.

   e. In the **Custom Data** field, enter this string:

      {"session-name-prefix": "CR"}

      Note - The variable "**session-name-prefix**" correlates to the variable used at the beginning of the script in Step 1. If these are not identical, this script cannot work and the process fails.



SmartTask

Validate Session Name Before Publish

Enter Object Comment

Description

Run a validation script that ensures that the a session name matches the expected name perfix as described in the Custom Data field.

Trigger and Action

Before Publish | Run Script

Select script from repository: Validate Session Name Pre...

Custom Data

```
{"session-name-prefix": "CR"}
```

3. Publish the SmartConsole session.
4. Add a network object.
5. Publish the changes using the required prefix.

Note - If you publish the session without using the prefix, the process fails.

Network Security for IoT Devices

Introduction

The complexity of using IoT devices in the modern work environment such as hospitals, industries, and smart-buildings has, at cost, exposed them to ill-natured and harmful cyber attacks. Malicious cyber invasions into IoT devices have caused considerable financial loss to a number of enterprises. In addition to monetary loss and physical damage, these attacks can lead to data breaches, data tampering, ransomware, and even denial of service.

Common IoT devices susceptible to attack:

Smart Buildings/Offices	Healthcare	Industry
HVAC	HVAC	HVAC
Printers, copiers, fax machines	Printers, copiers, fax machines	Printers, copiers, fax machines
Elevators	Elevators	Elevators
Surveillance Cameras	Surveillance Cameras	Surveillance Cameras
Unhardened kiosk connected to a LAN	Unhardened kiosk connected to a LAN	Unhardened kiosk connected to a LAN
Access control points	Access control points	Access control points
Programmable logic controllers (PLCs)	Programmable logic controllers (PLCs)	Programmable logic controllers (PLCs)
Thermostats	Thermostats	Thermostats
Lighting	Lighting	Lighting
Residential smart meters	MRI machines	--
Fire alarms	Fire alarms	Fire alarms
N/A	Ultrasound machines	--
--	C-arms	--
--	Infusion pumps	--
--	Blood glucose meter	--

Smart Buildings/Offices	Healthcare	Industry
--	Patient monitor	--

What makes IoT devices so vulnerable:

- Outdated software, legacy OS, or no OS
- Basic Micro Controllers
- No Security-by-Design
- Lack of device management
- Shadow Devices
- Operational Limitations

Check Point's Infinity for IoT provides comprehensive network security for enterprise IT and IoT devices, smart building devices, industrial IoT, and connected medical equipment in these ways:

1. Prevent malicious intents and unauthorized access to IoT devices by analyzing multiple threat indicators from various resources.
2. Prevent infected devices from compromising other network elements.
3. Minimize the attack surface through internal network segmentation.
4. Provide deep insight information per IoT device.
5. Uses 3rd party discovery engine for IoT assets discovery.
6. Create separated IoT policy layer, using the discovered IoT device's attributes.

Note - Enforcement of IoT assets in the Access Control policy is not supported on Centrally Managed Quantum Spark appliances running Gaia Embedded operating system.

Prerequisites

- Check Point certified IoT Discovery Service installed on the network with a connection to the Management Server.
- Discovery Service

  - Industrial / Enterprise:
    - Armis
    - Claroty
    - Indegy
    - Ordr
    - SAM
    - SCADAfence
  - Medical:
    - Medigate
    - CyberMDX
    - Cynerio
- Identity Awareness Web API must be activated on the enforcing Security Gateway (the configuration is done automatically).
- Security Gateway version R80.10 and above.

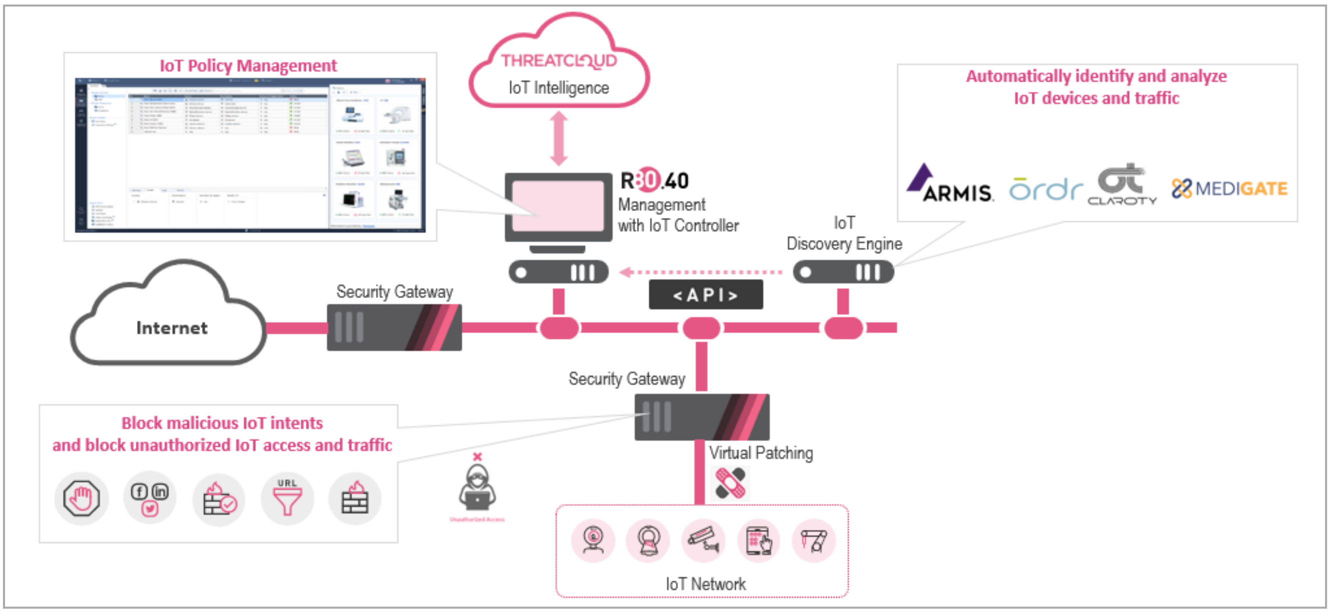
Note - Enforcement of IoT assets in the Access Control policy is not supported on Centrally Managed Quantum Spark appliances running Gaia Embedded operating system.

Network Overview

Check Point's Infinity for IoT delivers comprehensive IoT cyber-security by applying granular IoT-based policies. Check Point's IoT protection solution mobilizes hospitals, industries, smart buildings and offices to reduce and even eliminate IoT attacks.

- Identify and analyze IoT devices and traffic
- Deploy IoT policy enforcement points
- Identify and block IoT malicious intents

Network Diagram



Configuring the IoT Controller

Before Check Point Infinity for IoT can protect IoT devices from malicious attacks, you must configure the IoT Discovery Service. The IoT Third Party Discovery Service configures a connection between the Check Point Management Server and the IoT Third Party Discovery Engines.

The IoT Third Party Discovery Engines:

- Discover the connected IoT assets (mainly in the Industrial and Healthcare sectors).
- Group the discovered assets into zones.
- Share the discovered assets and the recommended policies with the Check Point Management Server.

To define the IoT Third Party Discovery Service

Step	Instructions
1	Go to **SmartConsole** > **Objects** > **New** > **More** > **IoT Discovery Service**. The **New IoT Discovery Service** window opens.

Step	Instructions
2	To configure the **General tab:** a. Enter the **Hostname**, **Port**, and **Pre-shared Key**. The pre-shared key must be provided from the certified IoT Third Party Discovery Service, and used for authorizing and authenticating the IoT Third Party Discovery Service. b. Click **OK.** The **Certificate Trust** window opens. Before verifying, check that the certificate is valid, and that the IoT Third Party Discovery Service is the certified owner. Infinity for IoT utilizes the Identity Awareness API. For easy activation, select the gateways where IoT enforcement will be done. To configure the **Gateways** tab: ■ Select the enforcing gateway for IoT traffic. To configure the **Policies** tab: a. Select the **Policy** to be applied on the **IoT layer**. b. Click **OK**.
3	Publish the SmartConsole session.
4	Install Policy.

Configuring a new IoT Third Party Discovery Service generates a new IoT policy layer on the selected policies, a new Threat Prevention profile, and a new rule in the Threat Prevention policy.

Adding IoT Assets to the Policy

After setting up the IoT policy, you can add IoT assets to the policy manually.

The policy is divided into three categories:

Category	Description
User-Defined	Used by administrators.
Auto-Generated	Rules generated from network traffic and IoT network patterns.
Cleanup	A set of rules for detected anomalies.

To define an IoT Access Rule

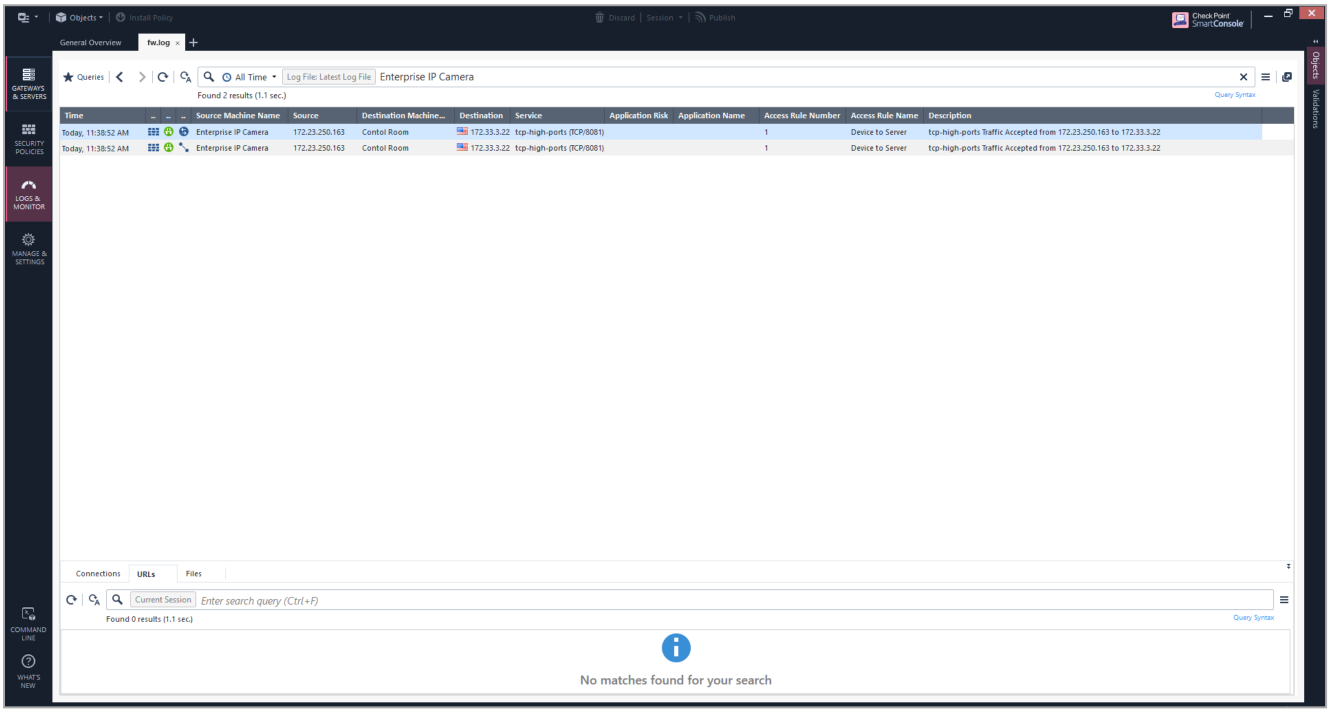
Step	Instructions
1	From **Security Policies** > **Access Control**, select the **IoT Layer**.
2	Click **User-Defined Section**, and then click the plus sign.
3	In the **Source and/or Destination field**, click the plus sign > **Add new item...**. The **Add new item** window opens.
4	Select **Import** > **IoT Controllers**, and then select the IoT asset to add to the rule.

Infinity for IoT Logs

Using Check Point's IoT Security Manager, security teams can see detailed IoT device information. With a thorough log they gain a clearer, contextual understanding about the device's behavior and forensics for event investigation.

Example 1 - Log Search by IoT Asset Information

Advanced log search using the enriched log data to simplify log filtering.



Enterprise IP Camera

Found 2 results (1.1 sec.)

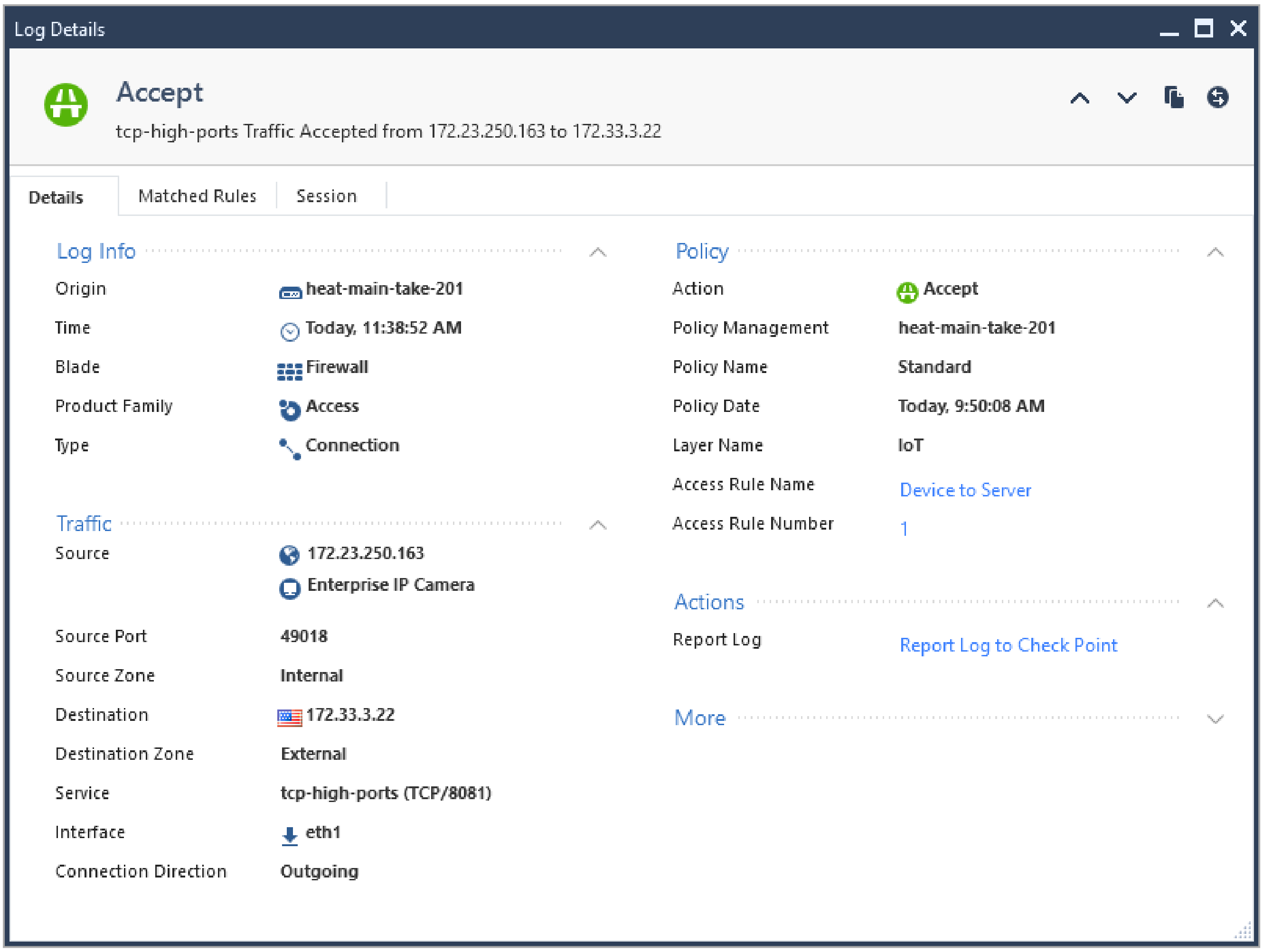
Time	...	...	...	Source Machine Name	Source	Destination Machine...	Destination	Service	Application Risk	Application Name	Access Rule Number	Access Rule Name	Description
Today, 11:38:52 AM				Enterprise IP Camera	172.23.250.163	Contol Room	172.33.3.22	tcp-high-ports (TCP/8081)			1	Device to Server	tcp-high-ports Traffic Accepted from 172.23.250.163 to 172.33.3.22
Today, 11:38:52 AM				Enterprise IP Camera	172.23.250.163	Contol Room	172.33.3.22	tcp-high-ports (TCP/8081)			1	Device to Server	tcp-high-ports Traffic Accepted from 172.23.250.163 to 172.33.3.22

Found 0 results (1.1 sec.)

No matches found for your search

Example 2 - Extended Log Data

IoT log data contains enriched information that helps identify the IoT assets in the log.



Log Details

Accept

tcp-high-ports Traffic Accepted from 172.23.250.163 to 172.33.3.22

Details | Matched Rules | Session

Log Info

Origin	heat-main-take-201
Time	Today, 11:38:52 AM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	172.23.250.163 Enterprise IP Camera
Source Port	49018
Source Zone	Internal
Destination	172.33.3.22
Destination Zone	External
Service	tcp-high-ports (TCP/8081)
Interface	eth1
Connection Direction	Outgoing

Policy

Action	Accept
Policy Management	heat-main-take-201
Policy Name	Standard
Policy Date	Today, 9:50:08 AM
Layer Name	IoT
Access Rule Name	Device to Server
Access Rule Number	1

Actions

Report Log	Report Log to Check Point

More

Management High Availability

This chapter descibes the configuration of Management High Availability.

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.

On-premises and cloud:

You can configure Check Point Management High Availability between on-premises Management Servers and Management Servers in a cloud.

You must make sure the required Check Point traffic can flow between the on-premises servers and the servers in the cloud.

Notes:

- For High Availability (and Load Sharing) environments for Security Gateways, see the *R80.40 ClusterXL Administration Guide*.
- For High Availability environments for Endpoint Security, see the *R80.40 Harmony Endpoint Security Server Administration Guide*.

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 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 notes about backing up and restoring in Management High Availability environment**:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R80.40 Gaia Administration Guide*.
- About the "`migrate export`" and "`migrate import`" commands, see the *R80.40 CLI Reference Guide*.
- About the "`mds_backup`" and "`mds_restore`" commands, see the *R80.40 CLI Reference Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Configuring a Secondary Security Management Server in SmartConsole

How to configure a Secondary Security Management Server in SmartConsole.

In the SmartConsole connected to the Primary Security Management Server, create a Check Point Host object for the Secondary Security Management Server. After you publish the SmartConsole session, synchronization starts between the Primary and Secondary Security Management Servers.

To configure the Secondary Security Management Server in SmartConsole:

1. Connect with SmartConsole to the Primary Security Management Server.
2. In the **Object Explorer**, click **New > More > Network Object > Gateways and Servers > Check Point Host**.
3. In the **General Properties** page, enter a unique name and IP address for the Secondary Security Management Server.
4. In the **Software Blades** section, go to the **Management** tab, and select **Network Policy Management**.

   This automatically selects the **Secondary Server**, **Logging and Status**, and **Provisioning**.
5. Create SIC trust between the Secondary Security Management Server and the Primary:
   1. Click **Communication**.
   2. Enter the SIC Activation Key of the secondary server.
   3. Click **Initialize**.
   4. Click **Close**.
6. Click **OK**.
7. Publish the SmartConsole session to save these session changes to the database.

   The initialization and synchronization between the Security Management Servers start.
8. 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.
9. Open the **High Availability Status** window and make sure there is one Active Security Management Server, and one Standby Security Management Server.
10. For each Security Gateway / Cluster, open the Security Gateway / Cluster object > go to **Fetch Policy**, click **Add**, and add the Secondary Security Management Server.

Synchronizing Active and Standby Servers

At intervals, the Active server synchronizes with the standby server or servers, and when you publish the SmartConsole 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.
- **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.

General Status messages in overview banner	Description
	The database of the primary Security Management Server is identical with the database of the secondary.
Some servers could not be synchronized	A communication issue prevents synchronization, or some other synchronization issue exists.
	The active and standby servers are not communicating.
Communication Problem	Some services are down or cannot be reached.
Collision or HA conflict	More than one management server configured as active. Two active servers cannot sync with each other.

When connected to a specified *active* management server:

Status window area:	Peer Status	Additional Information
Connected to:	Active	SmartConsole is connected to the active management server.
Peers	Standby	The peer is in standby. The message can also show: ▪ Sync problem, last time sync ▪ Synchronized successfully. Last sync time: <time> ▪ No communication
	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:

Status window area:	Peer Status	Description
Connected to:	Standby	Also shows: last sync time.
Peers	Active	The peer is on standby. The message can also show: ▪ No communication, last sync time ▪ OK., last sync time: <time> ▪ Sync problem, last sync time (in any direction)
	Standby *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 the SmartConsole session before initiating a changeover to the Standby Security Management Server.

To Interchange the Active and Standby

1. Connect with SmartConsole to the Standby Security Management Server.
2. Click the Menu button and select **High Availability**.

   The **High Availability Status** window opens.
3. 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.

Unlocking the Administrator

In a High Availability environment, if an administrator is locked on the Standby Management Server, the administrator is not locked and does not appear as locked on the Active Management Server. Therefore, you cannot unlock the administrator on the Active Management Server.

To unlock the administrator:

Use the API command `unlock-administrator` on the Standby Management Server. See the *Check Point Management API Reference*.

Environments with Endpoint Security

Environments that include Endpoint Security require additional steps and information.

For details, see *High Availability* in the *R80.40 Harmony Endpoint Security Server Administration Guide*.

High Availability Disaster Recovery

If the primary Management Server becomes permanently unavailable:

1. **Create a new Primary server with the IP address of the original Primary server.**

   Note - This is not supported for environments with Endpoint Security.

Step	Instruction
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 (see *"Promote the Secondary Management Server to Primary and create new licenses." below* - no need to remove instances of the old Primary Management object and install database).
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 switch back to the original setup (to set the original Primary Management Server as the Primary Management Server again):

Step	Instruction
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 (See *"Promote the Secondary Management Server to Primary and create new licenses." below* - no need to remove instances of the original Primary Management object and install database).
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 Secondary Management Server

2. **Promote the Secondary Management Server to Primary and create new licenses.**

   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 sync completes.

Note - This is the disaster recovery method supported for High Availability environments with Endpoint Security.

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.

Before you start - make sure that the primary server is offline.

Step	Instruction
1	Set the Secondary server to Active.

2	On the Secondary Management Server that you will promote, run:
	`#$FWDIR/bin/promote_util`
	`#cpstop`

3	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.
4	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.
5	Run `cpstart` on the promoted server.
6	Open SmartConsole, and: a. 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 Management Server, all previous licenses are revoked. b. Install database.

Compliance

The Check Point Compliance blade is a dynamic solution that continuously monitors the Check Point security infrastructure. The blade uses the Continuous Compliance Monitoring (CCM) technology to examine Security Gateways, Software Blades, policies, and configuration settings against an extensive database of regulatory standards and security best practices. The blade suggests corrective measures in case of deficiency. The Compliance blade incorporates visual representations and reports that describe Compliance to the compliance standards.

The Compliance blade performs these automatic scans:

- Daily - One automatic scan per day, which finds changes to gateway and policy configurations made with CLI or scripts.
- SmartConsole changes - Automatic scan when an administrator changes objects that have an effect on Security Gateway or policy configuration (the scan occurs after you publish the changes.)

You can also run manual scans, as necessary.

To enable the Compliance blade on your Security Management Server:

1. In SmartConsole, go to the **Gateways & Servers** view, and double-click on the Security Management Server object.

   The Security Management Server editor opens.

2. In the **General Properties** page, go to **Management**, and select **Compliance**.
3. Click **OK**.

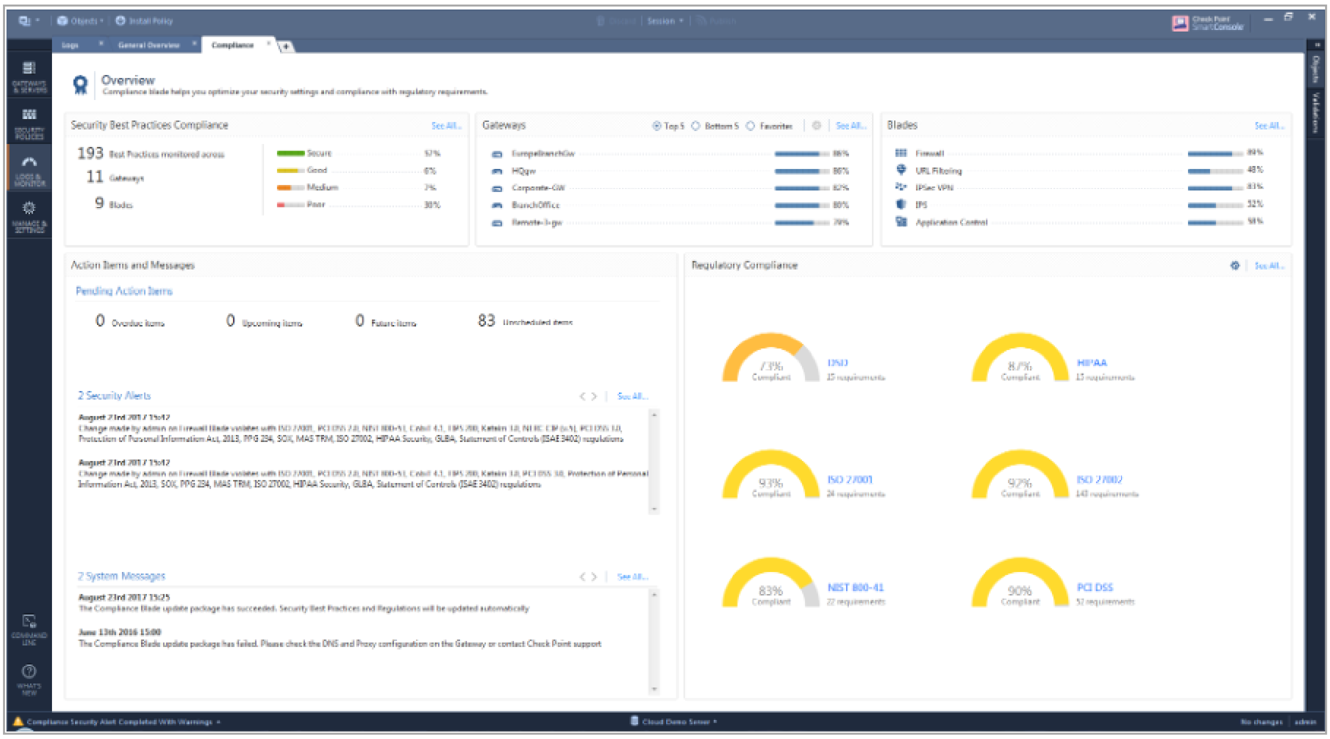
To view the Compliance dashboard:

1. In SmartConsole, go to the **Logs & Monitor** view, and click **+** sign to open a new tab.

   The **New Tab** opens.

2. Click **Compliance**.

The Compliance View



Compliance blade helps you optimize your security settings and compliance with regulatory requirements.

August 23rd 2017 15:42
Change made by admin on Firewall Blade violates with ISO 27001, PCI DSS 2.0, NIST 800-41, Cobit 4.1, FIPS 200, Katakin 1.0, NERC CIP (v5), PCI DSS 3.0, Protection of Personal Information Act, 2013, PPG 234, SOX, MAS TRM, ISO 27002, HIPAA Security, GLBA, Statement of Controls (ISAE 3402) regulations

August 23rd 2017 15:42
Change made by admin on Firewall Blade violates with ISO 27001, PCI DSS 2.0, NIST 800-41, Cobit 4.1, FIPS 200, Katakin 1.0, PCI DSS 3.0, Protection of Personal Information Act, 2013, SOX, PPG 234, MAS TRM, ISO 27002, HIPAA Security, GLBA, Statement of Controls (ISAE 3402) regulations

August 23rd 2017 15:25
The Compliance Blade update package has succeeded. Security Best Practices and Regulations will be updated automatically

June 13th 2016 15:00
The Compliance Blade update package has failed. Please check the DNS and Proxy configuration on the Gateway or contact Check Point support

Compliance Security Alert Completed With Warnings

The Compliance view includes 5 widgets:

- Security Best Practices
- Gateways
- Blades
- Action Items and Messages
- Regulatory Compliance

The Compliance Scoring System

The Compliance blade calculates a numeric score for each best practice test. The numeric score is the average of the results for each object examined. Average scores are given for the organization Security Gateways, Software Blades, and regulations.

This is the Check Point Compliance blade scoring system:

Security Status	Score in %	Comments
Poor	0-50	0=non-compliant
Medium	50-75	

Security Status	Score in %	Comments
Good	75-99	
Secure	100	Compliant
N/A	Not Applicable	Given if: ■ The applicable Software Blade is not installed on the Security Management Server. Or ■ The Security Gateway does not support the examined feature.

This chapter explains how to work with each Compliance view. For details about system requirements, troubleshooting and debugging, see sk120256.

The Security Best Practices Compliance View

The Security Best Practices Compliance view displays status information for each best practice.

The top table shows these details related to the best practice:

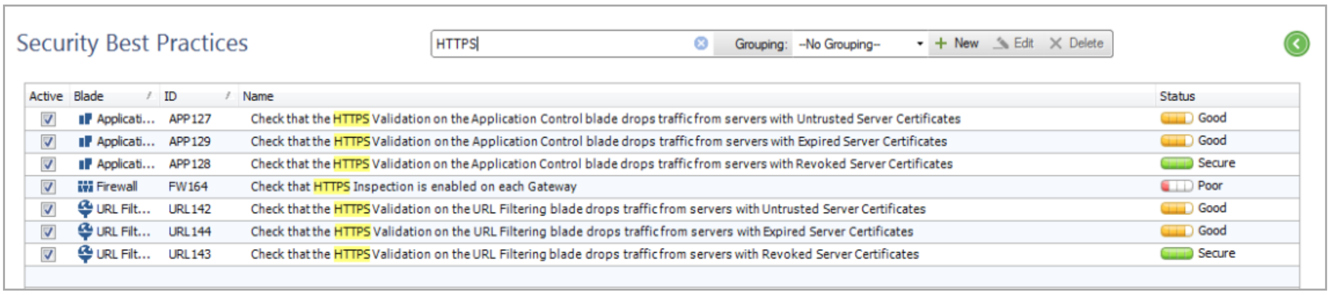
- **Active** - Select to activate the best practice test. Clear to deactivate it.
- **Blade** - Blade related to this best practice.
- **ID** -Check Point Compliance ID assigned to the best practice.
- **Name** - Name and brief description of the regulatory requirement related to the best practice.
- **Status** - Poor, Medium, Good, Secure, or N/A. We recommend that you resolve "Poor" status items immediately.

The bottom section shows these items for the selected best practice test:

- **Description** - Detailed description of the best practice test.
- **Action Item** - Steps required to become compliant, including alternative scenarios.
- **Dependency** - Shows when the selected best practice is dependent on another best practice. This test is only performed if the other best practice is compliant.
- **Relevant Objects** - Objects related to the selected best practice test and their status. You can activate or deactivate the selected best practice test for specified objects (this section shows only when the best practice is applicable to specific objects.)

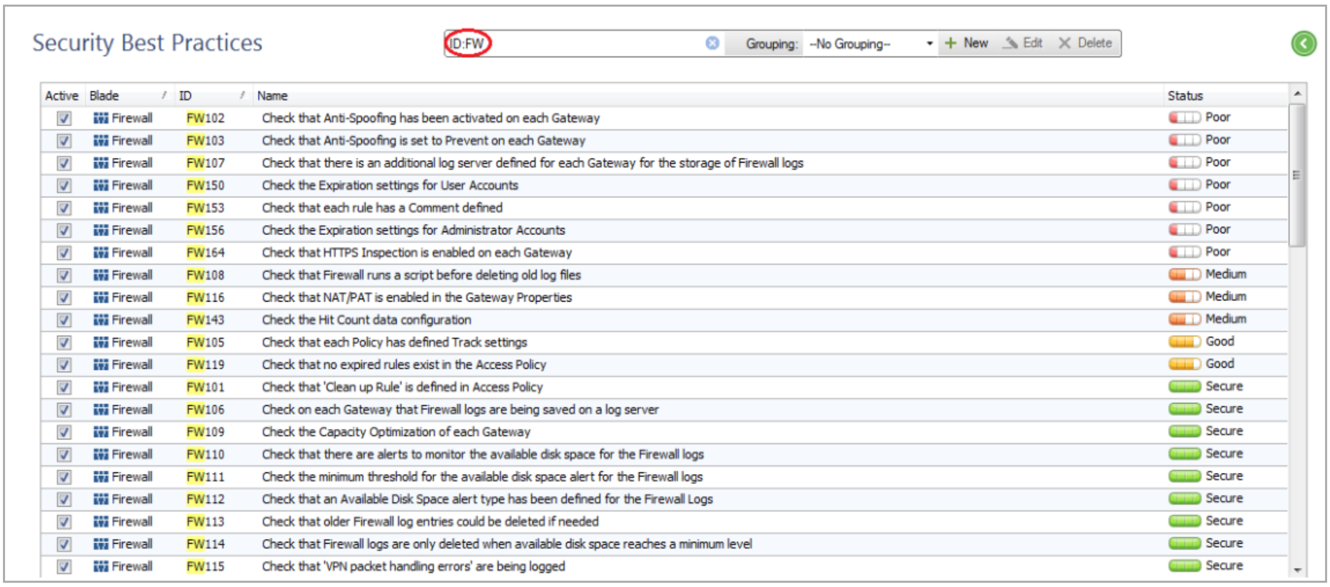
- **Relevant Regulatory Requirements** - Link to a list of all the regulatory standards which are applicable to the best practice.

