Important Information

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

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

To learn more, visit the Check Point Support Center

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Quantum Spark Portal R12.30 Administration Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 February 2021</td>
<td>Rebranded as Quantum Spark Portal</td>
</tr>
<tr>
<td>7 December 2017</td>
<td>Updated Configuring Large Scale VPN (on page 83).</td>
</tr>
<tr>
<td>23 July 2017</td>
<td>First release of this document</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Important Information ........................................................................... 3</td>
<td></td>
</tr>
<tr>
<td>Introduction to SMP ............................................................................... 9</td>
<td></td>
</tr>
<tr>
<td>Overview of the SMP ............................................................................. 9</td>
<td></td>
</tr>
<tr>
<td>Logging in to the SMP .......................................................................... 9</td>
<td></td>
</tr>
<tr>
<td>Managing Gateways with Plans ............................................................ 10</td>
<td></td>
</tr>
<tr>
<td>Managing the Gateway Settings from the SMP ....................................... 10</td>
<td></td>
</tr>
<tr>
<td>Using Software Blades and Services ..................................................... 10</td>
<td></td>
</tr>
<tr>
<td>Understanding the SMP Server ............................................................ 11</td>
<td></td>
</tr>
<tr>
<td>Implementing the SMP .......................................................................... 12</td>
<td></td>
</tr>
<tr>
<td>Creating a New Plan ............................................................................. 12</td>
<td></td>
</tr>
<tr>
<td>Using Software Blades .......................................................................... 13</td>
<td></td>
</tr>
<tr>
<td>Backing Up Gateway Settings to an FTP Server .................................... 13</td>
<td></td>
</tr>
<tr>
<td>Creating New Users ............................................................................... 14</td>
<td></td>
</tr>
<tr>
<td>Configuring Outgoing Mail Settings for Service Domains ...................... 14</td>
<td></td>
</tr>
<tr>
<td>SMP Scenarios and Workflows ................................................................ 15</td>
<td></td>
</tr>
<tr>
<td>Creating VPN Communities ..................................................................... 15</td>
<td></td>
</tr>
<tr>
<td>Configuring DNS Settings for the SMP Server ....................................... 16</td>
<td></td>
</tr>
<tr>
<td>Adding Gateways ................................................................................... 16</td>
<td></td>
</tr>
<tr>
<td>Managing Gateways behind NAT ............................................................ 18</td>
<td></td>
</tr>
<tr>
<td>Gateway Maintenance ............................................................................ 18</td>
<td></td>
</tr>
<tr>
<td>Upgrading a Gateway Remotely .............................................................. 18</td>
<td></td>
</tr>
<tr>
<td>Sending Security Reports ....................................................................... 19</td>
<td></td>
</tr>
<tr>
<td>Configuring Dynamic DNS for Gateways ................................................. 20</td>
<td></td>
</tr>
<tr>
<td>Configuring General SMP Settings ....................................................... 21</td>
<td></td>
</tr>
<tr>
<td>Using the SMP Portal ............................................................................ 21</td>
<td></td>
</tr>
<tr>
<td>Showing the SMP Status ........................................................................ 21</td>
<td></td>
</tr>
<tr>
<td>Showing Active User Sessions for Service Domains ................................. 22</td>
<td></td>
</tr>
<tr>
<td>Showing the Gateway Map View ............................................................. 22</td>
<td></td>
</tr>
<tr>
<td>Configuring Settings for the SMP Server ............................................... 23</td>
<td></td>
</tr>
<tr>
<td>Overview ............................................................................................... 23</td>
<td></td>
</tr>
<tr>
<td>Configuring General Settings for the SMP ............................................. 23</td>
<td></td>
</tr>
<tr>
<td>Configuring SMP Logging ....................................................................... 23</td>
<td></td>
</tr>
<tr>
<td>Configuring the SMP Portal to Use a Web Proxy Server ........................... 24</td>
<td></td>
</tr>
<tr>
<td>Configuring Outgoing Mail Settings for the SMP .................................... 25</td>
<td></td>
</tr>
<tr>
<td>Showing the SMP License ....................................................................... 25</td>
<td></td>
</tr>
<tr>
<td>Configuring SMP Backup Settings ......................................................... 26</td>
<td></td>
</tr>
<tr>
<td>Starting the SMP Backup ....................................................................... 26</td>
<td></td>
</tr>
<tr>
<td>Configuring the SMP Internal Certificate Authority ............................... 27</td>
<td></td>
</tr>
<tr>
<td>Configuring SMP Notifications ............................................................... 27</td>
<td></td>
</tr>
<tr>
<td>Configuring Management Access Control .............................................. 27</td>
<td></td>
</tr>
<tr>
<td>Configuring Admin Access Control ....................................................... 28</td>
<td></td>
</tr>
<tr>
<td>Managing Gateways .............................................................................. 29</td>
<td></td>
</tr>
<tr>
<td>Showing and Editing Gateways ............................................................. 29</td>
<td></td>
</tr>
<tr>
<td>Configuring General Settings ................................................................. 30</td>
<td></td>
</tr>
<tr>
<td>Setting the Gateway Location ................................................................ 30</td>
<td></td>
</tr>
<tr>
<td>Configuring Gateway Owners ............................................................... 31</td>
<td></td>
</tr>
</tbody>
</table>
Overview of the SMP

The Check Point SMP (Quantum Spark Portal) lets you centrally manage these small and medium business appliances:

- 600/1100
- 1200R
- 700/1400

The SMP provides a scalable and efficient mechanism to centrally configure and monitor Small/Medium Business gateways. You can use the SMP to create flexible business models and support different customers. The SMP lets you:

- Define different security policies and apply them to many gateways.
- Centrally manage VPN connections between different gateways.
- Generate network and security reports at regular intervals with information from all active Software Blades.
- Quickly search SMP and gateway logs.

Logging in to the SMP

Before you log in to the SMP, make sure you have a username and password for your Service Domain.

If you see a warning that the certificate for this site is not trusted, click Continue to safely use the SMP Portal.

SMP supports these Internet browsers:

- Firefox
- Chrome
- Internet Explorer 9 and higher

To log in to the SMP:

1. From the Internet browser,
Introduction to SMP

- If you use the Check Point Cloud Services, go here https://smbmgmtservice.checkpoint.com/SMP
- If you use a local server, go to https://<SMP Server IP address>/SMP or https://<SMP Server domain>/SMP

The Check Point Quantum Spark Portal login window opens.

2. From Domain, select or enter your Service Domain.
   For a new installation, there are no Service Domains to select.

3. Enter the Username and Password.

4. Click Login.
   The SMP Portal opens.

Managing Gateways with Plans

The SMP uses plans to manage gateways that share the same features or security settings. Each gateway that you define in the SMP is assigned to a plan. The gateways use all of the plan settings by default. You can manually unlock a gateway from specified features and Software Blades in the plan. See Locking and Unlocking Settings (on page 63).

Common situations for using different plans:

- Premium customers receive all security features and regular security reports.
- Basic customers receive only firewall and VPN functionality.
- Early adopters always receive the most recent firmware version.

Managing the Gateway Settings from the SMP

Use the SMP to centrally manage gateways and configure the appliances. The SMP lets you easily search for gateways and configure the settings. To configure a single appliance, you can connect to the Portal with a single click.

After the gateway connects to the SMP, the gateway contacts the SMP at specified intervals to get the most recent settings.

If the gateway finds a change, it downloads only the changed settings. The gateway does not reboot when it applies the new settings from the SMP.

**Note** - When you upgrade the gateway firmware, the gateway automatically reboots.

There may be a five minute interval before the new settings are applied to the gateway.

After you connect a gateway to the SMP, all the settings controlled by the SMP show a lock icon. You can configure these settings only from the SMP and not from the gateway Portal.

Using Software Blades and Services

The SMP lets you configure Software Blades and Services to help manage the gateway settings. You can access these from Home > Gateways.
Software Blades

Software Blades let Small/Medium Businesses manage the security requirements for their networks. Each blade is a security building block that is managed by the SMP. The gateway enforces the configured security settings on the network traffic.

Services

Each Service runs on the gateway based on the policy configured in the SMP. The Services define these behaviors and settings between the gateway and the SMP:

- Managed Services
- Firmware
- Periodic Backup
- Reports
- Report Recipients
- Dynamic DNS

Understanding the SMP Server

The SMP Portal runs on a Windows server. The server can be located on premises for a company, or in the Check Point cloud.

For on premise deployments, SMP must be installed on a Windows 2008 or 2012 R2 64-bit server.

To learn more about how to install the SMP Server, see the SMP Installation Guide for your version.
Implementing the SMP

In This Section:

Creating a New Plan ................................................................. 12
Creating New Users ................................................................. 14
Configuring Outgoing Mail Settings for Service Domains .............. 14

This chapter helps you to configure and implement the SMP for the first time.

Best Practices:

• Create a plan for gateways with common features and security policy settings.
• Create user accounts for system administrators.
• Configure the email settings so customers can easily communicate with you.

Creating a New Plan

A plan is a template that lets you define the settings for a group of gateway features. Each gateway is assigned to a plan and inherits the settings of the plan. You can also choose to override the specified plan settings for the gateway.

The SMP uses a wizard to help you configure the services and Software Blades for a new plan. After you complete the wizard, you can edit these settings.

• For plans that use VPN communities, see Creating VPN Communities (on page 15).
• For plans that support the Dynamic DNS service, see Configuring DNS Settings for the SMP Server (on page 16).

Note - Make sure that the applicable ports are open between the SMP and the gateways.

To create a new plan:

1. Go to Home > Plans.
2. Click New.
   The Create New Plan wizard opens.
3. Enter a Name [cannot be changed after you save] and a Description [optional].
4. Click Next.
   The Supply the following services window opens.
5. Select the services for the plan.
6. Click Next.
   The Activate the following Security Software Blades window opens.
7. Select the Software Blades for the plan.
8. Click Next.
9. Click Finish.
   The Edit window opens and shows the General tab.
Using Software Blades

You can activate these Software Blades on plans or gateways:

- **Firewall** - Makes sure that only specified traffic is allowed to enter the internal network.
- **Access Policy** - Create rules on the SMP for a specified plan or gateway.
- **Application & URL Filtering** - Monitors and control how a company uses the Internet.
- **IPS** - Analyzes traffic to detect and prevent known and future threats.
- **Traditional Anti-Virus** and **Anti-Virus** - Inspects connections to the Internet and scans file transfers and downloads to the internal network to find and prevent malware attacks.
- **Anti-Spam** - Eliminates unwanted emails and spam.
- **QoS** (Quality of Service) - Prioritizes business-critical traffic, such as database and Web services traffic, over less time-critical traffic.
- **Remote Access** - Creates secure connections and lets remote users easily use the Internet to connect to access internal networks.
- **Site to Site VPN** - The gateway creates a VPN connection with other gateways and they can share network resources.
- **User Awareness** - Enforces access control for individual users and groups.
- **Anti-Bot** - Automatically scans for bot-infected hosts and for communications with a C&C (Command and Control).
- **Threat Emulation** - Scans for infected files that are downloaded from the Internet or attached to emails.
  - **Note** - Threat Emulation is supported only for 700/1400/1200R appliances with versions R77.20.51 and higher.
- **Threat Prevention Policy** - Configure the confidence and performance settings for Anti-Virus, Anti-Bot, and Threat Emulation protections.

Backing Up Gateway Settings to an FTP Server

Back up the settings for the gateways in a plan to an FTP server. A separate backup file is created for each gateway. After you create a new plan, you can configure the FTP backup settings in the **Periodic Backup** window.

Use the gateway Portal to restore the settings from a backup file. For more about reverting a gateway, see the Administration Guide for your appliance.

To back up the gateway settings for a plan:

1. Go to **Home > Plans**.
2. Click the plan name.
   The **Edit** page opens.
3. Click **Services > Periodic Backup**.
4. Configure the settings to back up the gateways in this plan.
Creating New Users

Create new users with the **New User** wizard. For each user, you must:

- Assign a role that defines the privileges.
- Configure an expiration date for the user account.

**To create a user:**

1. Go to **Home > Users**.
2. Click **New**.
   The **Create New User** window opens.
3. Enter the information for the user.
   - **User ID** - The login name for this user. Click the Generate icon to create a random User ID.
     **Note** - After you save the User ID, you cannot edit or change it.
   - **First Name** and **Last Name**
   - **Email** - Enter the email address that SMP uses to contact the user.
4. Select a **Role** and enter a **Password** for the user.
   The Role defines privileges for the user.
5. Click **Finish**.
   The **Edit** user window opens and shows the details for the user.

Configuring Outgoing Mail Settings for Service Domains

The SMP sends emails to gateway owners. Configure the name and email address that the gateway owners use to reply to these emails.

**To configure the settings for outgoing emails:**

1. Go to **Service Domain > Settings**.
   The **Settings** page opens and shows the **General** tab.
2. Click **Mail**.
3. In **"Reply To:" Email Address**, enter the email address to send replies.
   This address appears in all reports, Service Domain notifications, and custom alerts sent by the SMP.
4. In **"Reply To:" Friendly Name**, enter the name in the **From** field.
5. Click **Save**.
Creating VPN Communities

Use a VPN community to create VPN site-to-site connections between gateways in a group. There are two types of VPN communities:

- A Full Mesh VPN Community connects all member gateways. Each gateway has a secure connection with other gateways. You can use this community to connect several offices to each other.
- A Star VPN Community connects multiple satellite gateways to a center gateway. Each gateway has a secure connection to the center. You can use this community to connect branch offices to a central headquarters.

To access the internal network resources, you must configure the internal network topology in the SMP. If the gateway is not configured for this topology, the internal network resources are available only to users in the same internal network. Users from other networks in the same community cannot access these internal network resources.

The SMP supports VPN communities that include an externally managed gateway.

To prepare a gateway to join a VPN community:

1. Go to click **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **VPN > Internal Network Topology**.
4. Configure the settings.

To create a VPN community:

1. Go to **Home > Communities**.
   The **Communities** page opens and shows the VPN communities.
2. Click **New**.
   The **Create New Community** wizard opens.
3. Enter these values:
   - **Name** - Name for the community (you cannot change it later).
   - **Description** - Optional description of the community.
4. Click **Finish**.
   The wizard closes and the **Edit Communities** window shows the new VPN community.
To edit the settings:
1. Click the community name.
   The Edit page opens.
2. Configure these settings for the community:
   • General Settings
   • VPN Settings
   • IKE Settings
3. From the Members window, click Add Gateway.
   The Add Gateways Wizard opens.
4. Complete the wizard and add the gateway to the community.
   You can add additional gateways.

For more information on VPN community configuration, see Configuring a VPN Community with External Gateways (on page 81).

Configuring DNS Settings for the SMP Server

For deployments that use on premises SMP Servers, the SMP DNS settings are different when there is one server or multiple servers. We recommend that you go to:

- Server Edit > Settings to configure DNS settings for deployments with one SMP Server.
- Settings > General to configure DNS settings for deployments with multiple SMP Servers.

Note - Make sure that the IP addresses on the Windows interface are configured correctly.

To configure the DNS settings for one SMP Server:
1. Go to System > SMP Servers.
   The SMP Servers page opens and shows a list of servers.
2. Click the server name.
   The Server Edit page opens and shows the Configure tab.
3. Click Settings.
4. Enter the DNS Name.
5. Click Save.

To configure the DNS settings for multiple SMP Servers:
1. Go to System > Settings.
   The Settings page opens.
2. Click General.
3. In SMP System DNS Name, enter the DNS name for the primary SMP Server.
4. Click Save.
5. Repeat for each SMP Server.

Adding Gateways
- To create a gateway, do the procedure below. To assign an owner, see Configuring Gateway Owners (on page 31).
To create a user, see Showing Users (on page 100). To add gateways, see Managing Gateways for a User (on page 105).

**To add a new gateway:**

1. Click Home > Gateways > New.  
The Create New Gateway window opens.  
2. Enter a Name or click Generate for a system generated name.  
3. Select Type.  
4. Clear Managed by SMP to create this gateway as an externally managed gateway.  
5. Select a Plan from the list. By default, the gateway inherits its default settings from this plan.  
6. The Registration Key field shows an automatically generated registration key. You can enter a registration key or click Generate to generate a new registration key.  
7. Enter a user name for Owner ID. Click Search to find an existing user or click New to create a new user.  
8. Complete the wizard instructions.  
9. Click Finish.  
The Home > Gateways > Edit window opens. The options you see depend on the plan you selected.  

After the gateway is created, the gateway owner receives an email that contains an activation link and the registration key.  
The activation key has 3 parts:  
- SMP IP address/DNS  
- `<Gateway Name, Service Domain>`  
- Registration Key (first auto generated and then set by the owner)  
If there is no object name, it appears as "-" in the activation key. The object is automatically created and the name is seen in the activation key when the gateway tries to connect.

**To enable automatic gateway creation:**

1. In Plans, click a plan name.  
The Edit page opens.  
2. Click Gateway Activation.  
3. Select Allow automatic gateway creation.  
4. Set a Registration Key.  
5. Gateways that use the on-screen Registration Key are automatically connected to the SMP and managed by this plan. There is no need to create a gateway object (in the SMP) prior to the activation.  

You can send the activation key to all the gateways that you want to connect through this plan.  
The email with the activation link also contains information on how to connect the appliance:  
- **If the appliance is set up** - When the gateway owner clicks the link, the login window to the WebUI application opens. After the owner logs in, the Cloud Services page opens and shows the activation details. The owner confirms the details and establishes a connection with the SMP.  
- **If the appliance is not set up** - When the gateway owner clicks the link, it opens the First Time Configuration Wizard. After the wizard is completed, the Cloud Services page opens and shows
the activation details. The owner confirms the details and establishes a connection with the SMP.

- **If Cloud Services is already activated in the appliance** - When the gateway owner clicks the link, the login window opens. After the owner logs in, the Cloud Services page opens and shows the activation details. The owner selects one of these options:
  - Clear the current services provider settings and connect to the SMP with the new provider details.
  - Stay connected to the current services provider.
- **If the link does not work** - The owner logs in to the appliance WebUI > Home > Cloud Services page, manually enters the registration key sent in the email, and connects to the SMP. If the owner did not receive the email, the SMP administrator should send the activation key to the owner to enter it manually.

⚠️ **Important** - When an appliance is behind a NAT device, you must enable the gateway to communicate with the SMP.

### Managing Gateways behind NAT

When a gateway is located behind a NAT device, the SMP does not have the correct IP address to communicate. Configure the SMP and gateway to use the correct NATed IP addresses.

**To manage a gateway behind NAT:**
- In the gateway Portal, enable the appliance to connect to SMP with the Check Point SMB Relay
- Define NAT port forwarding rules to enable communication between the appliance and the Service Domain

### Gateway Maintenance

#### Upgrading a Gateway Remotely

Use the SMP to manage the gateway firmware upgrades. You can manage the firmware upgrade for:

- A specified gateway
- All the gateways in a plan

**To upgrade all the gateways in a plan:**

1. Go to Home > Plans.
   - The Plans window opens.
2. Click the plan name.
   - The Edit page opens.
3. Click Services > Firmware.
4. Configure the firmware settings:
   - **Specific firmware version** - Select a specific firmware to each appliance type or set it to Do_Not_Upgrade.
- **Check Point latest** - The gateway is set to download the latest firmware version available from the Check Point Download Center.
- **The firmware is managed locally on the device** - Firmware upgrades are managed locally on the appliance.

5. Schedule automatic firmware upgrades.
   - **Upgrade immediately**.
   - **Daily** - Select the time of day range.
   - **Weekly** - Select the day of week and time of day range.
   - **Monthly** - Select the day of month and time of day range.

6. Click **Save**.

**To upgrade a specified gateway:**

1. Search for the gateway in the **Search field** at the upper right of the WebUI.
   Or
2. Go to **Home > Gateways** and click the gateway name.
   The **Edit** page opens.
3. Click **Services > Firmware**.
4. Click **Unlock from plan** to overwrite the plan settings.
5. Configure the firmware settings as above.
6. Click **Save**.

**Sending Security Reports**

Security reports show the gateway owner a summary of the security and network activity for the time interval.

You can send reports:
- **Daily**
- **Weekly**
- **Monthly**

Configure the SMP to send reports to:
- All the gateway owners in a plan
- Each gateway owner individually

**To send Security reports to all the gateways in a plan:**

1. Go to **Home > Plans**.
2. Click a plan name.
   The **Edit** page opens.
3. Click **Services > Managed Services**.
4. Click **Send periodic reports**.
5. Click **Save**.
6. Click **Services > Reports**.
7. Select **Report type** and **Reports language**.
8. Select the time interval.
9. Click **Save**.

**To send Security reports to one gateway:**

1. Search for the gateway name
   
   or
2. Go to Home > Gateways and click a gateway name.

   The **Edit** page opens.
3. Click **Services** > **Managed Services**.
4. Click **Send periodic reports**.
   
   **Note** - You may have to click **Unlock from plan** first.
5. Click **Save**.
6. Select **Services** > **Reports**.
7. Select **Report type** and **Reports language**.
8. Select the time interval.
9. Click **Save**.

---

**Configuring Dynamic DNS for Gateways**

Dynamic DNS lets users log in to the Portal of an appliance when the IP address changes. For more about configuring the SMP Server for Dynamic DNS, see *Using a Dynamic DNS Deployment* in the *R12.30 SMP Installation Guide*.

**To configure Dynamic DNS for gateways:**

1. Create a plan that includes the Dynamic DNS service.
   
   Select the **Dynamic DNS** service on the applicable page in the **Plan** wizard.
2. Assign gateways to the plan.
3. **Optional** - Configure the DNS settings for each gateway.
   
   These settings let you define additional DNS aliases to access the gateway.
Configuring General SMP Settings

In This Section:

- Using the SMP Portal ............................................................... 21
- Showing the SMP Status ....................................................... 21
- Showing Active User Sessions for Service Domains .......... 22
- Showing the Gateway Map View ......................................... 22
- Configuring Settings for the SMP Server ......................... 23

The Service Domain is the SMP virtual portal your company uses. The Service Domain settings apply to all plans and gateways.

Using the SMP Portal

The SMP Portal uses these buttons:

<table>
<thead>
<tr>
<th>Button or drop-down menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates a new object, for example a plan or a gateway.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes to the object. Note - If you configure settings for an object, the settings are only applied after you click Save.</td>
</tr>
<tr>
<td>Revert</td>
<td>Changes the object settings to previously saved values.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the window.</td>
</tr>
<tr>
<td>Filter</td>
<td>Opens a new window to filter objects based on the search parameters.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the object.</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>Opens the Portal for the gateway in a new window.</td>
</tr>
<tr>
<td>View</td>
<td>Shows additional reports for an object.</td>
</tr>
<tr>
<td>Actions</td>
<td>Shows additional actions for an object.</td>
</tr>
</tbody>
</table>

Showing the SMP Status

The Home > Overview Status page shows basic information about the Service Domain for the SMP.

To show the Status window:

1. Go to Home > Overview.
   The Overview page opens and shows the Status tab.
2. To show all the gateways that the SMP manages, click Show All.
3. In the **Gateways** section, click **Show** to see the gateway status:
   - **Connected** - Managed by the SMP.
   - **Not Connected** - These gateways are not connected. They are managed by the SMP when connected.
   - **Disabled** - Not managed by the SMP.
4. In the **Plans** section, click **Show**.
5. To create an Excel file with a report of the objects in the Service Domain, click **Generate Report**.

### Showing Active User Sessions for Service Domains

For users defined in the Service Domain, you can show a list of currently active sessions. For each user session, this information shows:

- SMP User ID.
- The date and time the user logged in to start the session (**Creation Date**).
- The IP address from which the user connected.