To search for a certain value, enter a string in the search box:



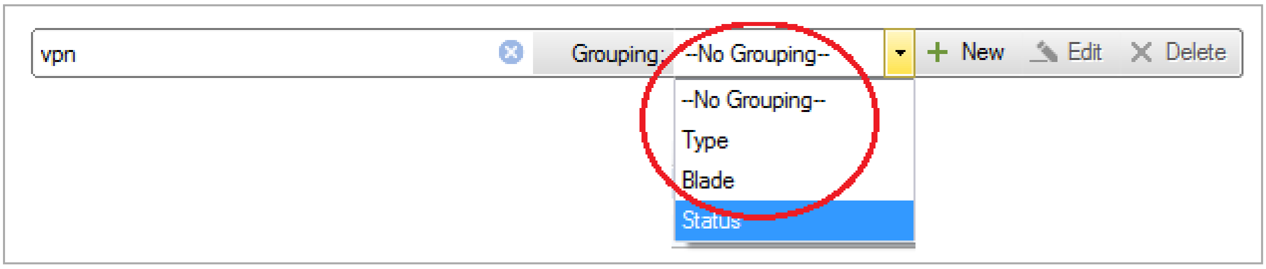
Active	Blade	ID	Name	Status
☑	Applicati...	APP127	Check that the HTTPS Validation on the Application Control blade drops traffic from servers with Untrusted Server Certificates	Good
☑	Applicati...	APP129	Check that the HTTPS Validation on the Application Control blade drops traffic from servers with Expired Server Certificates	Good
☑	Applicati...	APP128	Check that the HTTPS Validation on the Application Control blade drops traffic from servers with Revoked Server Certificates	Secure
☑	Firewall	FW164	Check that HTTPS Inspection is enabled on each Gateway	Poor
☑	URL Filt...	URL142	Check that the HTTPS Validation on the URL Filtering blade drops traffic from servers with Untrusted Server Certificates	Good
☑	URL Filt...	URL144	Check that the HTTPS Validation on the URL Filtering blade drops traffic from servers with Expired Server Certificates	Good
☑	URL Filt...	URL143	Check that the HTTPS Validation on the URL Filtering blade drops traffic from servers with Revoked Server Certificates	Secure

To search for a certain parameter in a specific field, enter: *field name:string*



Active	Blade	ID	Name	Status
☑	Firewall	FW102	Check that Anti-Spoofing has been activated on each Gateway	Poor
☑	Firewall	FW103	Check that Anti-Spoofing is set to Prevent on each Gateway	Poor
☑	Firewall	FW107	Check that there is an additional log server defined for each Gateway for the storage of Firewall logs	Poor
☑	Firewall	FW150	Check the Expiration settings for User Accounts	Poor
☑	Firewall	FW153	Check that each rule has a Comment defined	Poor
☑	Firewall	FW156	Check the Expiration settings for Administrator Accounts	Poor
☑	Firewall	FW164	Check that HTTPS Inspection is enabled on each Gateway	Poor
☑	Firewall	FW108	Check that Firewall runs a script before deleting old log files	Medium
☑	Firewall	FW116	Check that NAT/PAT is enabled in the Gateway Properties	Medium
☑	Firewall	FW143	Check the Hit Count data configuration	Medium
☑	Firewall	FW105	Check that each Policy has defined Track settings	Good
☑	Firewall	FW119	Check that no expired rules exist in the Access Policy	Good
☑	Firewall	FW101	Check that 'Clean up Rule' is defined in Access Policy	Secure
☑	Firewall	FW106	Check on each Gateway that Firewall logs are being saved on a log server	Secure
☑	Firewall	FW109	Check the Capacity Optimization of each Gateway	Secure
☑	Firewall	FW110	Check that there are alerts to monitor the available disk space for the Firewall logs	Secure
☑	Firewall	FW111	Check the minimum threshold for the available disk space alert for the Firewall logs	Secure
☑	Firewall	FW112	Check that an Available Disk Space alert type has been defined for the Firewall Logs	Secure
☑	Firewall	FW113	Check that older Firewall log entries could be deleted if needed	Secure
☑	Firewall	FW114	Check that Firewall logs are only deleted when available disk space reaches a minimum level	Secure
☑	Firewall	FW115	Check that 'VPN packet handling errors' are being logged	Secure

To group results, select **Blade** or **Status** in the grouping field;



To sort search results by a certain field, click the field header.

Creating User-Defined Best Practices

You can define your own, custom Security Best Practices based on organizational security requirements.

To create a new Firewall Security Best Practice:

1. In the '**Compliance** tab > **Security Best Practices** pane .> click **See All**.
2. Click **New**, and select **Firewall Best Practice**.

   The **New Firewall Best Practice** window opens.
3. Enter the **Name** and **Description** for this best practice.
4. Enter the **Action Item** generated by this best practice.
5. In the **Best Practice Rule Definition** section, enter the rule matching criteria in the table cells. A Security Best Practice match occurs when all table cells match one or more rules in the Rule Base (Logical AND).
   a. **Hit Count** - Select a hit count level. A match occurs when the hit count for a rule is equal to or exceeds the specified hit count level. For example: To check the Rule Base for unused rules, you can select **Hit CountZero**.
   b. **Name**
   c. **Source** - Select one or more source objects.
   d. **Destination** - Select one or more destination objects.
   e. **VPN** - Select one or more VPN communities.
   f. **Services & Applications** - Select one or more services or applications.
   g. **Action** - The action which the rule triggers.
   h. **Track** - The tracking method for the rule.
   i. **Install On** - Security Gateways / Security Clusters to which the rule applies.
   j. **Time** - Select the times at which the rule applies.
   k. **Comment** - Enter a comment if necessary.
   l. Optional: click **Advanced Settings** to select the percentage of the Rule Base to scan and the direction of scan (**Top** or **Bottom**). For example, select **Bottom 30%** to scan 30% of the Rule Base starting from the bottom (last rule in the Rule Base).

   Note - You can right-click a cell, and select **Negate Cell** to exclude the cell from matching. This feature is not available in the **Name** and **Comment** cells.
6. In the **Best Practice Scoring** section configure these settings:

a. **Violation Definition** - Define if a match occurs when the best practice is matched by a rule or not. Select one of these options:

   - Rule found - A match occurs when the best practice is matched by a rule in the Rule Base.
   - Rule not found - A match occurs when the best practice is not matched by a rule in the Rule Base.

   Select the level of **Tolerance** - A violation occurs when there are more than the specified number of matches (Default = 0). For example, if the tolerance is set to 0, the Compliance Blade creates a violation when the first match occurs. If the tolerance is set to 3, the Compliance Blade creates a violation when the fourth match occurs. The **Tolerance** option applies only to the **Rule found** option.

b. **Rule Index Display Criteria** - Define when the **Rule Index** (rule number) shows in the **Relevant Objects** pane in the **Security Best Practices** view. This lets you easily see which rules cause or prevent violations:

   - **Display rules that match** - Shows rules that match the criteria specified in a Security Best Practice.
   - **Display rules that don't match** - Shows rules that do not match the criteria specified in a Security Best Practice.
   - **Don't display rules** - Does not show the rule.

7. Click **OK**.

   The new best practice is added to the list of best practices.

8. Publish your changes.

To create a new Gaia OS Security Best Practice:

1. In the '**Compliance** tab > **Security Best Practices** pane .> click **See All**.
2. Click **New**, and select **Gaia OS Best Practice**.

   The new **Gaia OS Best Practice** window opens.

3. Enter the **Name** and **Description** for this best practice.
4. Enter the **Action Item** generated by this best practice.
5. Enter the **Practice Script** to run on the Security Gateways or load the script from a file.
6. Enter the **Expected Output** - If the script output is equal to the Expected Output, the best practice status is secure.
7. Click **OK**.

The new best practice is added to the list of best practices.

8. Publish your changes.

Best Practice - We recommend that you run a manual scan after you create a new Security Best Practice. The scan reevaluates the compliance status, to reflect any configuration changes. To do a manual scan . go to the **Manage & Settings** view > **Blades** > **Compliance** > **Settings** > click the **Rescan** button. You cannot perform any actions in the Compliance tab while the scan runs.

Activating and Deactivating Best Practice Tests

You can activate or deactivate enforcement of best practices by test, by Security Gateway, by Software Blade or by other objects. Activation changes are applied after the next scan.

By default, all best practice tests are active.

To deactivate a best practice for the entire organization:

1. Go to the **Security Best Practices** view > and select a best practice.
2. Right-click and select **Deactivate**.

   The **Expiration Details** window opens.
3. Select **Never** or enter an expiration date. If you select an expiration date, the best practice test is automatically activated on that date.
4. In the **Comment** box, explain why it is necessary to deactivate this Compliance test.

To activate a best practice test that is not currently active:

- Go to the **Security Best Practices** view, select a best practice, right-click and select **Activate**.

  Or
- Go to the **Manage & Settings** > view > **Blades** > **Compliance** > **Inactive Objects** > **Inactive Security Best Practices** > select the applicable security best practice and click **Remove**.

To deactivate a best practice for a specific Security Gateway:

1. Go to the **Manage & Settings** > view > **Blades** > **Compliance** > **Inactive Objects**.
2. In the **Inactive Gateways** section, click **Add**.
3. Enter or select a Security Gateway or a Security Cluster.

Note - To activate the best practice for the Security Gateway, select the Security Gateway and click **Remove**. When prompted, click **Yes**.

To deactivate a best practice for a specific object:

1. Go to the **Manage & Settings** > view > **Blades** > **Compliance** > **Inactive Security Best Practices on Specific Objects**.
2. In the **Inactive Gateways** section, click **Add**.
3. Enter or select a Security Gateway or a Security Cluster.

Best Practice - We recommend that you run a manual scan after you activate or deactivate best practice tests. The scan reevaluates the compliance status, to reflect any configuration changes. To do a manual scan . go to the **Manage & Settings** view > **Blades** > **Compliance** > **Settings** > click the **Rescan** button. You cannot perform any actions in the Compliance tab while the scan runs.

The Gateways View

This widget displays security status of the Security Gateway - the five Security Gateways with the highest Compliance scores, lowest Compliance scores, or a predefined set of Favorites. To see the results of all Security Gateways, click **See All**

To see the best practices which are applicable to a specific Security Gateway / Security Cluster, click the specific Security Gateway / Security Cluster.

The top table shows these details related to the best practice:

- **Active** - Select to activate the best practice test. Clear to deactivate it.
- **Blade** - Blade related to this best practice.
- **ID** -Check Point Compliance ID assigned to the best practice.
- **Name** - Name and brief description of the regulatory requirement related to the best practice.
- **Status** - Poor, Medium, Good, Secure, or N/A. We recommend that you resolve "Poor" status items immediately.

The bottom section shows these items for the selected best practice test:

- **Description** - Detailed description of the best practice test.
- **Action Item** - Steps required to become compliant, including alternative scenarios.
- **Dependency** - Shows when the selected best practice is dependent on another best practice. This test is only performed if the other best practice is compliant.
- **Relevant Objects** - Objects related to the selected best practice test and their status. You can activate or deactivate the selected best practice test for specified objects (this section shows only when the best practice is applicable to specific objects.)
- **Relevant Regulatory Requirements** - Link to a list of all the regulatory standards which are applicable to the best practice.

The Blades View

This widget displays the security status by Software Blade - the average scores for the five Software Blades with the highest number of security best practices implemented. To see the result for a specific Software Blade, click it. To see the results for all Software Blades, click **See All**

The top table shows these details related to the best practice:

- **Active** - Select to activate the best practice test. Clear to deactivate it.
- **Blade** - Blade related to this best practice.
- **ID** -Check Point Compliance ID assigned to the best practice.
- **Name** - Name and brief description of the regulatory requirement related to the best practice.
- **Status** - Poor, Medium, Good, Secure, or N/A. We recommend that you resolve "Poor" status items immediately.

The bottom section shows these items for the selected best practice test:

- **Description** - Detailed description of the best practice test.
- **Action Item** - Steps required to become compliant, including alternative scenarios.
- **Dependency** - Shows when the selected best practice is dependent on another best practice. This test is only performed if the other best practice is compliant.
- **Relevant Objects** - Objects related to the selected best practice test and their status. You can activate or deactivate the selected best practice test for specified objects (this section shows only when the best practice is applicable to specific objects.)
- **Relevant Regulatory Requirements** - Link to a list of all the regulatory standards which are applicable to the best practice.

The Action Items and Messages View

When a Best Practice test finds a deficiency, the Check Point Compliance blade automatically generates an Action Item. The Action Item shows a helpful description for the corrective measures to take in order to amend the deficiency. You can assign a due date to an Action Item and monitor corrective steps. Due dates are not assigned to Action Items when they are generated. When you complete the corrective steps, the Check Point Compliance blade deletes the Action Item after the next scan.

This widget has 3 sections:

- **Action Items**

  This widget displays the updated status of pending action items for your organization:

  - **Upcoming items** - Action items whose due dates is in the next 30 days.
  - **Future items** - Action items whose due dates is after more than 30 days.
  - **Unscheduled items** - Action items without defined due dates.
  - **Overdue items** - Action items that are overdue.

    ✪ **Best Practice** - Resolve overdue action items immediately

  To open the action items for a status category, click **Action Items**:

  In the top table, see these details related to the action item:

  - **Due Date** - Optionally assigned due date for resolving this Action Item. A due date is not automatically assigned when an Action Item is generated.
  - **Blade** - Blade related to the applicable best practice.
  - **ID** - Check Point Compliance ID assigned to the applicable best practice.
  - **Name** - Name and brief description of the regulatory requirement related to the applicable best practice.
  - **Status** - Poor, Medium, Good, Secure, or N/A. We recommend that you resolve "Poor" status items immediately.

  In the bottom section, you can see these items for the selected action item:

  - **Action Item Description** - Steps required to become complaint.
  - **Due Date** - Optionally assigned due date for resolving this Action Item.
  - **Dependency** - Shows when the selected best practice is dependent on another best practice. This test is only performed if the other best practice is compliant.
  - **Relevant Objects** - Objects related to the selected best practice test and their status. You can activate or deactivate the selected best practice test for specified objects (this section shows only when the best practice is applicable to specific objects.)
  - **Relevant Regulatory Requirements** - Link to a list of all the regulatory standards which are applicable to the best practice.

- **Alert Messages**

Alerts are generated when a configuration change causes Compliance status degradation. To see all alert messages, click **Security Alerts**.

- **System Messages**

  System Message inform about system issues related to the Compliance, for example, Compliance package update. To see all system messages, click **System Messages**.

To assign a due date to an Action Item:

1. In SmartConsole. go to the **Logs & Monitor** view > **Compliance** tab > **Action Items and Messages** > **Pending Action Items** > **Unscheduled items**.
2. Select an Action Item.
3. In the **Action Item Description** section, click **Schedule Now**. If the Action Item already has an assigned due date, click the date link to change it.
4. In the window that opens, enter or select a due date and click **OK**.

The Regulatory Compliance View

This widget displays Compliance statistics for selected regulatory standards:

- The number of regulatory requirements examined for each regulatory standard.
- Average Compliance scores.

To select the regulatory standards displayed:

1. Click this icon ⚙ in the top right corner of the **Regulatory Compliance** pane: .
2. In the **Select Regulations and Standards** window, select the standards to show in the **Overview**.

To see the compliance score for all regulatory requirements, click **See All**.

To see details of a specific standard, click the standard. The top table shows these items:

- **ID** - Check Point Compliance ID assigned to the best practice.
- **Status** - Poor, Medium, Good, Secure, or N/A. We recommend that you resolve "Poor" status items immediately.
- **Name** - Name and brief description of the regulatory requirement.

The bottom section shows these items:

- **Description** - Detailed description of the best practice test.
- **Relevant best practices** - Applicable best practice for the selected requirement, and their Compliance status.
- **Relevant objects** - Objects related to the selected best practice test and their status. You can activate or deactivate the selected best practice test for specified objects (this section shows only when the best practice is applicable to specific objects.)

You can select the regulatory standards that are applicable to your organization. By default, all supported regulatory standards are active.

To activate or deactivate regulatory standards:

1. Go to the **Manage & Settings** view > **Blades** > **Compliance** > **Settings**.

   The **Settings** window opens.
2. In the **Active Regulations** section, select / clear the applicable regulatory standards.
3. Publish you changes.

To import a regulatory standard to SmartConsole:

1. Save the applicable regulatory standard locally in an XML file.
2. Go to the **Manage & Settings** view > **Blades** > **Compliance** > **Settings**.

   The **Settings** window opens.
3. Go to the **Active Regulations** section and click **Actions** > **Import**.
4. Browse to the XML file you want to import, and click **Open**.

   The regulation now appears in the list of **User-defined Regulations**.
5. Double-click the regulation.

   The regulation window opens.
6. Click **Save**.

   The process may take a few minutes to complete.
7. Publish your changes.

Best Practice - We recommend that you run a manual scan after you make changes to the regulatory standards list. The scan reevaluates the compliance status, to reflect any configuration changes. To do a manual scan, click the **Rescan** button in the **Engine Status** section. You cannot perform any actions in the Compliance tab while the scan runs.

Creating Reports

You can generate a report to show a summary of the Compliance status or a report on the implementation of a specific regulatory standard.

To create a report:

1. In SmartConsole, go to the **Logs & Monitor** view, and click the **+** sign to open a **New Tab**..

   A **New Tab** opens.
2. Select the **Reports** view.
3. From the displayed list, select **Compliance Blade**.
4. Click **Open**.

   The report opens.
5. Optional : In the toolbar, go to **Actions** to create reports in the PDF and CSV formats. To find an exported report, go to the **Logs & Monitor** view > open a **New Tab** > **Archive**.

To create a report per regulation:

1. In the Compliance view, go to the **Regulatory Compliance** pane, and select **See All**.
2. Click the required regulatory standard.
3. In the top tool bar, click **Generate Report**.
4. From the top toolbar, you can select to create reports in these output formats:
   - PDF document
   - An email with attached PDF
   - Output to printer
   - HTML output to your browser.

The ICA Management Tool

In the ICA Management Tool, an administrator can:

- Manage certificates

  Warning - Do **not** use the ICA Management Tool to change SIC certificates or VPN certificates. Change SIC and VPN certificates in SmartConsole only. Use the ICA Management Tool for user certificate operations only, such as certificate creation.

- Recreate CRLs
- Configure the Internal Certificate Authority (ICA) parameters
- 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 sk102837: Best Practices - ICA Management Tool configuration

Connecting to the ICA Management Tool

The ICA Management Tool is disabled by default.

To connect to the ICA Management Tool:

1. In SmartConsole, configure the required administrator and user objects.

   You must create a certificate for these administrators and users.

   You use this certificate to configure the permitted users in the ICA Management Tool and in the client web browsers.

2. In the command line on the Management Server, add the required administrators and users that are permitted to use the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool add ...
   ```

   See *"cpca_client set_mgmt_tool" on page 561*

3. In the command line on the Management Server, start the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool on
   ```

See *"cpca_client set_mgmt_tool" on page 561*

4. Check the status of the ICA Management Tool:

   ```
   cpca_client set_mgmt_tool print
   ```

   See *"cpca_client set_mgmt_tool" on page 561*

5. Import the administrator's / user's certificate into the Windows Certificate Store:

   a. Right-click the *.p12 file you saved when you created the required administrator / user, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

   d. Enter the same certificate password you used when you created the required administrator / user certificate.

   e. Clear **Enable strong private key protection**.

   f. Select **Mark this key as exportable**.

   g. Click **Next**.

   h. Select **Place all certificates in the following store** > click **Browse** > select **Personal** > click **OK**.

   i. Click **Next**.

   j. Click **Finish**.

6. In a web browser, connect to the ICA Management Tool:

   ```
   https://<IP Address of the Management Server>:18265
   ```

   Important - The fact that the TCP port 18265 is open is not a vulnerability. The ICA Management Tool Portal is secured and protected by SSL. In addition, only authorized administrators and users are allowed to access it using a certificate.

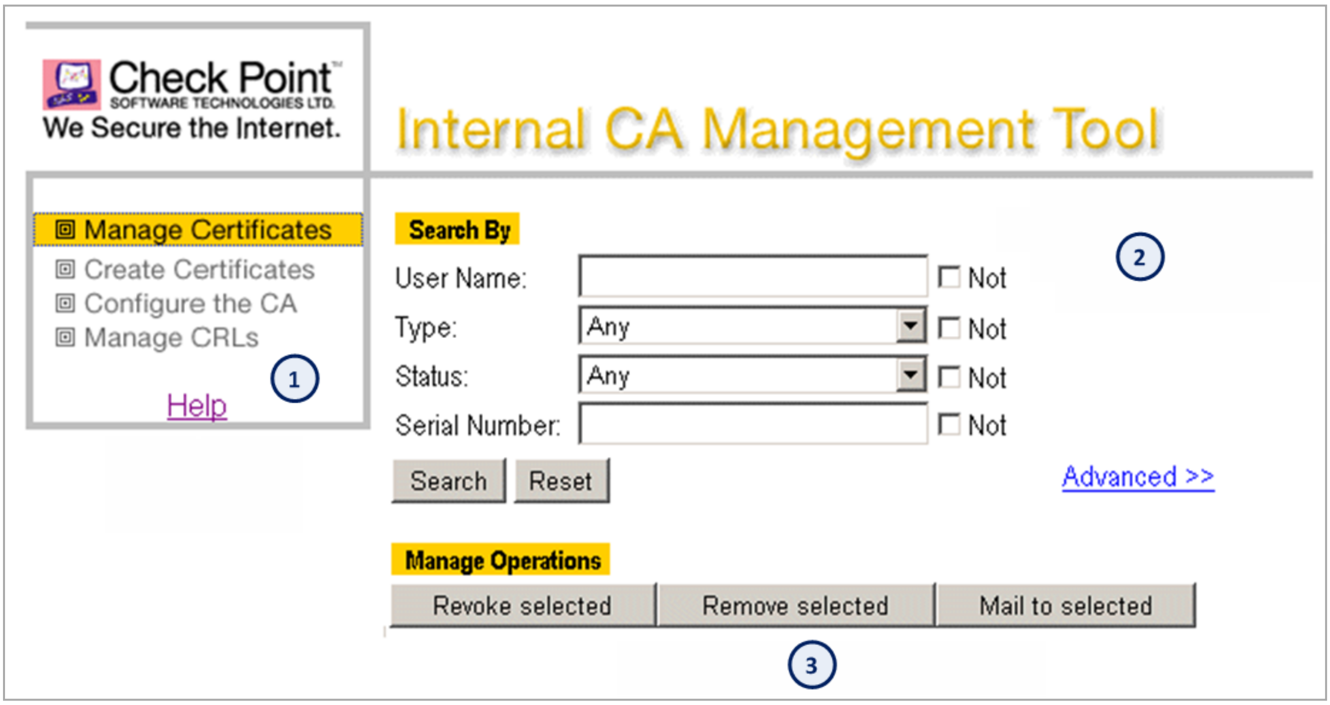
7. A dialog box with this message appears:

   ```
   Client Authentication

   Identification

   The Web site you want to view requests identification.
   ```

```
Select the certificate to use when connecting.
```

8. Select the appropriate certificate for authenticating to the ICA Management Tool.
9. Click **OK**.
10. In the **Security Alert** dialog box, click **Yes**.

The ICA Management Tool Portal



User Name: □ Not

Type: Any □ Not

Status: Any □ Not

Serial Number: □ Not

Item	Pane	Description
1	Menu	Shows a list of operation.
2	Operations	■ **Manage certificates** In this pane, you manage the existing certificates. The window divides into **Search attributes configuration** and **Bulk operation configuration**. ■ **Create Certificates** In this pane, you can create new certificates. ■ **Configure the CA** In this pane, you can configure the Internal Certificate Authority parameters. You can also view the CA's time, name, and the version and build number of the Security Management Server. ■ **Manage CRLs** In this pane, you can download, publish, and recreate CRLs.

Item	Pane	Description
3	Results	Shows the results of the applied operation. This window consists of a table with a list of certificates and certificate attributes.

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

Attributes	Default	Configurable	Comments
validity	2 years	yes	
key size	2048 bits	yes	Can be set to 4096 bits
DN of User certificates managed by the internal database	CN=user name, OU=users	no	This DN is appended to the DN of the ICA
DN of User certificates managed on an LDAP server		yes	Depends on LDAP branch
KeyUsage	5	yes	Digital signature and Key encipherment
ExtendedKeyUsage	0 (no KeyUsage)	yes	

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 Database Tool (GuiDBEdit Tool) (see 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

Operations with Certificates

Management of SIC Certificates

SIC certificates are managed using SmartConsole.

Management of Security 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 Security 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.

For more information, see *User Certificates* in the *R81 Remote Access VPN Administration Guide*.

Notifying Users about Certificate Initialization

The ICA Management Tool can be configured to send a notification to users about certificate initialization.

To send mail notifications:

1. In the Menu pane, click **Configure the CA**.
2. In the **Management Tool Mail Attributes** area, configure:
   - The mail server
   - The mail "`From`" address
   - An optional "`To`" address, which can be used if the users' address is not know

     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 Security Gateways and Remote Access 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://<IP address of Management Server>: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** - 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 a Certificate with set attributes (see *"Searching for a Certificate" on page 478*).

   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 CR

     Note - You can only remove expired or pending certificates.
   - **Mail to Selected** - sends mail for all selected *pending* certificate

     The mail includes the authorization codes. Messages to users that do not have an email defined are sent to a default address. For more information, see *"Notifying Users about Certificate Initialization" on page 477*.

Submitting a Certificate Request to the CA

There are three ways to submit certificate requests to the CA:

- **Initiate** - A registration key is created on the CA and used once by a user to create a certificate
- **Generate** - A certificate file is created and associated with a password which must be entered when the certificate is accessed
- **PKCS#10** - When the CA receives a PKCS#10 request, the certificate is created and delivered to the requester

To initiate a certificate

1. In the Menu pane, select **Create Certificates > Initiate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form:
   - **Certificate Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two years from the date of creation)

- **Registration Key Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two weeks from the date of creation)

3. Click **Go**.

   A registration key is created and show in the **Results** pane.

   If necessary, click **Send mail to user** to email the registration key. The number of characters in the email is limited to 1900.

4. The certificate becomes usable after entering the correct registration key.

To generate a certificate

1. In the Menu pane, select **Create Certificates > Generate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form:
   - **Certificate Expiration Date** - Select a date or enter the date in the format `dd-mm-yyyy [hh:mm:ss]` (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format `dd-mm-yyyy [hh:mm:ss]` (the default value is two weeks from the date of creation)
3. Enter a password.
4. Click **Go**.
5. Save the P12 file, and supply it to the user.

To create a PKCS#10 certificate

1. In the Menu pane, select **Create Certificates > PKCS#10**.
2. Paste into the space the encrypted base-64 buffer text provided.

   You can also click on **Browse for a file to insert (IE only)** to import the request file.
3. Click **Create** and save the created certificate.
4. Supply the certificate to the requester.

Initializing Multiple Certificates Simultaneously

You can initialize a batch of certificates at the same time.

To initialize several certificates simultaneously

1. Create a file with the list of DNs to initialize.

   Note - There are two ways to create this file - through an LDAP query or a non-LDAP query.

2. In the Menu pain, go to **Create Certificates > Advanced**.

3. Browse to the file you created.

   - To send registration keys to the users, select **Send registration keys via email**

   - To receive a file that lists the initialized DNs with their registration keys, select **Save results to file**

     This file can later be used in a script.

4. Click **Initiate from file**.

Files created through LDAP Queries

The file initiated by the LDAP search has this format:

- Each line after a blank line or the first line in the file represents one DN to be initialized

- If the line starts with "`mail=`", the string continues with the mail of the use

  If no email is given, the email address will be taken from the ICA's "Management Tool Mail To Address" attribute.

- If there is a line with the `not_after` attribute, then the value at the next line is the Certificate Expiration Date.

  The date is given in seconds from now.

- If there is a line with the is `otp_validity` attribute, then the value at the next line is the Registration Key Expiration Date.

  The date is given in seconds from now.

Here is an example of an LDAP Search output:

```
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 *"Configuring Administrators and Users on an External LDAP Server" on page 143*.

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 1> space <DN 1>
... blank line as a separator ...
<email address 2> space <DN 2>
```

CRL

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.
- Publish the SmartConsole session 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 Procedures

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:

1. Make sure that the time configured on the Management Server is correct (See the *R80.40 Gaia Administration Guide* > System Management chapter > Time section).
2. In the Menu pane, select **Manage CRLs > Clean the CA's Database and CRLs from expired certificates**.

Automatic removal of expired certificates (Available from R80.40 Jumbo Hotfix Accumulator Take 126)

- After each restart, all expired certificates are cleaned automatically.
- In addition, an automatic cleaning operation is scheduled to set every 3 weeks, starting from:
  - The first time you turn on the Management Server.
  - Each restart you do on the Management Server.

Configuring the CA

To configure the CA

1. In the Menu pane, select **Configure the CA**.
2. Edit the *"CA Data Types and Attributes" on the next page* as necessary.
3. In the **Operations** pane, select an operation:

- **Apply** - Save and enter the CA configuration settings.

  If the values are valid, the configured settings become immediately effective. All non-valid strings are changed to the default values.
- **Cancel** - Reset all values to the values in the last saved configuration.
- **Restore Default** - Revert the CA to its default configuration settings.

  Entering the string `Default` in one of the attributes will also reset it to the default after you click **Configure**. Values that are valid will be changed as requested, and others will change to default values.

CA Data Types and Attributes

The CA data types are:

- **Time** - displayed in the format: `<number> days <number> seconds`, for example: `CRL Duration: 7 days 0 seconds`

  You can enter the values in the format in which they are displayed (`<number> days <number> seconds`) or as a number of seconds.
- **Integer** - a regular integer, for example: `SIC Key Size: 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:

Attribute	Comment	Values	Default
Authorization Code Length	The number of characters of the authorization codes.	min-6 max-12	6
CRL Duration	The period of time for which the CRL is valid.	min-5 minutes max-1 year	1 week
Enable Renewal	For User certificates. This is a Boolean value setting which stipulates whether to enable renewal or not.	true or false	true

Attribute	Comment	Values	Default
Grace Period Before Revocation	The amount of time the old certificate will remain in Renewed (superseded) state.	*min-0* *max-5 years*	1 week
Grace Period Check Period	The amount of time between sequential checks of the *Renewed (superseded)* list in order to revoke those whose duration has passed.	min-10 minutes max-1 week	1 day
IKE Certificate Validity Period	The amount of time an IKE certificate will be valid.	min-10 minutes max: ■ 3 years starting from R80.40 Jumbo Hotfix Accumulator Take 119 ■ 20 years in lower takes and GA	■ 1 year starting from R80.40 Jumbo Hotfix Accumulator Take 119 ■ 5 years in lower takes and GA
IKE Certificate Extended Key Usage	Certificate purposes for describing the type of the extended key usage for IKE certificates. Refer to RFC 2459.		means no KeyUsage
IKE Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459.		Digital signature and Key encipherment
Management Tool DN prefix	Determines the DN prefix of a DN that will be created when entering a user name.	possible values CN= UID=	CN=
Management Tool DN suffix	Determines the DN suffix of a DN that will be created when entering a user name.		ou=users

Attribute	Comment	Values	Default
Management Tool Hide Mail Button	For security reasons the mail sending button after displaying a single certificate can be hidden.	true or false	false
Management Tool Mail Server	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.		-
Management Tool Registration Key Validity Period	The amount of time a registration code is valid when initiated using the Management Tool.	min-10 minutes max-2 months	2 weeks
Management Tool User Certificate Validity Period	The amount of time that a user certificate is valid when initiated using the Management Tool.	min-one week max-20 years	2 years
Management Tool Mail From Address	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.		-
Management Tool Mail Subject	The email subject field.		-
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`

Attribute	Comment	Values	Default
Management Tool Mail To address	When the **send** mail option is used, the emails to users that have no email address defined will be sent to this address.		-
Max Certificates Per Distribution Point	The maximum capacity of a CRL in the new CRL mode.	min-3 max-400	400
New CRL Mode	A Boolean value describing the CRL mode.	0 for old CRL mode 1 for new mode	true
Number of certificates per search page	The number of certificates that will be displayed in each page of the search window.	min-1 max-approx 700	approx 700
Number of Digits for Serial Number	The number of digits of certificate serial numbers.	min-5 max-10	5
Revoke renewed certificates	This flag determines whether to revoke an old certificate after it has been renewed. The reason for not revoking this is to prevent the CRL from growing each time a certificate is renewed. If the certificate is not revoked the user may have two valid certificates.	true or false	true
SIC Key Size	The key size in bits of keys used in SIC.	possible values: 1024 2048 4096	2048

Attribute	Comment	Values	Default
SIC Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459.		Digital signature and Key encipherment
SIC Certificate Validity Period	The amount of time a SIC certificate will be valid.	min-10 minutes max-20 years	5 years
User Certificate Extended Key Usage	Certificate purposes for describing the type of the extended key usage for User certificates. Refer to RFC 2459.		means no KeyUsage
User Certificate Key Size	The key size in bits of the user's certificates.	Possible values: 1024 2048 4096	2048
User Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459		Digital signature and Key encipherment

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 Security 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.

Command Line Reference

See the *R80.40 CLI Reference Guide*.

Below is a limited list of applicable commands.

Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

<table>
<tr><th>Character</th><th>Description</th></tr>
<tr><td>TAB</td><td>Shows the available nested subcommands:
<pre>
main command
→ nested subcommand 1
→ → nested subsubcommand 1-1
→ → nested subsubcommand 1-2
→ nested subcommand 2
</pre>
Example:
<pre>
cpwd_admin
    config
        -a <options>
        -d <options>
        -p
        -r
    del <options>
</pre>
Meaning, you can run only <b>one</b> of these commands:
<ul>
<li>This command:<pre>cpwd_admin config -a <options></pre></li>
<li>Or this command:<pre>cpwd_admin config -d <options></pre></li>
<li>Or this command:<pre>cpwd_admin config -p</pre></li>
<li>Or this command:<pre>cpwd_admin config -r</pre></li>
<li>Or this command:<pre>cpwd_admin del <options></pre></li>
</ul></td></tr>
<tr><td>Curly brackets or braces
<b>{ }</b></td><td>Enclose a list of available commands or parameters, separated by the vertical bar <b>|</b>.
User can enter only one of the available commands or parameters.</td></tr>
</table>

Character	Description
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

contract_util

Description

Works with the Check Point Service Contracts.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d]
    check <options>
    cpmacro <options>
    download <options>
    mgmt
    print <options>
    summary <options>
    update <options>
    verify
```

Parameters

Parameter	Description
`check <options>`	Checks whether the Security Gateway is eligible for an upgrade. See *"contract_util check" on page 496*.
`cpmacro <options>`	Overwrites the current `cp.macro` file with the specified `cp.macro` file. See *"contract_util cpmacro" on page 497*.
`download <options>`	Downloads all associated Check Point Service Contracts from the User Center, or from a local file. See *"contract_util download" on page 498*.
`mgmt`	Delivers the Service Contract information from the Management Server to the managed Security Gateways. See *"contract_util mgmt" on page 500*.
`print <options>`	Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not. See *"contract_util print" on page 501*.

Parameter	Description
`summary <options>`	Shows post-installation summary. See *"contract_util summary" on page 502*.
`update <options>`	Updates Check Point Service Contracts from your User Center account. See *"contract_util update" on page 503*.
`verify`	Checks whether the Security Gateway is eligible for an upgrade. This command also interprets the return values and shows a meaningful message. See *"contract_util verify" on page 504*.

contract_util check

Description

Checks whether the Security Gateway is eligible for an upgrade.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util check
    {-h | -help}
    hfa
    maj_upgrade
    min_upgrade
    upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`hfa`	Checks whether the Security Gateway is eligible for an upgrade to a higher Hotfix Accumulator.
`maj_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Major version.
`min_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Minor version.
`upgrade`	Checks whether the Security Gateway is eligible for an upgrade.

contract_util cpmacro

Description

Overwrites the current `cp.macro` file with the specified `cp.macro` file, if the specified is newer than the current file.

For more information about the `cp.macro` file, see sk96217: What is a cp.macro file?

Syntax

```
contract_util cpmacro /<path_to>/cp.macro
```

This command shows one of these messages:

Message	Description
`CntrctUtils_Write_cp_macro returned -1`	The `contract_util cpmacro` command failed: ■ Failed to create a temporary file. ■ Failed to write to a temporary file. ■ Failed to replace the current file.
`CntrctUtils_Write_cp_macro returned 0`	The `contract_util cpmacro` command was able to overwrite the current file with the specified file, because the specified file is newer.
`CntrctUtils_Write_cp_macro returned 1`	The `contract_util cpmacro` command did not overwrite the current file, because it is newer than the specified file.

contract_util download

Description

Downloads all associated Check Point Service Contracts from User Center, or from a local file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util download
      {-h | -help}
      local
            {-h | -help}
            [{hfa | maj_upgrade | min_upgrade | upgrade}] <Service
Contract File>
      uc
            {-h | -help}
            [-i] [{hfa | maj_upgrade | min_upgrade | upgrade}]
<Username> <Password> [<Proxy Server> [<Proxy Username>:<Proxy
Password>]]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-i`	Interactive mode - prompts the user for the User Center credentials and proxy server settings.
`local`	Specifies to download the Service Contract from the local file. This is equivalent to the "`cplic contract put`" command (see *"cplic contract" on page 578*).
`uc`	Specifies to download the Service Contract from the User Center.
`hfa`	Downloads the information about a Hotfix Accumulator.
`maj_upgrade`	Downloads the information about a Major version.
`min_upgrade`	Downloads the information about a Minor version.
`upgrade`	Downloads the information about an upgrade.
`<Username>`	Your User Center account e-mail address.
`<Password>`	Your User Center account password.
`<Proxy Server> [<Proxy Username>:<Proxy Password>]`	Specifies that the connection to the User Center goes through the proxy server. - `<Proxy Server>` - IP address of resolvable hostname of the proxy server - `<Proxy Username>` - Username for the proxy server. - `<Proxy Password>` - Password for the proxy server. Note - If you do not specify the proxy server explicitly, the command uses the proxy server configured in the management database.
`<Service Contract File>`	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your User Center account.

contract_util mgmt

Description

Delivers the Service Contract information from the Management Server to the managed Security Gateways.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util mgmt
```

contract_util print

Description

Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not.

This command can show which licenses are not recognized by the Service Contract file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d] print
      {-h | -help}
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`{-h	-help}`	Shows the applicable built-in usage.
`-d`	Shows a formatted table header and more information.
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util summary

Description

Shows post-installation summary and whether this Check Point computer is eligible for upgrades.

Syntax

```
contract_util summary
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util update

Description

Updates the Check Point Service Contracts from your User Center account.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util update
      [-proxy <Proxy Server>:<Proxy Port>]
      [-ca_path <Path to ca-bundle.crt File>]
```

Parameters

Parameter	Description
`update`	Updates Check Point Service Contracts (attached to pre-installed licenses) from your User Center account.
`-proxy <Proxy Server>:<Proxy Port>`	Specifies that the connection to the User Center goes through the proxy server: ■ `<Proxy Server>` - IP address of resolvable hostname of the proxy server. ■ `<Proxy Port>` - The applicable port on the proxy server. Note - If you do not specify the proxy explicitly, the command uses the proxy configured in the management database.
`-ca_path <Path to ca-bundle.crt File>`	Specifies the path to the Certificate Authority Bundle file (`ca-bundle.crt`). **Note** - If you do not specify the path explicitly, the command uses the default path.

contract_util verify

Description

Checks whether the Security Gateway is eligible for an upgrade.

This command is the same as the *"contract_util check" on page 496* command, but it also interprets the return values and shows a meaningful message.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util verify
```

cp_conf

Description

Configures or reconfigures a Check Point product installation.

Note - The available options for each Check Point computer depend on the configuration and installed products.

Syntax on a Management Server

```
cp_conf
      -h
      admin <options>
      auto <options>
      ca <options>
      client <options>
      finger <options>
      lic <options>
      snmp <options>
```

Parameters

Parameter	Description
`-h`	Shows the entire built-in usage.
`admin <options>`	Configures Check Point system administrators for the Security Management Server. See *"cp_conf admin" on page 507*.
`auto <options>`	Shows and configures the automatic start of Check Point products during boot. See *"cp_conf auto" on page 510*.
`ca <options>`	■ Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN). ■ Initializes the Internal Certificate Authority (ICA). See *"cp_conf ca" on page 511*.
`client <options>`	Configures the GUI clients that can use SmartConsole to connect to the Security Management Server. See *"cp_conf client" on page 513*.

Parameter	Description
`finger <options>`	Shows the ICA's Fingerprint. See *"cp_conf finger" on page 517*.
`lic <options>`	Manages Check Point licenses. See *"cp_conf lic" on page 518*.
`snmp <options>`	Do **not** use these outdated commands. To configure SNMP, see the *R80.40 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.

cp_conf admin

Description

Configures Check Point system administrators for the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- Only one administrator can be defined in the *"cpconfig" on page 569* menu.
  To define additional administrators, use SmartConsole.
- This command corresponds to the option **Administrator** in the *"cpconfig" on page 569* menu.

Syntax

```
cp_conf admin
      -h
      add [<UserName> <Password> {a | w | r}]
      add -gaia [{a | w | r}]
      del <UserName1> <UserName2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add [<UserName> <Password> {a | w | r}]`	Adds a Check Point system administrator: ■ `<UserName>` - Specifies the administrator's username ■ `<Password>` - Specifies the administrator's password ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`add -gaia [{a | w | r}]`	Adds the Gaia administrator user `admin`: ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`del <UserName1> <UserName2> ...`	Deletes the specified system administrators.
`get`	Shows the list of the configured system administrators.
`get -gaia`	Shows the management permissions assigned to the Gaia administrator user `admin`.

Example 1 - Adding a Check Point system administrator

```
[Expert@MGMT:0]# cp_conf admin add
Administrator name: admin
Administrator admin already exists.
Do you want to change Administrator's Permissions (y/n) [n] ? y

Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w

Administrator admin was modified successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; )
[Expert@MGMT:0]#
```

Example 2 - Adding the Gaia administrator user

```
[Expert@MGMT:0]# cp_conf admin add -gaia
Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w
Administrator admin was added successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get -gaia

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; ) - Gaia admin
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia a
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products with Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia w
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products without Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia r
Administrator admin already exists.

Administrator admin was modified successfully and has
Read Only Permission for all products
[Expert@MGMT:0]#
```

cp_conf auto

Description

Shows and controls which of Check Point products start automatically during boot.

Note - This command corresponds to the option **Automatic start of Check Point Products** in the *"cpconfig" on page 569* menu.

Syntax

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`{enable | disable} <Product1> <Product2> ...`	Controls whether the installed Check Point products start automatically during boot. This command is for Check Point use only.
`get all`	Shows which of these Check Point products start automatically during boot: ■ Check Point Security Gateway ■ QoS (former FloodGate-1) ■ SmartEvent Suite

Example from a Security Management Server

```
[Expert@MGMT:0]# cp_conf auto get all
Check Point Security Gateway is not installed

QoS is not installed

The SmartEvent Suite will start automatically at boot time.

[Expert@MGMT:0]#
```

cp_conf ca

Description

This command changes the settings of the Internal Certificate Authority (ICA).

Note - On a Security Management Server, this command corresponds to the option **Certificate Authority** in the *"cpconfig" on page 569* menu.

Syntax

```
cp_conf ca
      -h
      fqdn <FQDN Name>
      init
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`fqdn <FQDN Name>`	Configures the Fully Qualified Domain Name (FQDN) for the Internal Certificate Authority (ICA). The "`<FQDN Name>`" is the text string in this format: *hostname.domainname* **Notes:** ▪ The existing certificates for configured objects are **not** revoked. ▪ The existing ICA certificate is **not** changed. ▪ The Management Server uses the specified "`<FQDN Name>`" to configure the Certificate Revocation List Distribution Point (CRL DP) property in all certificates that the ICA generates. Refer to this command: *"cpca_client get_crldp" on page 547*
`init`	Initializes the Internal Certificate Authority (ICA).

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cp_conf ca fqdn MyMGMT.checkpoint.com
Trying to contact Certificate Authority. It might take a while...
Certificate was created successfully
MyMGMT.checkpoint.com was successfully set to the Internal CA
[Expert@MyMGMT:0]#
```

cp_conf client

Description

Configures the GUI clients that are allowed to connect with SmartConsoles to the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- This command corresponds to the option **GUI Clients** in the *"cpconfig" on page 569* menu.

Syntax

```
cp_conf client
      add <GUI Client>
      createlist <GUI Client 1> <GUI Client 2> ...
      del <GUI Client 1> <GUI Client 2> ...
      get
```

Parameters

Parameter	Description
-h	Shows the built-in usage.
<*GUI Client*>	<*GUI Client*> can be one of these: ■ One IPv4 address (for example, 192.168.10.20), or one IPv6 address (for example, 3731:54:65fe:2::a7) ■ One hostname (for example, MyComputer) ■ "Any" - To denote all IPv4 and IPv6 addresses without restriction ■ A range of IPv4 addresses (for example, 192.168.10.0/255.255.255.0), or a range of IPv6 addresses (for example, 2001::1/128) ■ IPv4 address wildcard (for example, 192.168.10.*)
add <*GUI Client*>	Adds a GUI client.
createlist <*GUI Client 1*> <*GUI Client 2*> ...	Deletes the current allowed GUI clients and creates a new list of allowed GUI clients.
del <*GUI Client 1*> <*GUI Client 2*> ...	Deletes the specified the GUI clients.
get	Shows the allowed GUI clients.

Examples

Example 1 - Configure one IPv4 address

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.15
172.20.168.15 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.15
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.15
172.20.168.15 was deleted successfully
[Expert@MGMT:0]#
```

Example 2 - Configure one hostname

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add MySmartConsoleHost
MySmartConsoleHost was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
MySmartConsoleHost
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del MySmartConsoleHost
MySmartConsoleHost was deleted successfully
[Expert@MGMT:0]#
```

Example 3 - Configure "Any"

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add "Any"
Any was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del "Any"
Any was deleted successfully
[Expert@MGMT:0]#
```

Example 4 - Configure a range of IPv4 addresses

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was deleted successfully
[Expert@MGMT:0]#
```

Example 5 - Configure IPv4 address wildcard

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.*
172.20.168.* was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.*
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.*
172.20.168.* was deleted successfully
[Expert@MGMT:0]#
```

Example 6 - Delete the current list and create a new list of allowed GUI clients

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist 192.168.40.0/255.255.255.0 172.30.40.55
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
192.168.40.0/255.255.255.0
172.30.40.55
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist "Any"
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#
```

cp_conf finger

Description

Shows the Internal Certificate Authority's Fingerprint.

This fingerprint is a text string derived from the ICA certificate on the Security Management Server, Multi-Domain Server, or Domain Management Server.

This fingerprint verifies the identity of the Security Management Server, Multi-Domain Server, or Domain Management Server when you connect to it with SmartConsole.

Note - This command corresponds to the option **Certificate's Fingerprint** in the *"cpconfig" on page 569* menu.

Syntax

```
cp_conf finger
      -h
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`get`	Shows the ICA's Fingerprint.

Example

```
[Expert@MGMT:0]# cp_conf finger get
EDNA COCO MOLE ATOM ASH MOT SAGE NINE ILL TINT HI CUBE
[Expert@MGMT:0]#
```

cp_conf lic

Description

Shows, adds and deletes Check Point licenses.

Note - This command corresponds to the option **Licenses and contracts** in the *"cpconfig" on page 569* menu.

Syntax

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Parameters

Parameter	Description
-h	Shows the applicable built-in usage.
add -f *<Full Path to License File>*	Adds a license from the specified Check Point license file. You get this license file in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 580*.
add -m *<Host> <Date> <Signature Key> <SKU/Features>*	Adds the license manually. You get these license details in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 580*.
del *<Signature Key>*	Delete the license based on its signature. This is the same command as the *"cplic del" on page 585*.
get [-x]	Shows the local installed licenses. If you specify the "-x" parameter, output also shows the signature key for every installed license. This is the same command as the *"cplic print" on page 589*.

Example 1 - Adding the license from the file

```
[Expert@HostName:0]#  cp_conf lic add -f ~/License.lic
License was installed successfully.
[Expert@HostName:0]#

[Expert@HostName:0]# cp_conf lic get
Host             Expiration   Signature                             Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@HostName:0]#
```

Example 2 - Adding the license manually

```
[Expert@MyHostName:0]# cp_conf lic add -m MyHostName 25Aug2019
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX
License was successfully installed
[Expert@MyHostName:0]#

[Expert@MyHostName:0]# cp_conf lic get
Host             Expiration   Signature                              Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@MyHostName:0]#
```

cp_log_export

Description

Exports Check Point logs over syslog.

For more information, see sk122323 and *R80.40 Logging and Monitoring Administration Guide*.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cp_log_export
```

```
cp_log_export <command-name> help
```

Parameters

Parameter	Description
No Parameters	Shows the built-in general help.
`<command-name> help`	Shows the built help for the specified internal command.

Internal Commands

Name	Description
`add`	Configures a new Check Point Log Exporter. `cp_log_export add name <Name> target-server <Target-Server> target-port <Target-Server-Port> protocol {udp | tcp} [Optional Arguments]`
`delete`	Removes an existing Log Exporter. `cp_log_export delete name <Name>`
`reconf`	Applies the Log Exporter configuration to all existing exporters. `cp_log_export reconf [name <Name>]`

`reexport`	Resets the current log position and exports all logs again based on the configuration.
	`cp_log_export reexport name <Name> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Last Exported Log> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Gap Start> end-position <Position of Gap End> --apply-now`

`restart`	Restarts a Log Exporter process. `cp_log_export restart name <Name>`
`set`	Updates an existing Log Exporter configuration. `cp_log_export set name <Name> [<Optional Arguments>]`
`show`	Shows the current Log Exporter configuration. `cp_log_export show [<Optional Arguments>]`
`start`	Starts an existing Log Exporter process. `cp_log_export start name <Name>`
`status`	Shows a Log Exporter overview status. `cp_log_export status [<Optional Arguments>]`

Name	Description
`stop`	Stops an existing Log Exporter process. `cp_log_export stop name <Name>`

Internal Command Arguments

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`--apply-now`	Applies immediately any change that was done with the "`add`", "`set`", "`delete`", or "`reexport`" command.	Optional	Optional	**Mandatory**	N / A	N / A	**Mandatory**
`ca-cert <Path>`	Specifies the full path to the CA certificate file `*.pem`. ⓘ **Important -** Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`client-cert <Path>`	Specifies the full path to the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A
`client-secret <Phrase>`	Specifies the challenge phrase used to create the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`domain-server {mds | all}`	On a Multi-Domain Server, specifies the applicable Domain Management Server context. On a Multi-Domain Log Server, specifies the applicable Domain Log Server context. **Important:** ■ "`mds`" (in small letters) - Exports all logs from only the main **MDS** level. ■ "`all`" (in small letters) - Exports all logs from **all** Domains.	**Mandatory**	**Mandatory**	**Mandatory**	N / A	Optional	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`enabled {true | false}`	Default: `true`	Optional	Optional	N / A	N / A	N / A	N / A
`encrypted {true | false}`	Specifies whether to use TSL (SSL) encryption to send the logs. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-attachment-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card and automatically opens the attachment. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-link-ip {true | false}`	Specifies whether to make the links to SmartView use a custom IP address (for example, for a Log Server behind NAT). ⓘ **Important** - Applicable only when the value of the "`export-link`" argument is "`true`", or the value of the "`export-attachment-link`" argument is "`true`". Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-action-in {"Action1","Action2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Action**" field. Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab. 2. In the top query field, enter **action:** and a letter. Examples of values:	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	- **Accept** - **Block** - **Bypass** - **Detect** - **Drop** - **HTTPS Bypass** - **HTTPS Inspect** - **Prevent** - **Reject** ⓘ **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-blade-in {"Blade1","Blade2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Blade**" field (the object name of the Software Blade that generated these logs). Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	2. In the top query field, enter **blade:** and a letter. Examples of values: - **Anti-Bot** - **Firewall** - **HTTPS Inspection** - **Identity Awareness** - **IPS** Valid Software Blade families: - **Access** - **TP** - **Endpoint** - **Mobile**						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-origin-in {"Origin1","Origin2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Origin**" field (the object name of the Security Gateway / Cluster Member that generated these logs). Each origin value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						
`format {cef | syslog}`	Specifies the format, in which the logs are exported. Default: `syslog`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`name "<Name>"`	Specifies the unique name of the Log Exporter configuration.	**Mandatory**	**Mandatory**	**Mandatory**	Optional. By default, applies to all.	Optional. By default, applies to all.	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Notes: ■ Allowed characters are: Latin letters, digits ("`0-9`"), minus ("`-`"), underscore ("`_`"), and period ("`.`"). ■ Must start with a letter. ■ The minimum length is two characters. ■ The "`add`" command creates a new target directory with the specified unique name in the `$EXPORTERDIR/targets/` directory.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`protocol {tcp | udp}`	Specifies the Layer 4 Transport protocol to use (TCP or UDP). There is no default value.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`read-mode {raw | semi-unified}`	Specifies the mode, in which to read the log files. - `raw` - Specifies to export log records without any unification. - `semi-unified` - Specifies to export log records with step-by-step unification. That is, for each log record, export a record that unifies this record with all previously-encountered records with the same ID. Default: `raw`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`target-port <Target-Server-Port>`	Specifies the listening port on the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A
`target-server <Target-Server>`	Specifies the IP address or FQDN of the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

cpca_client

Description

Execute operations on the Internal Certificate Authority (ICA).

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d]
      create_cert <options>
      double_sign <options>
      get_crldp <options>
      get_pubkey <options>
      init_certs <options>
      lscert <options>
      revoke_cert <options>
      revoke_non_exist_cert <options>
      search <options>
      set_cert_validity <options>
      set_mgmt_tool <options>
      set_sign_hash <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`create_cert <options>`	Issues a SIC certificate for the Security Management Server or Domain Management Server. See *"cpca_client create_cert" on page 543*.
`double_sign <options>`	Creates a second signature for a certificate. See *"cpca_client double_sign" on page 545*.

Parameter	Description
`get_crldp <options>`	Shows how to access a CRL file from a CRL Distribution Point. See *"cpca_client get_crldp" on page 547*.
`get_pubkey <options>`	Saves the encoding of the public key of the ICA's certificate to a file. See *"cpca_client get_pubkey" on page 548*.
`init_certs <options>`	Imports a list of DNs for users and creates a file with registration keys for each user. See *"cpca_client init_certs" on page 549*.
`lscert <options>`	Shows all certificates issued by the ICA. See *"cpca_client lscert" on page 550*.
`revoke_cert <options>`	Revokes a certificate issued by the ICA. See *"cpca_client revoke_cert" on page 553*.
`revoke_non_exist_cert <options>`	Revokes a non-existent certificate issued by the ICA. See *"cpca_client revoke_non_exist_cert" on page 556*.
`search <options>`	Searches for certificates in the ICA. See *"cpca_client search" on page 557*.
`set_cert_validity <options>`	Configures the default certificate validity period for new certificates. See *"cpca_client set_cert_validity" on page 560*.
`set_mgmt_tool <options>`	Controls the ICA Management Tool. See *"cpca_client set_mgmt_tool" on page 561*.
`set_sign_hash <options>`	Sets the hash algorithm that the CA uses to sign the file hash. See *"cpca_client set_sign_hash" on page 566*.

cpca_client create_cert

Description

Issues a SIC certificate for the Security Management Server or Domain Management Server.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] create_cert [-p <CA port number>] -n "CN=<Common
Name>" -f <Full Path to PKCS12 file> [-w <Password>] [-k {SIC |
USER | IKE | ADMIN_PKG}] [-c "<Comment for Certificate>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-n "CN=<Common Name>"`	Sets the CN to the specified `<Common Name>`.
`-f <Full Path to PKCS12 file>`	Specifies the PKCS12 file, which stores the certificate and keys.
`-w <Password>`	Optional. Specifies the certificate password.
`-k {SIC | USER | IKE | ADMIN_PKG}`	Optional. Specifies the certificate kind.
`-c "<Comment for Certificate>"`	Optional. Specifies the certificate comment (must enclose in double quotes).

Example

```
[Expert@MGMT:0]# cpca_client create_cert -n "cn=cp_mgmt" -f $CPDIR/conf/sic_cert.p12
```

cpca_client double_sign

Description

Creates a second signature for a certificate.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] double_sign [-p <CA port number>] -i <Certificate
File in PEM format> [-o <Full Path to Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-i <Certificate File in PEM format>`	Imports the specified certificate (only in PEM format).
`-o <Full Path to Output File>`	Optional. Saves the certificate into the specified file.

Example

```
[Expert@MGMT:0]# cpca_client double_sign -i certificate.pem

 Requesting Double Signature for the following Certificate:
        refCount: 1
        Subject: Email=example@example.com,CN=http://www.example.com/,OU=ValiCert Class 2 Policy
Validation Authority,O=exampleO\, Inc.,L=ExampleL Validation Network

 Double Sign of Cert:
 ======================
 (
        : (
                :dn ("Email=example@example.com,CN=http://www.example.com/,OU=exampleOU Class 2
Policy Validation Authority,O=exampleO\, Inc.,L=exampleL Validation Network")
                :doubleSignCert (52016390... ... ...ebb67e96)
                :return_code (0)
        )
)

[Expert@MGMT:0]#
```

cpca_client get_crldp

Description

Shows the Fully Qualified Domain Name (FQDN) configured for the Internal Certificate Authority (ICA) with the "*"cp_conf ca" on page 511*" command.

The Management Server uses this FQDN:

1. To configure the Certificate Revocation List Distribution Point (CRL DP) property in all certificates that the ICA generates.
2. To create the URL for accessing the CRL.

   Example: `http://MyMGMT.checkpoint.com:18264/ICA_CRL1.crl`

Syntax

```
cpca_client [-d] get_crldp [-p <ICA port number>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <ICA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18264.

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cpca_client get_crldp
MyMGMT.checkpoint.com
[Expert@MyMGMT:0]
```

cpca_client get_pubkey

Description

Saves the encoding of the public key of the ICA's certificate to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_pubkey [-p <CA port number>] <Full Path to
Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`<Full Path to Output File>`	Saves the encoding of the public key of the ICA's certificate to the specified file.

Example

```
[Expert@MGMT:0]# cpca_client get_pubkey /tmp/key.txt[Expert@MGMT:0]#
[Expert@MGMT:0]# cat /tmp/key.txt
3082010a... ... ...f98b8910
[Expert@MGMT:0]#
```

cpca_client init_certs

Description

Imports a list of Distinguished Names (DN) for users and creates a file with registration keys for each user.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] init_certs [-p <CA port number>] -i <Full Path to
Input File> -o <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

`-i <Full Path to Input File>`	Imports the specified file.
	Make sure to use the full path.
	Make sure that there is an empty line between each DN in the specified file.
	Example:
	`...CN=test1,OU=users...`
	`&lt;Empty Line&gt;`
	`...CN=test2,OU=users...`

`-o <Full Path to Output File>`	Saves the registration keys to the specified file. This command saves the error messages in the `<Name of Output File>.failures` file in the same directory.

cpca_client lscert

Description

Shows all certificates issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] lscert [-dn <SubString>] [-stat {Pending | Valid
| Revoked | Expired | Renewed}] [-kind {SIC | IKE | User | LDAP}]
[-ser <Certificate Serial Number>] [-dp <Certificate Distribution
Point>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <SubString>`	Optional. Filters the search results to those with a DN that matches the specified `<SubString>`. This command does not support multiple values.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Filters the search results to those with certificate status that matches the specified status. This command does not support multiple values.
`-kind {SIC | IKE | User | LDAP}`	Optional. Filters the search results to those with certificate kind that matches the specified kind. This command does not support multiple values.
`-ser <Certificate Serial Number>`	Optional. Filters the search results to those with certificate serial number that matches the specified serial number. This command does not support multiple values.
`-dp <Certificate Distribution Point>`	Optional. Filters the search results to the specified Certificate Distribution Point (CDP). This command does not support multiple values.

Example

```
[Expert@MGMT:0]# cpca_client lscert -stat Revoked
Operation succeeded. rc=0.
5 certs found.

Subject = CN=VSX2,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 5521   DP = 0
Not_Before: Sun Apr  8 14:10:01 2018   Not_After: Sat Apr  8 14:10:01 2023

Subject = CN=VSX1,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 9113   DP = 0
Not_Before: Sun Apr  8 14:09:02 2018   Not_After: Sat Apr  8 14:09:02 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#


[Expert@MGMT:0]# cpca_client lscert -kind IKE
Operation succeeded. rc=0.
3 certs found.

Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 27214   DP = 1
Not_Before: Wed Apr 11 17:26:02 2018   Not_After: Tue Apr 11 17:26:02 2023

Subject = CN=VSX_Cluster VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 64655   DP = 1
Not_Before: Mon Apr  9 19:36:31 2018   Not_After: Sun Apr  9 19:36:31 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#
```

cpca_client revoke_cert

Description

Revokes a certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_cert [-p <CA port number>] -n "CN=<Common
Name>" -s <Certificate Serial Number>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p` *`<CA port number>`*	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

`-n "CN=`*`<Common Name>`*`"`	Specifies the certificate CN.
	To get the CN, run the *"cpca_client lscert" on page 550* command and examine the text that you see between the "`Subject =`" and the "`,O=...`".
	Example
	From this output:
	`Subject = `**`CN=VS1 VPN Certificate`**`,O=MyDomain_Server.checkpoint.com.s6t98x`
	`Status = Valid   Kind = IKE   Serial = 27214   DP = 1`
	`Not_Before: Wed Apr 11 17:26:02 2018   Not_After: Tue Apr 11 17:26:02 2023`
	you get this syntax:
	`-n "CN=VS1 VPN Certificate`
	Note - You can use the parameter '`-n`' only, or together with the parameter "`-s`".

`-s` *`<Certificate Serial Number>`*	Specifies the certificate serial number. To see the serial number, run the *"cpca_client lscert" on page 550* command. **Note** - You can use the parameter "`-s`" only, or together with the parameter "`-n`".

Example 1 - Revoking a certificate specified by its CN

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -n "CN=VS1 VPN Certificate"
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

Example 2 - Revoking a certificate specified by its serial number.

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -s 27214
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

cpca_client revoke_non_exist_cert

Description

Revokes a non-existent certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_non_exist_cert -i <Full Path to Input
File>
```

Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>-d</td><td>Runs the cpca_client command under debug.</td></tr>
<tr><td>-i <i>&lt;Full Path to Input File&gt;</i></td><td>Specifies the file that contains the list of the certificate to revoke.
You must create this file in the same format as the "cpca_client lscert" on page 550 command prints its output.
<b>Example</b>

```
Subject = CN=cp_mgmt,O=MGMT.5p72vp
Status = Valid   Kind = SIC   Serial = 30287   DP = 0
Not_Before: Sat Apr  7 19:40:12 2018   Not_After: Fri
Apr  7 19:40:12 2023
&lt;Empty Line&gt;
Subject = CN=cp_mgmt,O=MGMT.5p72vp
Status = Valid   Kind = SIC   Serial = 60870   DP = 0
Not_Before: Sat Apr  7 19:40:13 2018   Not_After: Fri
Apr  7 19:40:13 2023
```

</td></tr>
</table>

Note - This command saves the error messages in the *<Name of Input File>*.failures file.

cpca_client search

Description

Searches for certificates in the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] search <String> [-where {dn | comment | serial |
device_type | device_id | device_name}] [-kind {SIC | IKE | User |
LDAP}] [-stat {Pending | Valid | Revoked | Expired | Renewed}] [-
max <Maximal Number of Results>] [-showfp {y | n}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`<String>`	Specifies the text to search in the certificates. You can enter only one text string that does not contain spaces.

Parameter	Description
`-where {dn | comment | serial | device_type | device_id | device_name}`	Optional. Specifies the certificate's field, in which to search for the string: - `dn` - Certificate DN - `comment` - Certificate comment - `serial` - Certificate serial number - `device_type` - Device type - `device_id` - Device ID - `device_name` - Device Name The default is to search in all fields.
`-kind {SIC | IKE | User | LDAP}`	Optional. Specifies the certificate kind to search. You can enter multiple values in this format: `-kind` *`<Kind1> <Kind2> <Kind3>`* The default is to search for all kinds.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Specifies the certificate status to search. You can enter multiple values in this format: `-stat` *`<Status1> <Status2> <Status3>`* The default is to search for all statuses.
`-max` *`<Maximal Number of Results>`*	Optional. Specifies the maximal number of results to show. - Range: 1 and greater - Default: 200
`-showfp {y | n}`	Optional. Specifies whether to show the certificate's fingerprint and thumbprint: - `y` - Shows the fingerprint and thumbprint (this is the default) - `n` - Does not show the fingerprint and thumbprint

Example 1

```
[Expert@MGMT:0]# cpca_client search samplecompany -where comment -kind SIC LDAP -stat Pending
Valid Renewed
```

Example 2

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dnOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
Fingerprint = XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX
Thumbprint = xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
[Expert@MGMT:0]#
```

Example 3

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dn -showfp nOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
[Expert@MGMT:0]#
```

cpca_client set_cert_validity

Description

This command configures the default certificate validity period for new certificates.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- The new certificate validity period applies only to certificate you create after this change.

Syntax

```
cpca_client set_cert_validity -k {SIC | IKE | USER} [-y <Number of
Years>] [-d <Number of Days>] [-h <Number of Hours>] [-s <Number
of Seconds>]
```

Parameters

Parameter	Description
`-k {SIC | IKE | USER}`	Specifies the certificate type.
`-y <Number of Years>`	Specifies the validity period in years.
`-d <Number of Days>`	Specifies the validity period in days.
`-h <Number of Hours>`	Specifies the validity period in hours.
`-s <Number of Seconds>`	Specifies the validity period in seconds.

Example

```
[Expert@MGMT:0]# cpca_client set_cert_validity -k IKE -y 3
 cert validity period was changed successfully.
[Expert@MGMT:0]#
```

cpca_client set_mgmt_tool

Description

Controls the ICA Management Tool.

This tool is disabled by default.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

See sk102837: Best Practices - ICA Management Tool configuration

Syntax

```
cpca_client [-d] set_mgmt_tool {on | off | add | remove | clean |
print} [-p <CA port number>] [{-a <Administrator DN> | -u <User
DN> | -c <Custom User DN>}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`on`	Starts the ICA Management Tool.
`off`	Stops the ICA Management Tool.
`add`	Adds the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`remove`	Removes the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`clean`	Removes all administrators, users, or custom users that are permitted to use the ICA Management Tool.
`print`	Shows the configured administrators, users, or custom users that are permitted to use the ICA Management Tool.

Parameter	Description
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18265.
`-a <Administrator DN>`	Optional. Specifies the DN of the administrator that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-a "CN=ICA_Tool_Admin,OU=users,O=MGMT.s6t98x"`
`-u <User DN>`	Optional. Specifies the DN of the user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole: **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-u "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Parameter	Description
`-c <Custom User DN>`	Optional. Specifies the DN for the custom user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole. **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-c "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Note - If you run the "`cpca_client set_mgmt_tool`" command without the parameter "`-a`" or "`-u`", the list of the permitted administrators and users is not changed. The previously defined permitted administrators and users can start and stop the ICA Management Tool.

To connect to the ICA Management Tool

1. In SmartConsole, configure the required administrator and user objects.

   You must create a certificate for these administrators and users.

   You use this certificate to configure the permitted users in the ICA Management Tool and in the client web browsers.

2. In the command line on the Management Server, add the required administrators and users that are permitted to use the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool add ...
   ```

3. In the command line on the Management Server, start the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool on
   ```

4. Check the status of the ICA Management Tool:

   ```
   cpca_client set_mgmt_tool print
   ```

5. Import the administrator's / user's certificate into the Windows Certificate Store:.

   a. Right-click the *.p12 file you saved when you created the required administrator / user, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

   d. Enter the same certificate password you used when you created the required administrator / user certificate.

   e. Clear **Enable strong private key protection**.

   f. Select **Mark this key as exportable**.

   g. Click **Next**.

   h. Select **Place all certificates in the following store** > click **Browse** > select **Personal** > click **OK**.

   i. Click **Next**.

   j. Click **Finish**.

6. In a web browser, connect to the ICA Management Tool:

   ```
   https://<IP Address of the Management Server>:18265
   ```

   Important - The fact that the TCP port 18265 is open is not a vulnerability. The ICA Management Tool Portal is secured and protected by SSL. In addition, only authorized administrators and users are allowed to access it using a certificate.

7. A dialog box with this message appears:

   ```
   Client Authentication

   Identification

   The Web site you want to view requests identification.

   Select the certificate to use when connecting.
   ```

8. Select the appropriate certificate for authenticating to the ICA Management Tool.

9. Click **OK**.

10. In the **Security Alert** dialog box, click **Yes**.

cpca_client set_sign_hash

Description

Sets the hash algorithm that the CA uses to sign the file hash. Also, see sk103840.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] set_sign_hash {sha1 | sha256 | sha384 | sha512}
```

Important - After this change, you must restart the Check Point services with these commands:

- On Security Management Server, run:
  1. `cpstop`
  2. `cpstart`
- On a Multi-Domain Server, run:
  1. `mdsstop_customer <Name or IP Address of Domain Management Server>`
  2. `mdsstart_customer <Name or IP Address of Domain Management Server>`

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{sha1 | sha256 | sha384 | sha512}`	The hash algorithms that the CA uses to sign the file hash. The default algorithm is SHA-256.

Example

```
[Expert@MGMT:0]# cpca_client set_sign_hash sha256

You have selected the signature hash function SHA-256
WARNING: This hash algorithm is not supported in Check Point gateways prior to R71.
WARNING: It is also not supported on older clients and SG80 R71.