**To view user sessions for Service Domain:**

1. Go to **Home > Overview**.
   - The **Overview** window opens and shows the **Status** tab.
2. Click the **Sessions** tab.
3. To refresh the information on this page, click **Refresh**.

### Showing the Gateway Map View

The **Map View** shows the physical locations of gateways connected to the Service Domain. The icon color shows if the gateway is connected, disconnected, or disabled.

If the window shows a **Map Permission Error**, click **Continue in trial mode** to use the 30-day trial license.

Multiple gateways at a near location are clustered together. You can click on the cluster and zoom in to show those gateways. The clusters show rings in these colors:

- Green - All the gateways are connected to the SMP.
- Yellow - One or more gateways are disconnected from the SMP.
- Red - All the gateways are disconnected from the SMP.

When a gateway is connected to the SMP, you can set the gateway location. See Setting the Gateway Location (on page 30).

**To show the Map View window:**

1. Go to **Home > Map**.
2. Click a gateway icon.
   - The **Gateway Details** window opens and shows information about the gateway:
     - **Name** - The gateway status shows (connected - green, disconnected - red). Click the name to open the **Edit** page for this gateway.
Configuring General SMP Settings

- **IP address** - Click to open the Portal of the gateway in a new tab.
- **Plan** - Click to open the Edit page for this plan.
- **Owner** - Click to open the Edit page for this user.
- **MAC address**
- **Directions to the gateway location**

Configuring Settings for the SMP Server

**Overview**

The **System > Settings > Overview** page shows the status and numbers of:

- Connected Gateways
- Disconnected Gateways
- Disabled Gateways
- Active Service Domains
- Disabled Service Domains
- Logged in Users

**To refresh the display:**

Click **Refresh**.

Configuring General Settings for the SMP

To configure general settings:

1. Go to **System > Settings**.
   The **Settings** page opens.
2. Click **General**.
3. For **SMP System DNS Name**, enter the DNS name of the active or primary server (for deployments that use multiple SMP Servers).
4. For **Minimum user password length**, enter a value between 7 - 25.
5. For **Default registration key length**, enter a value between 8 - 20. This is the number of characters used to generate a new Registration Key.
6. For **Gateways keep-alive interval (seconds)**, enter a time interval.
7. To generate a report that summarizes the SMP settings, click **Generate Report**.
   The Internet browser saves the report as an Excel file.
8. Click **Save**.

Configuring SMP Logging

You can configure logging for the SMP Server. SMP system logs are all logs that are not specific to a certain Service Domain.
Use the Log Level option to configure the minimum log severity level that is written to the General Logs table. For example, if you select Alert, all logs with the severity level of Alert and Emergency are written to the General Logs table.

You can define old logs as older than a specified number of days, and specify if these logs are automatically deleted, or are compressed and moved to an archive folder.

To show the Logging page:
1. Go to System > Settings.
2. Click Logging.

To configure the severity level for the logs:
1. Go to System > Settings > Logging.
2. In Log Level, select the severity level.
3. Click Save.

To configure the SMP Server as a Syslog client for system logs:
1. Go to System > Settings > Logging.
2. In System Logs Logging, select Forward logs to an external Syslog Server.
3. In Syslog Server, enter the Syslog server IP address.
4. In Syslog Port, enter the port used to send Syslog messages.
5. Click Save.

To configure log file storage for SMP system logs:
1. Go to System > Settings > Logging.
2. In System Logs Logging, select Purge old logs.
3. In Older than, enter the number of days that log files are saved in the SMP.
4. For Action:
   - To automatically delete old logs, select Delete.
   - To compress old logs and move to an archive folder, select Archive. Add the path where the logs are archived.
5. Click Save.

Configuring the SMP Portal to Use a Web Proxy Server

If your network requires a Web proxy server to access the Internet, you must configure the SMP Portal.

To configure the Portal to use a Web proxy server:
1. Go to System > Settings.
   The Settings page opens.
2. Click HTTP Proxy.
3. Click Use a proxy server.
4. For Proxy host, enter the domain or IP address of the proxy server host.
5. For Proxy port, enter the proxy server port.
6. For Proxy user, enter the user name.
7. For **Proxy password**, enter the password.
8. Click **Save**.
   You must now restart the SMP.
9. Log in to the SMP Server.
10. From the Windows Start menu, go to **Administrative Tools > Services**.
11. Restart the Apache-Catalina service.

**Configuring Outgoing Mail Settings for the SMP**

If SMP system notifications are enabled, you must configure the settings for the outgoing mail server.

SMP Server only uses the default SMTP port (25) for outgoing emails.

**To configure outgoing mail settings for the SMP:**

1. Go to **System > Settings**.
   The **Settings** page opens.
2. Click **Mail Settings**.
3. For **SMTP Server**, enter the IP address or domain for the outgoing mail server.
4. For "**Reply To:** email address", enter the email address to send replies. This address appears in all SMP system notifications.
5. For "**Reply to:** friendly name", enter the name that shows in the **From** field.
6. Select **Use authenticated SMTP** if the SMTP server requires authentication.
7. Click **Save**.

**Showing the SMP License**

The SMP is licensed to manage the specified number of gateways. Add additional licenses to increase the number of managed gateways.

For deployments with multiple SMP Servers, we recommend that you use the CLI or Check Point Configuration Tool to add licenses to Secondary servers. See Managing Licenses without the Portal (on page 128)

**Note** - Make sure that the IP address for the license is a real IP address for an interface that is configured on SMP Server. Do not use 127.0.0.1 as the IP address for the license.

**To show the SMP system license:**

1. Go to **System > Settings**.
2. Click **License Management**.
3. Click **View License**.

**To add a license:**

1. Go to **System > Settings > License Management > View License**.
2. Click **Add License**.
   The **Add SMP License** wizard opens.
3. For **IP address**, enter the SMP Server IP address.
4. For **Expiration date**, enter the date that the SMP license expires.
5. For **Signature**, copy and paste the string for the license.
6. For **SKU**, Copy and paste the SKU for the license.
7. Click **Finish**.
8. Click **Apply License**.
9. Click **Save**.

### Configuring SMP Backup Settings

System backup settings are used for both automatic and manual SMP configuration backup.

**To save the back-up file:**
- For SMP Servers located in the Check Point Cloud Services, upload the back-up file to an FTP server.
- For on-site SMP Servers, you can upload the file to an FTP server or save it to a local folder. The default path is the installation folder: `c:\Checkpoint\SMP\`

**To configure SMP backup settings:**

1. Go to **System > Settings**.
2. Click **System Backup**.
3. To enable automatic backups, click **Perform** and select the time frame:
   - Daily
   - Weekly
   - Monthly
4. In **File Storage**, select **Upload backup file to FTP**.
5. Enter the **FTP server**, **Path on server**, and **Password**
   Or
   Click **Save the file** and enter the path.
6. In **File Name**, select **Automatically generate filename** or **Use static filename**.
7. If you select **Use static filename**, enter the **Filename** for the backup file.
8. Select **Overwrite file if already exists**.
   **Note** - If there is a backup file with the same name, the backup operation stops if you do not select this option.
9. Click **Save**.

### Starting the SMP Backup

**To manually start the SMP system backup status:**

1. Go to **System > Settings**.
2. Click **System Backup > Status**.
3. Click **Run Now**.
   A confirmation window opens.
4. Click **OK**.
5. To refresh the fields, click **Refresh**.
Configuring the SMP Internal Certificate Authority

After you initialize the internal CA, configure the certificate settings.

**To configure certificate settings:**

1. Go to **System > Settings**.
2. Click **Certificate Authority**.
3. For **The root certificate expires every**, enter the number of months after CA initialization that the CA root certificate expires.
4. For **Automatically renew** (in **Root Certificate**), enter when the root certificate is automatically renewed.
5. For **The gateway certificate expires every**, enter the number of months.
6. For **Automatically renew** (in **Gateway Certificate**), enter the number of months before expiration when the gateway certificate is automatically renewed.
7. For **Revocation answer is valid for**, enter the number of hours the gateway stores the answer in the cache.
8. Click **Save**.
9. Click **Reinitialize CA**.
10. To export the certificate to a file, click **Export X.509**.

When the root certificate is renewed, the CA is reinitialized. All the certificates for the gateways are automatically renewed.

When gateways authenticate to each other, each gateway performs online revocation and checks with the Security Management Server to verify that the other gateway's certificate has not been revoked. To enhance VPN performance, the gateway then caches this answer. The revocation answer is purged from the cache after the specified period.

Configuring SMP Notifications

Configure the notifications for the:

- **SMP Server**
- **Service Domains**

Configuring Management Access Control

**Management Access Control** lets you define the only IP addresses and subnets that can log in to the SMP. When you enable this feature, unauthorized IP addresses are blocked and cannot connect to the SMP Portal.

**Note** - The localhost address (127.0.0.1) is always allowed and you cannot block it.

**To define an allowed IP address:**

1. Go to **System > Settings > Access Control**.
2. Click **Management Access Control**.
3. Click **Allow web access (HTTPS) to the SMP from the following IP addresses and subnets**.
4. Click **New**.
   - The **Management Access Control** window opens.
5. From **Source Type**, select **IP Address** or **Network**.
6. Enter the **IP address**.
   If the **Source Type** is **Network**, you must also enter the **Subnet Mask**.

7. Click **Finish**.

8. Click **Save**.

**To allow all IP addresses:**
1. Click **Allow web access (HTTPS) to the SMP from any IP address**.
2. Click **Save**.

**To delete an allowed IP address or subnet:**
1. Select one or more IP addresses and subnets.
2. Click **Delete**.
3. Click **Save**.

### Configuring Admin Access Control

The **Admin Access Control** page lets you define the only IP addresses and subnets that administrators can use to log in to the SMP. When you enable this feature, administrators cannot log in to the SMP from unauthorized IP addresses.

**To define an allowed IP address:**
1. Go to **System > Settings > Access Control**.
2. Click **Admin Access Control**.
3. Click **Allow administrators to login only from the following IP addresses and subnets**:
4. Click **New**.
   The **Administrator Access** window opens
5. For **Source Type**, select **IP Address** or **Network**.
6. Enter the **IP address**.
   If the **Source Type** is **Network**, you must also enter the **Subnet Mask**.
7. Click **Finish**.
8. Click **Save**.

**To delete an allowed IP address:**
1. Click the checkbox next to the IP address.
2. Click **Delete**.

**To allow all IP addresses:**
1. Click **Allow administrators to login from any IP address**.
2. Click **Save**.
Managing Gateways

In This Section:

- Showing and Editing Gateways................................................................. 29
- Using Plans for Gateways ...................................................................... 62
- Locking and Unlocking Settings.............................................................. 63
- Searching for Gateways.......................................................................... 64
- Exporting Gateway Information............................................................... 67
- Sending Email to Gateway Owners.......................................................... 68
- Deleting Gateways.................................................................................. 68
- Accessing Local Gateways..................................................................... 68

Showing and Editing Gateways

In the Home > Gateways page you can:

- Add a new gateway
- Search for a specified gateway
- Delete a gateway
- Export gateway information to Excel
- Send emails to gateway owners
- Reset all settings of a gateway to its plan simultaneously
- See or edit the details of a gateway
- Access a gateway

To see or edit the properties of a gateway:

1. Go to Home > Gateways.
2. Click the gateway Name.
   The Edit page opens.
3. Select a node to see or edit.

To connect to a local gateway in Home > Gateways:

1. Click the IP Address for the local gateway.
2. If a security warning message shows, confirm it and continue.
   A browser page opens and shows the progress of the SMP connection to the gateway.
3. If a local administrator is already logged in to the appliance, click OK to override that connection. Click Cancel to cancel your login attempt.
   When logged in, you can update the local appliance.

Note - The certificate for the gateway is a self-signed certificate. When you show information for the certificate, the “Issued to” and “Issued by” fields show a unique string. The syntax of this string includes my.gateway and the gateway MAC address.
To make sure that the gateway you connect to is correct, check that the MAC address in the middle part of the string matches the gateway’s. You can find the MAC address of the gateway in the General tab of the gateway.

To connect to a local gateway:
In the Edit page, click Access gateway.

Configuring General Settings

To configure general settings for a gateway:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Enter a Description.
4. To enable the gateway, click Enabled. If you clear this option, the gateway is disabled and cannot connect to the SMP.
5. Select Managed by for the SMP to manage the gateway.
6. Select a Plan for the gateway to specify the settings.
7. Enter the MAC address. This field is automatically entered when the gateway connects to the SMP for the first time.
8. For gateways that are not managed by the SMP, enter the gateway’s Static IP address.
9. Enter the Registration Key or click the Generate icon to randomly generate a new key.
10. Enter the Activation Key sent to the gateway owner in an email.
11. To set the physical location of the gateway on the map, in Search, enter the location of the gateway
    Or
    In the map, click the location of the gateway.
12. Click Save.

Setting the Gateway Location

The Location page lets you set the physical location of the gateway.

To set the gateway location manually:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Location.
4. In the Search an address field, enter the gateway location or click the map.
   The map shows the gateway.
5. Click Save.
   A text message above the map states that you set the gateway’s location manually.

The location of a manually configured gateway shows on the map as a blue icon.
To clear a manually set location:
Click the **Clear location** link.

**Configuring Gateway Owners**

You can add or remove an owner from the gateway owner list. A gateway can have only one owner.

When you set a new gateway owner and save the configuration, an activation email is sent to the appliance owner. This email contains an activation link and the registration key (if manual activation is necessary).

- **If the appliance is set up** - When the gateway owner clicks the link, the login window to the WebUI application opens. After the owner logs in, the Cloud Services page opens and shows the activation details. The owner confirms the details and establishes a connection with the SMP.
- **If the appliance is not set up** - When the gateway owner clicks the link, it opens the First Time Configuration Wizard. After the wizard is completed, the Cloud Services page opens and shows the activation details. The owner confirms the details and establishes a connection with the SMP.
- **If Cloud Services is already activated in the appliance** - When the gateway owner clicks the link, the login window opens. After the owner logs in, the Cloud Services page opens and shows the activation details. The owner can select one of these options:
  - Clear the current services provider settings and connect to the SMP with the new provider details.
  - Stay connected to the current services provider.
- **If the link does not work** - The owner logs in to the appliance WebUI > Home > Cloud Services page, manually enters the registration key sent in the email, and connects to the SMP.

**To add an owner to a gateway:**

1. Go to **Home > Gateways**.
2. Click the gateway name. The Edit page opens.
3. Click **Owner**.
4. Click **Set**.
   The **Add User** wizard opens.
5. To add an existing user, enter the User ID.
6. Click **Next** and then **Done**.

**To search for users:**

1. In **Home > Gateways > Edit > Owner**, click **Set**.
   The **Add User** wizard opens.
2. Select **Search for users**.
3. Click **Next**.
4. Select the options from the drop-down lists.
5. Click **Next**.
6. The **Add User** window opens with a list of users.
7. Select the applicable user.
Managing Gateways

Note - You cannot assign a specific gateway to more than one user.

8. Click Next.
10. Click Done.
11. To create a new user, see Creating New Users (on page 14).
12. Click Save.

To remove an owner from a gateway:
1. In Home > Gateways > Edit, click Owner.
   The Owner fields are shown.
2. Click Remove.
   A confirmation message opens.
3. Click OK.
   The owner is removed from the gateway.
4. Click Save.
Note - The owner is not deleted from the user database. Only the association between the gateway and the user is deleted.

Showing Gateway Status

To see the gateway status:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Status.
   The Status page opens and shows this information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>The date and time the gateway was added to the SMP.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>The time and date that the gateway was last modified.</td>
</tr>
<tr>
<td>Last Connection Day</td>
<td>The date that the gateway last connected to the SMP.</td>
</tr>
<tr>
<td>Last Connected IP Address</td>
<td>The IP address of the appliance when it last connected to the SMP.</td>
</tr>
<tr>
<td>Reported Firmware</td>
<td>The firmware version that the gateway uses.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>The status of the connection between the gateway and the SMP [Connected/Not Connected].</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>The time and date when the gateway status last changed. Shows only when the gateway is connected to the SMP.</td>
</tr>
<tr>
<td>Current Server</td>
<td>The CMLS server name to which the gateway is connected. Shows only when the gateway is connected to the SMP.</td>
</tr>
<tr>
<td>Connection Address</td>
<td>The gateway’s current IP address. Shows only when the gateway is connected to the SMP.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Sync Status</td>
<td>Shows Success or Error.</td>
</tr>
<tr>
<td>Last Sync Time</td>
<td>Shows the date and time that the gateway status was last changed.</td>
</tr>
<tr>
<td></td>
<td>Shows only when the gateway is connected to the SMP.</td>
</tr>
<tr>
<td>Error Details</td>
<td>Shows only if there is an error.</td>
</tr>
</tbody>
</table>

### Showing Gateway Logs

The **Gateway Logs** window shows the last 50 log records.

To load more records, scroll down the page. The log table is automatically refreshed.

**Note** - To see Gateway logs, you must select **Store gateway logs** in **Services > Managed Services**.

#### To show gateway logs:
1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Logs**.
   A table with log entries shows.

#### To search for a log:

Enter your query in the search query box. You can search for multiple fields at a time using Boolean operators (AND|OR|NOT).

For more details, click **Query Syntax** in the table header.

#### To see the logs for a specified Software Blade:

From the **All blades** list, select the Software Blade.

The table is refreshed and shows the applicable logs.

#### To show specified fields in the table:

From **View > Columns**, select the checkboxes of the fields to show.

The table is refreshed and shows the selected fields. The changes made are local to the gateway.

#### To see the logs for a specified time frame:

From the **Anytime** list, select one of these options:
- Last 24 hours
- Last week
- Anytime

#### To see the log record:

1. Select a log entry from the list.
2. Click **Details** or double-click the log.
   The **Log Details** window opens.
To refresh the log data:
Click the Refresh icon.

Note - You can also click Logs > Gateway Logs to see the log entries.

Configuring Device Settings

The Device Settings section lets you configure these settings for gateways or a plan:

- NTP
- Time Zone
- DNS
- Gateway Administrators

These features are only supported on R77.20 and higher gateways.

**NTP**

Use an NTP server to configure the SMP to synchronize time settings for specified plans and gateways.

This feature is only supported on R77.20 and higher gateways.

**To configure the NTP settings of a plan:**

1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Device Settings > NTP.
4. Select Manage in SMP.
5. Enter the host name or IP address for the Primary and Second NTP Server.
6. In Update Interval, enter the time interval in minutes that SMP contacts the NTP server to update the time settings.
7. Optional - To configure the settings to authenticate to the NTP server, click NTP Authentication and enter the Shared Secret and Shared Secret Identifier.
8. Click Save.

**To override the NTP settings set by a plan:**

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Device Settings > NTP.
4. If the NTP settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Configure the NTP settings (see above).
7. Click Save.

**To connect to the appliance:**

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click **Device Settings** > **NTP**.
4. Click **Access Gateway: Date and Time**.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the **Date and Time** page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Time Zone**

Configure the Time Zone settings for the specified plans and gateways.

This feature is only supported on R77.20 and higher gateways.

**To configure the Time Zone settings of a plan:**
1. Go to **Home** > **Plans**.
2. Click the plan name.
   The Edit page opens.
3. Click **Device Settings** > **Time Zone**.
4. Select **Manage in SMP**.
5. In the **Local Time Zone** list, select the correct time zone option.
6. Select **Automatically adjust clock for daylight saving changes** to enable automatic daylight saving changes.
7. Click **Save**.

**To override the Time Zone settings set by a plan:**
1. Go to **Home** > **Gateways**.
2. Click the gateway name.
   The Edit page opens.
3. Click **Device Settings** > **Time Zone**.
4. If the Time Zone settings are locked, click **Unlock from plan**.
5. To stop remote management of the blade, clear **Manage in SMP**.
6. Configure the Time Zone settings (see above).
7. Click **Save**.

**To connect to the appliance:**
1. Go to **Home** > **Gateways**.
2. Click the gateway name.
   The Edit page opens.
3. Click **Device Settings** > **Time Zone**.
4. Click **Access Gateway: Date and Time**.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the **Date and Time** page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message is shown. Click **OK** to override that connection or **Cancel** to stop the current login attempt.
**DNS**

Configure the DNS server settings and define the domain name. You can define up to three DNS servers which apply to all Internet connections or use the DNS configuration from the active Internet connection (Primary).

We recommend that you configure up to three DNS servers, if they are located in the headquarters office. All DNS requests from this branch office go to these DNS servers.

By default, the gateway functions as the DNS proxy and provides DNS resolving services to internal hosts behind it (network objects). This option is global and applies to all internal networks.

The Domain Name is automatically appended to:

- Local hosts (the gateways and network objects) are appended with the domain name when the DNS resolves.
- The domain name is automatically appended to DNS queries that do not contain one.

By default, the DNS settings are unlocked from plans for new gateways.

This feature is only supported on R77.20 and higher gateways.

**To configure the DNS settings of a plan:**

1. Go to Home > Plans.
2. Click the plan name. The Edit page opens.
3. Click Device Settings > DNS.
4. Select Manage in SMP.
5. To configure the DNS servers, click Configure DNS servers and enter the IP addresses for the DNS servers.
6. To use the Internet connection DNS settings, click Use DNS servers configured for the active Internet connection(s).
7. To configure the gateways to provide DNS resolving services to internal hosts, click Enable DNS Proxy.
8. To use the DNS Proxy gateways to treat the local network objects as a hosts list, click Resolve Network Objects.
9. Enter the Domain Name appended to DNS queries.
10. Click Save.

**To override the DNS settings set by a plan in a gateway:**

1. Go to Home > Gateways.
2. Click the gateway name. The Edit page opens.
3. Click Device Settings > DNS.
4. If the DNS settings are locked, click Unlock from plan.
5. To stop remote management of the DNS settings, clear Manage in SMP.
6. Configure the DNS settings (see above).
7. Click Save.
To connect to the appliance:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Device Settings > DNS.
4. Click Access Gateway: DNS.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the DNS page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message is shown. Click OK to override that connection or Cancel to stop the current login attempt.

**Gateway Administrators**

The Gateway Administrators page lets you configure the administrator accounts that can log in to the local gateway.

You must create at least one Gateway administrator with Read-Write permissions to manage these administrators in the SMP.

**Note** - The first gateway administrator that you create automatically has Read Write permissions and cannot be deleted.

After you create a gateway administrator, you cannot change the password. Instead, delete the administrator and create a new one.

When you use the SMP to manage gateway administrators, the administrators on the local appliance are deleted. If a gateway is no longer managed by the SMP, the gateway administrators are saved on the local appliance.

This feature is only supported on R77.20 and higher gateways.

To configure the Gateway administrators of a plan:
1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Device Settings > Administrators.
4. Select Manage in SMP.

To create a new Gateway Administrator:
1. Click New.
   The Add Gateway Administrator window opens.
2. Enter the Name and Password.
3. Select the Permission for the administrator.
4. Click Finish.

To delete a Gateway administrator:
1. Select the administrator.
2. Click Delete.
   A confirmation window opens.
3. Click OK.
The administrator is deleted.

4. Click **Save**.

**To override the Gateway administrator settings set by a plan:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Device Settings > Administrators**.
4. If the Gateway administrator settings are locked, click **Unlock from plan**.
5. To stop remote management of the blade, clear **Manage in SMP**.
6. Configure the Gateway administrator settings (see above).
7. Click **Save**.

**To connect to the appliance:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Device Settings > Administrators**.
4. Click **Access Gateway: Administrators**.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the **Administrators** page. You can now update the local appliance.
5. **Note** - If a local administrator is already logged in to the appliance, a message is shown. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Configuring Security Software Blades**

Enable and configure the Software Blades of your appliances:

- Firewall
- Access Policy
- Application Control and URL Filtering
- IPS
- Traditional Anti-Virus
- Anti-Spam
- QoS
- Remote Access
- Site to Site VPN
- User Awareness
- Threat Prevention Anti-Virus
- Threat Prevention Anti-Bot
- Threat Prevention Threat Emulation
- Threat Prevention Policy
You can set Blade Control to On or Off for each Software Blade. This lets you keep the settings if you disable a Software Blade.

**Firewall**

In the settings of the Firewall Software Blade for the plan, define default behavior for traffic that does not match specified rules.

You can override the Firewall Software Blade settings in a plan for a specified gateway. You must first unlock the Firewall Software Blade from the plan.

**To configure the Firewall settings of a plan:**

1. Go to Home > Plans.
2. Click the plan name. The Edit page opens.
3. Click Security Software Blades > Firewall.
4. Select Manage in SMP.
5. Set the Policy:
   - **Strict** - Blocks traffic that is not specified as Allowed in the Firewall. Configure the Rule Base in gateway Portal.
   - **Standard** - Blocks incoming traffic unless the Firewall Rule Base allows it. Traffic to the Internet is Allowed. Traffic between internal networks and between trusted wireless networks is Allowed.
6. Select to log Blocked Traffic, Accepted Traffic, or both.
7. Click Save.

**To override the Firewall settings set by a plan:**

1. Go to Home > Gateways.
2. Click the gateway name. The Edit page opens.
3. Click Security Software Blades > Firewall.
4. If the Firewall settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Set the Policy and Log options [see above].
7. Click Save.

**To connect to the appliance:**

1. Click Home > Gateways.
2. Click the gateway name. The Edit page opens.
3. Click Security Software Blades > Firewall.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Firewall Policy page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.
**Access Policy**

On the **Access Policy** page, you can create firewall rules on the SMP for a specified plan or gateway. These rules set policy for:

- Outgoing access to the internet
- Incoming, internal and VPN traffic

**Pre local rules** are fetched before the local manual rules (created in the local settings of the Firewall Software Blades). A local administrator cannot create manual rules to override pre local rules configured by the SMP administrator.

**Post local rules** are fetched after the local manual rules. The SMP administrator gives recommended policy, but the local administrator can override it by creating manual rules.

**Note** - The gateway local administrator can edit only the manual rules. Pre/post local rules are locked.

Pre/post local rules are managed by Cloud Services. When you turn off Cloud Services, the pre/post local rules are deleted.

There is no repository for network objects and services. They are created and deleted with the rule.

**To create new pre or post local rules:**

1. Go to **Home > Plans**.
2. Click the plan name.
   The **Edit** page opens.
3. Click **Security Software Blades > Access Policy**.
4. Select **Manage in SMP**.
5. In the applicable rule table, click **New**.
   The **Edit Firewall Rule** window opens.
6. Configure these fields:
   - **Source**
   - **Destination**
   - **Service**
   - **Action**
   - **Log**
7. **Optional** - Enter the **Description**.
8. To enable the rule, click **Enabled**.
9. Click **Finish**.

**Note** - If you clear **Manage in SMP** and click **Save**, all pre/post local rules are deleted. To undo changes, click **Revert**.

**To edit a rule:**

1. Click the rule number or click the **Edit** icon.
   The **Edit Firewall Rule** window opens.
2. Edit the applicable fields.
3. Click **Finish**.
To enable/disable a rule:

In the **Edit Firewall Rule** window, select or clear the **Enabled** checkbox.

To delete a rule:

1. Click the checkbox next to the rule number.
2. Click **Delete**.

To change the rule order in the table:

Drag and drop the rule or rule number up or down.

To override the settings set by a plan:

1. Go to **Home > Gateways**.
2. Click the gateway name.
   
   The **Edit** page opens.
3. Click **Security Software Blades > Access Policy**.
4. If the Access Policy settings are locked, click **Unlock from plan**.

**Application Control and URL Filtering**

In the settings of the Application & URL Filtering Software Blade for the plan, define the types of applications and Web sites to block.

You can override the Application & URL Filtering Software Blade settings in a plan for a specified gateway. You must first unlock the Application & URL Filtering Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 63).

To configure the Application & URL Filtering Software Blade settings of a plan:

1. Go to **Home > Plans**.
2. Click the plan name.
   
   The **Edit** page opens.
3. Click **Security Software Blades > Application and URLs**.
4. Select **Manage in SMP**.
5. Select these checkboxes to set the **Policy**:
   
   - **Block security risk categories** - for example, spyware, phishing, botnet, spam, anonymizer, and hacking
   - **Block torrents and P2P applications** - for example, torrent trackers, BitTorrent and Gnutella protocols, file storage and sharing, media sharing, Facebook file sharing
   - **Block inappropriate content** - for example, weapons, violence, sex, gambling, hate, illegal activities, and illegal drugs
6. Click **Save**.

To override the Application & URL Filtering settings set by a plan:

1. Go to **Home > Gateways**.
2. Click the gateway name.
   
   The **Edit** page opens.
3. Click **Security Software Blades > Application and URLs**.
4. If the Application & URL Filtering settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Set the Policy options (see above).
7. Click Save.

To connect to the appliance:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Application and URLs.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Firewall Policy page. You can now update the local appliance.
   Note - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.

IPS

In the settings of the IPS Software Blade for the plan, define the IPS profile for the gateways.

You can override the IPS Software Blade settings in a plan for a specified gateway. You must first unlock the IPS Software Blade from the plan.

To configure the IPS Software Blade settings of a plan:
1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Security Software Blades > IPS.
4. Select Manage in SMP.
5. Set the Policy:
   - Strict - Use the IPS profile with most of the protection categories enabled.
   - Typical - Use the IPS profile that blocks the most dangerous threats.
   - Custom - Change the policy for which protection groups (by confidence level, severity, performance, and impact) are enabled or disabled.
6. Select Detect-only mode to monitor IPS rule matches. Clear the checkbox to implement IPS protections on the gateways.
7. Click Save.

To override the IPS settings set by a plan:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > IPS.
4. If the IPS settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Set the Policy and Mode options (see above).
7. Click **Save**.

**To connect to the appliance:**

1. Go to Home > Gateways.
2. Click the gateway name. The **Edit** page opens.
3. Click **Security Software Blades > IPS**.
4. Click **Access Gateway:IPS**. A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the IPS page. You can now update the local appliance.

**Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Traditional Anti-Virus**

In the settings of the Traditional Anti-Virus Software Blade for the plan, define the files that are scanned automatically for viruses, worms, and other malware. The Traditional Anti-Virus engine is based on Check Point technology for R75.x versions.

You can override the Traditional Anti-Virus Software Blade settings in a plan for a specified gateway. You must first unlock the Traditional Anti-Virus Software Blade from the plan.

Gateways that are R77.20 and higher automatically use the Threat Prevention Anti-Virus Software Blade. Gateways that are R75.x automatically use the Traditional Anti-Virus Software Blade.

**To configure the Traditional Anti-Virus Software Blade settings of a plan:**

1. Go to Home > Plans.
2. Click the plan name. The **Edit** page opens.
3. Click **Security Software Blades > Traditional Anti-Virus**.
4. Select **Manage in SMP**.
5. Set the **Policy**:
   - **Scan incoming files** - Scans incoming files on the gateway.
   - **Scan outgoing files** - Scans sent files. This option is cleared by default.
   - **Scan files between networks** - Scans files sent between internal networks or from the DMZ to internal. You can filter to scan only the files that use selected protocols.
6. Set **Tracking** - **Log, Alert** (as defined in the System Settings), **None**.
7. Select **Detect-only mode** to monitor Traditional Anti-Virus rule matches. Clear to implement Traditional Anti-Virus on the gateways.
8. Click **Save**.

**To override the Traditional Anti-Virus settings set by a plan:**

1. Go to Home > Gateways.
2. Click the gateway name. The **Edit** page opens.
3. Click **Security Software Blades > Traditional Anti-Virus**.
4. If the Anti-Virus settings are locked, click **Unlock from Plan**.
5. To stop remote management of the blade, clear Manage in SMP.
6. Set the Policy, Tracking, and Mode options (see above).
7. Click Save.

To connect to the appliance:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Traditional Anti-Virus.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Anti-Virus page. You can now update the local appliance.
   Note - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.

Anti-Spam
In the settings of the Anti-Spam Software Blade for the plan, define how email spam is handled.
You can override the Anti-Spam Software Blade settings in a plan for a specified gateway. You must first unlock the Anti-Spam Software Blade from the plan.

To configure the Anti-Spam Software Blade settings of a plan:
1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Security Software Blades > Anti-Spam.
4. Select Manage in SMP.
5. Click Filter spam based on email content.
6. Set the Policy:
   • Block spam emails
   • Flag spam email subject
   • Flag spam email header
7. Set Tracking: Log, Alert (as defined in the System Settings), None.
8. To monitor Anti-Virus rule matches, select Detect-only mode. Clear this checkbox to implement Anti-Virus on the gateways.
9. Click Save.

To override the Anti-Spam settings set by a plan:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Anti-Spam.
4. If the Anti-Spam settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Click Filter spam based on email content.
7. Set the **Policy**, **Tracking**, and **Mode** options (see above).
8. Click **Save**.

**To connect to the appliance:**
1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Security Software Blades > Anti-Spam**.
4. Click **Access Gateway:Anti-Spam**.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Anti-Spam page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**QoS**
In the settings of the QoS Software Blade for the plan, you can give more bandwidth to more important traffic.
You can override the QoS Software Blade settings in a plan for a specified gateway. You must first unlock the QoS Software Blade from the plan.

**To configure the QoS Software Blade settings of a plan:**
1. Go to **Home > Plans**.
2. Click the plan name.
   The **Edit** page opens.
3. Click **Security Software Blades > QoS**.
4. Select **Manage in SMP**.
5. Select **Ensure low latency for delay sensitive services** to give more bandwidth to delay-sensitive traffic. These services are defined by default as delay sensitive:
   - H323 and SIP services for Video over IP
   - MGCP services for media
   - SCCP services for Voice over IP.
   You can change the list of services in the WebUI of the gateway.
6. Select **Guarantee _% of the bandwidth to** to set a minimum ratio of the bandwidth for traffic that is not preferred.
7. Select **Limit bandwidth consuming applications** to set the limits for upload and download for applications that are defined as *bandwidth consuming*. These application types are defined by default:
   - P2P file sharing
   - Media sharing and streaming
   You can change the list of application categories in the WebUI of the gateway.
8. Click **Save**.

**To override the QoS settings set by a plan:**
1. Go to **Home > Gateways**.
2. Click the gateway name. The Edit page opens.
3. Click Security Software Blades > QoS.
4. If the QoS settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Set the Policy options [see above].
7. Click Save.

To connect to the appliance:
1. Go to Home > Gateways.
2. Click the gateway name. The Edit page opens.
3. Click Security Software Blades > QoS.
4. Click Access Gateway:QoS.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the QoS page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.

**Remote Access**

In the settings of the Remote Access VPN Software Blade for the plan, enable access to your VPN from authenticated remote users.

You can override the Remote Access VPN Software Blade settings in a plan for a specified gateway. You must first unlock the Remote Access VPN Software Blade from the plan.

To configure the Remote Access VPN Software Blade settings of a plan:
1. Go to Home > Plans.
2. Click the plan name. The Edit page opens.
4. Select Manage in SMP.
5. Select Allow traffic from Remote Access users (by default) to enable log in to the network from a remote site. It does not give access without authentication.
6. Select Log traffic from Remote Access users - (by default) to log this traffic.
7. Click Save.

To override the Remote Access VPN settings set by a plan:
1. Go to Home > Gateways.
2. Click the gateway name. The Edit page opens.
4. If the Remote Access VPN settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Set the Policy options [see above].
7. Click **Save**.

**To connect to the appliance:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Security Software Blades > Remote Access VPN**.
4. Click **Access Gateway:Remote Access**.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Remote Access page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Site to Site VPN**

In the settings of the Site to Site VPN Software Blade for the plan, enable encrypted connectivity between the networks of your organization. Make sure that the Site to Site VPN settings for the gateway are configured correctly before you manage it with the SMP.

You can override the Site to Site VPN Software Blade settings in a plan for a specified gateway. You must first unlock the Site to Site VPN Software Blade from the plan.

**To configure the Site to Site VPN Software Blade settings of a plan:**

1. Go to **Home > Plans**.
2. Click the plan name.
   The **Edit** page opens.
3. Click **Security Software Blades > Site to Site VPN**.
4. Select **Manage in SMP**.
5. Select **Allow traffic from remote VPN sites (by default)** to enable VPN traffic.
6. Select **Log VPN sites traffic (by default)** to log this traffic.
7. Click **Save**.

**To override the Site to Site VPN settings set by a plan:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Security Software Blades > Site to Site VPN**.
4. If the Site to Site VPN settings are locked, click **Unlock from plan**.
5. To stop remote management of the blade, clear **Manage in SMP**.
6. Set the **Policy** options [see above].
7. Click **Save**.

**To connect to the appliance:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Security Software Blades > Site to Site VPN**.

4. Click **Access Gateway:Site to Site**.
   
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Site to Site VPN Blade Control page. You can now update the local appliance.

   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**User Awareness**

In the settings of the User Awareness Software Blade for the plan, enable user identification in the local network. You can track user traffic, and you can set policy rules for user requirements.

You can override the User Awareness Software Blade settings in a plan for a specified gateway. You must first unlock the User Awareness Software Blade from the plan.

**To enable the User Awareness Software Blade settings of a plan:**

1. Go to **Home > Plans**.
2. Click the plan name.
   
   The **Edit** page opens.
3. Click **Security Software Blades > User Awareness**.
4. Select **Manage in SMP**.
5. Select **On**.
6. Click **Save**.

**To override the User Awareness settings set by a plan:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   
   The **Edit** page opens.
3. Click **Security Software Blades > User Awareness**.
4. If the User Awareness settings are locked, click **Unlock from plan**.
5. To stop remote management of the blade, clear **Manage in SMP**.
6. Make necessary changes.
7. Click **Save**.

**To connect to the appliance:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   
   The **Edit** page opens.
3. Click **Security Software Blades > User Awareness**.
4. Click **Access Gateway:User Awareness**.
   
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the User Awareness page. You can now update the local appliance.

   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.
**Threat Prevention Anti-Virus**

In the settings of the Threat Prevention Anti-Virus Software Blade for the plan, enable the gateways to scan automatically for viruses, worms, and other malware. The Threat Prevention Anti-Virus engine is based on Check Point technology for R77.x versions.

You can override the Anti-Virus Software Blade settings in a plan for a specified gateway. You must first unlock the Anti-Virus from the plan.

Gateways that are R77.20 and higher automatically use the Anti-Virus Software Blade. Gateways that are R75.x automatically use the Traditional Anti-Virus Software Blade.

**To configure the Threat Prevention Anti-Virus Software Blade settings of a plan:**

1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Security Software Blades > Anti-Virus.
4. Select Manage in SMP.
5. Select On.
6. Click Detect-only mode to monitor Anti-Virus protection matches. Clear to implement Anti-Virus protections on the gateways.
7. Click Save.

**To override the Anti-Virus settings set by a plan:**

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Anti-Virus.
4. If the Anti-Virus settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Make necessary changes to the mode (see above).
7. Click Save.

**To connect to the appliance:**

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Anti-Virus.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Anti-Virus page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.
Managing Gateways

**Threat Prevention Anti-Bot**

In the settings of the Threat Prevention Anti-Bot Software Blade for the plan, enable the gateways to scan automatically for bot-infected hosts and for communications with a C&C (Command and Control).

You can override the Anti-Bot Software Blade settings in a plan for a specified gateway. You must first unlock the Anti-Bot Software Blade from the plan.

This feature is only supported on R77.20 and higher gateways.

**To configure the Anti-Bot Software Blade settings of a plan:**

1. Go to **Home > Plans**.
2. Click the plan name.
   The **Edit** page opens.
3. Click **Security Software Blades > Anti-Bot**.
4. Select **Manage in SMP**.
5. Select **On**.
6. Click **Detect-only mode** to monitor Anti-Bot protection matches. Clear to implement Anti-Bot protections on the gateways.
7. Click **Save**.

**To override the Anti-Bot settings set by a plan:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Security Software Blades > Anti-Bot**.
4. If the Anti-Bot settings are locked, click **Unlock from plan**.
5. To stop remote management of the blade, clear **Manage in SMP**.
6. Click **Save**.

**To connect to the appliance:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Security Software Blades > Threat Prevention Anti-Bot**.
4. Click **Access Gateway: Threat Prevention**.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Threat Prevention Anti-Bot page. You can now update the local appliance.
   **Note** - If a local administrator is already logged in to the appliance, a message shows. Click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Threat Prevention Threat Emulation**

In the settings of the Threat Emulation Software Blade for the plan, enable the gateways to scan for infected files.
Note - Threat Emulation is supported only for 700/1400/1200R appliances with version R77.20.51 and higher.

You can override the Threat Emulation Software Blade settings in a plan for a specified gateway. You must first unlock the Threat Emulation from the plan.

To configure the Threat Emulation Software Blade settings of a plan:

1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Security Software Blades > Threat Emulation.
4. Select Manage in SMP.
5. Select On.
6. Select the HTTP Connection handling mode:
   - Background - Allows traffic to pass while it is inspected (default). This option has less impact on performance.
   - Hold - Traffic cannot pass until it is inspected and found not to contain malicious files. This option can impact performance but is more secure.
7. Click Detect-only mode to monitor Threat Emulation protection matches. Clear to implement Threat Emulation protections on the gateways.
8. Click Save.

To override the Threat Emulation settings set by a plan:

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Threat Emulation.
4. If the Threat Emulation settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Make necessary changes to the mode [see above].
7. Click Save.

To connect to the appliance:

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Security Software Blades > Threat Emulation.
   A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Threat Emulation page. You can now update the local appliance.
   Note - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.
Threat Prevention Policy

The Threat Prevention Policy configures the Anti-Virus, Anti-Bot, and Threat Emulation settings for a set of activated protections and instructions for how to handle traffic inspection that matches activated protections. Protections help manage the threats against the network.

Set protection activation:

- **Confidence level** - How confident the Software Blade is that recognized attacks are actually bot traffic or malicious files. Some attack types are more subtle than others and legitimate traffic is sometimes mistakenly recognized as a threat. The higher the Confidence level of a protection, the more confident Check Point is that recognized attacks are indeed attacks. Lower Confidence levels indicate that some legitimate traffic may be identified as an attack.

- **Protection action** - The action that the gateway enforces on matching traffic. Notifications for these actions are set based on the defined tracking option (none, logged, or logged with an alert).
  - **Prevent** - Blocks identified bot traffic.
  - **Detect** - Allows identified bot traffic to pass through the gateway, but detects and logs it.
  - **Ask** - Traffic is blocked until the user confirms that it is allowed. To configure the user message, see the Threat Prevention > Engine Settings page.
  - **Inactive** - The protection is deactivated.

- **Performance impact** - Indicates the impact level on gateway performance

You can override the Threat Prevention Policy settings in a plan for a specified gateway. You must first unlock the Threat Prevention Policy from the plan.

Anti-Virus and Anti-Bot are supported on R77.20 and higher gateways. Threat Emulation is supported only for 700/1400/1200R appliances with version R77.20.51 and higher.

To configure the Threat Prevention Policy settings of a plan:

1. Go to Home > Plans.
2. Click the plan name. The Edit page opens.
4. Select Manage in SMP.
5. Select On.
   - **High**, **Medium**, and **Low confidence**
   - **Performance impact**
   - **Tracking options**
7. Click Save.

To override the Threat Prevention Policy settings set by a plan:

1. Go to Home > Gateways.
2. Click the gateway name. The Edit page opens.
4. If the Threat Prevention Policy settings are locked, click Unlock from plan.
5. To stop remote management of the blade, clear Manage in SMP.
6. Make necessary changes.
7. Click Save.

To connect to the appliance:
1. Go to Home > Gateways.
2. Click the gateway name.
3. The Edit page opens.

A browser page opens and shows the progress of the SMP connection to the gateway. The appliance opens on the Threat Prevention Policy page. You can now update the local appliance.

Note - If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the current login attempt.

Configuring Services

When you configure Services in a plan, the gateways inherit these properties.

- Managed Services
- Firmware
- Backup
- Reports
- Report Recipients
- Dynamic DNS - Only in gateways

Managed Services

By default, all gateways subscribed to the plan take their managed services settings from the plan.

You can override the inherited managed services settings for a specific gateway. You must first unlock the managed services from the plan.

To configure the managed services settings of a plan:
1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Services > Managed Services.
4. Select or clear these services:
   - Store gateway logs - Send logs from the gateways to the SMP with SmartLog.
   - Send periodic reports - Send Check Point Executive reports that contain security and network analysis details from the SMP to the gateway owners.
   - Firmware upgrades - Controls the gateway firmware upgrades.
   - Periodic backup - Schedule periodic backups of the appliance settings.
   - Dynamic DNS - Gateways use the Dynamic DNS services.
• **Send cloud notifications** - Send notifications to the recipients specified on the **Notifications Recipients** pages.

5. Click **Save**.

**To override managed services for a gateway:**

1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Services > Managed Services**.
4. If **Managed Services** are locked, click **Unlock from plan**.
5. Select or clear the necessary services.
6. Click **Save**.

**Firmware for Gateways and Plans**

If a plan specifies firmware upgrades, you can configure these firmware settings in the plan:

- Firmware to use for the gateways
- Firmware upgrade schedule

By default, all gateways subscribed to a plan get their firmware settings from the plan.

You can override the inherited firmware settings for a specified gateway. You must first unlock the firmware service from the plan.

The appliance reboots after the upgrade to new firmware. You can limit the firmware upgrade to specified days and hours.

**Note** - The upgrade schedule uses the gateway's local time zone. For example, if you configure firmware upgrades to occur between 1:00 to 6:00 AM, gateways in New York receive firmware upgrades between 1:00 and 6:00 AM Eastern Time (ET). Gateways in California receive firmware updates between 1:00 and 6:00 AM Pacific Time (PT).

**To configure the plan firmware settings:**

1. Go to **Home > Plans**.
   The **Edit** window opens.
2. Click **Services > Firmware**.
3. Select a firmware for all gateways:
   - **Specific firmware version** - Click the downward arrow next to each appliance type to select a specific firmware or to set it to **Do_Not_Upgrade**.
   - **Check Point latest** - The gateway downloads the latest firmware version available.
   - **The firmware is managed locally on the device** - The gateway does not download firmware.
4. Schedule automatic firmware upgrades:
   - **Upgrade immediately**
   - **Daily** - Select the **time of day** range.
   - **Weekly** - Select the **day of week** and **time of day** range.
   - **Monthly** - Select the **day of month** and **time of day** range.
5. Click **Save**.
To override firmware settings for a gateway:
1. Go to Home > Gateways.
2. Click the gateway name.
3. The Edit page opens.
4. Click Services > Firmware.
   The Firmware window opens.
5. Click Unlock from plan.
   The fields are enabled.
6. Select the firmware and schedule options (see above).
7. Click Save.

Private firmware is available only to specified service domains and not globally to all service domains on the SMP.

To set private firmware:
1. Go to Service Domain > Settings
   The General tab opens.
2. Click Firmware.
3. Click New Private Firmware.
   The Add Private Firmware window opens.
4. Enter your Firmware unique ID.
5. Click Finish.
6. Click Save.

**Periodic Backup**

By default, all gateways subscribed to the plan take their backup settings from the plan. The backup file backs up the settings for each gateway in a separate zip file.

The naming convention of the file:  
<gateway name>_<firmware version>_<date: YYYY-MM-DD_HH_MM_SS>.zip

Make sure to create the path on your FTP server before you set a backup schedule. If the directory you set does not exist on the FTP server, the gateway does not create it and the backup fails.