Are you sure? (y/n)
y
Internal CA signature hash changed successfully.
Note that the signature on the Internal CA certificate has not changed, but this has no security
implications.
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpstop ; cpstart
```

cpca_create

Description

Creates new Check Point Internal Certificate Authority database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_create [-d] -dn <CA DN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <CA DN>`	Specifies the Certificate Authority Distinguished Name (DN).

cpconfig

Description

This command starts the Check Point Configuration Tool.

This tool configures specific settings for the installed Check Point products.

Syntax

```
cpconfig
```

Note - On a Multi-Domain Server, run the "`mdsconfig`" command.

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this server.
Administrator	Configures Check Point system administrators for this server.
GUI Clients	Configures the GUI clients that can use SmartConsole to connect to this server.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R80.40 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.
Certificate Authority	Initializes the Internal Certificate Authority (ICA) and configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN).
Certificate's Fingerprint	Shows the ICA's Fingerprint. This fingerprint is a text string derived from the server's ICA certificate. This fingerprint verifies the identity of the server when you connect to it with SmartConsole.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

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 Check Point computer at the time of execution.

It is mandatory to collect these data when you contact *Check Point Support* about an issue on your Check Point server.

For more information, see sk92739.

cplic

Description

The cplic command manages Check Point licenses.

You can run this command in Gaia Clish or in the Expert mode.

License Management is divided into three types of commands:

Licensing Commands	Applies To	Description
Local licensing commands	Management Servers, Security Gateways and Cluster Members	You execute these commands locally on the Check Point computers.
Remote licensing commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the managed Security Gateways and Cluster Members.
License Repository commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the licenses stored in the local license repository.

Syntax for Local Licensing on a Management Server itself

```
cplic [-d]
      {-h | -help}
      check <options>
      contract <options>
      del <options>
      print <options>
      put <options>
```

Syntax for Remote Licensing on managed Security Gateways and Cluster Members

```
cplic [-d]
      {-h | -help}
      del <options>
      get <options>
      put <options>
      upgrade <options>
```

Syntax for License Database Operations on a Management Server

```
cplic [-d]
      {-h | -help}
      db_add <options>
      db_print <options>
      db_rm <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the applicable built-in usage.
`check <options>`	Confirms that the license includes the feature on the local Security Gateway or Management Server. See *"cplic check" on page 576*.
`contract <options>`	Manages (deletes and installs) the Check Point Service Contract on the local Check Point computer. See *"cplic contract" on page 578*.
`db_add <options>`	Applies only to a Management Server. Adds licenses to the license repository on the Management Server. See *"cplic db_add" on page 580*.

Parameter	Description
`db_print <options>`	Applies only to a Management Server. Shows the details of Check Point licenses stored in the license repository on the Management Server. See *"cplic db_print" on page 582*.
`db_rm <options>`	Applies only to a Management Server. Removes a license from the license repository on the Management Server. See *"cplic db_rm" on page 584*.
`del <options>`	Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses. See *"cplic del" on page 585*.
`del <Object Name> <options>`	Detaches a Central license from a remote managed Security Gateway or Cluster Member. See *"cplic del <object name>" on page 586*.
`get <options>`	Applies only to a Management Server. Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server. See *"cplic get" on page 587*.
`print <options>`	Prints details of the installed Check Point licenses on the local Check Point computer. See *"cplic print" on page 589*.
`put <options>`	Installs and attaches licenses on a Check Point computer. See *"cplic put" on page 591*.
`put <Object Name> <options>`	Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members. See *"cplic put <object name>" on page 593*.
`upgrade <options>`	Applies only to a Management Server. Upgrades licenses in the license repository with licenses in the specified license file. See *"cplic upgrade" on page 596*.

cplic check

Description

Confirms that the license includes the feature on the local Security Gateway or Management Server. See sk66245.

Syntax

```
cplic check {-h | -help}
```

```
cplic [-d] check [-p <Product>] [-v <Version>] [{-c | -count}] [-t <Date>] [{-r | -routers}] [{-S | -SRusers}] <Feature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <Product>`	Product, for which license information is requested. Some examples of products: ■ `fw1` - FireWall-1 infrastructure on Security Gateway / Cluster Member (all blades), or Management Server (all blades) ■ `mgmt` - Multi-Domain Server infrastructure ■ `services` - Entitlement for various services ■ `cvpn` - Mobile Access ■ `etm` - QoS (FloodGate-1) ■ `eps` - Endpoint Software Blades on Management Server
`-v <Version>`	Product version, for which license information is requested.
`{-c | -count}`	Outputs the number of licenses connected to this feature.

Parameter	Description
`-t <Date>`	Checks license status on future date. Use the format **ddmmyyyy**. A feature can be valid on a given date on one license, but invalid on another.
`{-r | -routers}`	Checks how many routers are allowed. The *`<Feature>`* option is not needed.
`{-S | -SRusers}`	Checks how many SecuRemote users are allowed.
`<Feature>`	Feature, for which license information is requested.

Example from a Management Server

```
[Expert@MGMT]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 24Mar2016 ::CK-XXXXXXXXXXXX fw1:6.0:swb fw1:6.0:comp fw1:6.0:compunlimited fw1:6.0:cluster-1 fw1:6.0:cpxmgmt_qos_u_sites
fw1:6.0:sprounl fw1:6.0:nxunlimit fw1:6.0:swp evnt:6.0:smrt_evnt fw1:6.0:fwc fw1:6.0:ca fw1:6.0:rtmui fw1:6.0:sstui fw1:6.0:fwlv
fw1:6.0:cmd evnt:6.0:alzd5 evnt:6.0:alzc1 evnt:6.0:alzs1 fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:sme10 etm:6.0:rtm_u fw1:6.0:cep1 fw1:6.0:rt
fw1:6.0:cemid fw1:6.0:web_sec_u fw1:6.0:workflow fw1:6.0:ram1 fw1:6.0:routers fw1:6.0:supmgmt fw1:6.0:supunlimit fw1:6.0:prov
fw1:6.0:atlas-unlimit fw1:6.0:filter fw1:6.0:ui psmp:6.0:psmsunlimited fw1:6.0:vpe_unlimit fw1:6.0:cluster-u fw1:6.0:remote1 fw1:6.0:aes
fw1:6.0:strong fw1:6.0:rdp fw1:6.0:des fw1:6.0:isakmp fw1:6.0:dbvr_unlimit fw1:6.0:cmpmgmt fw1:6.0:rtmmgmt fw1:6.0:fgmgmt fw1:6.0:blades
fw1:6.0:cpipv6 fw1:6.0:mgmtha fw1:6.0:remote
[Expert@MGMT]#
```

Example from a Management Server in High Availability

```
[Expert@MGMT]# cplic check -p fw1 -v 6.0 -c mgmtha
cplic check 'mgmtha': 1 licenses
[Expert@MGMT]#
```

cplic contract

Description

Deletes the Check Point Service Contract on the local Check Point computer.

Installs the Check Point Service Contract on the local Check Point computer.

Note

- For more information about Service Contract files, see sk33089: What is a Service Contract File?
- If you install a Service Contract on a managed Security Gateway / Cluster Member, you must update the license repository on the applicable Management Server - either with the *"cplic get" on page 587* command, or in SmartUpdate.

Syntax

```
cplic contract -h
```

```
cplic [-d] contract
      del
            -h
            <Service Contract ID>
      put
            -h
            [{-o | -overwrite}] <Service Contract File>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`del`	Deletes the Service Contract from the `$CPDIR/conf/cp.contract` file on the local Check Point computer.
`put`	Merges the Service Contract to the `$CPDIR/conf/cp.contract` file on the local Check Point computer.
`<Service Contract ID>`	ID of the Service Contract.
`{-o | -overwrite}`	Specifies to overwrite the current Service Contract.
`<Service Contract File>`	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your *Check Point User Center* account.

cplic db_add

Description

Adds licenses to the license repository on the Management Server.

When you add Local licenses to the license repository, Management Server automatically attaches them to the managed Security Gateway / Cluster Member with the matching IP address.

When you add Central licenses, you must manually attach them.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic db_add {-h | -help}
```

```
cplic [-d] db_add -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Features>]
```

Parameters

Parameter	Description
`{-h	-help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l <License File>`	Name of the file that contains the license.
`<Host>`	Hostname or IP address of the Security Management Server / Domain Management Server.
`<Expiration Date>`	The license expiration date.
`<Signature>`	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` Case sensitive. Hyphens are optional.

Parameter	Description
< SKU/Features>	The SKU of the license summarizes the features included in the license. For example, `CPSUITE-EVAL-3DES-vNG`

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:

```
[Expert@MGMT]# cplic db_add -l 192.0.2.11.lic
Adding license to database ...
Operation Done
[Expert@MGMT]#
```

cplic db_print

Description

Shows the details of Check Point licenses stored in the license repository on the Management Server.

Syntax

```
cplic db_print {-h | -help}
```

```
cplic [-d] db_print {<Object Name> | -all} [{-n | -noheader}] [-x]
[{-t | -type}] [{-a | -attached}]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`<Object Name>`	Prints only the licenses attached to *`<Object Name>`*. *`<Object Name>`* is the name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-all`	Prints all the licenses in the license repository.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signatures.
`{-t | -type}`	Prints licenses with their type: Central or Local.
`{-a | -attached}`	Shows to which object the license is attached. Useful, if the parameter "`-all`" is specified.

Example

```
[Expert@MGMT:0]# cplic db_print -all
 Retrieving license information from database ...

The following licenses appear in the database:
===============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXXX
[Expert@MGMT:0]#

[Expert@MGMT:0]# cplic db_print -all -x -a
 Retrieving license information from database ...

The following licenses appear in the database:
===============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXXX  MGMT
[Expert@MGMT:0]#
```

cplic db_rm

Description

Removes a license from the license repository on the Management Server.

After you remove the license from the repository, it can no longer use it.

Warning - You can run this command ONLY after you detach the license with the *"cplic del" on page 585* command.

Syntax

```
cplic db_rm {-h | -help}
```

```
cplic [-d] db_rm <Signature>
```

Parameters

Parameter	Description
`{-h	-help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 589* command.

Example

```
[Expert@MGMT:0]# cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

cplic del

Description

Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses.

This command can delete a license on both local computer, and on remote managed computers.

Syntax

```
cplic del {-h | -help}
```

```
cplic [-d] del [-F <Output File>] <Signature> <Object Name>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-F <Output File>`	Saves the command output to the specified file.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 589* command.
`<Object Name>`	The name of the Security Gateway / Cluster Member object as defined in SmartConsole.

cplic del <object name>

Description

Detaches a Central license from a remote managed Security Gateway or Cluster Member.

When you run this command, it automatically updates the license repository.

The Central license remains in the license repository as an unattached license.

Syntax

```
cplic del {-h | -help}
```

```
cplic [-d] del <Object Name> [-F <Output File>] [-ip <Dynamic IP
Address>] <Signature>
```

Parameters

Parameter	Description
`{-h	-help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`<Object Name>`	The name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-F` *`<Output File>`*	Saves the command output to the specified file.
`-ip` *`<Dynamic IP Address>`*	Deletes the license on the DAIP Security Gateway with the specified IP address. **Note** - If this parameter is used, then object name must be a DAIP Security Gateway.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 589* command.

cplic get

Description

Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server.

This command helps synchronize the license repository with the managed Security Gateways and Cluster Members.

When you run this command, it updates the license repository with all local changes.

Syntax

```
cplic get {-h | -help}
```

```
cplic [-d] get
      -all
      <IP Address>
      <Host Name>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-all`	Retrieves licenses from all Security Gateways and Cluster Members in the managed network.
`<IP Address>`	The IP address of the Security Gateway / Cluster Member, from which licenses are to be retrieved.
`<Host Name>`	The name of the Security Gateway / Cluster Member object as defined in SmartConsole, from which licenses are to be retrieved.

Example

If the Security Gateway with the object name `MyGW` contains four Local licenses, and the license repository contains two other Local licenses, the command "`cplic get MyGW`" produces output similar to this:

```
[Expert@MGMT:0]# cplic get MyGW
Get retrieved 4 licenses.
Get removed 2 licenses.
[Expert@MGMT:0]#
```

cplic print

Description

Prints details of the installed Check Point licenses on the local Check Point computer.

Note - On a Security Gateway / Cluster Member, this command prints all installed licenses (both Local and Central).

Syntax

```
cplic print {-h | -help}
```

```
cplic [-d] print[{-n | -noheader}] [-x] [{-t | -type}] [-F <Output File>] [{-p | -preatures}] [-D]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signature.
`{-t | -type]`	Prints licenses showing their type: Central or Local.
`-F <Output File>`	Saves the command output to the specified file.
`{-p | -preatures}`	Prints licenses resolved to primitive features.
`-D`	On a Multi-Domain Server, prints only Domain licenses.

Example 1

```
[Expert@HostName:0]# cplic print
Host             Expiration     Features
192.168.3.28     25Aug2019      CPMP-XXX   CK-XXXXXXXXXXXX
[Expert@HostName:0]#
```

Example 2

```
[Expert@HostName:0]# cplic print -x
Host             Expiration   Signature                          Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    CPMP-XXX  CK-XXXXXXXXXXXX
[Expert@HostName:0]#
```

cplic put

Description

Installs one or more Local licenses on a Check Point computer.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] 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

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-o | -overwrite}`	On a Security Gateway / Cluster Member, this command erases only the local licenses, but not central licenses that are installed remotely.
`{-c | -check-only}`	Verifies the license. Checks if the IP of the license matches the Check Point computer and if the signature is valid.
`{-s | -select}`	Selects only the local license whose IP address matches the IP address of the Check Point computer.
`-F <Output File>`	Saves the command output to the specified file.
`{-P | -Pre-boot}`	Use this option after you have upgraded and before you reboot the Check Point computer. Use of this option will prevent certain error messages.

Parameter	Description
`{-K | -kernel-only}`	Pushes the current valid licenses to the kernel. For use by Check Point Support only.
`-l` *`<License File>`*	Name of the file that contains the license.
`<Host>`	Hostname or IP address of the Security Gateway / Cluster Member for a local license. Hostname or IP address of the Security Management Server / Domain Management Server for a central license.
`<Expiration Date>`	The license expiration date.
`<Signature>`	The signature string within the license. Case sensitive. The hyphens are optional.
`<SKU/Features>`	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IP address of the external interface (in quad-dot notation). The last part cannot be 0 or 255.
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	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`

Example

```
[Expert@HostName:0]# cplic put -l License.lic
Host Expiration SKU
192.168.2.3 14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
[Expert@HostName:0]#
```

cplic put <object name>

Description

Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members.

When you run this command, it automatically updates the license repository.

Note

- You get the license details in the *Check Point User Center*.
- You can attach more than one license.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put <Object Name> [-ip<Dynamic IP Address> ] [-F
<Output File>] -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Feature>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`<Object Name>`	The name of the Security Gateway / Cluster Member object, as defined in SmartConsole.
`-ip <Dynamic IP Address>`	Installs the license on the Security Gateway with the specified IP address. This parameter is used to install a license on a Security Gateway with dynamically assigned IP address (DAIP). **Note** - If you use this parameter, then the object name must be that of a DAIP Security Gateway.
`-F <Output File>`	Saves the command output to the specified file.
`-l <License File>`	Installs the licenses from the *<License file>*.
`<Host>`	Hostname or IP address of the Security Management Server / Domain Management Server.
`<Expiration Date>`	The license expiration date.
`<Signature>`	The license signature string. Case sensitive. The hyphens are optional.
`<SKU/Features>`	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IP address of the external interface (in quad-dot notation). The last part cannot be 0 or 255.
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	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`

cplic upgrade

Description

Upgrades licenses in the license repository with licenses in the specified license file.

Note - You get this license file in the *Check Point User Center*.

Syntax

```
cplic upgrade {-h | -help}
```

```
cplic [-d] upgrade -l <Input File>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-l <Input File>`	Upgrades the licenses in the license repository and Check Point Security Gateways / Cluster Members to match the licenses in the specified file.

Example

This example explains the procedure to upgrade the licenses in the license repository.

There are two Software Blade licenses in the input file:

- One license does not match any license on a remote managed Security Gateway.
- The other license matches an NGX-version license on a managed Security Gateway that has to be upgraded.

Workflow in this example:

1. 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.

2. Import all licenses into the license repository.

   You can also do this after you upgrade the products on the remote Security Gateways.

3. Run this command:

```
cplic get -all
```

Example:

```
[Expert@MyMGMT]# cplic get -all
Getting licenses from all modules ...
MyGW:
Retrieved 1 licenses
```

4. To see all the licenses in the repository, run this command:

```
cplic db_print -all -a
```

Example:

```
[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 MyGW1
192.0.2.11 26Nov2017 CPSB-SWB CPSB-ADNC-M CK0123456789ab MyGW2
```

5. In the *Check Point User Center*, view the licenses for the products that were upgraded from version NGX to a Software Blades license.

   You can also create new upgraded licenses.

6. Download a file containing the upgraded licenses.

   Only download licenses for the products that were upgraded from version NGX to Software Blades.

7. If you did not import the version NGX licenses into the repository, import the version NGX licenses now.

   Use this command:

```
cplic get -all
```

8. Run the license upgrade command:

```
cplic upgrade -l <Input File>
```

   - 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.

cppkg

Description

Manages the SmartUpdate software packages repository on the Security Management Server.

Important - Installing software packages with the SmartUpdate is not supported for Security Gateways running on Gaia OS.

Syntax

```
cppkg
      add <options>
      {del | delete} <options>
      get
      getroot
      print
      setroot <options>
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run `mdsenv`).

Parameters

Parameter	Description
`add <options>`	Adds a SmartUpdate software package to the repository. See *"cppkg add" on page 600*.
`{del | delete} <options>`	Deletes a SmartUpdate software package from the repository. See *"ppkg delete" on page 601*.
`get`	Updates the list of the SmartUpdate software packages in the repository. See *"cppkg get" on page 603*.
`getroot`	Shows the path to the root directory of the repository (the value of the environment variable `$SUROOT`). See *"cppkg getroot" on page 604*.
`print`	Prints the list of SmartUpdate software packages in the repository. See *"cppkg print" on page 605*.
`setroot <options>`	Configures the path to the root directory of the repository. See *"cppkg setroot" on page 606*.

cppkg add

Description

Adds a SmartUpdate software package to the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- This command does not overwrite existing packages. To overwrite an existing package, you must first delete the existing package.
- You get the SmartUpdate software packages from the *Check Point Support Center*.

Syntax

```
cppkg add <Full Path to Package | DVD Drive [Product]>
```

Parameters

Parameter	Description
`<Full Path to Package>`	Specifies the full local path on the computer to the SmartUpdate software package.
DVD Drive `[`*`Product`*`]`	Specifies the DVD root path. Example: `/mnt/CPR80`

Example - Adding R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product             Version    OS                    Minor Version
--------------------------------------------------------------------------------
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg add /var/log/CP1100_6.0_4_0_-.tgz
Adding package to the repository
Getting the package type...
Extracting the package files...
Copying package to the repository...
Package was successfully added to the repository
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg print
Vendor          Product             Version    OS                    Minor Version
--------------------------------------------------------------------------------
Check Point     CP1100              R77.20     Gaia Embedded         R77.20
[Expert@MGMT:0]#
```

ppkg delete

Description

Deletes SmartUpdate software packages from the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg del ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

```
cppkg delete ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

Parameters

Parameter	Description
`del | delete`	When you do not specify optional parameters, the command runs in the interactive mode. The command shows the menu with applicable options.
`"<Vendor>"`	Specifies the package vendor. Enclose in double quotes.
`"<Product>"`	Specifies the product name. Enclose in double quotes.
`"<Major Version>"`	Specifies the package Major Version. Enclose in double quotes.
`"<OS>"`	Specifies the package OS. Enclose in double quotes.
`"<Minor Version>"`	Specifies the package Minor Version. Enclose in double quotes.

Notes:

- To see the values for the optional parameters, run the *"cppkg print" on page 605* command.
- You must specify all optional parameters, or no parameters.

Example 1 - Interactive mode

```
[Expert@MGMT:0]# cppkg delete

Select package:
--------------------
(0) Delete all
(1) CP1100 Gaia Embedded Check Point R77.20 R77.20

(e) Exit

Enter your choice : 1

You chose to delete 'CP1100 Gaia Embedded Check Point R77.20 R77.20', Is this correct? [y/n] : y

Package was successfully removed from the repository
[Expert@MGMT:0]#
```

Example 2 - Manually deleting the specified package

```
Expert@MGMT:0]# cppkg print
Vendor          Product             Version    OS                  Minor Version
----------------------------------------------------------------------------------
Check Point     CP1100              R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg delete "Check Point" "CP1100" "R77.20" "Gaia Embedded" "R77.20"
Package was successfully removed from the repository
[Expert@MGMT:0]#
```

cppkg get

Description

Updates the list of the SmartUpdate software packages in the SmartUpdate software packages repository based on the real content of the repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg get
```

Example

```
[Expert@MGMT:0]# cppkg get
Update successfully completed
[Expert@MGMT:0]#
```

cppkg getroot

Description

Shows the path to the root directory of the SmartUpdate software packages repository (the value of the environment variable `$SUROOT`)

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg getroot
```

Example

```
[Expert@MGMT:0]# cppkg getroot
[cppkg 7119 4128339728]@MGMT[29 May 19:16:06] Current repository root is set to :
/var/log/cpupgrade/suroot
[Expert@MGMT:0]#
```

cppkg print

Description

Prints the list of SmartUpdate software packages in the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg print
```

Example - R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
----------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded        R77.20
[Expert@MGMT:0]#
```

cppkg setroot

Description

Configures the path to the root directory of the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- The default path is: `/var/log/cpupgrade/suroot`
- When changing repository root directory:
  - This command copies the software packages from the old repository to the new repository. A package in the new location is overwritten by a package from the old location, if the packages have the same name.
  - This command updates the value of the environment variable `$SUROOT` in the Check Point Profile shell scripts (`$CPDIR/tmp/.CPprofile.sh` and `$CPDIR/tmp/.CPprofile.csh`).

Syntax

```
cppkg setroot <Full Path to Repository Root Directory>
```

Example

```
[Expert@MGMT:0]# cppkg setroot /var/log/my_directory

Repository root is set to : /var/log/cpupgrade/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/log/my_directory

Notice : To complete the setting of your directory, reboot the machine!
[Expert@MGMT:0]#
```

cpprod_util

Description

This utility works with Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) without manually opening it:

- Shows which Check Point products and features are enabled on this Check Point computer.
- Enables and disables Check Point products and features on this Check Point computer.

Syntax

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}
```

```
cpprod_util -dump
```

Parameters

Parameter	Description
`CPPROD_GetValue`	Gets the configuration status of the specified product or feature: - 0 - Disabled - 1 - Enabled
`CPPROD_SetValue`	Sets the configuration for the specified product or feature. ℹ **Important** - Do not run these commands unless explicitly instructed by Check Point Support or R&D to do so.
`"<`*`Product`*`>"`	Specifies the product or feature.
`"<`*`Parameter`*`>"`	Specifies the configuration parameter for the specified product or feature.
`"<`*`Value`*`>"`	Specifies the value of the configuration parameter for the specified product or feature: - One of these integers: 0, 1, 4 - A string
`dump`	Creates a dump file of Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) in the current working directory. The name of the output file is `RegDump`.

Notes

- On a Multi-Domain Server, you must run this command in the context of the relevant Domain Management Server.
- If you run the `cpprod_util` command without parameters, it prints:
  - The list of all available products and features (for example, "`FwIsFirewallMgmt`", "`FwIsLogServer`", "`FwIsStandAlone`")
  - The type of the expected argument when you configure a product or feature ("`no-parameter`", "`string-parameter`", or "`integer-parameter`")
  - The type of the returned output ("`status-output`", or "`no-output`")
- To redirect the output of the `cpprod_util` command, it is necessary to redirect the *stderr* to *stdout*:

  ```
  cpprod_util <options> > <output file> 2>&1
  ```

  Example:

  ```
  cpprod_util > /tmp/output_of_cpprod_util.txt 2>&1
  ```

Examples

Example - Showing a list of all installed Check Point Products Packages on a Management Server

```
[Expert@MGMT:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
NGXCMP
EdgeCmp
SFWCMP
SFWR75CMP
SFWR77CMP
FLICMP
R75CMP
R7520CMP
R7540CMP
R76CMP
R77CMP
PROVIDER-1
Reporting Module
SmartLog
CPinfo
VSEC
DIAG
[Expert@MGMT:0]#
```

Example - Checking if this Check Point computer is configured as a Management Server

```
[Expert@MGMT:0]# cpprod_util FwIsFirewallMgmt
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point computer is configured as a Standalone

```
[Expert@MGMT:0]# cpprod_util FwIsStandAlone
0
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as a Primary in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsPrimary
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Active in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsActiveManagement
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Backup in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsSMCBackup
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point computer is configured as a dedicated Log Server

```
[Expert@MGMT:0]# cpprod_util FwIsLogServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartProvisioning blade is enabled

```
[Expert@MGMT:0]# cpprod_util FwIsAtlasManagement
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Server blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Correlation Unit blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerCorrelationUnit
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the Endpoint Policy Management blade is enabled

```
[Expert@MGMT:0]# cpprod_util UepmIsInstalled
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Endpoint Policy Server

```
[Expert@MGMT:0]# cpprod_util UepmIsPolicyServer
0
[Expert@MGMT:0]#
```

cprid

Description

Manages the Check Point Remote Installation Daemon (`cprid`).

This daemon is used for remote upgrade and installation of Check Point products on the managed Security Gateways.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run these commands in the context of the MDS (run `mdsenv`).

Commands

Syntax	Description
`cpridstart`	Starts the Check Point Remote Installation Daemon (`cprid`).
`cpridstop`	Stops the Check Point Remote Installation Daemon (`cprid`).
`run_cprid_restart`	Stops and then starts the Check Point Remote Installation Daemon (`cprid`).

cprinstall

Description

Performs installation of Check Point product packages and associated operations on remote managed Security Gateways.

Important - Installing software packages with this command is not supported for Security Gateways that run on Gaia OS.

Notes:

- This command requires a license for SmartUpdate.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- On the remote Security Gateways these are required:
  - SIC Trust must be established between the Security Management Server and the Security Gateway.
  - The `cpd` daemon must run.
  - The `cprid` daemon must run.

Syntax

```
cprinstall
      boot <options>
      cprestart <options>
      cpstart <options>
      cpstop <options>
      delete <options>
      get <options>
      install <options>
      revert <options>
      show <options>
      snapshot <options>
      transfer <options>
      uninstall <options>
      verify <options>
```

Parameters

Parameter	Description
`boot <options>`	Reboots the managed Security Gateway. See *"cprinstall boot" on page 616*.
`cprestart <options>`	Runs the `cprestart` command on the managed Security Gateway. See *"cprinstall cprestart" on page 617*.
`cpstart <options>`	Runs the `cpstart` command on the managed Security Gateway. See *"cprinstall cpstart" on page 618*.
`cpstop <options>`	Runs the `cpstop` command on the managed Security Gateway. See *"cprinstall cpstop" on page 619*.
`delete <options>`	Deletes a snapshot (backup) file on the managed Security Gateway. See *"cprinstall delete" on page 620*.
`get <options>`	▪ Gets details of the products and the operating system installed on the managed Security Gateway. ▪ Updates the management database on the Security Management Server. See *"cprinstall get" on page 621*.
`install <options>`	Installs Check Point products on the managed Security Gateway. See *"cprinstall install" on page 622*.
`revert <options>`	Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway. See *"cprinstall revert" on page 625*.
`show <options>`	Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS. See *"cprinstall show" on page 626*.
`snapshot <options>`	Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway. See *"cprinstall snapshot" on page 627*.
`transfer <options>`	Transfers a software package from the repository to the managed Security Gateway without installing the package. See *"cprinstall transfer" on page 628*.
`uninstall <options>`	Uninstalls Check Point products on the managed Security Gateway. See *"cprinstall uninstall" on page 630*.

Parameter	Description
`verify <options>`	Confirms these operations were successful: - If a specific product can be installed on the managed Security Gateway. - That the operating system and currently installed products the managed Security Gateway are appropriate for the software package. - That there is enough disk space to install the product the managed Security Gateway. - That there is a CPRID connection with the managed Security Gateway. See *"cprinstall verify" on page 632*.

cprinstall boot

Description

Reboots the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Syntax

```
cprinstall boot <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall boot MyGW
```

cprinstall cprestart

Description

Runs the `cprestart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cprestart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# cprinstall cprestart MyGW
```

cprinstall cpstart

Description

Runs the `cpstart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstart MyGW
```

cprinstall cpstop

Description

Runs the `cpstop` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstop {-proc | -nopolicy} <Object Name>
```

Parameters

Parameter	Description
`-proc`	Kills the Check Point daemons and Security Servers, while it maintains the active Security Policy running in the Check Point kernel. Rules with generic *Allow*, *Drop* or *Reject* action based on services, continue to work.
`-nopolicy`	Kills the Check Point daemons and Security Servers and unloads the Security Policy from the Check Point kernel.
`<Object Name>`	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstop -proc MyGW
```

cprinstall delete

Description

Deletes a snapshot (backup) file on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Syntax

```
cprinstall delete <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Specifies the name of the snapshot (backup) on SecurePlatform OS.

Example

```
[Expert@MGMT]# cprinstall delete MyGW Snapshot25Apr2017
```

cprinstall get

Description

- Gets details of the products and the operating system installed on the managed Security Gateway.
- Updates the management database on the Security Management Server.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall get <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example:

```
[Expert@MGMT]# cprinstall get MyGW
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system   Major Version      Minor Version
------------------------------------------------------------------------
SecurePlatform     R75.20             R75.20

Vendor             Product            Major Version       Minor Version
------------------------------------------------------------------------
Check Point        VPN-1 Power/UTM    R75.20              R75.20
Check Point        SecurePlatform     R75.20              R75.20
Check Point        SmartPortal        R75.20              R75.20
[Expert@MGMT]#
```

cprinstall install

Description

Installs Check Point products on the managed Security Gateway.

Important - Installing software packages with this command is not supported for Security Gateways that run Gaia OS.

Notes:

- Before transferring the software package, this command runs the *"cprinstall verify" on page 632* command.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 605* command.

Syntax

```
cprinstall install [-boot] [-backup] [-skip_transfer] <Object
Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after installing the package. **Note** - Only reboot after ALL products have the same version. Reboot is canceled in certain scenarios.
`-backup`	Creates a snapshot on the managed Security Gateway before installing the package. **Note** - Only on Security Gateways that runs on SecurePlatform OS.
`-skip_transfer`	Skip the transfer of the package.
`<Object Name>`	The name of the Security Gateway object as configured in SmartConsole.
`"<Vendor>"`	Specifies the package vendor. Enclose in double quotes. Example: - `checkpoint` - `Check Point`
`"<Product>"`	Specifies the product name. Enclose in double quotes. Examples: - `SVNfoundation` - `firewall` - `floodgate` - `CP1100` - `VPN-1 Power/UTM` - `SmartPortal`
`"<Major Version>"`	Specifies the package Major Version. Enclose in double quotes.
`"<Minor Version>"`	Specifies the package Minor Version. Enclose in double quotes.

Example

```
[Expert@MGMT]# cprinstall install -boot MyGW "checkpoint" "firewall" "R75" "R75.20"

Installing firewall R75.20 on MyGW...
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.
[Expert@MGMT]#
```

cprinstall revert

Description

Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall revert <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 626* command.

cprinstall show

Description

Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall show <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall show GW1
SU_backup.tzg
[Expert@MGMT]#
```

cprinstall snapshot

Description

Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall snapshot <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 626* command.

cprinstall transfer

Description

Transfers a software package from the repository to the managed Security Gateway without installing the package.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- To see the values for the package attributes, run the *"cppkg print" on page 605* command.

Syntax

```
cprinstall transfer <Object Name> "<Vendor>" "<Product>" "<Major
Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`<Object Name>`	The name of the Security Gateway object as configured in SmartConsole.
`"<Vendor>"`	Specifies the package vendor. Enclose in double quotes. Example: - `checkpoint` - `Check Point`
`"<Product>"`	Specifies the product name. Enclose in double quotes. Examples: - `SVNfoundation` - `firewall` - `floodgate` - `CP1100`
`"<Major Version>"`	Specifies the package major version. Enclose in double quotes.
`"<Minor Version>"`	Specifies the package minor version. Enclose in double quotes.

cprinstall uninstall

Description

Uninstalls Check Point products on the managed Security Gateway.

Important - Uninstalling software packages with this command is not supported for Security Gateways running on Gaia OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- Before uninstalling product packages, this command runs the *"cprinstall verify" on page 632* command.
- After uninstalling a product package, you must run the *"cprinstall get" on page 621* command.
- To see the values for the package attributes, run the *"cppkg print" on page 605* command.

Syntax

```
cprinstall uninstall [-boot] <Object Name> "<Vendor>" "<Product>"
"<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after uninstalling the package. **Note** - Reboot is canceled in certain scenarios.
`<Object Name>`	The name of the Security Gateway object as configured in SmartConsole.
`"<Vendor>"`	Specifies the package vendor. Enclose in double quotes. Example: ▪ `checkpoint` ▪ `Check Point`
`"<Product>"`	Specifies the product name. Enclose in double quotes. Examples: ▪ `SVNfoundation` ▪ `firewall` ▪ `floodgate` ▪ `CP1100`
`"<Major Version>"`	Specifies the package major version. Enclose in double quotes.
`"<Minor Version>"`	Specifies the package minor version. Enclose in double quotes.

Example

```
[Expert@MGMT]# cprinstall uninstall MyGW "checkpoint" "firewall" "R75.20" "R75.20"
Uninstalling firewall R75.20 from MyGW...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
[Expert@MGMT]#
[Expert@MGMT]# cprinstall get
```

cprinstall verify

Description

Confirms these operations were successful:

- If a specific product can be installed on the managed Security Gateway.
- That the operating system and currently installed products the managed Security Gateway are appropriate for the software package.
- That there is enough disk space to install the product the managed Security Gateway.
- That there is a CPRID connection with the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- To see the values for the package attributes, run the *"cppkg print" on page 605* command.

Syntax

```
cprinstall verify <Object Name> "<Vendor>" "<Product>" "<Major
Version>" ["<Minor Version>"]
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ▪ `checkpoint` ▪ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ▪ `SVNfoundation` ▪ `firewall` ▪ `floodgate` ▪ `CP1100` ▪ `VPN-1 Power/UTM` ▪ `SmartPortal`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes. This parameter is optional.