You can override the inherited backup settings for a specific gateway. You must first unlock the managed services from the plan.

To configure the backup settings of a plan:
1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Services > Periodic Backup.
   The Periodic Backup window opens.
4. Enter the information for these fields:
   - Path
   - Username
   - Password
5. To use **File Encryption**, click the checkbox, then enter and confirm a password.
6. Click **Save**.

**To schedule periodic backups:**
1. Select **Daily**, **Weekly**, or **Monthly**.
2. Select the time range.
3. For **Weekly**, select the day of the week.
4. For **Monthly**, select the day of the month.
5. Click **Save**.

**To override the backup settings set by a plan:**
1. In **Home > Gateways**, click the gateway name.
   The **Edit** page opens.
2. Click **Services > Periodic Backup**.
   The **Periodic Backup** window opens.
3. Click **Unlock from plan**.
   The fields are enabled.
4. Set the necessary fields.
5. Click **Save**.

**Reports**
By default, report service settings are managed in the gateway plan.
You can override the reports settings set by a plan for a specified gateway. You must first unlock the reports service from the plan.

**To configure a plan's report settings:**
1. Go to **Home > Plans**.
2. Click the plan name.
   The **Edit** page opens.
3. Go to **Services > Reports**.
   The **Reports** page opens.
4. In **Report type**, select Classic or Detailed report. Detailed reports are generated by the SmartEvent based on the logs the gateway sends to the SMP.
5. In **Report content**, click the down arrow to select the report language.
6. Click the checkbox to embed the report in the email message body.
   **Note** - This option is only available for classic reports. Detailed reports are sent only as attachments.
7. In **Periodic report settings**, select the desired report frequency.
8. Click **Save**.

**To override the report settings set by a plan:**
1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Go to Services > Reports.
   The Reports page opens.
4. Click Unlock from plan.
   The fields are enabled.
5. Set the applicable options.
6. Click Save.

Gateway reports created in the SMP are deleted after 7 days. To disable or change this feature, you must change the property `KEEP_REPORT_TEMP_FILES` in the configuration file `INFO.properties` from false to true.

**Report Recipients**

By default, all gateways subscribed to the plan take their report recipient settings from the plan. You can override the reports settings set by a plan for a specified gateway. You must first unlock the reports service from the plan.

**To configure the report settings of a plan:**

1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Services > Report Recipients.
4. Set the applicable options:
   - **Send to owner** - If this is selected, the owner receives security reports.
   - **Additional emails** - Enter email address (separated by a semicolon) to receive security reports.
   - **Unsubscribed emails** - Enter email addresses (separated by a semicolon) to unsubscribe from receiving security reports.
     
     **Note** - Security report emails also contain a link for recipients to unsubscribe.
5. Click Save.

**To override the report settings set by a plan:**

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Services > Report Recipients.
4. If Report Recipients is locked, click Unlock from plan.
5. Set the applicable options.
6. Click Save.

**Dynamic DNS**

You can add DNS aliases to the primary domain name.

**To add a DNS alias:**

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Services > Dynamic DNS.
4. Click New.
5. Enter the DNS alias.
6. Repeat steps 2-3 to add more DNS aliases.
7. Click Save.

To delete a DNS alias:
1. Select the checkbox next to the DNS alias you want to delete.
2. Click Delete.
3. Click OK in the confirmation message.
   The DNS alias is deleted.

Configuring Setup Settings
Use the Setup page to define SMP access.

- **Administrators Access** - To let SMP administrators access appliances over HTTPS and SSH, add IP addresses to this table.
- **Gateways behind NAT** - A gateway that connects to the Internet behind a NAT device does not have a publicly accessible IP address.

**To configure SMP for gateway IP address access:**
1. On the NAT device, configure port forwarding for the required ports:
   - Local admin access = 4434
   - Push to gateway = 18209
   These are default values.
2. Enter the ports here.

**Administrators Access**
Add IP addresses or a network to the Administrators Access table to access appliances over HTTPS and SSH. All gateways subscribed to the plan take their administrator access settings from the plan, by default.

You can override the administrator access settings set by a plan. You must first unlock the administrator access settings from the plan.

**To configure administrator access for a plan:**
1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click Setup > Administrators Access.
4. Click New.
   The Administrator Access page opens.
5. Select the Source Type (Network or IP Address).
6. Enter the **IP Address**.
7. For a network source type, enter a **Subnet Mask**.
8. Click **Finish**.
   The details are shown in a table in the Administrators Access window.
9. Click **Save**.

**To override administrator access set by a plan:**
1. Go to **Home > Gateways**.
2. Click the gateway name.
   The **Edit** page opens.
3. Click **Setup > Administrators Access**.
4. If Administrators Access is locked, click **Unlock from plan**.
5. Click **New**.
   The **Administrator Access** page opens.
6. Configure the options (see above).
7. Click **Save**.

**To delete an IP address from the list:**
1. Select the IP address.
2. Click **Delete**.
3. Click **OK** in the confirmation message.
4. Click **Save**.

**Gateway behind NAT**
A gateway that connects to the Internet behind a NAT device does not have a publicly accessible IP address. To enable some features, the SMP must access the gateway. All gateways subscribed to the plan take their NAT settings from the plan, by default.

You can override the Gateway behind NAT settings set by a plan. You must first unlock the Gateway behind NAT settings from the plan. For more information, see Locking and Unlocking Settings (on page 63).

You can configure the NAT port forwarding rules, or you can log in to the gateway and configure it to connect to the SMP.

**To configure the SMP for gateway IP address access:**
1. Configure port forwarding for the required ports (default: local admin access = 4434, push to gateway = 18191) on the NAT device.
2. Go to **Home > Plans**.
3. Click the plan name.
   The **Edit** page opens.
4. Click **Setup > Gateways behind NAT**.
5. Enter the port numbers in **Local admin access port** and **Push actions to gateway on port**.
6. Click **Save**.
To override the gateway behind NAT settings set by a plan:

1. Configure port forwarding for the required ports (default: local admin access = 4434, push to gateway = 18191) on the NAT device.
2. Go to Home > Gateways.
3. Click the gateway name.
   The Edit page opens.
4. Click Setup > Gateway behind NAT.
5. If this option is locked, click Unlock from plan.
6. Enter the port numbers in Local admin access port and Push actions to gateway on port.
7. Click Save.

To configure the gateway to connect to SMP with the Check Point SMB Relay:

1. Go to Home > Gateway and click the gateway name.
   The Edit page opens.
2. Click Setup > Gateway behind NAT.
3. If this option is locked, click Unlock from plan.
5. Paste the Web URL from the gateway.
6. Click Save.

Using CLI Scripts

You can create scripts that control gateway settings, even settings that are not in the SMP WebUI. If you delete a script, its settings are kept on the gateways, unless those settings are configured in SMP. After the gateway receives the script from the SMP, it runs the script one time.

Do not use the CLI to edit settings that are remotely managed by a plan. If you do, the script fails.

For more about the supported Clish commands, see the Check Point 600/700/1100/1200R/1400 Appliance CLI and Advanced Routing Guide.

You can override the CLI script settings set by a plan. You must first unlock the CLI script from the plan. For more information, see Locking and Unlocking Settings (on page 63).

When the CLI script runs, any errors show in the Gateway’s CLI Script page in the Last script result section.

You can configure up to five different scripts. The gateway runs the scripts in sequential order: first Script1, then Script2, and so on.

To use a script in a plan:

1. Go to Home > Plans.
2. Click a plan name.
   The Edit page opens.
3. Click CLI Scripts > CLI Script 1 - 5.
4. Click Manage in SMP.
5. Enter the CLI commands for the script to run.
6. To disable the CLI script, clear Manage in SMP.
7. Click Save.
To override the script set by a plan in a gateway:
1. Go to Home > Gateways.
2. Click a gateway name.
   The Edit page opens.
3. Click CLI Script > CLI Script 1 - 5.
4. If the CLI script is locked, click Unlock from plan.
5. Select Manage in SMP.
6. Enter the CLI commands that you want the script to run.
7. To disable the CLI script, clear Manage in SMP.
8. Click Save.
   The gateway runs the CLI script, and the script in the plan is not run.

Editing Custom Fields (Gateways)
If the Service Domain uses Custom Fields for gateways, configure the settings on this page.

To edit the gateway custom fields information:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Custom Fields.
4. Edit the appropriate fields.
5. Click Save.
Using Plans for Gateways

_In This Section:_

   Editing Plans ....................................................................................................... 62
   Filtering the Plans Table...................................................................................... 63
   Deleting Plans ..................................................................................................... 63

A plan is a template of gateway features. Each gateway is assigned to a plan and inherits its settings from the plan. You can override the plan settings, and customize the gateway for a customer.

Plans and inherited gateway settings configured in SMP are centrally managed. You cannot change settings for a centrally managed gateway in the Portal.

Editing Plans

You can see or change the properties of a plan in Home > Plans.

If you change a plan, all its assigned gateways get the changes automatically. Make sure you know that the changes are valid for the assigned gateways. An invalid plan can cause unexpected issues.

To configure a plan:

1. Go to Home > Plans.
2. Click the plan name.
   The Edit window opens.
3. Configure the settings for the plan.
4. Click Save.

Configuring General Settings (Plan)

To configure a plan’s managed services:

1. Go Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click General.
4. To disable the plan, clear Enabled.
5. Click Save.
   If you disable a plan, you cannot configure gateways to use it. You cannot disable a plan if it is assigned to gateways.

Showing Plan Histories

You can see the date and time that a service plan was added to SMP and when it was last changed.

To show the plan history:

1. Go to Home > Plans.
2. Click the plan name.
The Edit page opens.
3. Click History.

Filtering the Plans Table

To filter the Plans:
1. Go to Home > Plans.
2. Click Filter.
   The Filter Plans window opens.
3. For Name and Description, select {is | not | contains} <text>
4. For Creation Date and Modification Date, select {anytime | today | yesterday | last 7 days | last month | this month | on or after <date> | before <date> | between <date>-<date>}
   You can use the asterisk (*) as an "any character, any number of times” wildcard.
5. Click Apply.
6. Click Filter.
   The Filter window shows the filtered Plans.

Deleting Plans

You cannot delete a plan if it is currently in use by a gateway.

To delete a plan:
1. Go to Home > Plans.
2. Select one or more plans.
3. Click Delete.
   A confirmation message shows.
4. Click OK.
   All selected plans are deleted.

Locking and Unlocking Settings

By default, a gateway managed by the SMP inherits its settings from its plan. To override these settings, you must first unlock the gateway from the plan.

In the Home > Gateways > Edit, individual gateways are marked with icons that indicate if a gateway settings are locked to a plan (inherited) or unlocked from a plan (overridden).

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🗝️</td>
<td>The gateway settings are locked to a plan. The gateway page cannot be edited.</td>
</tr>
<tr>
<td>🗝️</td>
<td>The gateway settings are unlocked from a plan.</td>
</tr>
</tbody>
</table>
Unlocking Gateways from a Plan

To unlock a gateway from a plan:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Unlock from Plan.
4. Make the necessary changes.
5. Click Save.

Locking Gateways to a Plan

You can reset an individual gateway and lock it to the plan.

To lock a gateway to a plan:
1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Lock to Plan.
   The gateway is locked and cannot be edited. The settings are taken from the plan.
4. Click Save.

Searching for Gateways

The Search for gateways field is located in the upper-right of the WebUI and is shown in all the SMP pages. You can search by

- Gateway name
- Owner
- Plan
- MAC Address
- IP Address
- Description

To search for gateways:
1. In the Search for gateways field, enter a gateway name or other specification. A partial entry also yields results.
   Note - You do not need to click Enter. The search occurs instantly.
2. Click View gateway results.
   The Home > Gateways page opens. The default number of gateways shown is 10. To navigate the table, use the up/down arrow keys.
   Note - If you click description next to the gateway name, the Home > Gateways > Edit page opens and shows all the information for that gateway.
3. For seamless login to a gateway, click the IP address.
To filter the search results:

1. Click **Filter**.
   
The **Search for gateways** window opens.

2. To perform an advanced search, click **Advanced Search Mode**.
   
   **Note** - Click **Simple Search Mode** to revert to a simple search.

3. Use the information in Gateway Search Fields, and select from the Drop-down List Options.
   
   To show wildcards (for an unlimited number of characters), enter an asterisk (*). For example, to search for all gateways whose name starts with gw, enter gw* in the search input field.

4. Click **Apply**.
   
   A table shows the gateways that match the specified search. The **Status** column shows if the gateway is currently connected (.isConnected), not connected (isDisconnected), or disabled (isDisabled).
   
   **Note** - More specific search parameters have shorter search times.

### Gateway Search Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>What to enter</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the gateway.</td>
<td>gw157</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the unique physical identifier of the device. The format is XX:XX:XX:XX:XX:XX, where X is a numeral from 1-9, or a letter from A-F. Alternatively, browse to a file containing the MAC addresses of the gateways you want to add. The MAC address file must be a *.txt file with each MAC address appearing on a separate line.</td>
<td>00:00:26:22:28:26</td>
</tr>
<tr>
<td>Owner</td>
<td>Enter the user ID of the user who owns the gateway.</td>
<td>Nkern</td>
</tr>
<tr>
<td>Gateway Type</td>
<td>Select the appliance type of the gateway.</td>
<td>600 Appliance</td>
</tr>
<tr>
<td>Status</td>
<td>Select the current status of the gateway. This can be any of the following:</td>
<td>Connected</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any</strong> - The status of the gateway is not important.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Connected</strong> - The gateway is connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Downloading</strong> - The gateway is currently downloading data from the SMS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Client login failed</strong> - The gateway’s attempt to authenticate to the SMP failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> - The gateway is disabled.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>What to enter</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>Select the gateway’s management type. This can be any of the following:</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any</strong> - The gateway’s management type is not important.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Internal</strong> - The gateway is remotely managed by the SMP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local</strong> - The gateway is locally managed.</td>
<td></td>
</tr>
<tr>
<td>Plan</td>
<td>Select the plan configured for the gateway.</td>
<td>Silver</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the gateway.</td>
<td>Appliance used in NY office</td>
</tr>
<tr>
<td>First Connection</td>
<td>Select when the gateway first connected to the SMP.</td>
<td>last 7 days</td>
</tr>
<tr>
<td>Last Connection Day</td>
<td>Select when the gateway last connected to the SMP.</td>
<td>today</td>
</tr>
<tr>
<td>Reported IP</td>
<td>Enter the IP address that the gateway used when it last connected to the SMP.</td>
<td>62.90.10.1</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Select when the gateway was created.</td>
<td>today</td>
</tr>
<tr>
<td>Modification Date</td>
<td>Select when the gateway was last modified.</td>
<td>last 7 days</td>
</tr>
</tbody>
</table>

**List Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>is</strong></td>
<td>Searches for gateways that match the data in the field. For example, if you type “gw352” in the Name text box, the search will return only gw352.</td>
</tr>
<tr>
<td><strong>not</strong></td>
<td>Searches for gateways that do not match the data in the field. For example, if you type not “gw352” in the Name text box, the search will return all gateways except for gw352.</td>
</tr>
<tr>
<td><strong>contains</strong></td>
<td>Searches for gateways that contain the data in the field.</td>
</tr>
<tr>
<td><strong>none</strong></td>
<td>Searches for gateways that do not have this feature. For example, if for Owner you select none, the search will return all gateways without an owner.</td>
</tr>
<tr>
<td><strong>from file</strong></td>
<td>Loads a file containing MAC addresses and searches according to its content.</td>
</tr>
<tr>
<td><strong>don’t care</strong></td>
<td>Searches for gateways where the desired date/time can be anytime or non-existent. For example, if for Expiration Date you select don’t care, the search will return both gateways with and without an expiration date.</td>
</tr>
</tbody>
</table>
## Managing Gateways

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anytime</td>
<td>Searches for gateways where the desired date/time can be anytime, but must be existent. For example, if for <em>Expiration Date</em> you select anytime, the search will return gateways with any expiration date, but not gateways without an expiration date.</td>
</tr>
<tr>
<td>today</td>
<td>Searches for gateways where the desired date/time is today.</td>
</tr>
<tr>
<td>yesterday</td>
<td>Search for gateways where the desired date/time is yesterday.</td>
</tr>
<tr>
<td>last 7 days</td>
<td>Searches for gateways where the desired date/time is during the last seven days (7 x 24 hours). For example, if for <em>Expiration Date</em> you select last 7 days, and it is currently Monday at 17:00, the search will return all gateways with an expiration date between last Tuesday at 17:00 and the current time.</td>
</tr>
<tr>
<td>last month</td>
<td>Searches for gateways where the desired date/time is during the last calendar month. For example, if for <em>Creation Time</em> you select last month, and it is currently February 10, the search will return all gateways that were created during the month of January.</td>
</tr>
<tr>
<td>this month</td>
<td>Searches for gateways where the desired date/time is this month.</td>
</tr>
<tr>
<td>on or after</td>
<td>Searches for gateways where the desired date/time is on or after a specific date. If you select this option, new fields are shown. Use the drop-down lists to specify the exact time period.</td>
</tr>
<tr>
<td>before</td>
<td>Searches for gateways where the desired date/time is before (not including) a specific date. If you select this option, new fields are shown. Use the drop-down lists to specify the exact time period.</td>
</tr>
<tr>
<td>between</td>
<td>Searches for gateways where the desired date/time is between (including) two specific dates. If you select this option, new fields are shown. Use the drop-down lists to specify the exact time period.</td>
</tr>
</tbody>
</table>

### Exporting Gateway Information

You can export groups of gateways that match specified parameters to Microsoft Excel format. The exported information includes the gateway type, assigned plan, product key, gateway settings, and owner’s email address.

**To export gateway information to Microsoft Excel:**

1. Click **Home > Gateways**.
2. Select the check boxes of the applicable gateways or Filter the list and then select the applicable check boxes.
3. Click **Actions > To Excel**. Information for the selected gateways is saved to an Excel file.
Sending Email to Gateway Owners

To send an email to gateway owners:

1. Search for the gateway owners.
   You can also click Home > Gateways to show all the gateways.
2. Select one or more of the gateways with the specified owners.
3. Click Actions > Mail to owner.
   The General Mail window opens and shows the Preview tab.
4. Click Edit to make any changes in the email.
5. Click Preview.
6. Click Send Email.

Deleting Gateways

To delete a gateway (in the Gateways page):

1. Go to Home > Gateways.
2. Select the check box next to the gateway name.
3. Click Delete.
   A confirmation message appears.
4. Click OK.
   The selected gateway is deleted.
   The gateway’s certificate is revoked and listed in the Certificate Revocation List as revoked.

To delete a gateway (in the Edit page):

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Delete.
   A confirmation message appears.
4. Click OK.
   The gateway is deleted.
   The gateway’s certificate is revoked and listed in the Certificate Revocation List as revoked.
   Note - When you delete a gateway, you do not delete the user (on page 104) who owns the gateway.

Accessing Local Gateways

The SMP administrator can connect to a gateway to force an update of the gateway, restart the gateway, and make changes to gateway settings.

Note - If you use Internet Explorer, install the SMP certificate before you access the gateway (on page 153).
Connecting to Gateways

After you connect to the gateway, these identification details show:

- At the bottom of the WebUI login page - The gateway name (as defined in the SMP for the appliance) and the MAC address of the appliance.
- At the top of the WebUI application (near the search box) - The name of the appliance.

To connect to a gateway (from the Edit page):

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click Access Gateway.
4. If a security warning message shows, confirm it and continue.
   A browser page opens and shows the progress of the SMP connection to the gateway.
5. If a local administrator is already logged in to the appliance, a message shows. Click OK to override that connection or Cancel to stop the login attempt.
   Update the local appliance as necessary.

The certificate for the gateway is a self-signed certificate. When you show information for the certificate, the "Issued to" and "Issued by" fields show a unique string. The syntax of this string includes my.gateway and the MAC address of the gateway.

To make sure that the gateway you connect to is correct, check that the MAC address in the middle part of the string matches the gateway’s. You can find the MAC address of the gateway in the General tab of the gateway.

Connecting to Gateways behind NAT

When a gateway is behind a NAT device, by default the SMP cannot access the local Portal. You must configure the SMP and the gateway to allow users to access it from the SMP.

To configure the gateway behind a NAT device:

1. Log in to the gateway.
2. Click Device > DDNS & Access Services.
3. From the Appliance Access Service section, click Allow connections to the appliance from the internet via the Check Point SMB Relay cloud service.
   The Appliance Access Service window opens.
5. Enter the gateway Host name.
6. Click Apply.
7. Copy the Web URL and paste in the SMP Portal.
8. Click Apply.
   The gateway allows the SMP to access it.

To configure the SMP to access the gateway behind NAT:

1. Go to Home > Gateways.
2. Click the gateway name.
The **Edit** window opens.

3. Click **Setup > Gateways behind NAT**.
4. If the gateway is locked, click **Unlock from plan**.
5. Click **Use Access Services Web URL for Access Gateway**.
6. Paste the URL in the field.
7. Click **Save**.
Managing VPN Communities

In This Section:

Overview ............................................................................................................. 71
VPN Community Types ........................................................................................ 71
Creating VPN Communities ................................................................................. 73
Configuring the Community General Settings ...................................................... 73
Showing Communities ......................................................................................... 73
Filtering the Communities Table .......................................................................... 74
Deleting Communities ......................................................................................... 74
Configuring VPN Settings .................................................................................... 75
Managing VPN Community with an External Gateway........................................... 81

Overview

The SMP lets you define a group of gateways as a VPN community. A VPN community is a group made up of several gateways that share the same VPN security settings. When you add a gateway to a VPN community, the gateway automatically inherits the appropriate properties, and can establish secure sessions with other members of the VPN community. The VPN community’s type determines with which members the gateway can communicate. A gateway can be a member of multiple communities.

You can also configure a VPN community with gateways that are not managed by the SMP.

VPN Community Types

These are the VPN communities you can use:

- **Fully Meshed**
  In a fully meshed community, all the gateways in the VPN community can communicate directly with each other and fully access the networks behind the gateways, without an intermediary or “center” gateway. A fully meshed topology allows the highest performance, lowest transmission delay, and the best fault tolerance possible.

- **Star**
  A star community has two types of members:
  - **The center (“hub”) gateway** can communicate with each satellite gateway.
  - **Satellite (“spoke”) gateways** can be configured to communicate with each other through the center gateway.

- **Nested**
  You can nest communities to create advanced VPN topologies. For example, you can create a meshed community whose members are star communities, a star community whose members are meshed communities, and so on.
Understanding Nested Communities

When two gateways communicate with each other, they use the encryption and authentication type (and all other Phase1/Phase2 parameters, such as PFS and DH group), of the innermost common community. In the diagram below, communities Y and Z are nested in community X. Gateways A and B are members of both communities X and Z. VPN tunnels between these gateways use the parameters of community Z instead of X, because Z is the innermost common community. VPN tunnels between gateways A and C use the parameters of community X, as X is the innermost common community of A and C.
### Creating VPN Communities

**To create a new VPN community:**

1. Go to Home > Communities.
2. Click New.
   - The **Create New Community** wizard opens.
3. Enter the **Name** for the community.
4. Optional - Enter a **Description** of the community.
5. Click **Finish**.
   - The community is created.

### Configuring the Community General Settings

**To configure the General settings for a community:**

1. Go to Home > Communities.
   - The **Communities** window opens and shows the communities.
2. Click the community name.
   - The Edit page opens.
3. Click **General**.
4. Enter a **Description** (optional).
5. To create a nested community, select the **Parent Community**.
6. Click **Save**.

### Showing Communities

The **Home > Communities** page shows the communities in a table.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the community</td>
</tr>
<tr>
<td>VPN Type</td>
<td>VPN configurations:</td>
</tr>
<tr>
<td></td>
<td>• Full Mesh</td>
</tr>
<tr>
<td></td>
<td>• Star</td>
</tr>
<tr>
<td>Member of</td>
<td>Shows the parent community.</td>
</tr>
<tr>
<td>Status</td>
<td>Values for the community status:</td>
</tr>
<tr>
<td></td>
<td>• ✓ - OK</td>
</tr>
<tr>
<td></td>
<td>• ✗ - Topology not up to date</td>
</tr>
<tr>
<td></td>
<td>• ✗ - Star community has no center</td>
</tr>
<tr>
<td>Topology Error</td>
<td>Shows the error for the community.</td>
</tr>
</tbody>
</table>

## Filtering the Communities Table

To filter the communities window:

1. Go to **Home > Communities**.
   The **Communities** window opens and shows the communities.

2. Click **Filter**.
   The **Select communities** window opens.

3. For each search field:
   a) Select a search string modifier:
      - **is** - The string exactly matches the community data.
      - **contains** - The community data contains the string or option.
      - **not** - The community data does not match the string or option.
      - **none** - This field is empty for the community.

   b) Enter one or more search strings.

   c) Select the time settings for the **Creation** and **Modification Date** for the communities.

4. Click **Apply**.

## Deleting Communities

To delete a community with gateways, you must first remove the gateways.

To delete a community:

1. Go to **Home > Communities**.
   The **Communities** window opens and shows the communities.

2. Select one or more communities.

3. Click **Delete**.
   A confirmation window opens.

4. Click **OK**.
The community is deleted.

Configuring VPN Settings

You can configure these VPN settings from the gateway or from the plan.

From the gateway:
- Community
- Authentication Method
- Internal Network Topology

From the plan:
- Community

VPN Community Settings

When you configure VPN Communities for a plan, all gateways that belong to the plan become members of those VPN Communities.

You can override the VPN community settings set by a plan for a specified gateway. You must first unlock the community settings from the plan. For more information, see Locking and Unlocking Settings (on page 63).

Make sure that the Site to Site VPN blade is turned on in the appliance for the gateway to get the community settings.

To configure community settings (plan)

1. Go to Home > Plans.
2. Click the plan name.
   The Edit page opens.
3. Click VPN > Community.
   The Participates in the following communities table is shown.
4. To add a community, click New and select the Community.
   Note - Member Type cannot be configured in a plan. All gateways are Normal Members.
5. To delete a community, click the community name and click Delete.
6. Click Save.

To configure community settings (gateway):

1. Go to Home > Gateways.
2. Click the gateway name.
   The Edit page opens.
3. Click VPN > Community.
   The Participates in the following communities table is shown.
4. If the settings are locked, click Unlock from plan.
5. To add a community, click New and select the Community and Member Type.
   If the selected community is a Star Community, the Member Type is Normal or Center. To change a gateway to be the Center, configure the gateway properties.
6. To delete a community, click the community name and click Delete.
Managing VPN Communities

7. To use a DNS name instead of an IP address, click **Use DNS name**.

8. Click **Save**.

Authentication Method

The Authentication Method page shows information about the VPN authentication settings for the gateway.

You can also export the certificate in X.509 format, or revoke and renew it.

To show the authentication method for a gateway:

1. Go to **Home > Gateways**
2. Click the gateway name. The Edit page opens.
3. Click **VPN > Authentication Method**.
4. Select an Authentication Method. The gateway uses a **Certificate** to authenticate for VPN traffic.
5. Select a Certificate Authority. The CA for the gateway is the SMP Internal CA.
6. Select and copy the Distinguished Name to paste the DN in an external Security Management Server.
7. Click **Save**.

**Note** - For externally managed gateways, only the Authentication Method field shows.

To manage the certificates for the gateway:

1. In the Authentication Method page, click **Manage Certificate**. The Export Wizard window opens.
2. Select one of these options:
   - Revoke and renew the certificate
   - Export the certificate (X.509 format)
3. Click **Next**.
4. When you export a certificate, click **Save As**. The Internet browser saves the certificate to a CRT file in X.509 format.
5. Click **Done**.

Configuring Network Topology for Gateways

If the gateway is a member of a VPN community, to expose networks behind this gateway to other members, you must configure network topology settings for the gateway. The internal network topology is the list of internal networks or IP addresses behind this gateway.

To manually configure network topology settings:

1. Go to **Home > Gateways**.
2. Click the gateway name. The Edit page opens.
3. Click **VPN > Internal Network Topology**.
4. Click **New**.
The Internal Network Edit window opens.

5. Enter the information for these fields:
   - Network Name
   - Network Address
   - Network Mask

6. Click Finish.
   The network information appears in the Manually configured networks area.

7. Repeat steps 4 – 6 for other networks.

8. To edit the settings, click the network’s name.
   The Internal Network Edit window opens.

9. To delete a network’s settings, select the check box next to the network and click Delete.
   A confirmation message appears.

10. Click OK.
    The network’s settings are deleted.

11. Click Save.

Configuring Community VPN Settings

Satellite members in a star VPN can be configured to communicate with each other through the center gateway. The default setting is no communication between satellites.

When you use the Disable NAT feature, the VPN connections use the original IP address, even if Hide NAT is configured for the gateway.

To configure VPN settings for the community:

1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click VPN Settings.
4. From VPN Type select, Star or Full Mesh.
5. For a star VPN, configure the Center Gateway.
   Use the Add Gateway wizard to assign a center gateway.
6. In Satellite Routing, configure communication:
   - No communication between satellites (default)
   - Route to other satellites through center
   - Route to other satellites and internet through center - Supported only for externally managed centers.
7. To make sure that VPN tunnels between gateways in the community are always open, click Permanent VPN.
8. To disable Hide NAT for connections between the gateways in this community, click Disable NAT.

Configuring IKE Settings

To configure IKE settings for the community:

1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click VPN Settings > IKE Settings.
4. Configure the IKE settings shown in the table below.
5. Click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Phase-1</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Select the encryption type that gateways use for Phase-1 IKE negotiations</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the authentication protocol for Phase-1 IKE negotiations</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>Select the Diffie-Hellman group to use for Phase-1 IKE negotiations</td>
</tr>
<tr>
<td>Renegotiate every</td>
<td>Enter the length of the IKE Phase-1 key lifetime in minutes</td>
</tr>
<tr>
<td>IKE Phase-2</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Select the encryption type that gateways use for Phase-2 IKE negotiations</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the integrity for Phase-2 IKE negotiations</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>Enable or disable PFS (Perfect Forward Secrecy)</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>When PFS is enabled, select the Diffie-Hellman group to use for Phase-2 IKE negotiations</td>
</tr>
<tr>
<td>Renegotiate every</td>
<td>Enter the length of the IKE Phase-2 key lifetime in seconds</td>
</tr>
<tr>
<td>VPN Tunnel Sharing</td>
<td>Click the level of VPN tunnel sharing between peer gateways</td>
</tr>
</tbody>
</table>

### Assigning a Center Gateway

In a star VPN configuration, the center gateway lets the satellite Security Gateways connect to the internal network of the central Security Gateway.

**To show the VPN settings window for the community:**
1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click VPN Settings.

**To assign the center gateway for a Star VPN community:**
1. In the VPN Settings window of the community, click Topology > Choose.
   The Add Gateway wizard opens.
2. In the Select Method window, select an option to locate the center gateway.
   - Name
   - MAC Address
   - Search for gateways
3. Click Next.
To search for the gateway:
1. Enter the search values.
2. Click Next.
3. Select the gateway.
4. Click Next.
5. Click Done.
   The Done window shows that the gateway is the center of the Star community.

Configuring Communities' Custom Fields
You can configure custom community fields that are defined for the Service Domain.

To configure a community's custom fields:
1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click Custom Fields.
4. Enter the information for the fields.
5. Click Save.

Configuring Communities' Members Lists
You can add or remove gateways and sub-communities from a community's list of members.

Note - A gateway can be a member of multiple communities.

To show the gateway members of a community:
1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click Members.
   The Members window opens and shows the gateway members for the community.

To add a gateway to a community:
1. From the Members window, click Add Gateway.
   The Add Gateways window opens.
2. Select the method for adding gateways.
3. Click Next.
4. Use the wizard to add the gateway to the community.

To add a community to a gateway's list of communities:
1. Go to Home > Gateways and click the gateway name.
   The Edit window opens.
2. Click VPN > Community.
3. The Participates in the following communities table is shown.
4. Click New.
The Community window opens.

5. Select the Community and Member Type.
6. Click Finish.

The community is added to the table.

To add a subcommunity:
1. From the Members window, click Add Community.
   The Select Community window opens.
2. Select the community.
3. Click OK.

The subcommunity is added to the community.

To remove a gateway member from a community:
1. From the Members window, select the member gateways.
2. Click Remove.
   A confirmation window opens.
3. Click OK.

The gateways are removed from the community.

Creating Community Topologies

A community’s topology is created automatically. You can manually create the community topology if:

- The topology terminates early (there is an error message after the topology is created).
- The topology is invalid (there is an error message next to the community).

To create a topology for a community:
1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click Actions > Generate Topology.
   A confirmation message appears.
4. Click OK.

Viewing Community Histories

To show history for a community:
1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click History.
   The History window shows the date and time when the community was:
   - First created
   - Most recently modified
Showing the Summary for a Community

To show the summary for a community:
1. Go to Home > Communities.
2. Click the community name.
   The Edit page opens.
3. Click View > Summary.
   The Community Details Summary window opens.

To email the summary:
1. In To, enter the email addresses.
2. Click Send Email.

Managing VPN Community with an External Gateway

When you add gateways that are NOT managed by the SMP to a VPN community, you must install the CAs to decrypt the VPN traffic. Similar procedures are required for the SMP and the external Security Management Server for the external gateway:

1. Configure the VPN community. Make sure that it has the same settings in the SMP and the external Security Management Server.
2. Create objects for the externally managed gateways.
3. For the SMP and Security Management Server:
   a) Export the CA to file.
   b) Import the CA from the other Security Management Server.
4. If necessary for the external gateways, install the security policy.

Preparing to Add an External Gateway

Before you add an external gateway to a VPN community, make sure that these items are ready:
- VPN community in the SMP is configured.
- Credentials to log in to the external Security Management Server with Administrator permissions.
- Static IP address for each external gateway.

Note - The VPN community in the external Security Management Servers can include gateways with dynamic IP addresses. The specific settings depend on your external Security Management Server.

Configuring a VPN Community with External Gateways

This high-level work flow describes how to create a VPN community with externally managed gateways.
1. In the external Security Management Server, export the CA to a file.
2. In the SMP:
   a) Create a new object for the externally managed gateway for the VPN community.
b) Import the external Management CA.

c) Export the SMP CA to a file.

3. In the external Security Management Server:
   a) Import the SMP CA.
   b) Create a new object for each SMP gateway in the VPN community.
   c) If necessary, install or push the policy to the gateway.

### Adding External Gateways to the SMP

To add the external gateway in the SMP:

1. Go to **Home > Communities**.
2. Click the community name.
   The **Edit** page opens.
3. Click the **Members** tab.
4. Click **Add Gateway**.
   The **Add Gateways** wizard opens and shows the **Select Method** window.
5. Click **Create a new gateway**.
6. Click **Next**.
   The **Create New Gateway** window opens.
7. Enter the **Name** of the external gateway.
   **Note** - You do not need to use the same name for the external gateway in the SMP as in the external Security Management Server.
8. Clear **Managed by SMP**.
9. Enter the **Static IP** for the external gateway.
10. Click **Finish**.
   The gateway object is created and added to the VPN community.

### Importing and Exporting the CA

The SMP and external gateways in the VPN community can only communicate after the SMP and external Security Management Server exchange CAs.

To import the external Management CA to the SMP:

1. Go to **Service Domain > Settings**.
   The **General** page opens.
2. Click the **Certificates** tab.
3. Click **Add**.
   The **External CA** page opens.
4. Click **Import X.509**.
5. Click **Choose File**.
6. Select the file with the certificate.
7. Click **OK**.
8. Enter the details for the certificate.
9. Click **Save**.
   The external CA is updated with the new certificate.

**Configuring Large Scale VPN**

These procedures explain how to configure a Check Point Security Gateway that is not managed by the SMP as the center of a VPN community.

**On the R77.30 Security Management Server:**


1. Open SmartDashboard.
2. Go to **Server and OPSEC**.
3. Expand the **Trusted CAs** branch.
4. Click the **internal_ca** object.
5. Go to the **Local Security Management Server** tab, click **Save As...**, and export the **internal_ca.crt** file.

**On the SMP:**

1. Activate all the appliances you want to add to the VPN community.
2. Open your gateway object. Under **VPN > Internal Network Topology**, add the encryption domain of the gateway.
3. Create a new external gateway object:
   - Clear the **Managed by SMP** checkbox.
   - Add the static IP address.
4. Edit the external gateway object. In **VPN > Internal Network Topology**, add the encryption domain.
5. Go to **Home > Communities** and create a new community
6. In **VPN Settings**, enter information for the VPN Community settings:
   - Select **Permanent Tunnel** (optional).
   - Enable **Disable NAT**.
   - Select the **Encryption** method.
   - In the **IKE Settings**, select the relevant IKE settings.
   - Select the **One VPN tunnel per Gateway pair** option.
7. Click **Save**.
8. Add your gateway object and the externally managed gateway object as community members.
9. Go to **Service Domain > Settings > Certificates** tab.
10. Click **Add** and import the internal CA that you exported from the external Security Management Server.
11. Open **Service Domain > Settings > General > Certificates**.
    You can also access it through **System > Settings > Certificate Authority**.
12. Click **Export X.509** and export the SMP .crt file.
13. Connect to your appliance gateway and verify the CA of the Security Management Server shows under **Trusted CAs**. If not, fetch settings from the **Cloud Services** page.

**On the external Security Management Server:**

1. Go to **Server and OPSEC**.
2. Right-click on **Trusted CAs**, and select **New CA > Trusted...**

3. Go to the **OPSEC PKI** tab, click **Get..** and import the SMP CA.

4. On an internal environment, disable the **Retrieve CRL** option.
   
   **Note** - You do not need to disable this option in an environment with a CRL service.

5. Configure the gateway object for the externally managed gateway:
   
   - Enable the **IPsec VPN** blade and set the encryption domain.
   - If the main IP of the gateway is different from the external IP, go to **IPSec VPN > Link Selection**. Instead of **Main address**, select **Selected address from topology table** and select the external IP.

For **R77.20** or lower only:

You must create an externally managed gateway on SmartDashboard for each appliance managed by SMP.

1. Right-click **Check Point** and select **Check Point > More > Externally Managed VPN Gateway...**.
2. Enter the gateway name and IP address.
3. Select your hardware.
4. Turn on the **IPsec VPN** blade.
5. In the **Topology** tab, configure the **Topology table** and select **All IP Addresses behind Gateway are based on Topology Table**.

For **R77.30** or higher only:

1. Go to **Network Objects**. Right-click on **Network Objects** and select **LSV profile...**.
2. Configure the LSV profile:
   
   a) In **General > Peer certs are signed by CA**, select the SMP CA
   
   b) In **Advanced**, clear **Limit peers’ VPN Domain size**
   
   c) Click **Save** and close.
3. Create a VPN community.
   
   **Note** - This community must have the same settings as the one you created on SMP.
4. In **General**, select **Accept all encrypted traffic**.
   
   If you leave this option disabled, you must create firewall rules to allow VPN traffic from the VPN community.
5. Add all the gateways or LSV profiles required as members of the community.
6. Configure the **Encryption** topic with the SMP settings.
7. In **Tunnel Management**, enable **Set Permanent Tunnels** [if this is enabled on the SMP] and select **One VPN tunnel per Gateway pair**.
8. In **Advanced VPN Properties**, enable **Disable NAT inside the VPN community**.
   
   **Note** - For a star community, you must select **To center only** in the VPN routing topic, as it is the only supported option by SMP.
9. Click **Save** and install policy.

**On the appliance side:**

Run the command:

```
set vpn site-to-site advanced-settings tunnel-test-from-internal true
```

This allows the tunnel test to run properly from the internal encryption domain IP.

**Note** - You can place this command in a CLI script in your SMP plan for all your gateways.
Basic troubleshooting:

If there are problems in the tunnel tests:

1. In Global Properties, turn on the implied rules logging in the center gateway.
2. Clear the previous IKE parameters:
   a) In expert mode, run: `vpn tu`
      The IKE and SPI parameters show.
   b) Select 0 to clear all.
      Note - You may also need to do this on the center gateway.
3. In the center gateway, to see the LSV peers:
   a) Run: `vpn lsv`
      You can now see and remove peers and their encryption domains.
   b) If you remove any LSV peers, you must use `vpn tu` to clear the remembered IKE parameters.

Sample Configuration with SmartDashboard

This section contains sample configurations that explain how to use Check Point Security Management Server and Security Gateway as the externally managed gateway for the VPN community. The VPN community is shared between SmartDashboard and the SMP.

These objects and settings are already configured in the applicable Security Management Servers:

- SMP - gateways
- SmartDashboard - VPN community and VPN Security Gateway

High-level Workflow

1. Add gateways to SmartDashboard.
2. In SmartDashboard, configure the settings for the shared VPN community.
3. In SmartDashboard, export the Security Management Server CA.
4. Add the VPN Security Gateway to the SMP.
5. Import the Security Management Server CA to the SMP.
6. In the SMP, create the shared VPN community.
7. Export the SMP CA.
8. In SmartDashboard, import the SMP CA and update the security policy for the VPN Security Gateway.

Adding Gateways to SmartDashboard (Static IP Address)

Create new objects for the gateways as Externally Managed VPN Gateways in SmartDashboard that use static IP addresses. Configure the external and internal IP address for each gateway.

This procedure is for gateways that use a static external IP address. You can also add gateways that use a dynamic IP address.

To add a gateway to SmartDashboard with a static IP address:

1. Log in to SmartDashboard.
2. Right-click the Network Objects tree and select **Check Point > More > Externally Managed Gateway.**
   The gateway window opens and shows the **General Properties** page.

3. Enter the SMP gateway **Name.**

4. For **IPv4 Address**, enter the IP address of the external interface.

5. For **Hardware**, select the appliance.

6. From **Network Security**, click **IPsec VPN**

7. From the navigation tree, click **Topology.**

8. Click **Manually defined on the Security Management Server, based on the below Topology Table**

9. Click **All IP Addresses behind Gateway are based on the below Topology Table**

10. Double-click the external interface.

11. Make sure the **Name** is the name of the external interface.

12. Make sure the **Network Type** is **External (leads out to the Internet)**

13. Make sure the **Static IP address** and **Net Mask** are the same settings as the external interface on the gateway.

14. Click **OK.**

15. Double-click the internal interface or click **New.**

16. Enter the **Name** of internal interface

17. For **Network Type**, select **Internal (leads to the local network).**

18. For static **IP Address** and **Net Mask**, enter the IPv4 address and subnet mask for the interface.

19. For **Topology**, select **Network defined by the interface IP and Net Mask**

20. Click **OK.**

21. Click **OK.**

   The gateways with a static IP address are added to SmartDashboard.

---

**Configuring the VPN Community (SmartDashboard)**

Configure the VPN Security Gateway as the center gateway for the Site to Site VPN community. The gateways are the satellites.

The VPN communities in SmartDashboard and the SMP must have the same encryption settings.

**To add the satellite gateways to the new VPN community in SmartDashboard:**

1. Click **IPsec VPN tab > Communities.**

2. Click **New > Star Community.**
   The **Star Community Properties** window opens and shows the **General** page.

3. Enter the **Name** for the VPN community.

4. From the navigation tree, click **Center Gateways.**

5. Click **Add.**
   The **Add Center Gateways** window opens.


7. Click **OK.**
   The VPN Security Gateway is added to the **Participant Gateways** section.

8. From the navigation tree, click **Satellite Gateways.**
9. Click Add.
   The **Add Satellite Gateways** window opens.
10. Select the gateways.
11. Click OK.
    The satellite gateways are added to the **Participant Gateways** section.
12. Click OK.

**To configure the encryption settings for the VPN community:**
1. Right-click the VPN community and select **Edit**.
   The **Star Community Properties** window opens and shows the **General** page.
2. From the navigation tree, click **Encryption**.
3. In the **Encryption Method** section, click **IKEv1 only**.
4. In the **Encryption Suite** section, click **Custom**.
5. Click **Custom Encryption**.
6. Perform key exchange encryption with - **AES-256**
7. (Phase 1) Perform data integrity with **SHA1**
8. Perform IPsec data encryption with **AES 128**
9. (Phase 2) Perform data integrity with **SHA1**
10. Click OK.
11. From the navigation tree, click **Advanced Settings > Advanced VPN Properties**.
12. Use Diffie-Hellman group - **Group 2 (1024 bit)**
13. Renegotiate IKE security associations every **1440 minutes**
14. Renegotiate IPsec security associations every **3600 seconds**
15. Select **Disable NAT inside the VPN community**.
16. Click OK.

**Exporting the Security Management Server CA**
In SmartDashboard export the CA for the Security Management Server to a file. This is the CA for the external Security Management Server.

**To export the external Management CA:**
1. From the navigation tree, click the **Servers and OPSEC** icon.
2. Right-click **internal_ca** and select **Edit**.
3. Click the **Local Security Management Server** tab.
4. Click **Save As**.
5. Save the CA with the name **external_ca**.
6. Click OK.

**Adding the VPN Security Gateway to the SMP**

**To add the VPN Security Gateway to the SMP:**
1. Log in to the SMP.
2. Go to **Home > Gateways**.
3. Click **New**.
The Create New Gateway window opens.

4. Enter the Name of the VPN Security Gateway.

   Note - You do not need to use the same name for the external Security Gateway in the SMP as in SmartDashboard.

5. Enter the Static IP for the VPN Security Gateway.

6. Click Finish.

   The gateway object is created and shows the General page.

7. Click New.

8. The Internal Network Edit window opens.

9. For Network Name, enter the Interface name.

10. For Network Address, enter the IPv4 address.

11. For Network Mask, select the subnet mask.

12. Click Save.

13. Repeat steps 9 - 12 for each internal interface.

   The VPN Security Gateway is added to the SMP and is ready to be the center gateway for the VPN community.

**Importing the Security Management Server CA**

Import the CA from the Security Management Server [external Management] to the Service Domain in the SMP.

To import the CA to the Service Domain:

1. Go to Service Domain > Settings.

   The Service Domain Settings window opens and shows the General page.

2. Click the Certificates tab.

3. Click Add.

   The External CA page opens.

4. Click Import X.509.

   The Load X.509 Certificate File window opens.

5. Click Choose File.


7. Click OK.

8. Click Save.

   The certificate is added to the Service Domain.

**Creating and Configuring the VPN Community (SMP)**

Use the Edit Communities window in the SMP to create and then configure the VPN community. The VPN Security Gateway is the externally managed gateway and is the center gateway of the Star community. The gateways are the satellite gateways. You can configure a community to enable the satellites to communicate with each other through the center gateway.