Example 1 - Verification succeeds

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

Example 2 - Verification fails

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : SVN Foundation R75 is already installed on 192.0.2.134
Operation Success. Product cannot be installed, did not pass dependency check.
```

cpstart

Description

Manually starts all Check Point processes and applications.

Notes:

- For the `cprid` daemon, use the *"cprid" on page 612* command.
- For manually starting specific Check Point processes, see sk97638.

Syntax

```
cpstart
```

cpstat

Description

Displays the status and statistics information of Check Point applications.

Syntax

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Note - You can write the parameters in the syntax in any order.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The output shows the SNMP queries and SNMP responses for the applicable SNMP OIDs.
`-h <Host>`	Optional. When you run this command on a Management Server, this parameter specifies the managed Security Gateway. `<Host>` is an IPv4 address, a resolvable hostname, or a DAIP object name. The default is `localhost`. **Note** - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:`mdsenv <IP Address or Name of Domain Management Server>`.
`-p <Port>`	Optional. Port number of the Application Monitoring (AMON) server. The default port is 18192.
`-s <SICname>`	Optional. Secure Internal Communication (SIC) name of the Application Monitoring (AMON) server.

Parameter	Description
`-f <Flavor>`	Optional. Specifies the type of the information to collect. If you do not specify a flavor explicitly, the command uses the first flavor in the `<Application Flag>`. To see all flavors, run the `cpstat` command without any parameters.
`-o <Polling Interval>`	Optional. Specifies the polling interval (in seconds) - how frequently the command collects and shows the information. Examples: ■ 0 - The command shows the results only once and the stops (this is the default value). ■ 5 - The command shows the results every 5 seconds in the loop. ■ 30 - The command shows the results every 30 seconds in the loop. ■ N - The command shows the results every N seconds in the loop. Use this parameter together with the "`-c <Count>`" parameter and the "`-e <Period>`" parameter. Example: `cpstat os -f perf -o 2`
`-c <Count>`	Optional. Specifies how many times the command runs and shows the results before it stops. You must use this parameter together with the "`-o <Polling Interval>`" parameter. Examples: ■ 0 - The command shows the results repeatedly every `<Polling Interval>` (this is the default value). ■ 10 - The command shows the results 10 times every `<Polling Interval>` and then stops. ■ 20 - The command shows the results 20 times every `<Polling Interval>` and then stops. ■ N - The command shows the results N times every `<Polling Interval>` and then stops. Example: `cpstat os -f perf -o 2 -c 2`

Parameter	Description
`-e <Period>`	Optional. Specifies the time (in seconds), over which the command calculates the statistics. You must use this parameter together with the "`-o <Polling Interval>`" parameter. You can use this parameter together with the "`-c <Count>`" parameter. Example: `cpstat os -f perf -o 2 -c 2 -e 60`
`<Application Flag>`	Mandatory. See the table below with flavors for the application flags.

These flavors are available for the application flags

Note - The available flags depend on the enabled Software Blades. Some flags are supported only by a Security Gateway, and some flags are supported only by a Management Server.

Feature or Software Blade	Flag	Flavors
List of enabled Software Blades	`blades`	`fw, ips, av, urlf, vpn, cvpn, aspm, dlp, appi, anti_bot, default, content_awareness, threat-emulation, default`
Operating System	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, raidInfo, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
Firewall	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`

Feature or Software Blade	Flag	Flavors
HTTPS Inspection	`https_inspection`	`default, hsm_status, all`
Identity Awareness	`identityServer`	`default, authentication, logins, ldap, components, adquery, idc, muh`
Application Control	`appi`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
URL Filtering	`urlf`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
IPS	`ips`	`default, statistics, all`
Anti-Virus	`ci`	`default`
Threat Prevention	`antimalware`	`default, scanned_hosts, scanned_mails, subscription_status, update_status, ab_prm_contracts, av_prm_contracts, ab_prm_contracts, av_prm_contracts`

Feature or Software Blade	Flag	Flavors
Threat Emulation	`threat-emulation`	`default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts`
Threat Extraction	`scrub`	`default, subscription_status, threat_extraction_statistics`
Mobile Access	`cvpn`	`cvpnd, sysinfo, products, overall`
VSX	`vsx`	`default, stat, traffic, conns, cpu, all, memory, cpu_usage_per_core`
IPsec VPN	`vpn`	`default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all`
Data Loss Prevention	`dlp`	`default, dlp, exchange_agents, fingerprint`
Content Awareness	`ctnt`	`default`
QoS	`fg`	`all`
High Availability	`ha`	`default, all`
Policy Server for Remote Access VPN clients	`polsrv`	`default, all`

Feature or Software Blade	Flag	Flavors
Desktop Policy Server for Remote Access VPN clients	`dtps`	`default, all`
LTE / GX	`gx`	`default, contxt_create_info, contxt_delete_info, contxt_update_info, contxt_path_mng_info, GXSA_GPDU_info, contxt_initiate_info, gtpv2_create_info, gtpv2_delete_info, gtpv2_update_info, gtpv2_path_mng_info, gtpv2_cmd_info, all`
Management Server	`mg`	`default, log_server, indexer`
Certificate Authority	`ca`	`default, crl, cert, user, all`
SmartEvent	`cpsemd`	`default`
SmartEvent Correlation Unit	`cpsead`	`default`
Log Server	`ls`	`default`
CloudGuard Controller	`vsec`	`default`
SmartReporter	`svr`	`default`
Provisioning Agent	`PA`	`default`
Thresholds configured with the `threshold_config` command	`thresholds`	`default, active_thresholds, destinations, error`
Historical status values	`persistency`	`product, TableConfig, SourceConfig`

Examples

Example - CPU utilization

```
[Expert@HostName:0]# cpstat -f cpu os
CPU User Time (%):   1
CPU System Time (%): 0
CPU Idle Time (%):   99
CPU Usage (%):       1
CPU Queue Length:    -
CPU Interrupts/Sec:  172
CPUs Number:         8

[Expert@HostName:0]#
```

Example - Performance

```
[Expert@HostName:0]# cpstat os -f perf -o 2 -c 2 -e 60

Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741331456
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741331456
Free Real Memory (Bytes):                4489732096
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       0
CPU System Time (%):                     0
CPU Idle Time (%):                       100
CPU Usage (%):                           0
CPU Queue Length:                        -
CPU Interrupts/Sec:                      135
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296


Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741556736
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741556736
Free Real Memory (Bytes):                4489506816
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       3
CPU System Time (%):                     0
CPU Idle Time (%):                       97
CPU Usage (%):                           3
CPU Queue Length:                        -
CPU Interrupts/Sec:                      140
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296

[Expert@HostName:0]#
```

Example - List of current connected sessions on a Management Server

```
[Expert@MGMT:0]# cpstat -f default mg

Product Name:  Check Point Security Management Server
Major version: 6
Minor version: 0
Build number:  994000031
Is started:    1
Active status: active
Status:        OK

Connected clients
-------------------------------------------------------
|Client type |Administrator|Host        |Database lock|
-------------------------------------------------------
|SmartConsole|admin        |JOHNDOE-PC  |false        |
-------------------------------------------------------

[Expert@MGMT:0]#
```

cpstop

Description

Manually stops all Check Point processes and applications.

Notes:

- For the `cprid` daemon, use the *"cprid" on page 612* command.
- For manually stopping specific Check Point processes, see sk97638.

Syntax

```
cpstop
```

cpview

Overview of CPView

Description

CPView is a text based built-in utility on a Check Point computer.

CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway).

The CPView continuously updates the data in easy to access views.

On Security Gateway, you can use this statistical data to monitor the performance.

For more information, see sk101878.

Syntax

```
cpview --help
```

CPView User Interface

The CPView user interface has three sections:

Section	Description
Header	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
Navigation	This menu bar is interactive. Move between menus with the arrow keys and mouse. A menu can have sub-menus and they show under the menu bar.
View	This view shows the statistics collected in that view. These statistics update at the refresh rate.

Using CPView

Use these keys to navigate the CPView:

Key	Description
Arrow keys	Moves between menus and views. Scrolls in a view.
Home	Returns to the **Overview** view.
Enter	Changes to the **View Mode**. On a menu with sub-menus, the **Enter** key moves you to the lowest level sub-menu.
Esc	Returns to the **Menu Mode**.
Q	Quits CPView.

Use these keys to change CPView interface options:

Key	Description
R	Opens a window where you can change the refresh rate. The default refresh rate is 2 seconds.
W	Changes between wide and normal display modes. In wide mode, CPView fits the screen horizontally.
S	Manually sets the number of rows or columns.
M	Switches on/off the mouse.
P	Pauses and resumes the collection of statistics.

Use these keys to save statistics, show help, and refresh statistics:

Key	Description
C	Saves the current page to a file. The file name format is: `cpview_<ID of the cpview process>.cap<Number of the capture>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

cpwd_admin

Description

The Check Point WatchDog (`cpwd`) is a process that invokes and monitors critical processes such as Check Point daemons on the local computer, and attempts to restart them if they fail.

Among the processes monitored by Watchdog are `fwm`, `fwd`, `cpd`, `DAService`, and others.

The list of monitored processes depends on the installed and configured Check Point products and Software Blades.

The Check Point WatchDog writes monitoring information to the `$CPDIR/log/cpwd.elg` log file.

The `cpwd_admin` utility shows the status of the monitored processes, and configures the Check Point WatchDog.

There are two types of Check Point WatchDog monitoring

Monitoring	Description
Passive	WatchDog restarts the process only when the process terminates abnormally. In the output of the `cpwd_admin list` command, the `MON` column shows `N` for passively monitored processes.
Active	WatchDog checks the process status every predefined interval. WatchDog makes sure the process is alive, as well as properly functioning (not stuck on deadlocks, frozen, and so on). In the output of the `cpwd_admin list` command, the `MON` column shows `Y` for actively monitored processes. The list of actively monitored processes is predefined by Check Point. Users cannot change or configure it.

Syntax

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 649*.
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 652*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 653*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 654*.
`flist <options>`	Saves the status of all monitored processes to a `$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst` file. See *"cpwd_admin flist" on page 655*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 657*.

Parameter	Description
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 658*. ⓘ **Important** - Do not run this command unless explicitly instructed by Check Point Support or R&D to do so.
`list`	Prints the status of all monitored processes on the screen. See *"cpwd_admin list" on page 659*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 662*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 663*.
`start_monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 665*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 666*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 668*.

cpwd_admin config

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the `cpstop` and cpstart commands (which restart *all* Check Point processes).

Syntax

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters. **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-p`	Shows the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 2000 ■ Default: 2000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`
`sleep_timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.

Configuration Parameter	Accepted Values	Description
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

Description

Temporarily deletes a monitored process from the WatchDog database of monitored processes.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 659* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 634* command.

Syntax on a Management Server

```
cpwd_admin del -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 659* command in the leftmost column `APP`. Examples: - `FWM` - `FWD` - `CPD` - `CPM`

Example

```
[Expert@HostName:0]# cpwd_admin del -name FWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

Description

Temporarily detaches a monitored process from the WatchDog monitoring.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 659* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 634* command.

Syntax on a Management Server

```
cpwd_admin detach -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 659* command in the leftmost column `APP`. Examples: - `FWM` - `FWD` - `CPD` - `CPM`

Example

```
[Expert@HostName:0]# cpwd_admin detach -name FWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

Description

Checks whether the WatchDog process `cpwd` is alive.

Syntax

```
cpwd_admin exist
```

Example

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

Description

Saves the status of all WatchDog monitored processes to a file

Syntax on a Management Server

```
cpwd_admin list [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Output

Column	Description
`APP`	Shows the WatchDog name of the monitored process.
`PID`	Shows the PID of the monitored process.
`STAT`	Shows the status of the monitored process: ▪ `E` - executing ▪ `T` - terminated
`#START`	Shows how many times the WatchDog started the monitored process.
`START_TIME`	Shows the time when the WatchDog started the monitored process for the last time.
`SLP/LIMIT`	In verbose output, shows the values of the `sleep_timeout` and `no_limit` configuration parameters (see *"cpwd_admin config" on page 649*).
`MON`	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 646*): ▪ `Y` - Active monitoring ▪ `N` - Passive monitoring
`COMMAND`	Shows the command the WatchDog run to start this process.

Example

```
[Expert@HostName:0]# cpwd_admin flist
/opt/CPshrd-R80.40/tmp/cpwd_list_1564617600.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

Description

Shows the PID of a WatchDog monitored process.

Syntax for a Management Server

```
cpwd_admin getpid -name <Application Name>
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 659* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

Example

```
[Expert@HostName:0]# cpwd_admin getpid -name FWD
5640
[Expert@HostName:0]#
```

cpwd_admin kill

Description

Terminates the WatchDog process cpwd.

Important - Do not run this command unless explicitly instructed by Check Point Support or R&D to do so.
To restart the WatchDog process, you must restart all Check Point services with the *"cpstop" on page 643* and *"cpstart" on page 634* commands.

Syntax

```
cpwd_admin kill
```

cpwd_admin list

Description

Prints the status of all WatchDog monitored processes on the screen.

Syntax on a Management Server

```
cpwd_admin list [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Output

Column	Description
`APP`	Shows the WatchDog name of the monitored process.
`PID`	Shows the PID of the monitored process.
`STAT`	Shows the status of the monitored process: ▪ `E` - executing ▪ `T` - terminated
`#START`	Shows how many times the WatchDog started the monitored process.
`START_TIME`	Shows the time when the WatchDog started the monitored process for the last time.
`SLP/LIMIT`	In verbose output, shows the values of the `sleep_timeout` and `no_limit` configuration parameters (see *"cpwd_admin config" on page 649*).
`MON`	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 646*): ▪ `Y` - Active monitoring ▪ `N` - Passive monitoring
`COMMAND`	Shows the command the WatchDog run to start this process.

Examples

Example - Default output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list
APP        PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD    19738  E     1       [17:50:44] 31/5/2019   N    cpviewd
HISTORYD   0      T     0       [17:54:44] 31/5/2019   N    cpview_historyd
CPD        19730  E     1       [17:54:45] 31/5/2019   Y    cpd
SOLR       19935  E     1       [17:50:55] 31/5/2019   N    java_solr /opt/CPrt-
R80.40/conf/jetty.xml
RFL        19951  E     1       [17:50:55] 31/5/2019   N    LogCore
SMARTVIEW  19979  E     1       [17:50:55] 31/5/2019   N    SmartView
INDEXER    20032  E     1       [17:50:55] 31/5/2019   N    /opt/CPrt-R80.40/log_indexer/log_
indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-
R80.40/smartlog_server
CP3DLOGD   20237  E     1       [17:50:55] 31/5/2019   N    cp3dlogd
EPM        20251  E     1       [17:50:56] 31/5/2019   N    startEngine
DASERVICE  20404  E     1       [17:50:59] 31/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list -full
APP        PID    STAT  #START  START_TIME             SLP/LIMIT  MON
--------------------------------------------------------------------------------
CPVIEWD    19738  E     1       [17:50:44] 31/5/2019   60/5       N
           PATH = /opt/CPshrd-R80.40/bin/cpviewd
           COMMAND = cpviewd
--------------------------------------------------------------------------------
HISTORYD   0      T     0       [17:54:44] 31/5/2019   60/5       N
           PATH = /opt/CPshrd-R80.40/bin/cpview_historyd
           COMMAND = cpview_historyd
--------------------------------------------------------------------------------
CPD        19730  E     1       [17:54:45] 31/5/2019   60/5       Y
           PATH = /opt/CPshrd-R80.40/bin/cpd
           COMMAND = cpd
--------------------------------------------------------------------------------
SOLR       19935  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R80.40/bin/java_solr
           COMMAND = java_solr /opt/CPrt-R80.40/conf/jetty.xml
--------------------------------------------------------------------------------
RFL        19951  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R80.40/bin/LogCore
           COMMAND = LogCore
--------------------------------------------------------------------------------
SMARTVIEW  19979  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R80.40/bin/SmartView
           COMMAND = SmartView
--------------------------------------------------------------------------------
INDEXER    20032  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R80.40/log_indexer/log_indexer
           COMMAND = /opt/CPrt-R80.40/log_indexer/log_indexer
--------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPSmartLog-R80.40/smartlog_server
           COMMAND = /opt/CPSmartLog-R80.40/smartlog_server
           ENV = LANG=C
--------------------------------------------------------------------------------
CP3DLOGD   20237  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPuepm-R80.40/bin/cp3dlogd
           COMMAND = cp3dlogd
--------------------------------------------------------------------------------
EPM        20251  E     1       [17:50:56] 31/5/2019   60/5       N
           PATH = /opt/CPuepm-R80.40/bin/startEngine
           COMMAND = startEngine
--------------------------------------------------------------------------------
DASERVICE  20404  E     1       [17:50:59] 31/5/2019   60/5       N
           PATH = /opt/CPda/bin/DAService_script
           COMMAND = DAService_script
[Expert@HostName:0]#
```

cpwd_admin monitor_list

Description

Prints the status of actively monitored processes on the screen.

See the explanation about the active monitoring in *"cpwd_admin" on page 646*.

Syntax

```
cpwd_admin monitor_list
```

Example

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
APP       FILE_NAME                     NO_MSG_TIMES  LAST_MSG_TIME
CPD       CPD_5420_4714.mntr            0/10          [19:00:33] 31/5/2019
[Expert@HostName:0]#
```

cpwd_admin start

Description

Starts a process as monitored by the WatchDog.

Syntax on a Management Server

```
cpwd_admin start -name <Application Name> -path "<Full Path to Executable>" -command "<Command Syntax>" [-env {inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_limit {<Limit> | u}]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name, under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R80.40/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd`" ■ For CPM: "`/opt/CPsuite-R80.40/fw1/scripts/cpm.sh`" ■ For SICTUNNEL: "`/opt/CPshrd-R80.40/bin/cptnl`"

Parameter	Description
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: - For FWM: "`fwm`" - For FWM on Multi-Domain Server: "`fwm mds`" - For FWD: "`fwd`" - For CPD: "`cpd`" - For CPM: "`/opt/CPsuite-R80.40/fw1/scripts/cpm.sh -s`" - For SICTUNNEL: "`/opt/CPshrd-R80.40/bin/cptnl -c "/opt/CPuepm-R80.40/engine/conf/cptnl_srv.conf"`"
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. - `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) - `<Env_Var>=<Value>` - Assigns the specified value to the specified environment variable
`-slp_timeout <Timeout>`	Configures the specified value of the "`sleep_timeout`" configuration parameter. See *"cpwd_admin config" on page 649*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 649*. - `<Limit>` - Tries to restart the process the specified number of times - `u` - Tries to restart the process unlimited number of times

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin start_monitor

Description

Starts the active WatchDog monitoring. WatchDog monitors the predefined processes actively.

See the explanation for the *"cpwd_admin" on page 646* command.

Syntax

```
cpwd_admin start_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

Description

Stops a WatchDog monitored process.

Important - This change does **not** survive reboot.

Syntax on a Management Server

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: - `FWM` - `FWD` - `CPD` - `CPM`
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: - For FWM: "`$FWDIR/bin/fwm`" - For FWD: "`/opt/CPsuite-R80.40/fw1/bin/fw`" - For CPD: "`$CPDIR/bin/cpd_admin`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: - For FWM: "`fw kill fwm`" - For FWD: "`fw kill fwd`" - For CPD: "`cpd_admin stop`"

Parameter	Description
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ *`<Env_Var>=<Value>`* - Assigns the specified value to the specified environment variable

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin stop_monitor

Description

Stops the active WatchDog monitoring. WatchDog monitors all processes only passively.

See the explanation for the *"cpwd_admin" on page 646* command.

Syntax

```
cpwd_admin stop_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

dbedit

Description

Edits the management database - the `$FWDIR/conf/objects_5_0.C` file - on the Security Management Server or Domain Management Server. See skI3301.

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

```
dbedit -help
```

```
dbedit [-globallock] [{-local | -s <Management_Server>}] [{-u
<Username> | -c <Certificate>}] [-p <Password>] [-f <File_Name>
[ignore_script_failure] [-continue_updating]] [-r "<Open_Reason_
Text>"] [-d <Database_Name>] [-listen] [-readonly] [-session]
```

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Parameters

Parameter	Description
`-help`	Prints the general help.
`-globallock`	When you work with the dbedit utility, it partially locks the management database. If a user configures objects in SmartConsole at the same time, it causes problems in the management database. This option does not let SmartConsole, or a dbedit user to make changes in the management database. When you specify this option, the dbedit commands run on a copy of the management database. After you make the changes with the `dbedit` commands and run the `savedb` command, the dbedit utility saves and commits your changes to the actual management database.
`-local`	Connects to the localhost (127.0.0.1) without using username/password. If you do not specify this parameter, the dbedit utility asks how to connect.

Parameter	Description
`-s <Management_Server>`	Specifies the Security Management Server - by IP address or HostName. If you do not specify this parameter, the dbedit utility asks how to connect.
`-u <Username>`	Specifies the username, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-c <Certificate>`	Specifies the user's certificate file, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-p <Password>`	Specifies the user's password, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" and "`-u <Username>`" parameters.
`-f <File_Name>`	Specifies the file that contains the applicable dbedit internal commands (see the section "*dbedit Internal Commands*" below): ■ `create <object_type> <object_name>` ■ `modify <table_name> <object_name> <field_name> <value>` ■ `update <table_name> <object_name>` ■ `delete <table_name> <object_name>` ■ `print <table_name> <object_name>` ■ `quit` **Note** - Each command is limited to 4096 characters.
`ignore_script_failure`	Continues to execute the dbedit internal commands in the file and ignores errors. You can use it when you specify the "`-f <File_Name>`" parameter.
`-continue_updating`	Continues to update the modified objects, even if the operation fails for some of the objects (ignores the errors and runs the `update_all` command at the end of the script). You can use it when you specify the "`-f <File_Name>`" parameter.
`-r "<Open_Reason_Text>"`	Specifies the reason for opening the database in read-write mode (default mode).

Parameter	Description
`-d <Database_Name>`	Specifies the name of the database, to which the dbedit utility should connect (for example, `mdsdb`).
`-listen`	The dbedit utility "listens" for changes (use this mode for advanced troubleshooting with the assistance of Check Point Support). The dbedit utility prints its internal messages when a change occurs in the management database.
`-readonly`	Specifies to open the management database in read-only mode.
`-session`	Session Connectivity.

`dbedit` Internal Commands

Note - To see the available tables, class names (object types), attributes and values, connect to Management Server with Database Tool (GuiDBEdit Tool) (see sk13009).

Command	Description, Syntax, Examples
`-h`	**Description:** Prints the general help. **Syntax:** `dbedit> -h`

`-q`
`quit`
	Description:
	Quits from dbedit.
	Syntax:
	`dbedit> -q`
	`dbedit> quit [-update_all | -noupdate]`
	Examples:
	- Exit the utility and commit the remaining modified objects (interactive mode):
	`dbedit> quit`
	- Exit the utility and update all the remaining modified objects:
	`dbedit> quit -update_all`
	- Exit the utility and discard all modifications:
	`dbedit> quit -no_update`

Command	Description, Syntax, Examples

`update`	**Description:**
	Saves the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`").
	Syntax:
	`dbedit> update <table_name> <object_name>`
	Example:
	Save the object *My_Service* in the table *services*:
	`dbedit> update services My_Service`

`update_all`	**Description:** Saves all the modified objects. **Syntax:** `dbedit> update_all`

`_print_set`	**Description:**
	Prints the specified object from the specified table (for example, "`network_objects`", "`services`", "`users`") as it appears in the `$FWDIR/conf/objects_5_0.C` file (sets of attributes).
	Syntax:
	`dbedit> _print_set <table_name> <object_name>`
	Example:
	Print the object *My_Obj* from the table *network_objects*:
	`dbedit> print network_objects My_Obj`

`print`	**Description:**
	Prints the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`").
	Syntax:
	`dbedit> print <table_name> <object_name>`
	Examples:
	■ Print the object *My_Obj* from the table *network_objects* (in "Network Objects"):
	`dbedit> print network_objects my_obj`
	■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"):
	`dbedit> print properties firewall_properties`

Command	Description, Syntax, Examples

`printxml`	**Description:**
	Prints in XML format the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`").
	You can export the settings from a Management Server to an XML file that you can use later with external automation systems.
	Syntax:
	`dbedit> printxml <table_name> [<object_name>]`
	Examples:
	■ Print the object *My_Obj* from the table *network_objects*:
	`dbedit> printxml network_objects my_obj`
	■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"):
	`dbedit> printxml properties firewall_properties`

`printbyuid`	**Description:**
	Prints the attributes of the object specified by its UID (appears in the `$FWDIR/conf/objects_5_0.C` file at the beginning of the object as "`chkpf_uid ({...})`").
	Syntax:
	`dbedit> printbyuid {object_id}`
	Example:
	Print the attributes of the object with the specified UID:
	`dbedit> printbyuid {D3833F1D-0A58-AA42-865F-39BFE3C126F1}`

Command	Description, Syntax, Examples

`query`	**Description:**
	Prints all the objects in the specified table.
	Optionally, you can query for objects with specific attribute and value - query is separated by a comma after "`query <table_name>`" (spaces are not allowed between the `<attribute>` and `'<value>'`).
	Syntax:
	`dbedit> query <table_name> [ , <attribute>='<value>' ]`
	Examples:
	■ Print all objects in the table *users*:
	`dbedit> query users`
	■ Print all objects in the table *network_objects* that are defined as Management Servers:
	`dbedit> query network_objects, management='true'`
	■ Print all objects in the table *services* with the name *ssh*:
	`command_sdbedit> query services, name='ssh'`
	■ Print all objects in the table *services* with the port *22*:
	`dbedit> query services, port='22'`
	■ Print all objects with the IP address *10.10.10.10*:
	`dbedit> query network_objects, ipaddr='10.10.10.10'`

`whereused`	**Description:**
	Checks where the specified object used in the database.
	Prints the number of places, where this object is used and relevant information about each such place.
	Syntax:
	`dbedit> whereused <table_name> <object_name>`
	Example:
	Check where the object *My_Obj* is used:
	`dbedit> whereused network_objects My_Obj`

Command	Description, Syntax, Examples

`create`	**Description:**
	Creates an object of specified type (with its default values) in the database.
	Restrictions apply to the object's name:
	■ Object names can have a maximum of 100 characters.
	■ Objects names can contain only ASCII letters, numbers, and dashes.
	■ Reserved words will be blocked by the Management Server (refer to sk40179).
	Syntax:
	`dbedit> create <object_type> <object_name>`
	Example:
	Create the service object *My_Service* of the type *tcp_service* (with its default values):
	`dbedit> create tcp_service my_service`

`delete`	**Description:**
	Deletes an object from the specified table.
	Syntax:
	`dbedit> delete <table_name> <object_name>`
	Example:
	Delete the service object *My_Service* from the table *services*:
	`dbedit> delete services my_service`

Command	Description, Syntax, Examples

`modify`	**Description:**
	Modifies the value of specified attribute in the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`") in the management database.
	Syntax:
	`dbedit> modify <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Modify the color to *red* in the object *My_Service* in the table *services*:
	`dbedit> modify services My_Service color red`
	■ Add a comment to the object *MyObj*:
	`dbedit> modify network_objects MyObj comments "Created by fwadmin with dbedit"`
	■ Set the value of the global property *ike_use_largest_possible_subnets* in the table *properties* to *false*:
	`dbedit> modify properties firewall_properties ike_use_largest_possible_subnets false`
	■ Create a new interface on the Security Gateway *My_FW* and modify its attributes - set the IP address / Mask and enable Anti-Spoofing on interface with *"Element Index"=3* (check the attributes of the object *My_FW* in Database Tool (GuiDBEdit Tool) (see sk13009)):

Command	Description, Syntax, Examples

	`dbedit> addelement network_objects My_FW interfaces interface`
	`dbedit> modify network_objects My_FW interfaces:3:officialname NAME_OF_INTERFACE`
	`dbedit> modify network_objects My_FW interfaces:3:ipaddr IP_ADDRESS`
	`dbedit> modify network_objects My_FW interfaces:3:netmask NETWORK_MASK`
	`dbedit> modify network_objects My_FW interfaces:3:security:netaccess:access specific`
	`dbedit> modify network_objects My_FW interfaces:3:security:netaccess:allowed network_objects:group_name`
	`dbedit> modify network_objects My_FW interfaces:3:security:netaccess:perform_anti_spoofing true`
	`dbedit> modify network_objects MyObj FieldA LINKSYS`
	■ In the Owned Object *MyObj* change the value of *FieldB* to *NewVal*:
	`dbedit> modify network_objects MyObj FieldA:FieldB NewVal`
	■ In the Linked Object *MyObj* change the value of *FieldA* from *B* to *C*:
	`dbedit> modify network_objects MyObj FieldA B:C`

Command	Description, Syntax, Examples

`lock`	**Description:**
	Locks the specified object (by administrator) in the specified table (for example, "`network_objects`", "`services`", "`users`") from being modified by other users.
	For example, if you connect from a remote computer to this Management Server with *admin1* and lock an object, you are be able to connect with *admin2*, but are not able to modify the locked object, until *admin1* releases the lock.
	Syntax:
	`dbedit> lock <table_name> <object_name>`
	Example:
	Lock the object *My_Service_Obj* in the table *services* in the database:
	`dbedit> lock services My_Service_Obj`

`addelement`	**Description:**
	Adds a specified multiple field / container (with specified value) to a specified object in specified table.
	Syntax:
	`dbedit> addelement <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Add the element *BranchObjectClass* with the value *Organization* to a multiple field *Read* in the object *My_Obj* in the table *ldap*:
	`dbedit> addelement ldap My_Obj Read:BranchObjectClass Organization`
	■ Add the service *MyService* to the group of services *MyServicesGroup* in the table *services*:
	`dbedit> addelement services MyServicesGroup '' services:MyService`
	■ Add the network *MyNetwork* to the group of networks *MyNetworksGroup* in the table *network_objects*:
	`dbedit> addelement network_objects MyNetworksGroup '' network_objects:MyNetwork`

Command	Description, Syntax, Examples

`rmelement`	**Description:**
	Removes a specified multiple field / container (with specified value) from a specified object in specified table.
	Syntax:
	`dbedit> rmelement <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Remove the service *MyService* from the group of services *MyServicesGroup* from the table *services*:
	`dbedit> rmelement services MyServicesGroup '' services:MyService`
	■ Remove the network *MyNetwork* from the group of networks *MyNetworksGroup* from the table *network_objects*:
	`dbedit> rmelement network_objects MyNetworksGroup '' network_objects:MyNetwork`
	■ Remove the element *BranchObjectClass* with the value *Organization* from the multiple field *Read* in the object *My_Obj* in the table *ldap*:
	`dbedit> rmelement ldap my_obj Read:BranchObjectClass Organization`

`rename`	**Description:**
	Renames the specified object in specified table.
	Syntax:
	`dbedit> rename <table_name> <object_name> <new_object_name>`
	Example:
	Rename the network object *london* to *chicago* in the table *network_objects*:
	`dbedit> rename network_objects london chicago`

Command	Description, Syntax, Examples

`rmbyindex`	**Description:**
	Removes an element from a container by element's index.
	Syntax:
	`dbedit> rmbyindex <table_name> <object_name> <field_name> <index_number>`
	Example:
	Remove the element *backup_log_servers* from the container *log_servers* by element index *1* in the table *network_objects*:
	`dbedit> rmbyindex network_objects g log_servers:backup_log_servers 1`

`add_owned_remove_name`	**Description:**
	Adds an owned object (and removes its name) to a specified owned object field (or container).
	Syntax:
	`dbedit> add_owned_remove_name <table_name> <object_name> <field_name> <value>`
	Example:
	Add the owned object *My_Gateway* (and remove its name) to the owned object field (or container) *my_external_products*:
	`dbedit> add_owned_remove_name network_objects My_Gateway additional_products owned:my_external_products`

`is_delete_allowed`	**Description:**
	Checks if the specified object can be deleted from the specified table (object cannot be deleted if it is used by other objects).
	Syntax:
	`dbedit> is_delete_allowed <table_name> <object_name>`
	Example:
	`dbedit> is_delete_allowed network_objects MyObj`
	Check if the object *MyObj* can be deleted from the table *network_objects*:

Command	Description, Syntax, Examples

`set_pass`	**Description:**
	Sets specified password for specified user.
	Notes:
	- The password must contain at least 4 characters and no more than 50 characters.
	- This command cannot change the administrator's password.
	Syntax:
	`dbedit> set_pass <Username> <Password>`
	Example:
	Set the password *1234* for the user *abcd*:
	`dbedit> set_pass abcd 1234`

`savedb`	**Description:** Saves the database. You can run this command only when the database is locked globally (when you start the dbedit utility with the "`dbedit -globallock`" command). **Syntax:** `dbedit> savedb`
`savesession`	**Description:** Saves the session. You can run this command only when you start the dbedit utility in session mode (with the "`dbedit -session`" command). **Syntax:** `dbedit> savesession`

fw

Description

- Performs various operations on Security or Audit log files.
- Kills the specified Check Point processes.
- Manages the Suspicious Activity Monitoring (SAM) rules.
- Manages the Suspicious Activity Policy editor.

Syntax

```
fw [-d]
      fetchlogs <options>
      hastat <options>
      kill <options>
      log <options>
      logswitch <options>
      lslogs <options>
      mergefiles <options>
      repairlog <options>
      sam <options>
      sam_policy <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`fetchlogs <options>`	Fetches the specified Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), from the specified Check Point computer. See *"fw fetchlogs" on page 684*.
`hastat <options>`	Shows information about Check Point computers in High Availability configuration and their states. See *"fw hastat" on page 686*.

Parameter	Description
`kill <options>`	Kills the specified Check Point process. See *"fw kill" on page 687*.
`log <options>`	Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw log" on page 688*.
`logswitch <options>`	Switches the current active Check Point log file - Security (`$FWDIR/log/fw.log`) or Audit (`$FWDIR/log/fw.adtlog`). See *"fw logswitch" on page 698*.
`lslogs <options>`	Shows a list of Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), located on the local computer or a remote computer. See *"fw lslogs" on page 702*.
`mergefiles <options>`	Merges several Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`), into a single log file. See *"fw mergefiles" on page 705*.
`repairlog <options>`	Rebuilds pointer files for Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw repairlog" on page 708*.
`sam <options>`	Manages the Suspicious Activity Monitoring (SAM) rules. See *"fw sam" on page 709*.

`sam_policy <options>`
or
`samp <options>`
	Manages the Suspicious Activity Policy editor that works with these type of rules:
	▪ Suspicious Activity Monitoring (SAM) rules.
	▪ Rate Limiting rules.
	See *"fw sam_policy" on page 717*.

fw fetchlogs

Description

Fetches the specified Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) from the specified Check Point computer.

Syntax

```
fw [-d] fetchlogs [-f <Name of Log File 1>] [-f <Name of Log File
2>]... [-f <Name of Log File N>] <Target>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File N>`	Specifies the name of the log file to fetch. Need to specify name only. **Notes:** ■ If you do not specify the log file name explicitly, the command transfers all Security log files (`$FWDIR/log/*.log*`) and all Audit log files (`$FWDIR/log/*.adtlog*`). ■ The specified log file name can include wildcards * and ? (for example, `2017-0?-*.log`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the `-f` parameter for each log file name pattern. ■ This command also transfers the applicable log pointer files.
`<Target>`	Specifies the remote Check Point computer, with which this local Check Point computer has established SIC trust. ■ If you run this command on a Security Management Server or Domain Management Server, then `<Target>` is the applicable object's name or main IP address of the Check Point Computer as configured in SmartConsole. ■ If you run this command on a Security Gateway or Cluster Member, then `<Target>` is the main IP address of the applicable object as configured in SmartConsole.