You can configure the community so that the VPN Security Gateway is the only encryption domain for the satellite gateways.
To create the VPN Community in the SMP:
1. Go to Home > Communities.
2. Click New.
   The Create New Community wizard opens.
3. Enter the Name for the community.
4. Optional - Enter a Description of the community.
5. Click Finish.
   The community is created. The Edit page opens.
6. Click VPN Settings.
7. From VPN Type, select Star.
8. In Center Gateway, click Choose.
9. Enter the gateway Name or MAC address, or click Search for Gateways.
10. Click Next.
11. Click Done.
12. For Satellite Routing, select communication method between satellites:
   - No communication between satellites
   - Route to other satellites through center
   - Route to other satellites and internet through center - Supported only for externally managed centers.
13. Click Permanent Tunnel.
14. Click Disable NAT.
15. In Encryption Method select IKEv1.
16. Go to VPN Settings > IKE Settings.
17. Configure these IKE Phase 1 settings:
   - Encryption - AES-256
   - Authentication - SHA1
   - Diffie Hellman Group - Group 2
   - Renegotiate every - 1440
18. Configure these IKE Phase 2 settings:
   - Encryption - AES-256
   - Authentication - SHA1
   - Perfect Forward Secrecy - Disabled
   - Renegotiate every - 3660
   - VPN Tunnel Sharing - One VPN tunnel per subnet pair.
19. Click Save.

To add the satellite gateways to the VPN community:
1. In the VPN Communities Edit window, click the Members tab.
2. Click Add Gateway.
   The Add Gateways window opens.
3. Select the method for adding gateways:
   - Enter the Name
   - Enter the MAC address
Managing VPN Communities

• Search for Gateways
• Create a new gateway

4. Click Next.
5. Use the wizard to add the satellite gateways.
6. Click Done.

Exporting the SMP CA

Export the SMP CA to a file. This file is for the external Security Management Server and it is necessary to import it to SmartDashboard.

Make sure that the SMP administrator has permission to access the System settings.

To export the SMP CA:
1. Go to System > Settings.
2. Click Certificate Authority.
3. In the Root Certificate section, click Export X.509.
   The Internet browser saves the CA to a file.

Importing the CA to SmartDashboard and Updating the Policy

Import the SMP CA to SmartDashboard as a new trusted CA. It is necessary to create a new rule that allows traffic for the VPN community.

To import the CA to SmartDashboard:
1. From the navigation tree, click the Servers and OPSEC icon.
2. Right-click Trusted CAs and select New CA > Trusted.
   The Certificate Authority Properties window opens.
3. Enter the Name for the CA. For example, smp_ca
4. Click the OPSEC PKI tab.
5. Make sure that all the options are cleared.
6. Click Get.
7. Select the SMP CA file.
   A warning window opens.
8. Click OK.
9. In the Certificate Authority Properties window, click OK.
   The SMP CA is added to the Trusted CAs folder.

To update the policy:
1. Click the Firewall tab.
2. From the navigation tree, click Policy.
3. Add a new rule to the policy that allows traffic to the new VPN community.
4. Install the policy on the VPN Security Gateway.

Sample Firewall Rule
### Adding Gateways to SmartDashboard (Dynamic IP Address)

Create new objects for the gateways with dynamic IP addresses as Externally Managed VPN Gateways in SmartDashboard. Configure the internal IP address for each internal gateway interface.

You must have the DN for a gateway with a dynamic IP address to add it to SmartDashboard. We recommend that you log in to the SMP to add this gateway.

Before you add the gateway, make sure that you import the SMP CA to SmartDashboard. You must assign the SMP CA to the gateway.

This procedure is for gateways that use a dynamic external IP address. You can also add gateways that use a static IP address.

#### To get the DN for a gateway in the SMP:

1. Go to **Home > Gateways**.
2. Click the gateway name. The **Edit** page opens.
3. Click **VPN > Authentication Method**.
4. Copy the **Distinguished Name** field.

#### To add a gateway to SmartDashboard as an Externally Managed VPN gateway:

1. Log in to SmartDashboard.
2. Right-click the Network Objects tree and select **Check Point > More > Externally Managed Gateway**.
   The gateway window opens and shows the **General Properties** page.
3. Enter the SMP gateway name.
4. For **IPv4 Address**, click **Dynamic Address**.
   A warning window opens.
5. Click **Yes**.
6. For **Hardware**, select appliance. For SMB {600/1100/700}, select 1100 Appliances
7. From **Network Security**, click **IPsec VPN**.
8. From the navigation tree, click **Topology**.
9. Click **Manually defined on the Security Management Server, based on the below Topology Table**
10. Click **All IP Addresses behind Gateway are based on the below Topology Table**
11. Double-click the external interface.
12. Enter the **Name** of the external interface.
13. For **Network Type**, select **External (leads out to the Internet)**
14. Make sure **Dynamic IP** is selected
15. Click **OK**.
16. Double-click the external interface or click **New**.
17. Enter the Name of the internal interface
18. For Network Type, select **Internal (leads to the local network)**
19. For Static IP Address and Net Mask, enter the IPv4 address and subnet mask for the interface.
20. For Topology, select **Network defined by the interface IP and Net Mask**
21. Click **OK**.
22. From the navigation tree, click **IPsec VPN**.
23. Click **Matching Criteria**.
   The **Certificate Matching Criteria** window opens.
24. From **Gateway must present a certificate issued by CA**, select the SMP CA.
25. Click **DN**.
26. Enter or paste the **DN** (Distinguished Name) for the gateway.
27. Click **OK**.
28. In the Gateway Properties window, click **OK**.
   The gateway with a dynamic IP address is added to SmartDashboard.
Managing Service Domains

In This Section:

Adding Service Domains ...................................................................................... 93
Showing Service Domains .................................................................................... 93
Editing the General Page ..................................................................................... 93
Deleting Service Domains .................................................................................... 94
Showing Service Domain Histories ....................................................................... 94
Configuring the Settings for an SMP Service Domain ........................................... 95

Adding Service Domains

To add a Service Domain:

1. Click System > Service Domains.
   The Service Domains window opens.
2. Click New.
   The Create New Service Domain wizard opens.
3. Enter the Service Domain name. You cannot change this name after you create the Service Domain.
4. Enter a Description.
5. Enter the Company name.
6. Enter the Contact.
7. Enter the Email. You cannot use the SMP to send emails to this address.
8. Click Finish.
   The new Service Domain opens and shows the General page.

Showing Service Domains

The Enabled column shows if the portal is enabled (green check mark) or not (red X).

To show the Service Domains:
Go to System > Service Domains.

Editing the General Page

If the Service Domain is disabled, all users defined in the Service Domain cannot log in, and all gateways defined in the Service Domain are disabled.
To edit the General page of a Service Domain:
1. Go to System > Service Domain.
2. Click the Service Domain name.
   The Edit page opens and shows the General tab.
3. To enable the Service Domain, click Enabled.
4. Change the settings:
   • Name
   • Description
   • Enabled
   • Company
   • Contact
   • Email
5. Click Save.

Note - You can only edit the Name field in System > Service Domains > Edit.

Deleting Service Domains

To delete a Service Domains:
1. Go to System > Service Domains.
2. Select the Service Domain.
3. Click Delete.
   A confirmation window opens.
4. Enter your administrator password.
5. Click OK.
   The Service Domain is deleted.

Showing Service Domain Histories

To show the history for a Service Domain:
1. Go to System > Service Domains.
2. Click the Service Domain name.
   The Edit page opens and shows the General tab.
3. Click History.
   The History page shows the date when the Service Domain was created and when it was most recently modified.
Configuring the Settings for an SMP Service Domain

Configuring General Settings for Service Domains

To configure general settings for a Service Domain:

1. Go to Service Domain > Settings.
   The Settings page opens and shows the General page.
2. In Service Center Name, enter the name of the Service Center.
3. Click Save.

Showing and Editing External CAs for Service Domains

After you add a CA (Certificate Authority) to a Service Domain, it is also installed on the gateways for that Service Domain. This CA lets you create externally managed VPN communities.

To show the external CA for a Service Domain:

1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click the Certificates tab.
3. Click the CA.

To load a new certificate as the external CA:

1. Click Add.
   The External CA page opens.
2. Click Import X.509.
3. Click Choose File.
4. Select the file with the certificate.
5. Click OK.
6. Enter the details for the certificate.
7. Click Save.
   The external CA is updated with the new certificate.

Configuring Logging for Service Domains

Use the SMP to configure logging:

- Configure the severity of the generated logs.
- Forward logs to an external Syslog server.
- Delete old logs.

Note - The logging settings for the SMP do not change the Gateway logs.

To configure logging for a Service Domain:

1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click Logging.
3. In the **Log Level**, select the minimum severity that generates logs.

**To configure the server as a Syslog client for logs from the Service Domain:**
1. Click **Forward logs to an external Syslog Server**.
2. In **Syslog Server**, enter the IP address of the Syslog server.
3. In **Syslog Port**, enter the port number that is used to send the logs.

**To delete old logs:**
1. Click **Purge old logs**.
2. In **Older than**, enter the maximum number of days that logs are saved.
3. In **Action**
   - Select **Delete** to automatically delete old logs are deleted from the server.
   - Select **Archive** to archive old logs on the server.
4. Click **Save**.

**Configuring DNS Settings for Service Domains**

To enable the Dynamic DNS services, you must configure the DNS settings.

**To configure the DNS settings:**
1. Go to **Service Domain > Settings**.
   The **Settings** page opens and shows the **General** tab.
2. Click **DNS**.
   The **DNS** fields show:
3. For **Domain Suffix**, enter the DNS suffix for the SMP domain registration.
4. For **Dynamic IP Time to Live**, enter the number of seconds that a dynamic IP address remains in the DNS server’s cache after resolution. A longer time reduces the load on the server. A shorter time makes sure there is less downtime when you change IP addresses.
5. For **Static IP Time to Live**, enter the number of seconds that a static IP address remains in the DNS server cache after resolution. Static IP addresses include gateways configured with static IP addresses and mail servers (MX records). A longer time reduces the load on the server.
   - **Note** - This is the DNS server for the SMP. It is not the DNS server that is used for Dynamic DNS.
6. Click **Save**.

**Configuring Custom Fields for Service Domains**

You can configure custom fields for these objects:
- Users
- Gateways
- VPN Communities

**To configure custom fields for a Service Domain:**
1. Go to **Service Domain > Settings**.
   The **Settings** page opens for the Service Domain and shows the **General** tab.
2. Click Custom Fields.

To add a custom field:
1. Click User, Gateway, or Community custom fields.
2. Click New.
   The custom field is shown.
3. Enter the name field.
4. For example, Billing Code or Shipping Date.
5. Click Save.

To delete a custom field:
1. Select the custom field.
2. Click Delete.
3. Click Save.

Showing Firmware for Service Domains
You can view and manage a list of firmwares that are available in a specific Service Domain.

To show firmwares for a Service Domain:
1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click Firmware.
   The Firmware window opens and shows the firmware images that are available for the Service Domain.

Configuring Advanced Settings for Service Domains
If a gateway becomes disconnected from the server, you can configure how long it waits before it attempts to reconnect.

To manage gateways reconnection settings for a Service Domain:
1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click Advanced.
3. Click Remotely manage Server Connection Permanent Error Wait Time.
4. In Server Connection Permanent Error Wait Time, enter the number of seconds the gateway waits to reconnect to the server.
5. Click Save.

Uploading Images for Email Templates
Use the Custom Email Template Images window to upload logo and image files to the SMP. Add these logos and images to the SMP templates for emails, reports, and notifications.

To upload an image file to the SMP:
1. Go to Service Domain > Advanced.
The **Custom Email Template Images** page opens and shows the image files that are available for the Service Domain.

2. Click **New**.
   The **Create New Custom Image** window opens.

3. Click **Choose File**.
4. Use Windows Explorer to locate the file and click **Open**.
5. Enter the **Name** for the file in the SMP.
6. Click **Finish**.
   The **General** page for the image file opens.

7. **Optional** - If the image does not show, in **Display Description** enter the text and click **Save**.

**To add the image to a SMP template:**
1. From **Usage in reports**, copy the HTML tags and content.
2. Go to the SMP template. For example, **Service Domain > Settings > Notifications > Users**.
3. Click **Customize**.
   The **Message Template** window opens.
4. Click the **Edit** tab.
5. Paste the HTML into applicable place in the **Content** window.
6. Click **OK**.

**To delete images from the SMP:**
1. From the **Custom Email Template Images** window, select one or more custom image files.
2. Click **Delete**.
3. In the confirmation window, click **OK**.

**General Settings (Custom Image)**

**To show the General page for Custom Email Template Images:**
1. Go to **Service Domain > Advanced**.
   The **Custom Email Template Images** window opens and shows the image files that are available for the Service Domain.
2. Click the custom image.
   The **General** page is shown.
3. Change these settings:
   - **Comment**
   - **Display Description** - Enter alternate text if the image cannot be shown.
   - **Usage in reports** - HTML tags and content that you paste into the SMP template.
4. Click **Save**.

**History (Custom Images)**

**To show the History page for Custom Images:**
1. Go to **Service Domain > Advanced**.
The Custom Email Template Images window opens and shows the image files that are available for the Service Domain.

2. Click the custom image.  
   The General page opens.

3. Click History.  
   The History page opens and shows when the image was Created and Last Modified.
Managing Users

In This Section:

- Showing Users .................................................................................................. 100
- Searching for Users........................................................................................... 100
- Editing Users..................................................................................................... 101
- Sending Emails to Users.................................................................................... 103
- Showing Logs (Users) ........................................................................................ 104
- Exporting Users................................................................................................. 104
- Deleting Users .................................................................................................. 104
- Managing Gateways for a User........................................................................... 105

Showing Users

The Users window shows data for SMP users in the database.

- **User ID** - the user login name.
- **Role** - user privileges.
- **Status** - if users are logged in to the SMP:
  - Green - Logged in.
  - Red - Logged out.
  - Gray - The user does not have a password or is deactivated.

To show the SMP users:

Go to **Home > Users**.

Searching for Users

In the Search Users window, you can show only the specified users. You can also:

- Export the specified users list to Excel.
- Send an email to one or more users.

To search for users:

1. Go to **Home > Users**.
2. Click **Filter**.
   - The Users Search window opens.
3. Enter the search settings.
4. Click **Apply**.
   - The Search Results window opens.

To export the users table to Excel:

1. Select one or more users.
2. Click Actions > To Excel.
   The Internet browser saves the Excel file.

To configure the fields in the Users Search window:
1. For each search field:
   a) Select a search string modifier:
      - *is* - The string exactly matches the user data.
      - *contains* - The user data contains the string.
      - *not* - The user data does not match the string.
      - *none* - This field is empty.
   b) Enter one or more search strings.
2. For Community and Role, select the search option.
3. Select the time settings for the Creation and Modification Date for the users.
4. Click Apply.
   The Search Results window opens.

To reset the search fields and options:
In the Search window, click Clear.

Emailing a User Summary
You can email the user a summary of the user data:
- Name
- Email
- Username
- Communities

To email a summary of user data:
1. Go to Home > Users.
2. Click the User ID.
   The Edit page opens and shows the General tab.
3. Click View > Summary.
   The User Details Summary window opens.
4. Click Send Email.
   The summary is sent to the user.

Editing Users
You can edit the settings for a user and the list of their gateways.

To edit the settings for a user:
1. Go to Home > Users.
2. Click the User ID.
The Edit page opens and shows the General tab.

3. Change the user settings:
   - **General** - Email address, change Role, change password.
   - **Expiration** - Time that account remains active.
   - **Contact** - User contact information.
   - **Status** - List of SMP sessions.
4. Click **Save**.

**General Settings (User)**

To change the email address or Role for the user:
1. Go to **Home > Users**.
2. Click the **User ID**.
   The Edit page opens and shows the General tab.
3. In Email, enter the new email address.
   SMP sends emails for the user to this address.
4. In Role, select the role or the user.
5. Click **Save**.

To change the password for a user:
1. In the General page, click **Change**.
   The Change Password window opens.
2. Enter the new password.
3. Click **OK**.
   The password is changed.
4. Click **Save**.

**Expiration Settings (User)**

Use the Expiration window to deactivate the user’s account at a set date or time. After you deactivate the account, the user cannot log in to the SMP or gateway.

To configure the expiration settings for a user:
1. Go to **Home > Users**.
2. Click the **User ID**.
   The Edit page opens and shows the General tab.
3. Click **Expiration > User will expire in**.
4. From the drop-down menu, select one of the time settings:
   - Hours
   - Days
   - Months
5. Enter the number of hours, days, or months when the account will deactivate.
6. In **Start From**, click one of these options:
   - **First login** - Starts from the first time the user logs in to SMP.
Managing Users

7. Click **Save**.

**Contact Settings (User)**

Use the **Contact** window to enter the contact information for the user.

**To edit the contact information:**
1. Edit the appropriate fields.
2. Click **Save**.

**Custom Fields Settings (User)**

If the Service Domain uses **Custom Fields** for users, configure the settings in this window.

**To edit the custom fields information for a user:**
1. Go to **Home > Users**.
2. Edit the appropriate fields.
3. Click **Save**.

**Status Settings (User)**

**Status** shows if the user is logged in to the SMP:
- Green - Logged in.
- Red - Logged out.
- Gray - The user does not have a password or is deactivated for SMP.

These are the fields in this window:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date the user account was created.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Date the user account was last edited.</td>
</tr>
<tr>
<td>#</td>
<td>Session number for the user.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Date and time the user logged in.</td>
</tr>
<tr>
<td>Application</td>
<td>If the user logged in to SMP.</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP address from which the user connects to SMP.</td>
</tr>
</tbody>
</table>

**Sending Emails to Users**

You can send email to one or more SMP users.

**To send an email to users:**
1. Search for users.
   - Or
   - Click **Home > Users** to show all the users.
2. Select one or more of the users.
3. Click Actions > Mail to selected.
   The General Mail window opens and shows the Preview tab.
4. To edit the email, click Edit.
5. Click Send Email.

Showing Logs (Users)
You can show system logs for a user. You can filter the logs for the date range, severity, and other settings.

To show logs for a user:
1. Go to Home > Users.
2. Click the User ID.
   The Edit page opens and shows the General tab.
3. Click View > Today's system logs.
   The System Logs window opens and shows the user logs.

To filter the logs:
1. Click Actions > Filter.
2. The Filter the Logs window opens.
3. Change the filter settings.
4. Click Apply.
   The System Logs window opens and shows the user logs.

Exporting Users
You can export one or more users to an Excel file.

To export users:
1. Search for users.
   Or
   Click Home > Users to show all the users.
2. Select one or more of the users.
3. Click Actions > To Excel.
   The Internet browser saves the user data to an Excel file.

Deleting Users

To delete one or more users:
1. Go to Home > Users.
2. Select one or more users.
3. Click Delete.
A confirmation window opens.

4. Click **OK**.
   The user is deleted.

Managing Gateways for a User

Make sure that the gateway is connected to the SMP before you add it to a user.

**To add a gateway to a user:**

1. Go to **Home > Users**.
2. Click the **User ID**.
   The **Edit** page opens and shows the **General** tab.
3. Click the **Gateways** tab.
   The **Gateways** page opens.
4. Click **Add**.
   The **Add Gateways** wizard opens and shows the **Select Method** page.
5. Select one of these methods to add the gateway to the user:
   - **Name**
   - **MAC Address**
   - **Search for a gateway**
   - **Create a new gateway**
6. Click **Next**.
   The applicable window opens.

**To remove a gateway from a user:**

1. Go to **Home > Users**.
2. Click the **User ID**.
   The **Edit** page opens and shows the **General** tab.
3. Click the **Gateways** tab.
   The **Gateways** page opens.
4. Click **Remove**.
   A confirmation window opens.
5. Click **OK**.

**Note** - The gateway is not deleted from the database. Only the user’s link to the gateway is deleted.

You can update the gateways for a user. Make sure that the gateways are:

- Subscribed to a Remote Management plan.
- Connected to the SMP.

Adding a Gateway (Name)

**To use the gateway name to add it to a user:**

1. Go to **Home > Users**.
2. Click the **User ID**.
   The **Edit** page opens and shows the **General** tab.
3. Click the **Gateways** tab > **Add**.
   The **Add Gateways** wizard opens.
4. In the **Select Method** window, click **Name**.
5. In **Name**, enter the gateway name.
6. Click **Next**.
   The **Completed** window opens, and the gateway is added to the user.
7. Click **Done**.

### Adding a Gateway (MAC Address)

**To use the gateway MAC address to add it to a user:**

1. Go to **Home > Users**.
2. Click the **User ID**.
   The **Edit** page opens and shows the **General** tab.
3. Click the **Gateways** tab > **Add**.
   The **Add Gateways** wizard opens.
4. In the **Select Method** window, click **MAC address**.
5. In **MAC Address**, enter the gateway MAC address.
6. Click **Next**.
   The **Completed** window opens, and the gateway is added to the user.
7. Click **Done**.

### Adding a Gateway (Search)

**To search for the gateway and add it to a user:**

1. Go to **Home > Users**.
2. Click the **User ID**.
   The **Edit** page opens and shows the **General** tab.
3. Click the **Gateways** tab > **Add**.
   The **Add Gateways** wizard opens.
4. In the **Select Method** window, click **Search**.
5. Click **Next**.
   The **Search for gateways** window opens.
6. Use the search fields to filter the gateways.
7. Click **Next**.
   The **Add Gateways** opens and shows the applicable gateways.
8. Select one or more gateways.
9. Click **Next**.
   The **Completed** window opens, and the gateway is added to the user.
10. Click **Done**.
Adding a New Gateway

To create a new gateway and add it to a user:

1. Go to Home > Gateways > New.
   The Create New Gateway window opens.
2. Enter a Name or click Generate for a system generated name.
3. Select Type.
4. Clear the Managed by SMP checkbox to create this gateway as an externally managed VPN community gateway.
5. Select a Plan from the list. By default, the gateway inherits its default settings from this plan.
6. The Registration Key field shows an automatically generated registration key. You can enter a registration key or click Generate to generate a new registration key.
7. Enter a user name for Owner ID. Click Search to find an existing user or click New to create a new user.
8. Click Finish.
Overview of Roles

Roles define privileges for users and the changes that they are allowed to make in the SMP. Actions for different roles:

- Add and configure users.
- Manage gateways and assign them to users.
- Read SMP logs.
- Configure VPN connections and communities.

You can assign each user to only one role.

Using Predefined Roles

The SMP includes predefined roles. You can edit or delete these roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User</td>
<td>• Receive emails from SMP to activate gateway.</td>
</tr>
<tr>
<td></td>
<td>• Cannot log in to SMP.</td>
</tr>
</tbody>
</table>
### Configuring Roles for Users

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power User</td>
<td>• Show SMP objects.</td>
</tr>
<tr>
<td></td>
<td>• Change gateways, plans and End Users.</td>
</tr>
<tr>
<td></td>
<td>• Cannot change other users and roles.</td>
</tr>
<tr>
<td></td>
<td>• Send emails.</td>
</tr>
<tr>
<td></td>
<td>• Show Service Domain logs.</td>
</tr>
<tr>
<td>Read Only User</td>
<td>• Show SMP objects.</td>
</tr>
<tr>
<td></td>
<td>• Show Service Domain logs.</td>
</tr>
<tr>
<td>Super User</td>
<td>• Change SMP objects.</td>
</tr>
<tr>
<td></td>
<td>• Send emails.</td>
</tr>
<tr>
<td></td>
<td>• Show Service Domain logs.</td>
</tr>
<tr>
<td>Support User</td>
<td>• Show SMP objects.</td>
</tr>
<tr>
<td></td>
<td>• Create and configure gateways and End Users.</td>
</tr>
<tr>
<td></td>
<td>• Change SMP objects.</td>
</tr>
<tr>
<td></td>
<td>• Send emails.</td>
</tr>
<tr>
<td></td>
<td>• Show Service Domain logs.</td>
</tr>
</tbody>
</table>

## Creating New Roles

**To add a new role**

1. Go to *Service Domain > Roles*.
2. Click **New**.
   - The *Create New Role* window opens.
3. Enter the **Name** and **Description** for the role.
4. Click **Finish**.

## Showing Roles

**To show the roles:**

Go to *Service Domain > Roles*.

## Deleting Roles

You can delete roles except for the predefined roles. You cannot delete a role when it is assigned to users.
To delete one or more roles:
1. Go to Service Domain > Roles.
2. Select one or more roles.
3. Click Delete.
   A confirmation window opens.
4. Click OK.
   The role is deleted.

Editing Roles

Define the Access Control policy for each role to configure the permissions for users.

The SMP applies rules for roles in sequential order. For example, if rule 2 blocks an action but it is allowed in rule 4, users cannot do that action.

Configuring Rules for Roles

Use these fields to configure a role:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td><img src="#" alt="List" /> Allow - Allow users with this role to do the specified operations.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="List" /> Block - Users with this role cannot do the specified operations.</td>
</tr>
<tr>
<td>Operations</td>
<td>Actions that the user can do in the SMP.</td>
</tr>
<tr>
<td>Object type</td>
<td>Select the SMP object for this rule.</td>
</tr>
<tr>
<td>Condition</td>
<td>Enter a condition that defines when the rule applies.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a condition string, the rule always applies.</td>
</tr>
</tbody>
</table>

To configure a rule for a role:
1. Go to Service Domain > Roles.
2. Click the role name.
   The Edit page opens.
4. Create or edit a rule:
   ![List](#) To create a new rule, click New.
   ![List](#) To edit a rule, click the rule number.
   The Edit Role Rule: Step 1 window opens.
5. Configure the Permission and Operations for the role.
6. Click Next.
   The Edit Role Rule: Step 2 window opens.
7. Configure the Object type and Condition criteria for the role.
8. Click Next.
   The Edit Role Rule: Step 3 window opens.
9. Click Finish.
   The Edit Role window closes.
10. Click **Save**.

**Using String Operators for Roles**

Basic condition string operators:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td>Condition string elements must be the same.</td>
<td>element == element</td>
<td>Rule applies when the user ID is the same as the current user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>uid == CurrentUser.uid</td>
</tr>
<tr>
<td>!=</td>
<td>Negates an equation between condition string elements.</td>
<td>element != element</td>
<td>Rule applies when the user ID is not the same as the current user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>uid != CurrentUser.uid</td>
</tr>
<tr>
<td>&amp;&amp;</td>
<td>Concatenates condition string elements. The rule must match all of the</td>
<td>element &amp;&amp; element</td>
<td>Rule applies when the role is not <strong>End User</strong> and not <strong>Power User</strong>:</td>
</tr>
<tr>
<td></td>
<td>condition string elements.</td>
<td>[&amp;&amp; element...]</td>
<td>role != &quot;End User&quot; &amp;&amp; role != &quot;Power User&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Alternates between condition string elements. The rule must match at least</td>
</tr>
<tr>
<td></td>
<td>one of the condition string elements.</td>
<td>[</td>
<td></td>
</tr>
<tr>
<td>Contains</td>
<td>Shows that the element is a member of the array.</td>
<td>Contains(array,</td>
<td>Rule applies for communities that contain the current user’s gateways:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>element)</td>
<td>Contains(communities, CurrentUser.gateways)</td>
</tr>
<tr>
<td>Intersects</td>
<td>Shows that the two arrays intersect.</td>
<td>Intersects(array1,</td>
<td>Rule applies for gateways that the current user owns:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>array2)</td>
<td>Intersects(gateways, CurrentUser.gateways)</td>
</tr>
<tr>
<td>!</td>
<td>Negates condition string elements.</td>
<td>! element</td>
<td>Rule applies only for gateways that do not belong to the current user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>!Intersects(gateways, CurrentUser.gateways)</td>
</tr>
<tr>
<td>Length</td>
<td>Shows the length of an array or the number of characters in a string.</td>
<td>Length(array</td>
<td>element)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Length(CurrentUser.gateways)!=0</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
<td>Syntax</td>
<td>Example</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Matches</td>
<td>Compares the value of a condition string element to a regular expression.</td>
<td>Matches(element, regular-expression)</td>
<td>Rule applies when the gateway name starts with &quot;gw&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Matches(name, &quot;gw.+&quot;)</td>
</tr>
</tbody>
</table>

Deleting Role Rules

**To delete a role rule**

1. Go to Service Domain > Roles.
2. Click a role name.
3. Select the rule.
4. Click **Delete**.
   - A confirmation message appears.
5. Click **OK**.
   - The rule is deleted.
6. Click **Save**.

Configuring Advanced Role Settings

You can configure additional permissions for a role and define the range of IP addresses that it can use to connect to the SMP.

**To configure advanced settings for a role:**

1. Go to Service Domain > Roles.
2. Click a role.
   - The Edit page opens.
3. Click **Advanced**.
4. Select the **Additional Permissions**:
   - Access SMP Portal
   - Enable Lost Password Recovery
   - Access API
   - View Logs
   - Send Email
5. Click **Save**.

**To define the range of IP addresses for a role:**

1. In the Restrictions section, select the **Allow access only from the following IP address ranges**.
2. Click **New**.
3. Enter the range of IP addresses.
4. Click **Save**.
To delete a range of IP addresses for a role:
1. In the Restrictions section, select the range of IP addresses.
2. Click Delete.
   A confirmation window opens.
3. Click OK.
   The IP address range is deleted from the list.
4. Click Save.

Resetting Predefined Roles to Default Settings

To reset a predefined role to its default settings
1. Go to Service Domain > Roles.
2. Click the role name.
   The Edit page opens.
3. Click Revert.
Configuring SMP Administrators

In This Section:

Showing Administrators .................................................................................... 114
Adding SMP Administrators ............................................................................... 114
Editing SMP Administrators ............................................................................... 115
Deleting SMP Administrators............................................................................. 115
Configuring SMP Administrator Account Expiration ........................................... 116
Configuring SMP Administrators’ Contact Details .............................................. 116
Showing SMP Administrator Statuses ................................................................ 116

Showing Administrators

The **Status** column shows if an administrator is currently logged on to the SMP [green icon] or not [red icon].

**To show the SMP administrators:**

Go to **System > Administrators**.

Adding SMP Administrators

**To add an SMP administrator:**

1. Go to **System > Administrators**.
2. Click **New**.
   The **Create New Administrator** window opens.
3. Enter this information:
   - **User ID** - Administrator user name. The User ID must not be used by other users or administrators.
   - **First Name**
   - **Last Name**
   - **Email**
   - **Type** - Select **Administrator** for permissions to edit all the SMP settings, or **Read Only Administrator** for permissions to only see all the windows.
   - **Password**
4. Click **Finish**.
   The **System > Administrators > Edit** window opens and shows with the **General** page for the administrator.
Editing SMP Administrators

To edit an SMP administrator:

1. Go to System > Administrators.
2. Click the SMP administrator name.
   
   **Note** - If you are a Read-Only administrator, you can only click on your User ID.
   The Edit page opens.
3. Configure the settings:
   - First name
   - Last Name
   - Title
   - Company
   - Email
   - Additional emails
   - Access rights - Select Administrator for permissions to edit all the SMP settings, or Read Only Administrator for permissions to only see all the windows.
   - Password
   - Description
4. Click Save.

To change the password for an administrator:

1. Go to System > Administrators.
2. Click the SMP administrator name.
   The Edit page opens.
3. In the General page, click Change.
   The Change Password window opens.
4. Enter the new password.
5. Click OK.
   The password is changed.
   Click Save.

You can also configure:

- SMP Administrator account expiration
- Administrators’ contact details

Deleting SMP Administrators

To delete an SMP administrator:

1. Go to System > Administrators.
2. Select the SMP administrator.
3. Click Delete.
   A confirmation message opens.
4. Click OK.
Configuring SMP Administrator Account Expiration

Use the Expiration window to deactivate the administrator’s account at a set date or time. After you deactivate the account, the administrator cannot log in to the SMP or gateway.

To configure the expiration settings for an SMP administrator:

1. Go to System > Administrators.
2. Click the SMP administrator.
   The Edit page opens.
3. Click Expiration.
   The Expiration page opens.
4. Click Expiration > User will expire in.
5. From the drop-down menu, select one of the time settings:
   - Hours
   - Days
   - Months
6. Enter the number of hours, days, or months when the account will deactivate.
7. In Start From, click one of these options:
   - First login - Starts from the first time the user logs in to SMP.
   - Specified date - Starts from the configured time.
8. Click Save.

Configuring SMP Administrators' Contact Details

To configure contact details for an SMP administrator:

1. Go to System > Administrators.
2. Click the SMP administrator.
   The Edit page opens.
3. Click Contact.
   The Contact page opens.
4. Enter the information in the applicable fields.
5. Click Save.

Showing SMP Administrator Statuses

The Status page shows if the administrator is logged in to the SMP Portal:

- Green - Logged in.
- Red - Logged out.
- Gray - The administrator does not have a password or is deactivated.

To view the status of an SMP administrator:

1. Go to System > Administrators.
2. Click the SMP administrator.
The **Edit** page opens.

3. **Click Status.**

The **Status** fields show:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date the user account was created.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Date the user account was last edited.</td>
</tr>
<tr>
<td>#</td>
<td>Session number for the user.</td>
</tr>
<tr>
<td>Login Time</td>
<td>Date and time the user logged in.</td>
</tr>
<tr>
<td>Application</td>
<td>Shows if the user logged in to SMP.</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP address from which the user is connecting to SMP.</td>
</tr>
</tbody>
</table>
Managing Firmwares for Gateways

In This Section:
- Showing Firmwares ........................................................................................... 118
- Adding Firmware to the SMP System ................................................................. 118
- Deleting Firmware from the SMP System .......................................................... 118
- Managing Firmware .......................................................................................... 119
- Showing Firmware Histories.............................................................................. 119
- Showing Firmware for Service Domains ............................................................ 119

Showing Firmwares

You can show all firmwares in the SMP system. The firmware packages are not stored on the SMP Server. Instead, the SMP saves links to the packages on the Check Point Support Center.

To show or edit a firmware:
Go to System > Firmware.

Adding Firmware to the SMP System

When you add a firmware image to the SMP, you add a link to that package on the Check Point Support Center. The gateway downloads the package from the Support Center.

To add a new firmware to the SMP:
1. Go to System > Firmware.
   The System > Firmware page opens and shows the firmware images.
2. Click New.
   The Add Firmware window opens and shows the available firmware packages.
3. Select one or more packages.
4. Click Next.
   The firmware is added to the SMP.
5. Click Done.

Deleting Firmware from the SMP System

Note - You cannot delete a firmware if it is currently in use by a gateway or plan.

To delete a SMP firmware from the server:
1. Go to System > Firmware.
2. Select the firmware image.
3. Click Delete.
   A confirmation message opens.
Managing Firmwares for Gateways

Managing Firmware

In the General Firmware page, you can enable or disable a firmware image for the SMP and gateways.

**To manage firmware images:**

1. Go to System > Firmware.
2. Click the Edit firmware icon.
   - The Edit Firmware window opens and shows the General page.
3. To manage the SMP firmware:
   - To enable the firmware for the SMP, select Enabled
   - To disable the firmware, clear Enabled
   - **Important** - If you disable the firmware, you cannot configure gateways to use it.
4. Click Save.

Showing Firmware Histories

Only SMP administrators can configure these settings.

**To show the history for the firmware:**

1. Go to System > Firmware.
2. Click the Edit firmware icon.
   - The Edit window opens and shows the General page.
3. Click History.

Showing Firmware for Service Domains

You can view and manage a list of firmwares that are available in a specific Service Domain.

**To show firmwares for a Service Domain:**

1. Go to Service Domain > Settings.
   - The Settings page opens and shows the General tab.
2. Click Firmware.
   - The Firmware window opens and shows the firmware images that are available for the Service Domain.
Managing SMP Servers

In This Section:
- Understanding the SMP Server Architecture ...................................................... 120
- Showing and Editing SMP Servers ..................................................................... 120
- Adding Security Management Servers ............................................................... 126
- Deleting an SMP Server ..................................................................................... 126
- Showing the Security Management Server Settings ........................................... 126
- Managing Licenses without the Portal ............................................................... 128

Understanding the SMP Server Architecture

SMP Server
SMP Server is the Windows Server on which the SMP is installed. To implement the SMP, it uses:
- Quantum Spark Portal
- Active Directory
- Check Point Security Management Server

Two SMP Server modules that manage the gateways:
- CMLS - Creates a secure connection between the SMP and the gateways
- JMLS - Processes data sent by the CMLS and the gateways

Active Directory Database
The data and settings for the gateways managed by SMP are stored in the Active Directory database.

SMP Portal
The SMP Portal is an Internet browser based application that helps you configure and manage the different SMP components, users, gateways, and system settings. You use a secure HTTPS connection to log in to the Portal.
The SMP Portal is hosted on an Apache Tomcat application server.

Showing and Editing SMP Servers
These icons show the status of an SMP module:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>●</td>
<td>Module is up</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>●</td>
<td>Module is down</td>
</tr>
<tr>
<td>●</td>
<td>Module is disabled</td>
</tr>
<tr>
<td>●</td>
<td>Module is up with errors</td>
</tr>
</tbody>
</table>

To show the SMP server modules:
1. Go to System > SMP Servers.
   The SMP Servers window opens and shows a list of servers.
2. Click the server.
   The Server window opens and shows the General page in the Configure tab.

Showing the General Page

To show the General page for a SMP Server:
1. Go to System > SMP Servers.
   The SMP Servers window opens and shows a list of servers.
2. Click the server name.
   The Server window opens and shows the General page in the Configure tab.

Configuring the Settings for a SMP Server

The SMP Address is the same as the settings for the Windows server interface.

For deployments with multiple SMP Servers, enter the DNS name in System > Settings > General page.

SMP deployments that use more than one server can configure the Load Balancing weight for these types of traffic:
- Gateway logs
- Gateway heartbeats

The higher the Load Balancing value, the higher the percentage of traffic that is sent to the specified server. For example, for a deployment with two servers:

<table>
<thead>
<tr>
<th>Load Balancing Field (Log Server)</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancing Weight</td>
<td>200</td>
<td>2/3 of the gateway logs are sent to this server</td>
</tr>
<tr>
<td>Load Balancing Weight</td>
<td>100</td>
<td>1/3 of the gateway logs are sent to this server</td>
</tr>
</tbody>
</table>

To configure the IP address settings for the SMP Server:
1. Go to System > SMP Servers.
   The SMP Servers window opens and shows a list of servers.
2. Click the server name.
   The Server window opens and shows the General page in the Configure tab.
3. Click Settings.
4. Configure these settings in the **Server IP Addresses** section:
   - **IP Address** - The IP Address for the SMP Server.
   - **NAT IP Address (external IP address)** - Optional - Enter the NAT IP address for the server. When this field is empty, the server uses the **SMP Address**.
   - **DNS Name** - Optional - Enter the DNS name for the SMP Server. When this field is empty, the server uses the **SMP NAT Address**.

5. Configure these settings in the **Load Balancing** section:
   - **Load Balancing Weight (as Log Server)** - Enter the value to increase or decrease the percentage of gateway logs that are sent to this server. The default value of 100 distributes gateway logs equally to all servers.
   - **Load Balancing Weight as Configuration Deployment Server** - Enter the value to increase or decrease the percentage of gateway heartbeat traffic that is sent to this server. The default value of 100 distributes gateway heartbeat traffic equally to all servers.

6. Click **Save**.

### Showing the Managed Modules

**To show the Managed Modules for a SMP Server:**

1. Go to **System > SMP Servers**.
   - The **SMP Servers** window opens and shows a list of servers.
2. Click the server name.
   - The **Server** window opens and shows the **General** page in the **Configure** tab.
3. Click **Managed Modules**.
   - These default processes are shown:
     - SMP - Main process of the SMP
     - JMLS - Process for communication between the SMP and the gateways
     - CPD - Main process of the Security Management Server
     - Log Server - Process that stores gateway logs
     - Syslog - Stores gateway Syslogs (system logs)

### Configuring the SMS Module

**To configure the settings for the SMS Module:**

1. Go to **System > SMP Servers**.
   - The **SMP Servers** window opens and shows a list of servers.
2. Click the server name.
   - The **Server** window opens and shows the **General** page in the **Configure** tab.
3. Click **SMS Module > SMS Settings**.
4. Configure the settings and the IP addresses for the server:
   - **Description**
   - **Server Relative Weight** - Enter the load balancing capacity relative to the other servers. The default setting is 1.
   - **Enabled** - Select this option to enable the SMS module. This module manages the Dynamic DNS requests. If the SMS is disabled, it does not respond to requests from gateways or participate in load balancing.
5. Click **Save**.

**Notes:**
- A server with a Server Relative Weight of 2 can handle twice as many gateways as a server with a setting of 1.
- Disable the SMS for a SMP Server that is not connected to the network.

**Configuring the IP Address for an SMS Module**

You must configure the IP address settings for the SMS (Security Management Server) module when:
- The Security Management Server has more than one IP address.
- You are using Dynamic DNS for the gateways.
  - The Security Management Server connects gateways to the Service Domain. The gateways must use their fully qualified ID to connect to the SMP.
  
  **Note** - Each IP address can be attached to a different default Service Domain.

**To configure the IP address settings for the SMS module:**

1. Go to **System > SMP Servers**.
   - The **SMP Servers** window opens and shows a list of servers.
2. Click the server name.
   - The **Server** window opens and shows the **General** page in the **Configure** tab.
3. Click **SMS Module > SMS Settings**.

**To add an IP address:**

1. Click **New**.
2. The **Edit Server Address** window opens.
3. Enter the **NAT Address** and **Default Service Domain**.
4. Click **Finish**.
5. Click **Save**.

**To edit the IP address:**

1. Click the IP address.
2. The **Edit Server Address** window opens.
3. Enter the **NAT Address** and **Default Service Domain**.
4. Click **Finish**.
5. Click **Save**.

**To delete an IP address:**

1. Select the IP address.
2. Click **Delete**.
3. A confirmation message opens.
4. Click **OK**.
5. Click **Save**.
Managing SMP Servers

**Configuring Advanced Settings**

**To configure advanced server settings:**

1. Go to **System > SMP Servers**.
   The **SMP Servers** window opens and shows a list of servers.
2. Click the server name.
   The **Server** window opens and shows the **General** page in the **Configure** tab.
3. Click **Advanced**.
4. Configure these settings:
   - **Console Port (TCP)** - This port is used to access the server from a browser to view its updated status. The default is **9283**.
   - **Concurrent downloads limit** - Enter the maximum number of items (such as a security policy or firmware) that the Security Management Server send to the gateways at the same time. Use this setting to limit the bandwidth the SMP uses to update the gateways. The default setting is **50**.
5. Click **Save**.

**Showing Security Management Server Status**

**To show the status of an SMP Server:**

1. Go to **System > SMP Servers**.
   The **SMP Servers** window opens and shows a list of servers.
2. Click the server name.
   The **Server** window opens and shows the **General** page in the **Configure** tab.
3. Click **SMS Module**.
   The table below lists the fields that show.
4. To refresh the data on this page, click **Refresh**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The SMS name.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time the SMS was added to the SMP.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>The date and time the SMS was last modified.</td>
</tr>
<tr>
<td>Server is</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Up</strong> - The SMS is active.</td>
</tr>
<tr>
<td></td>
<td><strong>Down</strong> - The SMS is not active or cannot be reached due to a network problem.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> - The SMS is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Up (with Errors)</strong> - The SMS is active, but there are errors.</td>
</tr>
<tr>
<td>Version</td>
<td>The SMS version number</td>
</tr>
<tr>
<td>Address</td>
<td>The SMS's IP address and port number in the format: <code>&lt;SMS IP&gt;:&lt;Port Number&gt;</code></td>
</tr>
<tr>
<td>NAT IP</td>
<td>The IP address of the NAT device behind which the SMS is located. If the SMS is not located behind a NAT device, this field displays N/A.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate will expire on</td>
<td>The date the SMS’s certificate expires, in the format: Month DD, YYYY</td>
</tr>
<tr>
<td>Up Since</td>
<td>The date and time when the SMS last started.</td>
</tr>
<tr>
<td>Downloads</td>
<td>The number of gateways currently downloading software from the SMS.</td>
</tr>
<tr>
<td></td>
<td>To view all downloading gateways, click View.</td>
</tr>
<tr>
<td>Modules</td>
<td>For each module that is enabled in the server, the status in this SMS:</td>
</tr>
<tr>
<td></td>
<td>• ON - The service is enabled in the SMS.</td>
</tr>
<tr>
<td></td>
<td>• OFF - The service is disabled in the SMS.</td>
</tr>
<tr>
<td></td>
<td>• FAIL - The service has failed.</td>
</tr>
<tr>
<td>Database - Primary</td>
<td>Indicates the primary database’s status, followed by the database’s name:</td>
</tr>
<tr>
<td></td>
<td>• Active - The primary database is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Standby - The primary database is disabled.</td>
</tr>
<tr>
<td>Database - Secondary</td>
<td>Indicates the secondary database’s status, followed by the database’s name:</td>
</tr>
<tr>
<td></td>
<td>• Active - The secondary database is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Standby - The secondary database is disabled.</td>
</tr>
<tr>
<td></td>
<td>• N/A - No secondary database is configured.</td>
</tr>
</tbody>
</table>

### Showing Security Management Server Diagnostics

Diagnostic information for an SMP Server is only available for servers that are currently active.

**To view diagnostics for an SMP Server:**

1. Go to System > SMP Servers.
   - The SMP Servers window opens and shows a list of servers.
2. Click the server name.
   - The Server window opens and shows the General page in the Configure tab.
3. Click the Diagnostics tab.
   - The CPU Usage and Memory Usage are shown.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Time</td>
<td>The percentage of time that the CPU is in User Mode.</td>
</tr>
<tr>
<td>System Time</td>
<td>The percentage of time that the CPU is in System Mode.</td>
</tr>
<tr>
<td>Real Active</td>
<td>The amount of physical memory the server uses.</td>
</tr>
<tr>
<td>Real Total</td>
<td>The amount of physical memory installed on the server.</td>
</tr>
<tr>
<td>Virtual Active</td>
<td>The amount of virtual memory the server uses.</td>
</tr>
</tbody>
</table>
Adding Security Management Servers

To add a new Security Management Server:

1. Go to System > SMS Servers.
2. Click New Server.
   The Create New Server Wizard opens the Create New Server: Step 1 dialog box.
3. Enter the information for these fields:
   • Server Name - You cannot change the name after you save.
   • SMS Address
   • SMP Server Address
   • SMP Nat Address (external IP address)
4. Click Next.
   The Create New Server: Step 2 dialog box opens.
5. Click Finish.

Deleting an SMP Server

To delete an SMP Server:

1. Go to System > SMP Servers.
   The SMP Server window opens and shows a list of servers.
2. Click the Delete icon in the server's row.
   A confirmation message opens.
3. Click OK.
   The SMP Server is deleted.

Showing the Security Management Server Settings

The SMS Servers Edit window lets you configure these Security Management Server settings:

• Security settings with the gateways
• SMP modules
• Logging policy

The settings apply to all the SMP Servers installed on the Security Management Server.

Showing the General Page for the Security Management Server

To show the General page for the SMP Servers:

1. From the navigation tree, click System > SMP Servers.
   The SMP Servers window opens and shows a list of servers.
2. Click SMS Global Settings.
   The SMS Global Settings window opens and shows the General page.
3. Enter the information for these fields:
   - **Description**
   - **Setup interval** - How often (in seconds) the gateways poll the SMP for a new configuration. The default is 600.
   - **Security lease time** - Select the amount of time that the encryption key between the SMP and the gateways is valid. The default is 1 day.

4. Select DRM (DNS Resolving Module) to enable the Dynamic DNS service for the SMP Server.

5. Click **Save**.

### Configuring the Log Policy

You can add an unlimited number of logging rules.