Notes:

- This command moves the specified log files from the `$FWDIR/log/` directory on the specified Check Point computer. Meaning, it deletes the specified log files on the specified Check Point computer after it copies them successfully.
- This command moves the specified log files to the `$FWDIR/log/` directory on the local Check Point computer, on which you run this command.
- This command cannot fetch the *active* log files `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`.

  To fetch these active log files:

  1. Perform log switch on the applicable Check Point computer:

     ```
     fw logswitch [-audit] [-h <IP Address or Hostname>]
     ```

  2. Fetch the rotated log file from the applicable Check Point computer:

     ```
     fw fetchlogs -f <Log File Name> <IP Address or Hostname>
     ```

- This command renames the log files it fetched from the specified Check Point computer. The new log file name is the concatenation of the Check Point computer's name (as configured in SmartConsole), two underscore (_) characters, and the original log file name (for example: `MyGW__2019-06-01_000000.log`).

Example - Fetching log files from a Management Server

```
[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      5796KB 2019-06-01_000000.log
      4610KB fw.log
[Expert@HostName:0]#

[Expert@HostName:0]# fw fetchlogs -f 2019-06-01_000000 MyGW
File fetching in process. It may take some time...
File MyGW__2019-06-01_000000.log was fetched successfully
[Expert@HostName:0]#

[Expert@HostName:0]# ls $FWDIR/log/MyGW*
/opt/CPsuite-R80.40/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R80.40/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R80.40/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R80.40/fw1/log/MyGW__2019-06-01_000000.logptr
[Expert@HostName:0]#

[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      4610KB fw.log
[Expert@HostName:0]#
```

fw hastat

Description

Shows information about Check Point computers in High Availability configuration and their states.

Note - This command is outdated. On Management Servers, run the *"cpstat" on page 635* command.

Syntax

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

Parameters

Parameter	Description
<Target1> *<Target2>* ... *<TargetN>*	Specifies the Check Point computers to query. If you run this command on the Management Server, you can enter the applicable IP address, or the resolvable HostName of the managed Security Gateway or Cluster Member. If you do not specify the target, the command queries the local computer.

Example - Querying the cluster members from the Management Server

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

fw kill

Description

Kills the specified Check Point processes.

Important - Make sure the killed process is restarted, or restart it manually. See sk97638.

Syntax

```
fw [-d] kill [-t <Signal Number>] <Name of Process>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-t` *`<Signal Number>`*	Specifies which signal to send to the Check Point process. For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). **Note** - Processes can ignore some signals.
`<Name of Process>`	Specifies the name of the Check Point process to kill. To see the names of the processes, run the `ps auxwf` command.

Example

```
fw kill fwd
```

fw log

Description

Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`).

Syntax

```
fw log {-h | -help}
```

```
fw [-d] log [-a] [-b "<Start Timestamp>" "<End Timestamp>"] [-c
<Action>] [{-f | -t}] [-g] [-H] [-h <Origin>] [-i] [-k {<Alert
Name> | all}] [-l] [-m {initial | semi | raw}] [-n] [-o] [-p] [-q]
[-S] [-s "<Start Timestamp>"] [-e "<End Timestamp>"] [-u
<Unification Scheme File>] [-w] [-x <Start Entry Number>] [-y <End
Entry Number>] [-z] [-#] [<Log File>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the built-in usage. **Note** - The built-in usage does not show some of the parameters described in this table.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-a`	Shows only Account log entries.

Parameter	Description
`-b "<Start Timestamp>" "<End Timestamp>"`	Shows only entries that were logged between the specified start and end times. - The `<Start Timestamp>` and `<End Timestamp>` may be a date, a time, or both. - If date is omitted, then the command assumes the current date. - Enclose the `"<Start Timestamp>"` and `"<End Timestamp>` in single or double quotes (`-b 'XX' 'YY"`, or `-b "XX" "YY"`). - You cannot use the "`-b`" parameter together with the "`-s`" or "`-e`" parameters. - See the date and time format below.
`-c <Action>`	Shows only events with the specified action. One of these: - `accept` - `drop` - `reject` - `encrypt` - `decrypt` - `vpnroute` - `keyinst` - `authorize` - `deauthorize` - `authcrypt` - `ctl` **Notes:** - The `fw log` command always shows the **Control** (`ctl`) actions. - For *login* action, use the `authcrypt`.
`-e "<End Timestamp>"`	Shows only entries that were logged before the specified time. **Notes:** - The `<End Timestamp>` may be a date, a time, or both. - Enclose the `<End Timestamp>` in single or double quotes (`-e '...'`, or `-e "..."`). - You cannot use the "`-e`" parameter together with the "`-b`" parameter. - See the date and time format below.

Parameter	Description
`-f`	This parameter: 1. Shows the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-g`	Does not show delimiters. The default behavior is: - Show a colon (`:`) after a field name - Show a semi-colon (`;`) after a field value
`-H`	Shows the High Level Log key.
`-h` *`<Origin>`*	Shows only logs that were generated by the Security Gateway with the specified IP address or object name (as configured in SmartConsole).
`-i`	Shows log UID.
`-k {`*`<Alert Name>`*` | all}`	Shows entries that match a specific alert type: - *`<Alert Name>`* - Show only entries that match a specific alert type: - `alert` - `mail` - `snmp_trap` - `spoof` - `user_alert` - `user_auth` - `all` - Show entries that match all alert types (this is the default).
`-l`	Shows both the date and the time for each log entry. The default is to show the date only once above the relevant entries, and then specify the time for each log entry.

Parameter	Description
`-m`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command shows one unified log entry for each ID. This is the default. If you also specify the `-f` parameter, then the output does not show any updates, but shows only entries that relate to the start of new connections. To shows updates, use the `semi` parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, the output shows an entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. The output shows all log entries.
`-n`	Does not perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.
`-o`	Shows detailed log chains - shows all the log segments in the log entry.
`-p`	Does not perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-q`	Shows the names of log header fields.
`-S`	Shows the Sequence Number.
`-s "<Start Timestamp>"`	Shows only entries that were logged after the specified time. **Notes:** ■ The `<Start Timestamp>` may be a date, a time, or both. ■ If the date is omitted, then the command assumed the current date. ■ Enclose the `<Start Timestamp>` in single or double quotes (`-s '...'`, or `-s "..."`). ■ You cannot use the "`-s`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-t`	This parameter: 1. Does not show the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-w`	Shows the flags of each log entry (different bits used to specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on).
`-x <Start Entry Number>`	Shows only entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Shows only entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), continues to show log entries. The default behavior is to stop.
`-#`	Show confidential logs in clear text.
`<Log File>`	Specifies the log file to read. If you do not specify the log file explicitly, the command opens the `$FWDIR/log/fw.log` log file. You can specify a switched log file.

Date and Time format

Part of timestamp	Format	Example
Date only	`MMM DD, YYYY`	`June 11, 2018`
Time only Note - In this case, the command assumes the current date.	`HH:MM:SS`	`14:20:00`

Date and Time	`MMM DD, YYYY`
	`HH:MM:SS`
		`June 11, 2018`
		`14:20:00`

Output

Each output line consists of a single log entry, whose fields appear in this format:

Note - The fields that show depends on the connection type.

```
HeaderDateHour ContentVersion HighLevelLogKey Uuid SequenceNum
Flags Action Origin IfDir InterfaceName LogId ...
```

This table describes some of the fields.

Field Header	Description	Example
`HeaderDateHour`	Date and Time	`12Jun2018 12:56:42`
`ContentVersion`	Version	`5`
`HighLevelLogKey`	High Level Log Key	`<max_null>`, or empty
`Uuid`	Log UUID	`(0x5b1f99cb,0x0,0x3403a8c0,0xc0000000)`
`SequenceNum`	Log Sequence Number	`1`

Field Header	Description	Example
`Flags`	Internal flags that specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on	`428292`
`Action`	Action performed on this connection	■ `accept` ■ `dropreject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl`
`Origin`	Object name of the Security Gateway that generated this log	`MyGW`
`IfDir`	Traffic direction through interface: ■ < - Outbound (sent by a Security Gateway) ■ > - Inbound (received by a Security Gateway)	■ `<` ■ `>`

Field Header	Description	Example
`InterfaceName`	Name of the Security Gateway interface, on which this traffic was logged If a Security Gateway performed some internal action (for example, log switch), then the log entry shows `daemon`	■ `eth0` ■ `daemon` ■ `N/A`
`LogId`	Log ID	`0`
`Alert`	Alert Type	■ `alert` ■ `mail` ■ `snmp_trap` ■ `spoof` ■ `user_alert` ■ `user_auth`
`OriginSicName`	SIC name of the Security Gateway that generated this log	`CN=MyGW,O=MyDomain_ Server.checkpoint.com.s6t98x`
`inzone`	Inbound Security Zone	`Local`
`outzone`	Outbound Security Zone	`External`
`service_id`	Name of the service used to inspect this connection	`ftp`

Field Header	Description	Example
`src`	Object name or IP address of the connection's source computer	`MyHost`
`dst`	Object name or IP address of the connection's destination computer	`MyFTPServer`
`proto`	Name of the connection's protocol	`tcp`
`sport_svc`	Source port of the connection	`64933`
`ProductName`	Name of the Check Point product that generated this log	■ `VPN-1 & FireWall-1` ■ `Application Control` ■ `FloodGate-1`
`ProductFamily`	Name of the Check Point product family that generated this log	`Network`

Examples

Example 1 - Show all log entries with both the date and the time for each log entry

```
fw log -l
```

Example 2 - Show all log entries that start after the specified timestamp

```
[Expert@MyGW:0]# fw log -l -s "June 12, 2018 12:33:00"
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

... ... ...

[Expert@MyGW:0]#
```

Example 3 - Show all log entries between the specified timestamps

```
[Expert@MyGW:0]# fw log -l -b "June 12, 2018 12:33:00" 'June 12, 2018 12:34:00'
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

 12Jun2018 12:33:45 5 N/A 1 ctl MyGW > LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; description: Contracts; reason: Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the gateway.; Severity: 2;
status: Failed; version: 1.0; failure_impact: Contracts may be out-of-date; update_service: 1; ProductName: Security
Gateway/Management; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 4 - Show all log entries with action "drop"

```
[Expert@MyGW:0]# fw log -l -c drop
 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 5 - Show all log entries with action "drop", show all field headers, and show log flags

```
[Expert@MyGW:0]# fw log -l -q -w -c drop
 HeaderDateHour: 12Jun2018 12:33:39; ContentVersion: 5; HighLevelLogKey: <max_null>; LogUid: ; SequenceNum: 1; Flags: 428292; Action:
drop; Origin: MyGW; IfDir: <; InterfaceName: eth0; Alert: ; LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 6 - Show only log entries from 0 to 10 (counting from the beginning of the log file)

```
[Expert@MyGW:0]# fw log -l -x 0 -y 10
... ...
[Expert@MyGW:0]#
```

fw logswitch

Description

Switches the current active log file:

1. Closes the current active log file
2. Renames the current active log file
3. Creates a new active log file with the default name

Notes:

- By default, this command switches the active Security log file - `$FWDIR/log/fw.log`
- You can specify to switch the active Audit log file - `$FWDIR/log/fw.adtlog`

Syntax

```
fw [-d] logswitch
        [-audit] [<Name of Switched Log>]
        -h <Target> [[+ | -]<Name of Switched Log>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-audit`	Specifies to switch the active Audit log file (`$FWDIR/log/fw.adtlog`). You can use this parameter only on a Management Server.
`-h <Target>`	Specifies the remote computer, on which to switch the log. **Notes:** ■ The local and the remote computers must have established SIC trust. ■ The remote computer can be a Security Gateway, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed computer by its main IP address or Object Name as configured in SmartConsole.

Parameter	Description

`<Name of Switched Log>`	Specifies the name of the switched log file.
	Notes:
	■ If you do not specify this parameter, then a default name is:
	`<YYYY-MM-DD_HHMMSS>.log`
	`<YYYY-MM-DD_HHMMSS>.adtlog`
	For example, *2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the switch log file is:
	`<Specified_Log_Name>.log`
	`<Specified_Log_Name>.adtlog`
	■ The log switch operation fails if the specified name for the switched log matches the name of an existing log file.
	■ The maximal length of the specified name of the switched log file is 230 characters.

`+`	Specifies to *copy* the active log from the remote computer to the local computer.
	Notes:
	■ If you specify the name of the switched log file, you must write it immediately after *this* + (plus) parameter.
	■ The command copies the active log from the remote computer and saves it in the `$FWDIR/log/` directory on the local computer.
	■ The default name of the saved log file is:
	`<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log`
	For example, *MyGW__2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the saved log file is:
	`<Gateway_Object_Name>__<Specified_Log_Name>.log`
	■ When this command copies the log file from the remote computer, it compresses the file.

Parameter	Description

-	Specifies to *transfer* the active log from the remote computer to the local computer.
	Notes:
	■ The command saves the copied active log file in the `$FWDIR/log/` directory on the local computer and then deletes the switched log file on the remote computer.
	■ If you specify the name of the switched log file, you must write it immediately after this - (minus) parameter.
	■ The default name of the saved log file is:
	`<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log`
	For example, *MyGW__2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the saved log file is:
	`<Gateway_Object_Name>__<Specified_Log_Name>.log`
	■ When this command transfers the log file from the remote computer, it compresses the file.
	■ As an alternative, you can use the *"fw fetchlogs" on page 684* command.

Compression

When this command transfers the log files from the remote computer, it compresses the file with the `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 file and is difficult to predict. Binary data are not compressed. Text data, such as user names and URLs, are compressed.

Example - Switching the active Security log on a Security Management Server or Security Gateway

```
[Expert@MGMT:0]# fw logswitch
Log file has been switched to: 2018-06-13_182359.log
[Expert@MGMT:0]#
```

Example - Switching the active Audit log on a Security Management Server

```
[Expert@MGMT:0]# fw logswitch -audit
Log file has been switched to: 2018-06-13_185711.adtlog
[Expert@MGMT:0]#
```

Example - Switching the active Security log on a managed Security Gateway and copying the switched log

```
[Expert@MGMT:0]# fw logswitch -h MyGW +
Log file has been switched to: 2018-06-13_185451.log
[Expert@MGMT:0]#
[Expert@MGMT:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R80.40/fw1/log/fw.log
/opt/CPsuite-R80.40/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R80.40/fw1/log/fw.log
/opt/CPsuite-R80.40/fw1/log/2018-06-13_185451.log
[Expert@MyGW:0]#
```

fw lslogs

Description

Shows a list of Security log files (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) residing on the local computer or a remote computer.

Syntax

```
fw [-d] lslogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]
... [-f <Name of Log File N>] [-e] [-r] [-s {name | size | stime |
etime}] [<Target>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ✪ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File>`	Specifies the name of the log file to show. Need to specify name only. **Notes:** ■ If the log file name is not specified explicitly, the command shows all Security log files (`$FWDIR/log/*.log`). ■ File names may include `*` and `?` as wildcards (for example, `2019-0?-*`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the "`-f`" parameter for each log file name pattern: `-f <Name of Log File 1> -f <Name of Log File 2> ... -f <Name of Log File N>`
`-e`	Shows an extended file list. It includes the following information for each log file: ■ `Size` - The total size of the log file and its related pointer files ■ `Creation Time` - The time the log file was created ■ `Closing Time` - The time the log file was closed ■ `Log File Name` - The file name
`-r`	Reverses the sort order (descending order).

Parameter	Description
`-s {name | size | stime | etime}`	Specifies the sort order of the log files using one of the following sort options: - `name` - The file name - `size` - The file size - `stime` - The time the log file was created (this is the default option) - `etime` - The time the log file was closed
<Target>	Specifies the remote Check Point computer, with which this local Check Point computer has established SIC trust. - If you run this command on a Security Management Server or Domain Management Server, then *<Target>* is the applicable object's name or main IP address of the Check Point Computer as configured in SmartConsole. - If you run this command on a Security Gateway or Cluster Member, then *<Target>* is the main IP address of the applicable object as configured in SmartConsole.

Example 1 - Default output

```
[Expert@HostName:0]# fw lslogs
     Size Log file name
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.log
         9KB 2019-06-16_000000.log
        10KB 2019-06-17_000000.log
         9KB fw.log
[Expert@HostName:0]#
```

Example 2 - Showing all log files

```
[Expert@HostName:0]# fw lslogs -f "*"
     Size Log file name
         9KB fw.adtlog
         9KB fw.log
         9KB 2019-05-29_000000.adtlog
         9KB 2019-05-29_000000.log
         9KB 2019-05-20_000000.adtlog
         9KB 2019-05-20_000000.log
[Expert@HostName:0]#
```

Example 3 - Showing only log files specified by the patterns

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
         9KB 2019-06-14_000000.adtlog
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 4 - Showing only log files specified by the patterns and their extended information

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
         9KB 2019-06-14_000000.adtlog
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 5 - Showing only log files specified by the patterns, sorting by name in reverse order

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' -e -s name -r
     Size Creation Time Closing Time Log file name
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.log
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.adtlog
         9KB 13Jun2018 18:23:59 14Jun2018 0:00:00 2019-06-14_000000.log
         9KB 13Jun2018 0:00:00 14Jun2018 0:00:00 2019-06-14_000000.adtlog
[Expert@HostName:0]#
```

Example 6 - Showing only log files specified by the patterns, from a managed Security Gateway with main IP address 192.168.3.53

```
[Expert@MGMT:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' 192.168.3.53
     Size Log file name
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
         9KB 2019-06-14_000000.log
         9KB 2019-06-14_000000.adtlog
[Expert@MGMT:0]#
```

fw mergefiles

Description

Merges several Security log files (`$FWDIR/log/*.log`) into a single log file.

Merges several Audit log files (`$FWDIR/log/*.adtlog`) into a single log file.

Important:

- Do not merge the *active* Security file `$FWDIR/log/fw.log` with other Security switched log files.
  Switch the active Security file `$FWDIR/log/fw.log` (with the *"fw logswitch" on page 698* command) and only then merge it with other Security switched log files.
- Do not merge the *active* Audit file `$FWDIR/log/fw.adtlog` with other Audit switched log files.
  Switch the active Audit file `$FWDIR/log/fw.adtlog` (with the *"fw logswitch" on page 698* command) and only then merge it with other Audit switched log files.
- This command unifies logs entries with the same Unique-ID (UID). If you rotate the current active log file before all the segments of a specific log arrive, this command merges the records with the same Unique ID from two different files, into one fully detailed record.
- If the size of the final merged log file exceeds 2GB, this command creates a list of merged files, where the size of each merged file size is not more than 2GB.
  The user receives this warning:

  ```
  Warning: The size of the files you have chosen to merge
  is greater than 2GB. The merge will produce two or more
  files.
  ```

  The names of merged files are:
  - `<Name of Merged Log File>.log`
  - `<Name of Merged Log File>_1.log`
  - `<Name of Merged Log File>_2.log`
  - `... ...`
  - `<Name of Merged Log File>_N.log`

Syntax

```
fw [-d] mergefiles {-h | -help}
```

```
fw [-d] mergefiles [-r] [-s] [-t <Time Conversion File>] <Name of
Log File 1> <Name of Log File 2> ... <Name of Log File N> <Name of
Merged Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the built-in usage.
`-r`	Removes duplicate entries.
`-s`	Sorts the merged file by the **Time** field in log records.
`-t` *`<Time Conversion File>`*	Specifies a full path and name of a file that instructs this command how to adjust the times during the merge. This is required if you merge log files from Log Servers configured with different time zones. The file format is: *`<IP Address of Log Server #1> <Signed Date Time #1 in Seconds>`* *`<IP Address of Log Server #2> <Signed Date Time #2 in Seconds>`* `... ...` **Notes** ■ You must specify the absolute path and the file name. ■ The name of the time conversion file cannot exceed 230 characters.
`<Name of Log File 1> ... <Name of Log File N>`	Specifies the log files to merge. **Notes:** ■ You must specify the absolute path and the name of the input log files. ■ The name of the input log file cannot exceed 230 characters.

Parameter	Description
`<Name of Merged Log File>`	Specifies the output merged log file. **Notes:** ■ The name of the merged log file cannot exceed 230 characters. ■ If a file with the specified name already exists, the command stops and asks you to remove the existing file, or to specify another name. ■ The size of the merged log file cannot exceed 2 GB. In such scenario, the command creates several merged log files, each not exceeding the size limit.

Example - Merging Security log files

```
[Expert@HostName:0]# ls -l $FWDIR/*.log
-rw-rw-r-- 1 admin root 189497 Sep  7 00:00 2019-09-07_000000.log
-rw-rw-r-- 1 admin root  14490 Sep  9 09:52 2019-09-09_000000.log
-rw-rw-r-- 1 admin root  30796 Sep 10 10:56 2019-09-10_000000.log
-rw-rw-r-- 1 admin root  24503 Sep 10 13:08 fw.log
[Expert@HostName:0]#
[Expert@HostName:0]# fw mergefiles -s $FWDIR/2019-09-07_000000.log $FWDIR/2019-09-09_000000.log
$FWDIR/2019-09-10_000000.log /var/log/2019-Sep-Merged.log
[Expert@HostName:0]#
[Expert@HostName:0]# ls -l /var/log/2019-Sep-Merged.log*
-rw-rw---- 1 admin root 213688 Sep 10 13:18 /var/log/2019-Sep-Merged.log
-rw-rw---- 1 admin root   8192 Sep 10 13:18 /var/log/2019-Sep-Merged.logLuuidDB
-rw-rw---- 1 admin root     80 Sep 10 13:18 /var/log/2019-Sep-Merged.logaccount_ptr
-rw-rw---- 1 admin root   2264 Sep 10 13:18 /var/log/2019-Sep-Merged.loginitial_ptr
-rw-rw---- 1 admin root   4448 Sep 10 13:18 /var/log/2019-Sep-Merged.logptr
[Expert@HostName:0]#
```

fw repairlog

Description

Check Point Security log file (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) are databases, with special pointer files.

If these log pointer files become corrupted (which causes the inability to read the log file), this command can rebuild them.

Log File Type	Log File Location	Log Pointer Files

Security log	`$FWDIR/log/*.log`	`*.logptr`
		`*.logaccount_ptr`
		`*.loginitial_ptr`
		`*.logLuuidDB`

Audit log	`$FWDIR/log/*.adtlog`	`*.adtlogptr`
		`*.adtlogaccount_ptr`
		`*.adtloginitial_ptr`
		`*.adtlogLuuidDB`

Syntax

```
fw [-d] repairlog [-u] <Name of Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Specifies to rebuild the unification chains in the log file.
`<Name of Log File>`	The name of the log file to repair.

Example - Repairing the Audit log file

```
fw repairlog -u 2019-06-17_000000.adtlog
```

fw sam

Description

Manages the Suspicious Activity Monitoring (SAM) rules. You can use the SAM rules to block connections to and from IP addresses without the need to change or reinstall the Security Policy. For more information, see sk112061.

You can create the Suspicious Activity Rules in two ways:

- In SmartConsole from Monitoring Results
- In CLI with the `fw sam` command

Notes:

- VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam_policy" on page 717* and *"sam_alert" on page 815* commands.
- SAM rules consume some CPU resources on Security Gateway.

  Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.
- Logs for enforced SAM rules (configured with the `fw sam` command) are stored in the `$FWDIR/log/sam.dat` file.
  By design, the file is purged when the number of stored entries reaches 100,000.
  This data log file contains the records in one of these formats:

`<type>,<actions>,<expire>,<ipaddr>`
`<type>,<actions>,<expire>,<src>,<dst>,<dport>,<ip_p>`

- SAM Requests are stored on the Security Gateway in the kernel table `sam_requests`.
- IP Addresses that are blocked by SAM rules, are stored on the Security Gateway in the kernel table `sam_blocked_ips`.

Note - To configure SAM Server settings for a Security Gateway or Cluster:

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server.
2. From the left navigation panel, click Gateways & Servers.
3. Open the Security Gateway or Cluster object.
4. From the left tree, click **Other > SAM**.
5. Configure the settings.
6. Click **OK**.
7. Install the Access Control Policy on this Security Gateway or Cluster object.

Syntax

- **To add or cancel a SAM rule according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-t <Timeout>] [-l <Log
Type>] [-C] [-e <key=val>]+ [-r] -{n|i|I|j|J} <Criteria>
```

- **To delete all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] -D
```

- **To monitor all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q} all
```

- **To monitor SAM rules according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q}
<Criteria>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-v`	Enables verbose mode. In this mode, the command writes one message to *stderr* for each Security Gateway, on which the command is enforced. These messages show whether the command was successful or not.
`-s <SAM Server>`	Specifies the IP address (in the X.X.X.X format) or resolvable HostName of the Security Gateway that enforces the command. The default is `localhost`.

Parameter	Description
`-S <SIC Name of SAM Server>`	Specifies the SIC name for the SAM server to be contacted. It is expected that the SAM server has this SIC name, otherwise the connection fails. **Notes:** ■ If you do not explicitly specify the SIC name, the connection continues without SIC names comparison. ■ For more information about enabling SIC, refer to the OPSEC API Specification. ■ On VSX Gateway, run the *fw vsx showncs -vs <VSID>* command to show the SIC name for the applicable Virtual System.
`-f <Security Gateway>`	Specifies the Security Gateway, on which to enforce the action. `<Security Gateway>` can be one of these: ■ *All* - Default. Specifies to enforce the action on all managed Security Gateways, where SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *localhost* - Specifies to enforce the action on this local Check Point computer (on which the `fw sam` command is executed). You can use this syntax only on Security Gateway or StandAlone. ■ *Gateways* - Specifies to enforce the action on all objects defined as Security Gateways, on which SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Security Gateway object* - Specifies to enforce the action on this specific Security Gateway object. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Group object* - Specifies to enforce the action on all specific Security Gateways in this Group object. **Notes:** ■ You can use this syntax only on Security Management Server or Domain Management Server. ■ VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
`-D`	Cancels all inhibit ("`-i`", "`-j`", "`-I`", "`-J`") and notify ("`-n`") parameters. **Notes:** ■ To "uninhibit" the inhibited connections, run the `fw sam` command with the "`-C`" or "`-D`" parameters. ■ It is also possible to use this command for active SAM requests.

Parameter	Description
`-C`	Cancels the `fw sam` command to inhibit connections with the specified parameters. **Notes:** - These connections are no longer inhibited (no longer rejected or dropped). - The command parameters must match the parameters in the original `fw sam` command, except for the `-t` *`<Timeout>`* parameter.
`-t` *`<Timeout>`*	Specifies the time period (in seconds), during which the action is enforced. The default is forever, or until you cancel the `fw sam` command.
`-l` *`<Log Type>`*	Specifies the type of the log for enforced action: - `nolog` - Does not generate Log / Alert at all - `short_noalert` - Generates a Log - `short_alert` - Generates an Alert - `long_noalert` - Generates a Log - `long_alert` - Generates an Alert (this is the default)
`-e` *`<key=val>`*`+`	Specifies rule information based on the keys and the provided values. Multiple keys are separated by the plus sign (+). Available keys are (each is limited to 100 characters): - `name` - Security rule name - `comment` - Security rule comment - `originator` - Security rule originator's username
`-r`	Specifies not to resolve IP addresses.
`-n`	Specifies to generate a "Notify" long-format log entry. **Notes:** - This parameter generates an alert when connections that match the specified services or IP addresses pass through the Security Gateway. - This action does not inhibit / close connections.
`-i`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** - Each inhibited connection is logged according to the log type. - Matching connections are rejected.

Parameter	Description
`-I`	Inhibits (drops or rejects) new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** - Matching connections are rejected. - Each inhibited connection is logged according to the log type.
`-j`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** - Matching connections are dropped. - Each inhibited connection is logged according to the log type.
`-J`	Inhibits new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** - Matching connections are dropped. - Each inhibited connection is logged according to the log type.
`-b`	Bypasses new connections with the specified parameters.
`-q`	Quarantines new connections with the specified parameters.
`-M`	Monitors the active SAM requests with the specified actions and criteria.
`all`	Gets all active SAM requests. This is used for monitoring purposes only.
`<Criteria>`	Criteria are used to match connections. The criteria and are composed of various combinations of the following parameters: - Source IP Address - Source Netmask - Destination IP Address - Destination Netmask - Port (see *IANA Service Name and Port Number Registry*) - Protocol Number (see *IANA Protocol Numbers*)

Parameter	Description
	Possible combinations are (see the explanations below this table): - `src <IP>` - `dst <IP>` - `any <IP>` - `subsrc <IP> <Netmask>` - `subdst <IP> <Netmask>` - `subany <IP> <Netmask>` - `srv <Src IP> <Dest IP> <Port> <Protocol>` - `subsrv <Src IP> <Src Netmask> <Dest IP> <Dest Netmask> <Port> <Protocol>` - `subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>` - `subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>` - `dstsrv <Dest IP> <Port> <Protocol>` - `subdstsrv <Dest IP> <Dest Netmask> <Port> <Protocol>` - `srcpr <IP> <Protocol>` - `dstpr <IP> <Protocol>` - `subsrcpr <IP> <Netmask> <Protocol>` - `subdstpr <IP> <Netmask> <Protocol>` - `generic <key=val>`

Explanation for the *<Criteria>* syntax

Parameter	Description
`src <IP>`	Matches the Source IP address of the connection.
`dst <IP>`	Matches the Destination IP address of the connection.
`any <IP>`	Matches either the Source IP address or the Destination IP address of the connection.
`subsrc <IP> <Netmask>`	Matches the Source IP address of the connections according to the netmask.
`subdst <IP> <Netmask>`	Matches the Destination IP address of the connections according to the netmask.

Parameter	Description
`subany <IP> <Netmask>`	Matches either the Source IP address or Destination IP address of connections according to the netmask.
`srv <Src IP> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol.
`subsrv <Src IP> <Netmask> <Dest IP> <Netmask> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol. Source and Destination IP addresses are assigned according to the netmask.
`subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, source netmask, destination netmask, Service (port number) and Protocol.
`subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>`	Matches specific Source IP address, Destination IP, destination netmask, Service (port number) and Protocol.
`dstsrv <Dest IP> <Service> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol.
`subdstsrv <Dest IP> <Netmask> <Port> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol. Destination IP address is assigned according to the netmask.
`srcpr <IP> <Protocol>`	Matches the Source IP address and protocol.
`dstpr <IP> <Protocol>`	Matches the Destination IP address and protocol.
`subsrcpr <IP> <Netmask> <Protocol>`	Matches the Source IP address and protocol of connections. Source IP address is assigned according to the netmask.
`subdstpr <IP> <Netmask> <Protocol>`	Matches the Destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.

Parameter	Description
`generic <key=val>+`	Matches the GTP connections based on the specified keys and provided values. Multiple keys are separated by the plus sign (+). Available keys are: ■ `service=gtp` ■ `imsi` ■ `msisdn` ■ `apn` ■ `tunl_dst` ■ `tunl_dport` ■ `tunl_proto`

fw sam_policy

Description

Manages the Suspicious Activity Policy editor that works with these types of rules:

- Suspicious Activity Monitoring (SAM) rules.

  See sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rules.

- Rate Limiting rules.

  See sk112454: How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 709*
- *"sam_alert" on page 815*

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Syntax for IPv6

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`add <options>`	Adds one Rate Limiting rule one at a time. See *"fw sam_policy add" on page 720*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 733*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 735*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 739*.

fw sam_policy add

Description

The "*fw sam_policy add*" and "*fw6 sam_policy add*" commands:

- Add one Suspicious Activity Monitoring (SAM) rule at a time.
- Add one Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Optional. Specifies that the rule category is `User-defined`. Default rule category is `Auto`.
`-a {d | n | b}`	Mandatory. Specifies the rule action if the traffic matches the rule conditions: ■ `d` - Drop the connection. ■ `n` - Notify (generate a log) about the connection and let it through. ■ `b` - Bypass the connection - let it through without checking it against the policy rules. **Note** - Rules with action set to *Bypass* cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.
`-l {r | a}`	Optional. Specifies which type of log to generate for this rule for all traffic that matches: ■ `-r` - Generate a regular log ■ `-a` - Generate an alert log

Parameter	Description
`-t <Timeout>`	Optional. Specifies the time period (in seconds), during which the rule will be enforced. Default timeout is indefinite.
`-f <Target>`	Optional. Specifies the target Security Gateways, on which to enforce the Rate Limiting rule. `<Target>` can be one of these: ■ `all` - This is the default option. Specifies that the rule should be enforced on all managed Security Gateways. ■ Name of the Security Gateway or Cluster object - Specifies that the rule should be enforced only on this Security Gateway or Cluster object (the object name must be as defined in the SmartConsole). ■ Name of the Group object - Specifies that the rule should be enforced on all Security Gateways that are members of this Group object (the object name must be as defined in the SmartConsole).
`-n "<Rule Name>"`	Optional. Specifies the name (label) for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`
`-c "<Rule Comment>"`	Optional. Specifies the comment for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`

Parameter	Description
`-o "<Rule Originator>"`	Optional. Specifies the name of the originator for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	Optional. Specifies the name of the Security Zone for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters.
`ip <IP Filter Arguments>`	Mandatory (use this `ip` parameter, or the `quota` parameter). Configures the *Suspicious Activity Monitoring (SAM)* rule. Specifies the IP Filter Arguments for the SAM rule (you must use at least one of these options): `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` See the explanations below.

Parameter	Description
`quota <`*`Quota Filter Arguments`*`>`	Mandatory (use this `quota` parameter, or the `ip` parameter). Configures the *Rate Limiting* rule. Specifies the Quota Filter Arguments for the Rate Limiting rule (see the explanations below): ■ `[flush true]` ■ `[source-negated {true | false}] source <`*`Source`*`>` ■ `[destination-negated {true | false}] destination <`*`Destination`*`>` ■ `[service-negated {true | false}] service <`*`Protocol and Port numbers`*`>` ■ `[<`*`Limit1 Name`*`> <`*`Limit1 Value`*`>] [<`*`Limit2 Name`*`> <`*`Limit2 Value`*`>] ...[<`*`LimitN Name`*`> <`*`LimitN Value`*`>]` ■ `[track <`*`Track`*`>]` **Important:** ■ The Quota rules are not applied immediately to the Security Gateway. They are only registered in the Suspicious Activity Monitoring (SAM) policy database. To apply all the rules from the SAM policy database immediately, add "`flush true`" in the `fw samp add` command syntax. ■ Explanation: For new connections rate (and for any rate limiting in general), when a rule's limit is violated, the Security Gateway also drops all packets that match the rule. The Security Gateway computes new connection rates on a per-second basis. At the start of the 1-second timer, the Security Gateway allows all packets, including packets for existing connections. If, at some point, during that 1 second period, there are too many new connections, then the Security Gateway blocks all remaining packets for the remainder of that 1-second interval. At the start of the next 1-second interval, the counters are reset, and the process starts over - the Security Gateway allows packets to pass again up to the point, where the rule's limit is violated.

Explanation for the *IP Filter Arguments* syntax for Suspicious Activity Monitoring (SAM) rules

Argument	Description
`-C`	Specifies that open connections should be closed.
`-s` *`<Source IP>`*	Specifies the Source IP address.
`-m` *`<Source Mask>`*	Specifies the Source subnet mask (in dotted decimal format - x.y.z.w).
`-d` *`<Destination IP>`*	Specifies the Destination IP address.
`-M` *`<Destination Mask>`*	Specifies the Destination subnet mask (in dotted decimal format - x.y.z.w).
`-p` *`<Port>`*	Specifies the port number (see *IANA Service Name and Port Number Registry*).
`-r` *`<Protocol>`*	Specifies the protocol number (see *IANA Protocol Numbers*).

Explanation for the *Quota Filter Arguments* syntax for Rate Limiting rules

Argument	Description
`flush true`	Specifies to compile and load the quota rule to the SecureXL immediately.
`[source-negated {true | false}] source <Source>`	Specifies the source type and its value: ■ `any` The rule is applied to packets sent from all sources. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent from: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent from: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the source IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the source IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `source-negated false` ■ The `source-negated true` processes all source types, *except* the specified type.

Argument	Description
`[destination-negated {true | false}] destination <Destination>`	Specifies the destination type and its value: ■ `any` The rule is applied to packets sent to all destinations. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent to: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent to: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the destination IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the destination IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `destination-negated false` ■ The `destination-negated true` will process all destination types except the specified type

Argument	Description
`[service-negated {true | false}] service <Protocol and Port numbers>`	Specifies the Protocol number (see *IANA Protocol Numbers*) and Port number (see *IANA Service Name and Port Number Registry*): - `<Protocol>` IP protocol number in the range 1-255 - `<Protocol Start>-<Protocol End>` Range of IP protocol numbers - `<Protocol>/<Port>` IP protocol number in the range 1-255 and TCP/UDP port number in the range 1-65535 - `<Protocol>/<Port Start>-<Port End>` IP protocol number and range of TCP/UDP port numbers from 1 to 65535 **Notes:** - Default is: `service-negated false` - The `service-negated true` will process all traffic except the traffic with the specified protocols and ports

Argument	Description
`[<Limit 1 Name> <Limit 1 Value>] [<Limit 2 Name> <Limit 2 Value>] ... [<Limit N Name> <Limit N Value>]`	Specifies quota limits and their values. **Note** - Separate multiple quota limits with spaces. ■ `concurrent-conns <Value>` Specifies the maximal number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximal ratio of the *concurrent-conns* value to the total number of active connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `pkt-rate <Value>` Specifies the maximum number of packets per second that match this rule. ■ `pkt-rate-ratio <Value>` Specifies the maximal ratio of the *pkt-rate* value to the rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `byte-rate <Value>` Specifies the maximal total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximal ratio of the *byte-rate* value to the bytes per second rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `new-conn-rate <Value>` Specifies the maximal number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximal ratio of the *new-conn-rate* value to the rate of all connections per second through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`).

Argument	Description
`[track <Track>]`	Specifies the tracking option: - `source` Counts connections, packets, and bytes for specific source IP address, and not cumulatively for this rule. - `source-service` Counts connections, packets, and bytes for specific source IP address, and for specific IP protocol and destination port, and not cumulatively for this rule.

Examples

Example 1 - Rate Limiting rule with a range

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

Explanations:

- This rule drops packets for all connections (`-a d`) that exceed the quota set by this rule, including packets for existing connections.
- This rule logs packets (`-l r`) that exceed the quota set by this rule.
- This rule will expire in 3600 seconds (`-t 3600`).
- This rule limits the rate of creation of new connections to 5 connections per second (`new-conn-rate 5`) for any traffic (`service any`) from the source IP addresses in the range 172.16.7.11 - 172.16.7.13 (`source range:172.16.7.11-172.16.7.13`).

  Note - The limit of the total number of log entries per second is configured with the *fwaccel dos config set -n <rate>* command.
- This rule will be compiled and loaded on the SecureXL, together with other rules in the Suspicious Activity Monitoring (SAM) policy database immediately, because this rule includes the "`flush true`" parameter.

Example 2 - Rate Limiting rule with a service specification

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

Explanations:

- This rule logs and lets through all packets (`-a n`) that exceed the quota set by this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all packets except (`service-negated true`) the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53 (`service 1,50-51,6/443,17/53`).
- This rule applies to all packets from source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule does not let any traffic through (`byte-rate 0`) except the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 3 - Rate Limiting rule with ASN

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the Autonomous System number 64500 (`asn:AS64500`).
- This rule applies to packets from source IPv6 addresses FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`).
- This rule applies to all traffic (`service any`).
- This rule does not let any traffic through (`pkt-rate 0`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 4 - Rate Limiting rule with whitelist

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

Explanations:

- This rule bypasses (`-a b`) all packets that match this rule.

  Note - The Access Control Policy and other types of security policy rules still apply.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the source IP addresses in the range 172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`).
- This rule applies to packets sent to TCP port 80 (`service 6/80`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 5 - Rate Limiting rule with tracking

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not log any packets (the `-l r` parameter is not specified).
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all traffic (`service any`).
- This rule applies to all sources except (`source-negated true`) the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule limits the maximal number of concurrent active connections to 655/65536=~1% (`concurrent-conns-ratio 655`) for any traffic (`service any`) except (`service-negated true`) the connections from the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule counts connections, packets, and bytes for traffic only from sources that match this rule, and not cumulatively for this rule.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

fw sam_policy batch

Description

The "*fw sam_policy batch*" and "*fw6 sam_policy batch*" commands:

- Add and delete many Suspicious Activity Monitoring (SAM) rules at a time.
- Add and delete many Rate Limiting rules at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Procedure

1. **Start the batch mode**

   - For IPv4, run:

     ```
     fw sam_policy batch << EOF
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy batch << EOF
     ```

2. **Enter the applicable commands**

   - Enter one "`add`" or "`del`" command on each line, on as many lines as necessary.

     Start each line with only "`add`" or "`del`" parameter (not with "`fw samp`").

   - Use the same set of parameters and values as described in these commands:

     - *"fw sam_policy add" on page 720*
     - *"fw sam_policy del" on page 735*

   - Terminate each line with a Return (ASCII 10 - Line Feed) character (press Enter).

3. **End the batch mode**

   Type `EOF` and press Enter.

Example of a Rate Limiting rule for IPv4

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota service
any source range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

Description

The "*fw sam_policy del*" and "*fw6 sam_policy del*" commands:

- Delete one configured Suspicious Activity Monitoring (SAM) rule at a time.
- Delete one configured Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy del '<Rule UID>'
```

Syntax for IPv6

```
fw6 [-d] sam_policy del '<Rule UID>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`'<Rule UID>'`	Specifies the UID of the rule you wish to delete. **Important:** - The quote marks and angle brackets (`'<...>'`) are mandatory. - To see the Rule UID, run the *"fw sam_policy get" on page 739* command.

Procedure

1. **List all the existing rules in the Suspicious Activity Monitoring policy database**

   List all the existing rules in the Suspicious Activity Monitoring policy database.

   - For IPv4, run:

     ```
     fw sam_policy get
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy get
     ```

   The rules show in this format:

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=...
   originator= ... src_ip_addr=... req_tpe=...
   ```

   Example for IPv4:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a>
   target=all timeout=300 action=notify log=log name=Test\ Rule
   comment=Notify\ about\ traffic\ from\ 1.1.1.1
   originator=John\ Doe src_ip_addr=1.1.1.1 req_tpe=ip
   ```

2. **Delete a rule from the list by its UID**

   - For IPv4, run:

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - For IPv6, run:

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   Example for IPv4:

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **Add the flush-only rule**

   - For IPv4, run:

     ```
     fw samp add -t 2 quota flush true
     ```

   - For IPv6, run:

     ```
     fw6 samp add -t 2 quota flush true
     ```

   Explanation:

   The "`fw samp del`" and "`fw6 samp del`" commands only remove a rule from the persistent database. The Security Gateway continues to enforce the deleted rule until the next time you compiled and load a policy. To force the rule deletion immediately, you must enter a flush-only rule right after the "`fw samp del`" and "`fw6 samp del`" command. This flush-only rule immediately deletes the rule you specified in the previous step, and times out in 2 seconds.

   Best Practice - Specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

fw sam_policy get

Description

The "*fw sam_policy get*" and "*fw6 sam_policy get*" commands:

- Show all the configured Suspicious Activity Monitoring (SAM) rules.
- Show all the configured Rate Limiting rules.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Syntax for IPv6

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Parameters

Note - All these parameters are optional.

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Controls how to print the rules: ■ In the default format (without "`-l`"), the output shows each rule on a separate line. ■ In the list format (with "`-l`"), the output shows each parameter of a rule on a separate line. ■ See *"fw sam_policy add" on page 720*.
`-u '<Rule UID>'`	Prints the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets ('<...>') are mandatory.
`-k '<Key>'`	Prints the rules with the specified predicate key. The quote marks are mandatory.
`-t <Type>`	Prints the rules with the specified predicate type. For Rate Limiting rules, you must always use "`-t in`".
`+{-v '<Value>'}`	Prints the rules with the specified predicate values. The quote marks are mandatory.
`-n`	Negates the condition specified by these predicate parameters: ■ `-k` ■ `-t` ■ `+-v`

Examples

Example 1 - Output in the default format

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 2 - Output in the list format

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

Example 3 - Printing a rule by its Rule UID

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 4 - Printing rules that match the specified filters

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated
true source cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service
6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ
concurrent-conns-ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
```

```
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
```

fwm

Description

Performs various management operations and shows various management information.

Notes:

- For debug instructions, see the description of the `fwm` process in sk97638.
- On a Multi-Domain Server, you must run these commands in the context of the applicable Domain Management Server.

Syntax

```
fwm [-d]
      dbload <options>
      exportcert <options>
      fetchfile <options>
      fingerprint <options>
      getpcap <options>
      ikecrypt <options>
      load [<options>]
      logexport <options>
      mds <options>
      printcert <options>
      sic_reset
      snmp_trap <options>
      unload [<options>]
      ver [<options>]
      verify <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`dbload <options>`	Downloads the user database and network objects information to the specified targets See *"fwm dbload" on page 748*.
`exportcert <options>`	Export a SIC certificate of the specified object to file. See *"fwm exportcert" on page 749*.
`fetchfile <options>`	Fetches a specified OPSEC configuration file from the specified source computer. See *"fwm fetchfile" on page 750*.
`fingerprint <options>`	Shows the Check Point fingerprint. See *"fwm fingerprint" on page 752*.
`getpcap <options>`	Fetches the IPS packet capture data from the specified Security Gateway. See *"fwm getpcap" on page 754*.
`ikecrypt <options>`	Encrypts a secret with a key. See *"fwm ikecrypt" on page 756*.
`load <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 801* command to load a policy to a managed Security Gateway. See *"fwm load" on page 757*.
`logexport <options>`	Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file. See *"fwm logexport" on page 758*.
`mds <options>`	Shows information and performs various operations on Multi-Domain Server. See *"fwm mds" on page 763*.
`printcert <options>`	Shows a SIC certificate's details. See *"fwm printcert" on page 765*.
`sic_reset`	Resets SIC on the Management Server. See *"fwm sic_reset" on page 771*.
`snmp_trap <options>`	Sends an SNMP Trap to the specified host. See *"fwm snmp_trap" on page 772*.
`unload <options>`	Unloads the policy from the specified managed Security Gateways. See *"fwm unload" on page 775*.

Parameter	Description
`ver <options>`	Shows the Check Point version of the Management Server. See *"fwm ver" on page 779*.
`verify <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 801* command to verify a policy. See *"fwm verify" on page 780*.

fwm dbload

Description

Copies the user database and network objects information to specified managed servers with one or more **Management** Software Blades enabled.

Important - This command is obsolete for R80 and higher.
Use the API command "`install-database`" to install the database on the applicable servers.
See the *Check Point Management API Reference*.

fwm exportcert

Description

Export a SIC certificate of the specified managed object to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] exportcert -obj <Name of Object> -cert <Name of CA> -file
<Output File> [-withroot] [-pem]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`<Name of Object>`	Specifies the name of the managed object, whose certificate you wish to export.
`<Name of CA>`	Specifies the name of Certificate Authority, whose certificate you wish to export.
`<Output File>`	Specifies the name of the output file.
`-withroot`	Exports the certificate's root in addition to the certificate's content.
`-pem`	Save the exported information in a text file. Default is to save in a binary file.

fwm fetchfile

Description

Fetches a specified OPSEC configuration file from the specified source computer.

This command supports only the `fwopsec.conf` or `fwopsec.v4x` files.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fetchfile -r <File> [-d <Local Path>] <Source>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-r <File>`	Specifies the relative `fw1` directory. This command supports only these files: - `conf/fwopsec.conf` - `conf/fwopsec.v4x`
`-d <Local Path>`	Specifies the local directory to save the fetched file.
`<Source>`	Specifies the managed remote source computer, from which to fetch the file. **Note** - The local and the remote source computers must have established SIC trust.

Example

```
[Expert@MGMT:0]# fwm fetchfile -r "conf/fwopsec.conf" -d /tmp 192.168.3.52
Fetching conf/fwopsec.conf from 192.168.3.52...
Done
[Expert@MGMT:0]#
```

fwm fingerprint

Description

Shows the Check Point fingerprint.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fingerprint [-d]
      <IP address of Target> <SSL Port>
      localhost <SSL Port>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The debug options are: ■ `fwm -d` Runs the complete debug of all `fwm` actions. For complete debug instructions, see the description of the `fwm` process in sk97638. ■ `fingerprint -d` Runs the debug only for the fingerprint actions.
`<IP address of Target>`	Specifies the IP address of a remote managed computer.
`<SSL Port>`	Specifies the SSL port number. The default is 443.

Example 1 - Showing the fingerprint on the local Management Server

```
[Expert@MGMT:0]# fwm fingerprint localhost 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.51,L=Locality Name (eg\, city)
#FINGER 11:A6:F7:1F:B9:F5:15:BC:F9:7B:5F:DC:28:FC:33:C5
##
[Expert@MGMT:0]#
```

Example 2 - Showing the fingerprint from a managed Security Gateway

```
[Expert@MGMT:0]# fwm fingerprint 192.168.3.52 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.52,L=Locality Name (eg\, city)
#FINGER 5C:8E:4D:B9:B4:3A:58:F3:79:18:F1:70:99:8B:5F:2B
##
[Expert@MGMT:0]#
```

fwm getpcap

Description

Fetches the IPS packet capture data from the specified Security Gateway.

This command only works with IPS packet captures stored on the Security Gateway in the `$FWDIR/log/captures_repository/` directory.

This command does not work with other Software Blades, such as Anti-Bot and Anti-Virus that store packet captures in the `$FWDIR/log/blob/` directory on the Security Gateway.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] getpcap -g <Security Gateway> -u '{<Capture UID>}' -p
<Local Path>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-g <Security Gateway>`	Specifies the main IP address or Name of Security Gateway object as configured in SmartConsole.
`-u '{<Capture UID>}'`	Specifies the Unique ID of the packet capture file. To see the Unique ID of the packet capture file, open the applicable log file in **SmartConsole > Logs & Monitor > Logs**.
`-p <Local Path>`	Specifies the local path to save the specified packet capture file. If you do not specify the local directory explicitly, the command saves the packet capture file in the current working directory.

Example

```
[Expert@MGMT:0]# fwm getpcap -g 192.168.162.1 -u '{0x4d79dc02,0x10000,0x220da8c0,0x1ffff}'
/var/log/
[Expert@MGMT:0]#
```

fwm ikecrypt

Description

Encrypts the password of an Endpoint VPN Client user using IKE. The resulting string must then be stored in the LDAP database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ikecrypt <Key> <Password>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Key>	Specifies the IKE Key as defined in the **LDAP Account Unit** properties window on the **Encryption** tab.
<Password>	Specifies the password for the Endpoint VPN Client user.

Example

```
[Expert@MGMT:0]# fwm ikecrypt MySecretKey MyPassword
OUQJHiNHCj6HJGH8ntnKQ7tg
[Expert@MGMT:0]#
```

fwm load

Description

Loads a policy on a managed Security Gateway.

Important - This command is obsolete for R80 and higher.
Use the API command "`install-policy`" to load a policy on a managed Security Gateway.
See the *Check Point Management API Reference*.

fwm logexport

Description

Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm logexport -h
```

```
fwm [-d] logexport [{-d <Delimiter> | -s}] [-t <Table Delimiter>]
[-i <Input File>] [-o <Output File>] [{-f | -e}] [-x <Start Entry
Number>] [-y <End Entry Number>] [-z] [-n] [-p] [-a] [-u
<Unification Scheme File>] [-m {initial | semi | raw}]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-d <Delimiter> | -s`	Specifies the output delimiter between fields of log entries: ■ `-d <Delimiter>` - Uses the specified delimiter. ■ `-s` - Uses the ASCII character #255 (non-breaking space) as the delimiter. **Note** - If you do not specify the delimiter explicitly, the default is a semicolon (`;`).

Parameter	Description
`-t <Table Delimiter>`	Specifies the output delimiter inside table field. Table field would look like: *ROWx:COL0,ROWx:COL1,ROWx:COL2*, and so on **Note** - If you do not specify the table delimiter explicitly, the default is a comma (`,`).
`-i <Input File>`	Specifies the name of the input log file. **Notes:** - This command supports only Security log file (`$FWDIR/log/*.log`) and Audit log file (`$FWDIR/log/*.adtlog`) - If you do not specify the input log file explicitly, the command processes the active Security log file `$FWDIR/log/fw.log`
`-o <Output File>`	Specifies the name of the output file. **Note** - If you do not specify the output log file explicitly, the command prints its output on the screen.
`-f`	After reaching the end of the currently opened log file, specifies to continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-e`	After reaching the end of the currently opened log file, continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-x <Start Entry Number>`	Starts exporting the log entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Starts exporting the log entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), specifies to continue the export of log entries. The default behavior is to stop.
`-n`	Specifies not to perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.

Parameter	Description
`-p`	Specifies to not to perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-a`	Exports only Account log entries.
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-m {initial | semi | raw}`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command exports one unified log entry for each ID. This is the default. If you also specify the "`-f`" parameter, then the output does not export any updates, but exports only entries that relate to the start of new connections. To export updates as well, use the "`semi`" parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, exports entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. Exports all log entries.

The output of the `fwm logexport` command appears in tabular format.

The first row lists the names of all log fields included in the log entries.

Each of the next rows consists of a single log entry, whose fields are sorted in the same order as the first row.

If a log entry has no information in a specific field, this field remains empty (as indicated by two successive semi-colons "`;;`").

You can control which log fields appear in the output of the command output:

Step	Instructions
1	Create the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# touch $FWDIR/conf/logexport.ini`
2	Edit the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# vi $FWDIR/conf/logexport.ini`
3	To include or exclude the log fields from the output, add these lines in the configuration file: `[Fields_Info]` `included_fields = `*`field1`*`,`*`field2`*`,`*`field3`*`,<REST_OF_FIELDS>,`*`field100`* `excluded_fields = `*`field10`*`,`*`field11`* Where: ■ You can specify only the `included_fields` parameter, only the `excluded_fields` parameter, or both. ■ The `num` field must always appear first. You cannot manipulate this field. ■ The `<REST_OF_FIELDS>` is an optional reserved token that refers to a list of fields. • If you specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on a list of fields from the `$FWDIR/conf/logexport_default.C` file. • If you do not specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on the input log file.
4	Save the changes in the file and exit the Vi editor.
5	Export the logs: `fwm logexport `*`<options>`*

Example 1 - Exporting all log entries

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_
name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
0;13Jun2018;19:47:54;CXL1_192.168.3.52;control; ;;daemon;inbound;VPN-1 & FireWall-1;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_Server.checkpoint.com.s6t98x;5;18446744073709551615;2;Log file
has been switched to: MyLog.log;Network;;;;;;;;;;;;
1;13Jun2018;19:47:54;CXL1_192.168.3.52;account;accept;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;;;;;;;;;;
... ...
35;13Jun2018;19:55:59;CXL1_192.168.3.52;account;accept;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
... ...
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could
not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy
configuration on the gateway.;2;Contracts may be out-of-date
... ...
[Expert@MGMT:0]#
```

Example 2 - Exporting only log entries with specified numbers

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log -x 36 -y 47
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_
name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
37;13Jun2018;19:56:06;CXL1_192.168.3.52;account;accept;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;2;;Network;Default;Default;Host
Redirect;;;;;;;;;
... ...
46;13Jun2018;19:56:59;CXL1_192.168.3.52;account;accept;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could
not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy
configuration on the gateway.;2;Contracts may be out-of-date
[Expert@MGMT:0]#
```

fwm mds

Description

- Shows the Check Point version of the Multi-Domain Server.
- Rebuilds status tree for Global VPN Communities.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

  ```
  mdsenv
  ```

- In the context of a Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain
  Management Server>
  ```

Syntax

```
fwm [-d] mds
        ver
        rebuild_global_communities_status {all | missing}
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`ver`	Shows the Check Point version of the Multi-Domain Server.
`rebuild_global_communities_status`	Rebuilds status tree for Global VPN Communities: ▪ `all` - Rebuilds status tree for all Global VPN Communities. ▪ `missing` - Rebuild status tree only for Global VPN Communities that do not have status trees.

Example

```
[Expert@MDS:0]# fwm mds ver
This is Check Point Multi-Domain Security Management R80.40 -
Build 11
[Expert@MDS:0]#
```

fwm printcert

Description

Shows a SIC certificate's details.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] printcert
      -obj <Name of Object> [-cert <Certificate Nick Name>] [-
verbose]
      -ca <CA Name> [-x509 <Name of File> [-p]] [-verbose]
      -f <Name of Binary Certificate File> [-verbose]
```

Parameters

Item	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-obj` *`<Name of Object>`*	Specifies the name of the managed object, for which to show the SIC certificate information.
`-cert` *`<Certificate Nick Name>`*	Specifies the certificate nick name.
`-ca` *`<CA Name>`*	Specifies the name of the Certificate Authority. **Note** - Check Point CA Name is `internal_ca`.
`-x509` *`<Name of File>`*	Specifies the name of the X.509 file.
`-p`	Specifies to show the SIC certificate as a text file.
`-f` *`<Name of Binary Certificate File>`*	Specifies the binary SIC certificate file to show.
`-verbose`	Shows the information in verbose mode.

Examples

Example 1 - Showing the SIC certificate of a Management Server

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca
Subject: O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Apr 8 13:41:00 2018 Local Time
Not Valid After: Fri Jan 1 05:14:07 2038 Local Time
Serial No.: 1
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Key Usage:
        digitalSignature
        keyCertSign
        cRLSign
Basic Constraint:
        is CA
MD5 Fingerprint:
   7B:F9:7B:4C:BD:40:B9:1C:AB:2C:AE:CF:66:2E:E7:06
SHA-1 Fingerprints:
1. A6:43:3A:2B:1A:04:7F:A6:36:A6:2C:78:BF:22:D9:BC:F7:7E:4D:73
2. KEYS HEM GERM PIT ABUT ROVE RAW PA IQ FAWN NUT SLAM
[Expert@MGMT:0]#
```

Example 2 - Showing the SIC certificate of a Management Server in verbose mode

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca -verbose
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: called
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: closing existing database
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] do_links_getver: strncmp failed. Returning -2
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] db_fetchkey: entering
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] PubKey:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Modulus:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ae b3 75 36 64 e4 1a 40 fe c2 ad 2f 9b 83 0b 45
f1 00 04 bc
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 77 77 76 d1 de 8a cf 9f 32 78 8b d4 b1 b4 be
db 75 cc c8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c2 6d ff 3e aa fe f1 2b c3 0a b0 a2 a5 e0 a8 ab
45 cd 87 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ac c6 9f a4 a9 ba 30 79 08 fa 59 4c d2 dc 3d 36
ca 17 d7 c1
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] b2 a2 41 f5 89 0f 00 d4 2d f2 55 d2 30 a5 32 c7
46 7a 6b 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 29 0f 53 9f 35 42 91 e5 7d f7 30 6d bc b3 f2 ae
f3 f0 ed 88
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c4 d7 7d 0c 2d f6 5f c8 ed 9f 9a 57 54 79 d0 0f
0b 2f 9c 0d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 94 2e f0 f4 66 62 f7 ae 2e f8 8e 90 08 ba 63 85
b6 46 2f b7
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a7 01 29 9a 14 58 a8 ef eb 07 17 4e 95 8b 2f 48
5f d3 18 10
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 00 d5 03 d7 fd 45 45 ca 67 5b 34 be b8 00 ae
ea 9a cd 50
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] d6 e7 a2 81 86 78 11 d7 bf 04 9f 8b 43 3f f7 36
5f ed 31 a8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a3 9d 8b 0a de 05 fb 5c 44 2e 29 e3 3e f4 dd 50
01 0f 86 9d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 55 16 a3 4d f8 90 2d 13 c6 c1 28 57 f8 3e 7c 59
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Exponent: 65537 (0x10001)
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52]
X509 Certificate Version 3
refCount: 1
Serial Number: 1
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Apr 8 13:41:00 2018 Local Time
Not valid after: Fri Jan 1 05:14:07 2038 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyCertSign
                cRLSign
        Basic Constraint (Critical):
                is CA

[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] destroy_rand_mutex: destroy
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] cpKeyTaskManager::~cpKeyTaskManager: called.
[Expert@MGMT:0]#
```

Example 3 - Showing the SIC certificate of a managed Cluster object

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244

printing all certificates of CXL_192.168.3.244

defaultCert:
Host Certificate (level 0):
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Jun 3 19:58:19 2018 Local Time
Not Valid After: Sat Jun 3 19:58:19 2023 Local Time
Serial No.: 85021
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Subject Alternate Names:
        IP Address: 192.168.3.244
CRL distribution points:
        http://192.168.3.240:18264/ICA_CRL2.crl
        CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x
Key Usage:
        digitalSignature
        keyEncipherment
Basic Constraint:
        not CA
MD5 Fingerprint:
   B1:15:C7:A8:2A:EE:D1:75:92:9F:C7:B4:B9:BE:42:1B
SHA-1 Fingerprints:
1. BC:7A:D9:E2:CD:29:D1:9E:F0:39:5A:CD:7E:A9:0B:F9:6A:A7:2B:85
2. MIRE SANK DUSK HOOD HURD RIDE TROY QUAD LOVE WOOD GRIT WITH


                *****
[Expert@MGMT:0]#
```

Example 4 - Showing the SIC certificate of a managed Cluster object in verbose mode

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244 -verbose
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: called
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: closing existing database
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] do_links_getver: strncmp failed. Returning -2

printing all certificates of CXL_192.168.3.244

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] db_fetchkey: entering
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 1 certificates
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] PubKey:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Modulus:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] df 35 c3 45 ca 42 16 6e 21 9e 31 af c1 fd 20 0a
3d 5b 6f 5d
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] e0 a2 0c 0e fa fa 5e e5 91 9d 4e 73 77 fa db 86
0b 5e 5d 0c
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] ce af 4a a4 7b 30 ed b0 43 7d d8 93 c5 4b 01 f4
3d b5 d8 f4
... ... ...
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 34 b1 db ac 18 4f 11 bd d2 fb 26 7d 23 74 5c d9
00 a1 58 1e
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 60 7c 83 44 fa 1e 1e 86 fa ad 98 f7 df 24 4a 21
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Exponent: 65537 (0x10001)
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45]
X509 Certificate Version 3
refCount: 1
Serial Number: 85021
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Jun 3 19:58:19 2018 Local Time
Not valid after: Sat Jun 3 19:58:19 2023 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyEncipherment
        Subject Alternate names:
                IP: 192.168.3.244
        Basic Constraint:
                not CA
        CRL distribution Points:
                URI: http://192.168.3.240:18264/ICA_CRL2.crl
                DN: CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x

defaultCert:

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] destroy_rand_mutex: destroy
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] cpKeyTaskManager::~cpKeyTaskManager: called.
                *****
[Expert@MGMT:0]#
```

fwm sic_reset

Description

Resets SIC on the Management Server.

For detailed procedure, see sk65764: How to reset SIC.

Warning:

- **Before you run this command, take a Gaia Snapshot and a full backup of the Management Server.**
  This command resets SIC between the Management Server and all its managed objects.
- **This operation breaks trust in all Internal CA certificates and SIC trust across the managed environment.**
  Therefore, we do not recommend it at all, except for real disaster recovery.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] sic_reset
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.

fwm snmp_trap

Description

Sends an SNMPv1 Trap to the specified host.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On a Multi-Domain Server, the SNMP Trap packet is sent from the IP address of the Leading Interface.

Syntax

```
fwm [-d] snmp_trap [-v <SNMP OID>] [-g <Generic Trap Number>] [-s
<Specific Trap Number>] [-p <Source Port>] [-c <SNMP Community>]
<Target> ["<Message>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ✪ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-v <SNMP OID>`	Specifies an optional SNMP OID to bind with the message.
`-g <Generic Trap Number>`	Specifies the generic trap number. One of these values: ■ 0 - For `coldStart` trap ■ 1 - For `warmStart` trap ■ 2 - For `linkDown` trap ■ 3 - For `linkUp` trap ■ 4 - For `authenticationFailure` trap ■ 5 - For `egpNeighborLoss` trap ■ 6 - For `enterpriseSpecific` trap (this is the default value)
`-s <Specific Trap Number>`	Specifies the unique trap type. Valid only of generic trap value is 6 (for `enterpriseSpecific`). Default value is 0.
`-p <Source Port>`	Specifies the source port, from which to send the SNMP Trap packets.
`-c <SNMP Community>`	Specifies the SNMP community.
`<Target>`	Specifies the managed target host, to which to send the SNMP Trap packets. Enter an IP address of a resolvable hostname.
`"<Message>"`	Specifies the SNMP Trap text message.

Example - Sending an SNMP Trap from a Management Server and capturing the traffic on the Security Gateway

```
[Expert@MGMT:0]# fwm snmp_trap -g 2 -c public 192.168.3.52 "My Trap Message"
[Expert@MGMT:0]#

[Expert@MyGW_192.168.3.52:0]# tcpdump -s 1500 -vvvv -i eth0 udp and host 192.168.3.51
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
22:49:43.891287 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: UDP (17), length: 103)
192.168.3.51.53450 > MyGW_192.168.3.52.snmptrap: [udp sum ok] { SNMPv1 { Trap(58) E:2620.1.1
192.168.3.240 linkDown 1486440 E:2620.1.1.11.0="My Trap Message" } }
Pressed CTRL+C
[Expert@MyGW_192.168.3.52:0]#
```

fwm unload

Description

Unloads the policy from the specified managed Security Gateways or Cluster Members.

Warning:

1. The `fwm unload` command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the specified Security Gateway (Cluster Member).
2. The `fwm unload` command removes all policies from the specified Security Gateway (Cluster Member).
   This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- If it is necessary to remove the current policy, but keep the Security Gateway (Cluster Member) protected, then run the "`comp_init_policy`" command on the Security Gateway (Cluster Member).
- To load the policies on the Security Gateway (Cluster Member), run one of these commands on the Security Gateway (Cluster Member), or reboot:
  - "`fw fetch`"
  - "`cpstart`"

Syntax

```
fwm [-d] unload <GW1> <GW2> ... <GWN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`<GW1> <GW2> ... <GWN>`	Specifies the managed Security Gateways by their main IP address or Object Name as configured in SmartConsole.

Example

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name: CXL_Policy
Policy install time: Wed Oct 23 18:23:14 2019
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 1
net.ipv6.conf.eth1.forwarding = 1
net.ipv6.conf.eth3.forwarding = 1
net.ipv6.conf.eth2.forwarding = 1
net.ipv6.conf.eth4.forwarding = 1
net.ipv6.conf.eth5.forwarding = 1
net.ipv6.conf.eth0.forwarding = 1
net.ipv6.conf.eth6.forwarding = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.lo.forwarding = 1
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 1
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 1
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 1
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
[Expert@MyGW:0]#


[Expert@MGMT:0]# fwm unload MyGW

Uninstalling Policy From: MyGW

 Security Policy successfully uninstalled from MyGW...

Security Policy uninstall complete.

[Expert@MGMT:0]#
```

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name:
Policy install time:
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth3.forwarding = 0
net.ipv6.conf.eth2.forwarding = 0
net.ipv6.conf.eth4.forwarding = 0
net.ipv6.conf.eth5.forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth6.forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
[Expert@MyGW:0]#
```

fwm ver

Description

Shows the Check Point version of the Security Management Server.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

  ```
  mdsenv
  ```

- In the context of a Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain
  Management Server>
  ```

Syntax

```
fwm [-d] ver [-f <Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-f <Output File>`	Specifies the name of the output file, in which to save this information.

Example

```
[Expert@MGMT:0]# fwm ver
This is Check Point Security Management Server R80.40 - Build 11
[Expert@MGMT:0]#
```

fwm verify

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 801* command to verify a policy on a managed Security Gateway.

Description

Verifies the specified policy package without installing it.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] verify <Policy Name>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Policy Name>	Specifies the name of the policy package as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# fwm verify Standard
 Verifier messages:
Error: Rule 1 Hides rule 2 for Services & Applications: any .
[Expert@MGMT:0]#
```

inet_alert

Description

Notifies an Internet Service Provider (ISP) when a company's corporate network is under attack. This command forwards log messages generated by the alert daemon on your Check Point Security Gateway to an external Management Station. This external Management Station is usually located at the ISP site. The ISP can then analyze the alert and react accordingly.

This command uses the Event Logging API (ELA) protocol to send the alerts. 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 external Management Station running the ELA Proxy at the ISP site and the Check Point Security Gateway generating the alert.

Procedure

Step	Instructions
1	Connect with SmartConsole to the applicable Security Management Server or Domain Management Server, which manages the applicable Security Gateway that should forward log messages to an external Management Station.
2	From the top left **Menu**, click **Global properties**.
3	Click on the **[+]** near the **Log and Alert** and click **Alerts**.
4	Clear the **Send user defined alert no. 1 to SmartView Monitor**.
5	Select the next option **Run UserDefined script under the above**.
6	Enter the applicable **inet_alert** syntax (see the *Syntax* section below).
7	Click **OK**.
8	Install the Access Control Policy on the applicable Security Gateway.

Syntax

```
inet_alert -s <IP Address> [-o] [-a <Auth Type>] [-p <Port>] [-f
<Token> <Value>] [-m <Alert Type>]
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Parameters

Parameter	Description
`-s <IP Address>`	The IPv4 address of the ELA Proxy (usually located at the ISP site).
`-o`	Prints the alert log received to `stdout`. Use this option when `inet_alert` is part of a pipe syntax (`<some command> | inet_alert ...`).
`-a <Auth Type>`	Specifies the type of connection to the ELA Proxy. One of these values: ▪ `ssl_opsec` - The connection is authenticated and encrypted (this is the default). ▪ `auth_opsec` - The connection is authenticated. ▪ `clear` - The connection is neither authenticated, nor encrypted.
`-p <Port>`	Specifies the port number on the ELA proxy. Default port is 18187.
`-f <Token> <Value>`	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. Cannot contain spaces. ▪ `<Value>` - The field's value. Cannot contain spaces. This option can be used multiple times to add multiple `<Token> <Value>` pairs to the log.

Parameter	Description
`-m <Alert Type>`	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: These alerts execute the OS commands: ■ `alert` - Popup alert command ■ `mail` - Mail alert command ■ `snmptrap` - SNMP trap alert command ■ `spoofalert` - Anti-Spoof alert command These NetQuota and ServerQuota alerts execute the OS commands specified in the `$FWDIR/conf/objects.C`: file: `value=clientquotaalert. Parameter=clientquotaalertcmd`

Exist Status

Exit Status	Description
`0`	Execution was successful.
`102`	Undetermined error.
`103`	Unable to allocate memory.
`104`	Unable to obtain log information from `stdin`
`106`	Invalid command line arguments.
`107`	Failed to invoke the OPSEC API.

Example

```
inet_alert -s 10.0.2.4 -a clear -f product cads -m alert
```

This command specifies to perform these actions in the event of an attack:

- 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. Set the product field of this log message to `cads`
- Trigger the OS command specified in the SmartConsole > **Menu > Global properties > Log and Alert > Popup Alert Command** field.

ldapcmd

Description

This is an LDAP utility that controls these features:

Feature	Description
Cache	LDAP cache operations, such as emptying the cache, as well as providing debug information.
Statistics	LDAP search 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 These statistics are saved in the `$FWDIR/log/ldap_pid_<Process PID>.stats` file.
Logging	View the alert and warning logs.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcmd [-d <Debug Level>] -p {<Process Name> | all} <Command>
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-p {<Process Name> | all}`	Runs on a specified Check Point process, or all supported Check Point processes.
`<Command>`	One of these commands: ■ `cacheclear {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Clears cache for all objects • `UserCacheObject` - Clears cache for user objects • `TemplateCacheObject` - Clears cache for template objects • `TemplateExtGrpCacheObject` - Clears cache for external template group objects ■ `cachetrace {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Traces cache for all objects • `UserCacheObject` - Traces cache for user objects • `TemplateCacheObject` - Traces cache for template objects • `TemplateExtGrpCacheObject` - Traces cache for external template group objects ■ `log {on | off}` • `on` - Creates LDAP logs • `off` - Does not create LDAP logs ■ `stat {<Print Interval in Sec> | 0}` • `<Print Interval in Sec>` - How frequently to collect the statistics • `0` - Stops collecting the statistics

ldapcompare

Description

This is an LDAP utility that performs compare queries and prints a message whether the result returned a match or not.

This utility opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcompare [-d <Debug Level>] [<Options>] <DN> {<Attribute>
<Value> | <Attribute> <Base64 Value>}
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`<Options>`	See the tables below: - Compare options - Common options
`<DN>`	Specifies the Distinguished Name.
`<Attribute>`	Specifies the assertion attribute.
`<Value>`	Specifies the assertion value.
`<Base64 Value>`	Specifies the Base64 encoding of the assertion value.

Compare options

Option	Description
`-E [!]<Extension> [=<Extension Parameter>]`	Specifies the compare extensions. **Note** - The exclamation sign "!" indicates criticality. For example: `!dontUseCopy` = Do **not** use Copy
`-M`	Enables the Manage DSA IT control. Use the "`-MM`" option to make it critical.
`-P <LDAP Protocol Version>`	Specifies the LDAP protocol version. Default version is 3.
`-z`	Enables the quiet mode. The command does not print anything. You can use the command return values.

Common options

Option	Description
`-D <Bind DN>`	Specifies the LDAP Server administrator Distinguished Name.

Option	Description
`-e [!]<Extension> [=<Extension Parameter>]`	Specifies the general extensions: **Note** - The exclamation sign "!" indicates criticality. ■ `[!]assert=<Filter>` RFC 4528; an RFC 4515 filter string ■ `[!]authzid=<Authorization ID>` RFC 4370; either "`dn:<DN>`", or "`u:<Username>`" ■ `[!]chaining[=<Resolve Behavior> [/<Continuation Behavior>]]` One of these: • `"chainingPreferred"` • `"chainingRequired"` • `"referralsPreferred"` • `"referralsRequired"` ■ `[!]manageDSAit` RFC 3296 ■ `[!]noop` ■ `ppolicy` ■ `[!]postread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]preread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]relax` ■ `abandon` SIGINT sends the abandon signal; if critical, does not wait for SIGINT. Not really controls. ■ `cancel` SIGINT sends the cancel signal; if critical, does not wait for SIGINT. Not really controls. ■ `ignore` SIGINT ignores the response; if critical, does not wait for SIGINT. Not really controls.
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname.
`-H <LDAP URI>`	Specifies the LDAP Server Uniform Resource Identifier (s).
`-I`	Specifies to use the SASL Interactive mode.
`-n`	Dry run - shows what would be done, but does not actually do it.

Option	Description
`-N`	Specifies not to use the reverse DNS to canonicalize SASL host name.
`-o <Option>[=<Option Parameter>]`	Specifies the general options: `nettimeout={<Timeout in Sec> | none | max}`
`-O <Properties>`	Specifies the SASL security properties.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-Q`	Specifies to use the SASL Quiet mode.
`-R <Realm>`	Specifies the SASL realm.
`-U <Authentication Identity>`	Specifies the SASL authentication identity.
`-v`	Runs in verbose mode (prints the diagnostics to *stdout*).
`-V`	Prints version information (use the "`-VV`" option only).
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password (for simple authentication).
`-W`	Specifies to prompt the user for the LDAP Server administrator password.
`-x`	Specifies to use simple authentication.
`-X <Authorization Identity>`	Specifies the SASL authorization identity (either "`dn:<DN>`", or "`u:<Username>`" option).
`-y <File>`	Specifies to read the LDAP Server administrator password from the `<File>`.
`-Y <SASL Mechanism>`	Specifies the SASL mechanism.
`-Z`	Specifies to start the TLS request. Use the "`-ZZ`" option to require successful response.

ldapmemberconvert

Description

This is an LDAP utility that ports from the "`Member`" attribute values in LDAP group entries to the "`MemberOf`" attribute values in LDAP member (User or Template) entries.

This utility converts the LDAP server data to work in either the "`MemberOf`" mode, or "`Both`" mode. The utility searches through all specified group or template entries that hold one or more "`Member`" attribute values and modifies each value. The utility searches through all specified group/template entries and fetches 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, the utility delete those "`Member`" attribute values from the group/template, unless you run the command in the "`Both`" mode.

When your run the command, it creates a log file `ldapmemberconvert.log` in the current working directory. The command logs all modifications done and errors encountered in that log file.

Important - Back up the LDAP server database *before* you run this conversion utility.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmemberconvert [-d <Debug Level>] -h <LDAP Server> -p <LDAP
Server Port> -D <LDAP Admin DN> -w <LDAP Admin Password> -m
<Member Attribute Name> -o <MemberOf Attribute Name> -c <Member
ObjectClass Value> [-B] [-f <File> | -g <Group DN>] [-L <LDAP
Server Timeout>] [-M <Number of Updates>] [-S <Size>] [-T <LDAP
Client Timeout>] [-Z]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-m <Member Attribute Name>`	Specifies the LDAP attribute name when fetching and (possibly) deleting a group `Member` attribute value.
`-o <MemberOf Attribute Name>`	Specifies the LDAP attribute name for adding an LDAP "`MemberOf`" attribute value.
`-c <Member ObjectClass Value>`	Specifies the LDAP "`ObjectClass`" attribute value that defines, which type of member to modify. You can specify multiple attribute values with this syntax: `-c <Member Object Class 1> -c <Member Object Class 2> ... -c <Member Object Class N>`
`-B`	Specifies to run in "`Both`" mode.

`-f <File>`	Specifies the file that contains a list of Group DNs separated by a new line:
	`<Group DN 1>`
	`<Group DN 2>`
	`...`
	`<Group DN N>`
	Length of each line is limited to 256 characters.

Parameter	Description
`-g <Group DN>`	Specifies the Group or Template Distinguished Name, on which to perform the conversion. You can specify multiple Group DNs with this syntax: `-g <Group DN 1> -g <Group DN 2> ... -g <Group DN N>`
`-L <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "`never`".
`-M <Number of Updates>`	Specifies the maximal number of simultaneous member LDAP updates. Default is 20.
`-S <Size>`	Specifies the Server side size limit for LDAP operations, in number of entries. Default is "`none`".
`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "`never`".
`-Z`	Specifies to use SSL connection.

Notes

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 the "`MemberOf`" attributes for their groups, then this conversion has to be applied on LDAP defined templates for their groups.

Troubleshooting

Symptom:

A command fails with an error message stating the connection stopped unexpectedly when you run it with the parameter `-M <Number of Updates>`.

Root Cause:

The LDAP server could not handle that many LDAP requests simultaneously and closed the connection.

Solution:

Run the command again with a lower value for the "`-M`" parameter. The default value should be adequate, but can also cause a connection failure in extreme situations. Continue to reduce the value until the command runs normally. Each time you run the command with the same set of groups, the command continues from where it left off.

Examples

Example 1

A group is defined with the DN "`cn=cpGroup,ou=groups,ou=cp,c=us`" and these attributes:

```
...
cn=cpGroup
uniquemember="cn=member1,ou=people,ou=cp,c=us"
uniquemember="cn=member2,ou=people,ou=cp,c=us"
...
```

For the two member entries:

```
...
cn=member1
objectclass=fw1Person
...
```

and:

```
...
cn=member2
objectclass=fw1Person
...
```

Run:

```
[Expert@MGMT:0]# ldapconvert -g cn=cpGroup,ou=groups,ou=cp,c=us -h MyLdapServer -d cn=admin -w secret -m uniquemember -o memberof -c
fw1Person
```

The result for the group DN is:

```
...
cn=cpGroup
...
```

The result for the two member entries is:

```
...
cn=member1
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

and:

```
...
cn=member2
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

If you run the same command with the "`-B`" parameter, it produces the same result, but the group entry is not modified.

Example 2

If there is another member attribute value for the same group entry:

```
uniquemember="cn=template1,ou=people, ou=cp,c=us"
```

and the template is:

```
cn=member1
objectclass=fw1Template
```

Then after running the same command, the template entry stays intact, because of the parameter "`-c fw1Person`", but the object class of "`template1`" is "`fw1Template`".

ldapmodify

Description

This is an LDAP utility that imports users to an LDAP server. The input file must be in the LDIF format.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmodify [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Server
Port>] [-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-a] [-b]
[-c] [-F] [-k] [-n] [-r] [-v] [-T <LDAP Client Timeout>] [-Z] [ -f
<Input File> .ldif | < <Entry>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.

Parameter	Description
`-a`	Specifies that this is the LDAP "`add`" operation.
`-b`	Specifies to read values from files (for binary attributes).
`-c`	Specifies to ignore errors during continuous operation.
`-F`	Specifies to force changes on all records.
`-k`	Specifies the Kerberos bind.
`-K`	Specifies the Kerberos bind, part 1 only.
`-n`	Specifies to print the LDAP "`add`" operations, but do not actually perform them.
`-r`	Specifies to replace values, instead of adding values.
`-v`	Specifies to run in verbose mode.
`-T` *`<LDAP Client Timeout>`*	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "`never`".
`-Z`	Specifies to use SSL connection.
`-f` *`<Input File>`*`.ldif`	Specifies to read from the *`<Input File>`*`.ldif` file. The input file must be in the LDIF format.
`<` *`<Entry>`*	Specifies to read the entry from the *stdin*. The "<" character is mandatory part of the syntax. It specifies the input comes from the standard input (from the data you enter on the screen).

ldapsearch

Description

This is an LDAP utility that queries an LDAP directory and returns the results.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapsearch [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Port>]
[-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-A] [-B] [-b
<Base DN>] [-F <Separator>] [-l <LDAP Server Timeout>] [-s
<Scope>] [-S <Sort Attribute>] [-t] [-T <LDAP Client Timeout>] [-
u] [-z <Number of Search Entries>] [-Z] <Filter> [<Attributes>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-A`	Specifies to retrieve attribute names only, without values.

Parameter	Description
`-B`	Specifies not to suppress the printing of non-ASCII values.
`-b <Base DN>`	Specifies the Base Distinguished Name (DN) for search.
`-F <Separator>`	Specifies the print separator character between attribute names and their values. The default separator is the equal sign (`=`).
`-l <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "`never`".
`-s <Scope>`	Specifies the search scope. One of these: ■ `base` ■ `one` ■ `sub`
`-S <Sort Attribute>`	Specifies to sort the results by the values of this attribute.

`-t`	Specifies to write values to files in the `/tmp/` directory.
	Writes each *<attribute>-<value>* pair to a separate file named:
	`/tmp/ldapsearch-<Attribute>-<Value>`
	For example, for the `fw1color` attribute with the value `a00188`, the command writes to the file named:
	`/tmp/ldapsearch-fw1color-a00188`

`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is `never`.
`-u`	Specifies to show user-friendly entry names in the output. For example: shows `cn=Babs Jensen, users, omi` instead of `cn=Babs Jensen, cn=users,cn=omi`
`-z <Number of Search Entries>`	Specifies the maximal number of entries to search on the LDAP Server.
`-Z`	Specifies to use SSL connection.
`<Filter>`	LDAP search filter compliant with RFC-1558. For example: `objectclass=fw1host`

Parameter	Description
<Attributes>	Specifies the list of attributes to retrieve. If you do not specify attributes explicitly, then the command retrieves all attributes.

Example

```
[Expert@MGMT:0]# ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass
```

With this syntax, the command:

1. Connects to the LDAP Server to port 18185.
2. Connects to the LDAP Server with Base DN "`cn=omi`".
3. Queries the LDAP directory for "`fw1host`" objects.
4. For each object found, prints the value of its "`objectclass`" attribute.

mgmt_cli

Description

The mgmt_cli tool works directly with the management database on your Management Server.

Syntax on Management Server or Security Gateway running on Gaia OS

```
mgmt_cli <Command Name> <Command Parameters> <Optional Switches>
```

Syntax on SmartConsole computer running on Windows OS 32-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Syntax on SmartConsole computer running on Windows OS 64-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles
(x86)%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Notes

- For a complete list of the mgmt_cli options, enter the mgmt_cli (mgmt_cli.exe) command and press Enter.
- For more information, see the *Check Point Management API Reference*.

migrate

Important - This command is used to migrate the management database from R80.10 and lower versions.
For more information, see the *R80.40 Installation and Upgrade Guide*.

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

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 Gaia Backup and Gaia Snapshot, see the *R80.40 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/bin/upgrade_tools/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R80.40/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R80.40/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R80.40/log/migrate-2019.06.14_11.21.39.log*

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# ./migrate -h
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate export [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full
Path>/<Name of Exported File> &
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate import [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full
Path>/<Name of Exported File>.tgz &
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`yes | nohup ./migrate ... &`	This syntax: 1. Sends the "`yes`" input to the interactive "`migrate`" command through the pipeline. 2. The "`nohup`" forces the "`migrate`" command to ignore the hangup signals from the shell. 3. The "`&`" forces the command to run in the background. As a result, when the CLI session closes, the command continues to run in the background. See: - sk133312 - https://linux.die.net/man/1/bash - https://linux.die.net/man/1/nohup
`export`	Exports the management database and applicable Check Point configuration.
`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.

Parameter	Description
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory. ⓘ **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory. ⓘ **Important:** ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-n`	Runs silently (non-interactive mode) and uses the default options for each setting. ⓘ **Important:** ■ If you export a management database in this mode and the specified name of the exported file matches the name of an existing file, the command overwrites the existing file without prompting. ■ If you import a management database in this mode, the "`migrate import`" command runs the "`cpstop`" command automatically.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.
`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
/<Full Path>/	Absolute path to the exported database file. This path must exist.

Parameter	Description
<Name of Exported File>	■ During the export operation, specifies the name of the output file. The command automatically adds the `*.tgz` extension. ■ During the import operation, specifies the name of the exported file. You must manually enter the `*.tgz` extension in the end.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# ./migrate export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R80.40/migrate-2019.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R80.40/log/migrate-2019.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

migrate_server

Important - This command is used to migrate the management database from R80.20.M1, R80.20, R80.20.M2, R80.30, and higher versions.
For more information, see:

- sk135172 - Upgrade Tools
- The *R80.40 Installation and Upgrade Guide*

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

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 Gaia Backup and Gaia Snapshot, see the *R80.40 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/scripts/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate_server` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R80.40/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R80.40/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R80.40/log/migrate-2020 - 2024.06.14_11.21.39.log*

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server -h
```

- To run the Pre-Upgrade Verifier:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server verify -v R80.40 [-skip_
upgrade_tools_check]
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R80.40 [-skip_
upgrade_tools_check] [-l | -x] [--include-uepm-msi-files] [--
exclude-uepm-postgres-db] [--ignore_warnings] /<Full
Path>/<Name of Exported File>
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server import -v R80.40 [-skip_
upgrade_tools_check] [-l | -x] [/var/log/mdss.json] [--
include-uepm-msi-files] [--exclude-uepm-postgres-db] /<Full
Path>/<Name of Exported File>.tgz
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`export`	Exports the management database and applicable Check Point configuration.

Parameter	Description

`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.
	Important:
	▪ This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands).
	▪ This note applies to a Multi-Domain Security Management environment, if at least one of the servers changes its IPv4 address comparing to the source server, from which you exported its database.
	You must do these steps **before** you start the upgrade and import:
	1. You must create a special JSON configuration file with the new IPv4 address(es).
	Syntax:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	Example:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`
	2. You must call this file: **mdss.json**
	3. You must put this file on **all** servers in this directory: **/var/log/**

`verify`	Verifies the management database and applicable Check Point configuration that were exported from another Management Server.
`-v R80.40`	Specifies the version, to which you plan to migrate / upgrade.
`-skip_upgrade_tools_check`	Does not try to connect to Check Point Cloud to check for a more recent version of the Upgrade Tools. **Best Practice** - Use this parameter on the Management Server that is **not** connected to the Internet.

Parameter	Description
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory. **Important:** - The command can export only closed logs (to which the information is not currently written). - If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory. **Important:** - This parameter only supports Management Servers and Log Servers R80.10 and higher. - The command can export only closed logs (to which the information is not currently written). - If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).

Parameter	Description

`/var/log/mdss.json`
Previously:
`-change_ips_file /<Full Path>/<Name of JSON File>.json`
	Important:
	■ In the Upgrade Tools for R80.40 build higher than 994000406, the syntax is (this filename is mandatory):
	`/var/log/mdss.json`
	You must create the file **/var/log/mdss.json** and not use the parameter "**-change_ips_file**".
	■ In the Upgrade Tools for R80.40 build 994000406 and lower, the syntax was:
	`-change_ips_file /<Full Path>/<Name of JSON File>.json`
	Specifies the absolute path to the special JSON configuration file with new IPv4 addresses.
	This file is mandatory during an upgrade of a Multi-Domain Security Management environment.
	Even if only one of the servers migrates to a new IP address, all the other servers must get this configuration file for the import process.
	Syntax:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	Example:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`

`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.
`-n`	Disables the interactive mode.

Parameter	Description
/<Full Path>/<Name of Exported File>	Specifies the absolute path to the exported database file. This path must exist. ■ During the export operation, specifies the name of the output file. The command automatically adds the `*.tgz` extension. ■ During the import operation, specifies the name of the exported file. You must manually enter the `*.tgz` extension in the end.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R80.40/migrate-2020 - 2024.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate_server export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R80.40/log/migrate-2020 - 2024.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

queryDB_util

Description

Searches in the management database for objects or policy rules.

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 801* command to search in the management database for objects or policy rules according to search parameters.

rs_db_tool

Description

Manages Dynamically Assigned IP address (DAIP) gateways in a DAIP database.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

- **To add an entry to the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation add -name <Object
Name> -ip <IPv4 Address> -ip6 <Pv6 Address> -TTL <Time-To-
Live>
```

- **To fetch a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation fetch -name
<Object Name>
```

- **To delete a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation delete -name
<Object Name>
```

- **To list all entries in the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation list
```

- **To synchronize the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation sync
```

Note - You must run this command from the Expert mode.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. ★ **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-name <Object Name>`	Specifies the name of the DAIP object.
`-ip <IPv4 Address>`	Specifies the IPv4 address of the DAIP object
`-ip6 <IPv6 Address>`	Specifies the IPv6 address of the DAIP object.
`-TTL <Time-To-Live>`	Specifies the relative time interval (in seconds), during which the entry is valid.

sam_alert

Description

For SAM v1, this utility executes Suspicious Activity Monitoring (SAM) actions according to the information received from the standard input.

For SAM v2, this utility executes Suspicious Activity Monitoring (SAM) actions with User Defined Alerts mechanism.

Important:

- You must run this command on the Management Server.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Notes:

- VSX Gateways and VSX Cluster Members do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam" on page 709* and *"fw sam_policy" on page 717* commands.

SAM v1 syntax

Syntax for SAM v1

```
sam_alert [-v] [-o] [-s <SAM Server>] [-t <Time>] [-f <Security
Gateway>] [-C] {-n|-i|-I} {-src|-dst|-any|-srv}
```

Parameters for SAM v1

Parameter	Description
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-o`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-s <SAM Server>`	Specifies the SAM Server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.

Parameter	Description
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. ⓘ **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-C`	Cancels the specified operation.
`-n`	Specifies to notify every time a connection, which matches the specified criteria, passes through the Security Gateway.
`-i`	Inhibits (drops or rejects) connections that match the specified criteria.
`-I`	Inhibits (drops or rejects) connections that match the specified criteria and closes all existing connections that match the specified criteria.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

SAM v2 syntax

Syntax for SAM v2

```
sam_alert -v2 [-v] [-O] [-S <SAM Server>] [-t <Time>] [-f
<Security Gateway>] [-n <Name>] [-c "<Comment">] [-o
<Originator>] [-l {r | a}] -a {d | r| n | b | q | i} [-C] {-ip
|-eth} {-src|-dst|-any|-srv}
```

Parameters for SAM v2

Parameter	Description
`-v2`	Specifies to use SAM v2.
`-v`	Enables the verbose mode for the `fw sam` command.
`-O`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-S <SAM Server>`	the SAM server to be contacted. Default is localhost
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-n <Name>`	Specifies the name for the SAM rule. Default is empty.
`-c "<Comment>"`	Specifies the comment for the SAM rule. Default is empty. You must enclose the text in the double quotes or single quotes.
`-o <Originator>`	Specifies the originator for the SAM rule. Default is "`sam_alert`".

Parameter	Description
`-l {r | a}`	Specifies the log type for connections that match the specified criteria: - `r` - Regular - `a` - Alert Default is `None`.
`-a {d | r| n | b | q | i}`	Specifies the action to apply on connections that match the specified criteria: - `d` - Drop - `r` - Reject - `n` - Notify - `b` - Bypass - `q` - Quarantine - `i` - Inspect
`-C`	Specifies to close all existing connections that match the criteria.
`-ip`	Specifies to use IP addresses as criteria parameters.
`-eth`	Specifies to use MAC addresses as criteria parameters.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

Example

See sk110873: How to configure Security Gateway to detect and prevent port scan.

stattest

Description

Check Point AMON client to query SNMP OIDs.

You can use this command as an alternative to the standard SNMP commands for debug purposes - to make sure the applicable SNMP OIDs provide the requested information.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Syntax

- **To query a Regular OID:**

  ```
  stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2> ...
  <Regular_OID_N>
  ```

  These are specified in the SNMP MIB files.

  For Check Point MIB files, see sk90470.

- **To query a Statistical OID:**

  ```
  stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
  <Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
  ```

  Statistical OIDs take some time to "initialize".

  For example, to calculate an average, it is necessary to collect enough samples.

  Check Point statistical OIDs are registered in the `$CPDIR/conf/statistical_oid.conf` file.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h <Host>`	Specifies the remote Check Point host to query by its IP address or resolvable hostname.
`-p <Port>`	Specifies the port number, on which the AMON server listens. Default port is 18192.
`-x <Proxy Server>`	Specifies the Proxy Server by its IP address or resolvable hostname. **Note** - Use only when you query a remote host.
`-l <Polling Interval>`	Specifies the time in seconds between queries. **Note** - Use only when you query a Statistical OID.
`-r <Polling Duration>`	Specifies the time in seconds, during which to run consecutive queries. **Note** - Use only when you query a Statistical OID.
`-v <VSID>`	On a VSX Gateway, specifies the context of a Virtual Device to query.
`-t <Timeout>`	Specifies the session timeout in milliseconds.
`<Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>`	Specifies the Regular OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.

Parameter	Description
<Statistical_OID_1> *<Statistical_OID_2>* ... *<Statistical_OID_N>*	Specifies the Statistical OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.

Example - Query a Regular OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

```
[Expert@HostName]# stattest get 1.3.6.1.4.1.2620.1.6.7.4.2
```

Example - Query a Statistical OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

Information is collected with intervals of 5 seconds during 5 seconds

```
[Expert@HostName]# stattest get -l 5 -r 5 1.3.6.1.4.1.2620.1.6.7.2.3
```

threshold_config

Description

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts.

You can use these thresholds to monitor many system components automatically without requesting information from each object or device.

You configure these SNMP Monitoring Thresholds only on the Security Management Server, Multi-Domain Server, or Domain Management Server.

During policy installation, the managed a Security Gateway and Clusters receive and apply these thresholds as part of their policy.

For more information, see sk90860: How to configure SNMP on Gaia OS.

Procedure

Step	Instructions
1	Connect to the command line on the Management Server.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, switch to the context of the applicable Domain Management Server: `[Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>`
4	Go to the Threshold Engine Configuration menu: `[Expert@HostName:0]# threshold_config`

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>5</td><td>

Select the applicable options and configure the applicable settings (see the **Threshold Engine Configuration Options** table below).

```
Threshold Engine Configuration Options:
---------------------------------------


 (1) Show policy name
 (2) Set policy name
 (3) Save policy
 (4) Save policy to file
 (5) Load policy from file
 (6) Configure global alert settings
 (7) Configure alert destinations
 (8) View thresholds overview
 (9) Configure thresholds

 (e) Exit (m) Main Menu

Enter your choice (1-9) :
```

</td></tr>
<tr><td>6</td><td>Exit from the Threshold Engine Configuration menu.</td></tr>
<tr><td>7</td><td>

Stop the CPD daemon:

```
[Expert@HostName:0]# cpwd_admin stop -name CPD -path
"$CPDIR/bin/cpd_admin" -command "cpd_admin stop"
```

See *"cpwd_admin stop" on page 666*.

</td></tr>
<tr><td>8</td><td>

Start the CPD daemon:

```
[Expert@HostName:0]# cpwd_admin start -name CPD -path
"$CPDIR/bin/cpd" -command "cpd"
```

See *"cpwd_admin start" on page 663*.

</td></tr>
<tr><td>9</td><td>Wait for 10-20 seconds.</td></tr>
<tr><td>10</td><td>

Verify that CPD daemon started successfully:

```
[Expert@HostName:0]# cpwd_admin list | egrep "STAT|CPD"
```

See *"cpwd_admin list" on page 659*.

</td></tr>
<tr><td>11</td><td>In SmartConsole, install the Access Control Policy on Security Gateways and Clusters.</td></tr>
</table>

Threshold Engine Configuration Options

Menu item	Description
`(1) Show policy name`	Shows the name of the current configured threshold policy.
`(2) Set policy name`	Configures the name for the threshold policy. If you do not specify it explicitly, then the default name is "`Default Profile`".
`(3) Save policy`	Saves the changes in the current threshold policy.
`(4) Save policy to file`	Exports the configured threshold policy to a file. If you do not specify the path explicitly, the file is saved in the current working directory.
`(5) Load policy from file`	Imports a threshold policy from a file. If you do not specify the path explicitly, the file is imported from the current working directory.
`(6) Configure global alert settings`	Configures global settings: - How frequently alerts are sent (configured delay must be greater than 30 seconds) - How many alerts are sent

`(7) Configure alert destinations`	Configures the SNMP Network Management System (NMS), to which the managed Security Gateways and Cluster Members send their SNMP alerts.
	`Configure Alert Destinations Options:`
	`-------------------------------------`
	`(1) View alert destinations`
	`(2) Add SNMP NMS`
	`(3) Remove SNMP NMS`
	`(4) Edit SNMP NMS`

`(8) View thresholds overview`	Shows a list of all available thresholds and their current settings. These include: - Name - Category (see the next option "`(9)`") - State (disabled or enabled) - Threshold (threshold point, if applicable) - Description

Menu item	Description

`(9) Configure thresholds`	Shows the list of threshold categories to configure.
	`Thresholds Categories`
	`----------------------`
	`(1) Hardware`
	`(2) High Availability`
	`(3) Local Logging Mode Status`
	`(4) Log Server Connectivity`
	`(5) Networking`
	`(6) Resources`
	See the **Thresholds Categories** table below.

Thresholds Categories

Category	Sub-Categories

`(1) Hardware`	`Hardware Thresholds:`
	`--------------------`
	`(1) RAID volume state`
	`(2) RAID disk state`
	`(3) RAID disk flags`
	`(4) Temperature sensor reading`
	`(5) Fan speed sensor reading`
	`(6) Voltage sensor reading`

`(2) High Availability`	`High Availability Thresholds:`
	`-----------------------------`
	`(1) Cluster member state changed`
	`(2) Cluster block state`
	`(3) Cluster state`
	`(4) Cluster problem status`
	`(5) Cluster interface status`

`(3) Local Logging Mode Status`	`Local Logging Mode Status Thresholds:`
	`-------------------------------------`
	`(1) Local Logging Mode`

`(4) Log Server Connectivity`	`Log Server Connectivity Thresholds:`
	`-----------------------------------`
	`(1) Connection with log server`
	`(2) Connection with all log servers`

Category	Sub-Categories
(5) Networking	Networking Thresholds: ---------------------- (1) Interface Admin Status (2) Interface removed (3) Interface Operational Link Status (4) New connections rate (5) Concurrent connections rate (6) Bytes Throughput (7) Accepted Packet Rate (8) Drop caused by excessive traffic
(6) Resources	Resources Thresholds: --------------------- (1) Swap Memory Utilization (2) Real Memory Utilization (3) Partition free space (4) Core Utilization (5) Core interrupts rate

Notes:

- If you run the `threshold_config` command *locally* on a Security Gateway or Cluster Members to configure the SNMP Monitoring Thresholds, then each policy installation erases these *local* SNMP threshold settings and reverts them to the *global* SNMP threshold settings configured on the Management Server that manages this Security Gateway or Cluster.
- On a Security Gateway and Cluster Members, you can save the local Threshold Engine Configuration settings to a file and load it locally later.
- The Threshold Engine Configuration is stored in the `$FWDIR/conf/thresholds.conf` file.
- In a Multi-Domain Security Management environment:
    - You can configure the SNMP thresholds in the context of Multi-Domain Server (MDS) and in the context of each individual Domain Management Server.
    - Thresholds that you configure in the context of the Multi-Domain Server are for the Multi-Domain Server only.
    - Thresholds that you configure in the context of a Domain Management Server are for that Domain Management Server and its managed Security Gateway and Clusters.
    - If an SNMP threshold applies both to the Multi-Domain Server and a Domain Management Server, then configure the SNMP threshold both in the context of the Multi-Domain Server and in the context of the Domain Management Server.
      However, in this scenario you can only get alerts from the Multi-Domain Server, if the monitored object exceeds the threshold.
      Example:
      If you configure the CPU threshold, then when the monitored value exceeds the configured threshold, it applies to both the Multi-Domain Server and the Domain Management Server. However, only the Multi-Domain Server generates SNMP alerts.

Glossary

A

Active Security Management Server
The Management Server in Management High Availability that is currently configured as Active.

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster

Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member

Security Gateway that is part of a cluster.

Compliance

Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness

Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL

Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance

On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND

Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE

Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway

Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention

Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type

Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment

Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object

Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management

Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode

The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia

Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish

The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal

Web interface for the Check Point Gaia operating system.

H

Hotfix

Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection

Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA

Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness

Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging

Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Inline Layer

Set of rules used in another rule in Security Policy.

Internal Network

Computers and resources protected by the Firewall and accessed by authenticated users.

IPS

Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN

Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator

Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management High Availability
Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

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

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access

Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server

Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server

Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object

Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management

Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server

Physical computer manufactured and distributed by a company, other than Check Point.

P

Package Repository

Collection of software packages that were uploaded to the Management Server. You can easily install these packages in SmartConsole on the managed Security Gateways.

Permission Profile

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

Policy Layer

Layer (set of rules) in a Security Policy.

Policy Package

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

Primary Security Management Server

The Security Management Server in Management High Availability that you install as Primary.

Provisioning

Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS

Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule

Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base

All rules configured in a given Security Policy. Synonym: Rulebase.

S

Secondary Security Management Server

The Security Management Server in Management High Availability that you install as Secondary.

SecureXL

Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway

Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server

Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy

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

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

Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard

Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning

Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate

Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade

Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone

Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

Standby Security Management Server

The Security Management Server in Management High Availability that is currently configured as Standby.

T

Threat Emulation

Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction

Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object

Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering

Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Database

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

User Directory

Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

User Group

Named group of users with related responsibilities.

User Template

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

V

VSX

Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway

Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing

Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.