**To configure the log policy for the Security Management Servers:**

1. Go to **System > SMP Servers**.
   The **SMP Servers** window opens and shows a list of servers.

2. Click **SMS Global Settings**.
   The **SMS Global Settings** window opens and shows the **General** page.

3. Click **Log Policy**.

4. The **Log Policy** page opens.

5. Configure the settings:
   - **Protocol** - Select the type of logging destination. If you select local, the Server URL field is disabled.
   - **Server URL** - The log server address.
   - **Severity** - Select the minimal message severity to send to the logging destination.
   - **Origin** - Select the message origin (Security Management Server or Gateway) to filter. Select * if you do not want to filter based on message origin.

6. To add a new rule, click **New**.

7. To edit a rule, click the rule name in the **Protocol** column.

8. Click **Finish**.
   The **Log Policy** table shows the logging rule.

9. Click **Save**.

### Deleting Logging Policy Rules

**To delete a logging policy rule:**

1. In the **Log Policy** page, select the logging rule.

2. Click **Delete**.
   A confirmation message opens.

3. Click **OK**.
   The logging rule is deleted from the logging policy.

4. Click **Save**.
Showing the SMP Server History

To show the History page for the Security Management Server:

1. Go to System > SMP Servers.
   The SMP Servers window opens and shows a list of servers.
2. Click SMS Global Settings.
   The SMS Global Settings window opens and shows the General page.
3. Click History.
   The History page opens and shows when the Security Management Server was Created and Last Modified.

Managing Licenses without the Portal

You can add SMP licenses without the SMP Portal. For example, for deployments with multiple SMP Servers, you cannot use the Portal for the Primary SMP Server to add licenses to the Secondary servers. These are the options to manually add a license:

- Run the cplic putlic CLI command
- Use the Check Point Configuration Tool

The license that you receive from the Check Point User Center contains the correct settings for all the cplic putlic parameters. Do not change these settings when you add a license.

Run cplic del to delete a license from the SMP. It is necessary to enter the license hash signature when you run this command.

To add an SMP license with the CLI:

1. From the SMP Server, click Start > Command Prompt.
2. Run cplic putlic <IP address> <Expiration> <license string>
3. From the SMP Portal, click System > Settings.
   The System Settings window opens and shows the General page.
4. Click License Management.
5. Click Apply Licenses.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the SMP Server</td>
</tr>
<tr>
<td>expiration</td>
<td>Date that the SMP license expires</td>
</tr>
<tr>
<td>license string</td>
<td>Hash signature for the license</td>
</tr>
</tbody>
</table>

To add an SMP license with the Check Point Configuration Tool:

1. From the Start menu, click All Program Files > Check Point SmartConsole R77.30 > Check Point Configuration.
   The Check Point Configuration Tool opens and shows the Licenses and contracts page.
2. Enter the license data:
   - Copy the license string and then click Paste License
   - Enter the settings for the license
   Click the User Center link to get more information about the SMP license.
3. Click OK.
4. From the SMP Portal, click **System > Settings.**
   The **System Settings** window opens and shows the **General** page.
5. Click **License Management.**
6. Click **Apply Licenses.**

**To delete a license from the SMP:**
1. From the SMP Server, click **Start > Command Prompt.**
2. Run: `cplic print -x` to show the hash signature for the license.
3. Run: `cplic del <hash signature>`
   The SMP license is deleted.
Importing and Exporting SMP Objects

In This Section:

- Moving SMP Object and Settings Data .............................................................. 130
- Exporting SMP Data .......................................................................................... 130
- Importing SMP Data ......................................................................................... 132

Moving SMP Object and Settings Data

The Tools window lets you move the SMP objects and settings data to different Service Domains or servers. Use this window to export to an XML file and then import the data. You can choose to move only system or Service Domain data or both.

These are the objects and settings that you can move for the SMP system:

- Firmware objects
- Server settings
- SMP Administrator objects
- System settings

These are the objects and settings that you can move for all or a single Service Domain:

- Service Domain users
- Gateways
- Plans
- VPN communities, Custom images, and Roles
- Service Domain settings

To show the Tools window:
Go to System > Tools.

Exporting SMP Data

Export the SMP and Service Domain data to an XML file. The file is saved by the Internet browser. You can use the file to move the data to one or more different Service Domains or SMP Servers.

Exporting Data with the SMP Portal

The Export Wizard helps you export data for the SMP system and Service Domains.

When you export gateways you must include the plans for the Service Domain. In addition, you can only import a gateway if the gateway owner is also configured in the Service Domain.

To export the SMP data with the Portal:
1. Go to System > Tools.
The Tools window opens.

2. Click Export.
   The Export Wizard opens and shows the Choose System Data window.

3. Select the SMP system settings and objects.
   This data is shared by all the Service Domains.

4. Click Next.
   The Choose Service Domain Data window opens.

5. In the Export the following Service Domains section, select one option:
   - To export only SMP system data, click None.
   - To export data for all the Service Domains, click All Service Domains.
   - To export for one Service Domain, click Choose a Service Domain and select the Service Domain.

6. In the Export the following Service Domain data section, select one or more Service Domain settings and objects.

7. Click Next.
   The data is converted to XML. The Export Database Completed page opens. If errors occurred during the export process, the window shows them in a table.

8. Click Save As.
   The Internet browser saves the XML file.

9. Click Done.
   The Export Wizard closes.

Exporting SMP Data from the Command Line

To export the SMP database through the command line:

1. Open a command line.

2. Enter this command:
   ```
   exporter [a][d][f][g][i][p][s][t][u][y][-] destination_file [SMP_IP_address username password]
   {none | all | Service Domain} [Service Domain_name]
   ```

   For information on the command’s flags, see the table below.

   For example, to export system settings and plans to the file SMP_data.xml, enter this command:
   ```
   exporter p t SMP_data.xml
   ```
   The data is exported to the specified file.

These are the Exporter Flags:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
</table>
| a    | Exports all data.  
This command overrides all other commands. |
| d    | Exports SMP administrators. |
| f    | Exports firmware. |
| g    | Exports gateways.  
Note - When you export gateways, you must also export plans. |
## Importing and Exporting SMP Objects

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>Exports items (Communities, User Interfaces, Policies, and Roles).</td>
</tr>
<tr>
<td>P</td>
<td>Exports plans.</td>
</tr>
<tr>
<td>s</td>
<td>Exports server groups and servers.</td>
</tr>
<tr>
<td>t</td>
<td>Exports system settings.</td>
</tr>
<tr>
<td>u</td>
<td>Exports users.</td>
</tr>
<tr>
<td>y</td>
<td>Exports SMP system settings and the SMP system license.</td>
</tr>
<tr>
<td>-</td>
<td>Exports the user and administrator passwords in cleartext. If you do not include this flag, the passwords are encrypted.</td>
</tr>
</tbody>
</table>

- **destination_file**: The path to the destination file. If the file already exists, it is overwritten.
- **SMP_IP_address**: The IP address of the SMP from which to export data.
- **username**: The username to access the SMP.
- **password**: The password to access the SMP.
- **none**: Exports only SMP system settings (without Service Domain-specific settings).
- **all**: Exports SMP system settings and Service Domain-specific data for all SMP virtual Service Domain in the system.
- **Service Domain**: Exports SMP system settings and Service Domain-specific data for a specific SMP virtual Service Domain.
- **Service Domain_name**: If more than one SMP virtual Service Domain is configured, and you use the Service Domain flag, specify from which Service Domain to export the data.

## Importing SMP Data

You can import only data that is not in the database or import all data and replace existing data with imported data.

### Importing Data with the SMP Portal

The Import Wizard lets you import an XML file that you exported from the SMP. This file contains settings and objects for the SMP system and Service Domains.

The XML file also contains data for the CA (Certificate Authority).

**To import SMP data with the Portal:**

1. Go to **System > Tools**. The **Tools** window opens.
2. Click **Import**. The **Import Wizard** opens and shows the **Import from File** page.
3. Click **Choose file**.
4. Use Windows explorer to browse to the XML file that contains the SMP data and then click **Open**.
5. In the **Options** section, select one of these options:

- **Do not override existing data** - Imports only data that is not currently in the SMP or Service Domain.
- **Replace existing data** - Imports all data and overwrites the data in the SMP system or Service Domain.

6. If necessary, select a **Certificate Handling** option:

- **Retain existing certificates** - Ignores the CA in the XML file. The SMP creates new certificates for objects that are not based on the SMP CA.
- **Import all certificates** - If there is a CA in the XML file, it is imported. The SMP creates new certificates for all objects based on the imported CA.
- **Revoke all certificates** - Revokes the root CA. The SMP creates new certificates for the imported and existing objects.

7. In the **Import into the following service domain** sections, select one of these options:

- **All Service Domains** - Imports the settings and objects in the XML file into all the Service Domains. New Service Domains in the XML file are created in the SMP.
- **Choose a Service Domain** - Imports the settings and objects in the XML file into the specified Service Domain.

8. Click **Next**.

   The **Import Database Completed** page opens.

9. Click **Done**.

**Importing SMP Data from the Command Line**

**To import SMP database from the command line**

1. Open a command line.

2. Enter this command:

   ```bash
   importer source_file {f|n} [SMP_IP_address username password] [Service Domain_name]
   ```

   For information on the command’s flags, see the table below.

   For example, if you want to import data from the file `SMP_data.xml` and not overwrite existing data, enter this command:

   ```bash
   importer n SMP_data.xml
   ```

   The data is imported from the specified file.

**Importer flags:**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source_file</td>
<td>The path to the source file.</td>
</tr>
<tr>
<td>f</td>
<td>Imports all data in the file and overwrites the data currently in the SMP database with the imported data, without asking for a confirmation.</td>
</tr>
<tr>
<td>n</td>
<td>Imports only data that does not currently exist in the database, and writes error messages to the console for data that already exists in the SMP database.</td>
</tr>
<tr>
<td>SMP_IP_address</td>
<td>The IP address of the SMP to which to import data.</td>
</tr>
<tr>
<td>username</td>
<td>The username to access the SMP.</td>
</tr>
<tr>
<td>Flag</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><em>password</em></td>
<td>The password to access the SMP.</td>
</tr>
<tr>
<td><em>Service</em></td>
<td>If more than one SMP virtual Service Domain is configured, you can specify the target Service Domain to which to import the data. Data is imported from the first Service Domain in the source file into the specified Service Domain.</td>
</tr>
<tr>
<td>Domain name</td>
<td>If you do not specify a target Service Domain, all of the data in the source file is imported to the relevant Service Domains.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>- By default, the original Service Domain names are used.</td>
</tr>
</tbody>
</table>
Monitoring and Logs

In This Section:

Showing Logs .......................................................................................................................... 135
Debugging Information ............................................................................................................ 137

Showing Logs

Showing Gateway Logs

Gateway logs detail all firewall-related events:
• Logged allowed connections
• Logged dropped connections
• Detected viruses
• Web sites blocked by URL filtering
• Suspected spam

To show the gateway logs:
1. Go to Logs > Gateway Logs.
   The Gateway Logs window opens and shows a table of log entries.
2. You can use these tools with the logs:
   • Show and hide columns
   • Filter the logs

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Connection Accepted</td>
<td>The firewall allowed the connection.</td>
</tr>
<tr>
<td>🟥</td>
<td>Connection Dropped</td>
<td>The firewall dropped the connection.</td>
</tr>
<tr>
<td>🔐</td>
<td>Connection Decrypted</td>
<td>The firewall decrypted the connection.</td>
</tr>
<tr>
<td>🤔</td>
<td>Connection Encrypted</td>
<td>The firewall encrypted the connection.</td>
</tr>
<tr>
<td>🚫</td>
<td>Connection Rejected</td>
<td>The firewall rejected the connection.</td>
</tr>
<tr>
<td>🕵️♀️</td>
<td>Connection Monitored</td>
<td>A security event was monitored, but not blocked.</td>
</tr>
</tbody>
</table>

Showing System Logs

System logs detail the following events:
• Scheduler events
  The Scheduler performs these scheduled tasks:
  • Renewing certificates
• Deleting expired certificates from the list of revoked certificates
• Actions performed by SMP users and administrators
• All non-recoverable errors
• All changes to SMP system settings

To show system logs:
1. Go to Logs > System Logs.
   The System Logs window opens.
2. To export the logs to an Excel file, click Actions > To Excel.

System Log Columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Severity of the event.</td>
</tr>
<tr>
<td>Date</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>Origin</td>
<td>The name of the host or gateway that generated the log.</td>
</tr>
<tr>
<td>Service Domain</td>
<td>The Service Domain for the log.</td>
</tr>
<tr>
<td>App</td>
<td>Application that generated the log message.</td>
</tr>
<tr>
<td>User</td>
<td>Username that generated the log.</td>
</tr>
<tr>
<td>Message</td>
<td>Description of the event.</td>
</tr>
<tr>
<td>Information</td>
<td>Additional information about the event.</td>
</tr>
</tbody>
</table>

System Log Severity Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟥</td>
<td>Error - These logs are usually connected to the database.</td>
</tr>
<tr>
<td>⚠</td>
<td>Warning</td>
</tr>
<tr>
<td>🔄</td>
<td>Notice - These logs are generated for actions that are completed successfully.</td>
</tr>
</tbody>
</table>

Showing Activity Logs

You can show the status and progress of all background activities in the SMP. You can sort the activities according to the columns.

To show the activity logs for a Service Domain:
1. Go to Logs > Activity Logs.
   The Activity Logs window opens.
2. To remove the completed activities from the log, click Actions > Clear Finished.
3. To cancel an activity:
   a) Select the row.
   b) Click Actions > Cancel.
      A confirmation message opens.
   c) Click OK.
4. To export the displayed tasks, click **Actions > To Excel**. The activity log is exported to an Excel file.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Checkmark]</td>
<td>Done</td>
<td>Activity completed successfully.</td>
</tr>
<tr>
<td>![Orange X]</td>
<td>Canceled</td>
<td>Activity was canceled and did not complete.</td>
</tr>
<tr>
<td>![Red X]</td>
<td>Failed</td>
<td>Activity failed and did not complete.</td>
</tr>
<tr>
<td>![Bell]</td>
<td>In progress</td>
<td>Activity is in progress.</td>
</tr>
<tr>
<td>![Clock]</td>
<td>Waiting</td>
<td>SMP waits for a response from the logging service.</td>
</tr>
</tbody>
</table>

**Filtering Logs**

You can set a filter on general logs and gateway logs to display:

- Logs from different date or time ranges
- Logs of different severities or actions
- Logs containing specific text

The filter settings are persistent through the user session.

**Setting Filters**

To set a filter:

1. Go to **Logs > Gateway Logs > Actions > Filter**. The **Filter the Logs** window opens.
2. Configure the settings for the log filter:
   - **Scope** - Select **This Service Domain** or **All Service Domains**.
   - **Start Date** - Select the earliest date for logs shown.
   - **End Date** - Select latest date for logs shown
   - **Origin** - **Is** shows only logs that match and **Not** shows only logs that do not match.
   - **User** - **Is** shows only logs that match and **Not** shows only logs that do not match.
   - **Free Text** - Filter the logs for any column that matches the string.
   - **Min. Severity** - Select the lowest severity for logs shown.
   - **Limit Results to** - Set the highest number of logs shown.
3. Click **Apply**.

**Debugging Information**

The SMC and JMLS logs are in addition to the logs accessible from the SMP WebUI.

**SMC logs**

These logs, located at `%SMP_HOME%\Tomcat\Logs\smc.log`, include:

- SMP logs for WebUI actions
- Periodic tasks
• Gateway Cloud Services - Cloud activation, security reports, firmware upgrade

To configure the logger level:

1. Open the file: `%SMP_HOME%\Tomcat\webapps\SMC\WEB-INF\INFO.properties`
2. Change the value of the property `CONSOLE_LOGGER_LEVEL` to the applicable level:
   - Debug
   - Info  (default)
   - Error.
3. Restart the Apache-Catalina service.

JMLS logs

Gateway SMP logs are located at:
%JMLS_HOME%\64bit\apache-tomcat-7.0.47\logs\jmls.log

To configure the logger level:

1. Go to: `%JMLS_HOME%\64bit\apache-tomcat-7.0.47\lib\log4j.properties`
2. Change the value of the property `log4j.rootLogger` to the applicable level:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>All levels including custom levels.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Fine-grained informational events. Most useful to debug an application.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Error events that still allow the application to continue to run.</td>
</tr>
<tr>
<td>INFO</td>
<td>Informational messages that highlight the progress of the application at coarse-grained level.</td>
</tr>
<tr>
<td>OFF</td>
<td>The highest possible level. Intended to turn off logging.</td>
</tr>
<tr>
<td>WARN</td>
<td>Designates potentially harmful situations.</td>
</tr>
</tbody>
</table>

3. Restart the Apache Tomcat Jmls service.
Using Reports, Notifications, and Custom Alerts

In This Section:

- Using SMP Notifications .................................................................................... 139
- Using Custom Alerts.......................................................................................... 144

This chapter explains how to use:

- Security reports
- Vulnerability reports
- Notifications
- Custom Alerts

Using SMP Notifications

You can configure the SMP to automatically email notifications to system administrators and gateway owners for different events.

The notifications are in HTML format. You can view them in the Portal and customize them.

Configuring SMP System Notifications

You can specify which types of system notifications are sent automatically.

To use SMP system notifications, you must configure mail settings for the SMP.

Note - This task is relevant for SMP administrators only.

Configuring System Administrator Notifications

You can configure SMP to send notifications to SMP system administrators for specified events.

To configure SMP system notifications:

1. Go to System > Settings.
   The Settings window opens and shows the General page.
2. Click Notifications.
3. Configure which notifications to send to system administrators:
   - Server and system failures
   - Logs low disk space
   - SMP license expiration when license expires in X days
   - SMP license exceeded
4. To edit the notification emails sent to administrators, click Customize.
5. Click Save.
**Configuring Portal Administrator Notifications**

You can configure SMP to send notifications to Service Domain administrators when the portal license has expired or been exceeded.

To enable Service Domain notifications:

1. Go to **System > Service Domains**.
2. Click the Service Domain name.
   
   The **Edit** window opens and shows the **General** tab.

3. Click **Notifications**.
4. Click **Notify Service Domain administrator of SMP license expiration or license exceeded**.
5. Click **Save**.

**Configuring Service Domain Statistics Reports**

To configure portal statistics reports:

1. Go to **System > Settings**.
   
   The **Settings** window opens and shows the **General** page.

2. Click **Notifications > Reports**.
3. Select one or more of these options:
   - **Send short Service Domain statistics report**
   - **Send extended Service Domain statistics report**
4. Specify the time ranges,
5. To edit the reports, click **Customize**.
6. Click **Save**.

**Configuring Service Domain Notifications**

You can specify which types of notifications are sent for a Service Domain.

To use Service Domain notifications, you must configure mail settings for the Service Domain.

**Configuring Gateway Notifications**

To configure gateway notifications:

1. Go to **Service Domain > Settings**.
   
   The **Settings** window opens.

2. Click **Notifications > Gateways**.
3. Click the checkboxes to specify notifications:
   - Notify owner of gateway added/changed
   - Notify when gateways connect or have been disconnected for over
4. Click **Save**.

Click **Customize** to specify the email notification details:

- When a new gateway is connected for the first time.
- When a gateway is disconnected.
• When a gateway is reconnected (only after a disconnect notification message was sent).

You can configure when to send disconnect notifications. By default, notifications are sent only if the disconnect is longer than 2 days. You can also configure the time of day to send the notification.

If the disconnect notification time is set to minutes, the default is 30 minutes.

Notifications for all disconnected gateways are sent in a single email. The administrator does not receive a separate email for each disconnected gateway.

**Configuring Gateway Report Notification**

**Gateway Reports** let you customize the email notification for gateway reports:

• Email with the report as an attachment
• Email with an embedded report

**To configure gateway report templates:**

1. Go to **Service Domain > Settings**.
   The **Settings** window opens.
2. Click **Notifications > Gateway Reports**.
3. Select the language for **Customize report’s message for this language**:
4. To select the email template, click **Customize** next to:
   - **Complete message (with report as an attachment)**
   - **Or**
   - **Preface text (to an embedded report)**

   The **Report** window opens in the **Preview** tab. You can edit the text, and add and remove administrators and users.

**Configuring User Notifications**

**To configure user notifications:**

1. Go to **Service Domain > Settings**.
   The **Settings** window opens.
2. Click **Notifications > Users**.
3. Select **Notify user of creation of new account or of change in account**.
4. To edit the notification emails that are sent, click **Customize**.
5. Click **Save**.

**Configuring Summary Messages**

**To configure summary messages:**

1. Go to **Service Domain > Settings**.
   The **Settings** window opens.
2. Click **Notifications > Summary Messages**.
3. To edit the summary messages, click **Customize**.
4. Click **Save**.
Configuring Summary Reports (Service Domains)

To configure summary reports:
1. Go to Service Domain > Settings. The Settings window opens for the Service Domain and shows the General page.
2. Click Notifications > Reports.
3. Select or clear Send summary report.
4. Configure the frequency of the reports:
   - Daily
   - Weekly
   - Monthly
5. From every, select the day of the week that reports are sent.
6. To edit the notification emails that are sent, click Customize.
7. Click Save.

Customizing Notifications

You can customize all notification types. For example, you can add your company’s logo to the notifications, or specify which SMP administrators should receive a copy.

Note - You cannot change the format of SMP system notifications.

To customize a notification
2. Click Notifications.
3. Click the type of Notification. The page opens.
4. Click Customize next to the notification. The Message Template dialog box appears and shows the Preview tab.
5. Click the Edit tab.
6. In the Subject field, enter the text.
7. In the BCC field, enter the email addresses to receive a copy of the notification.
8. In the script text box, edit the template.
   Or
   Load a notification template:
   a) Click Browse to browse to the file containing the report template, or enter the filename in the File text box. The file can be a *.txt or *.html file.
   b) Click Load File.
9. To reset the HTML script to its default settings, click Default.

To select the SMP administrators to receive a copy of the notification:
1. Click the Administrators tab.
2. Click Add.
3. Select the desired administrators.
4. Click Done.

**To send an email to an administrator:**
Click the administrator's email address.

**To remove an administrator:**
Select the administrator and click Remove.

**To select users who should receive a copy of the notification:**
*Note* - This is only relevant to configure Service Domain notifications.

1. Click the **Users** tab.
2. Click **Add**.
   
   The **Add User Wizard** appears and shows the **Select Method** dialog box.

**To select an existing user:**

1. Enter the **User ID**. *Note* - The User ID must already be defined in the system.
2. Click **Next**.
   
   The **Completed** dialog box appears.

**To search for users:**

1. Select **Search for users**.
2. Click **Next**.
   
   The **Search for Users** dialog box appears.
3. Complete the fields.
4. Click **Next**.
   
   The **Add User** dialog box appears with a list of users that meet the specified search criteria.
5. Click the checkboxes for desired users.
6. Click **Next**.
7. The **Completed** dialog box appears.

**To create a new user:**

1. Select **Create a new user**.
2. Click **Next**.
   
   The **Create New User Wizard** opens and shows the **Create New User: Step 1** dialog box.
3. Complete the fields using the information in User Details Fields.
4. Click **Next**.
   
   The **Create New User: Step 2** dialog box appears.
5. Complete the fields using the information in User Details Fields.
6. Click **Next**.
   
   The **Create New User: Step 3** dialog box appears.
7. Click **Finish**.
   
   The **Create New User Wizard** closes.
   
   The **Add User Wizard** reappears and shows the **Completed** dialog box.
8. Click **Done**.
   The specified user(s) appear in the **Users** tab.
   The user(s) will appear in the notification’s BCC field.

**To send an email to a user:**
Click the user’s email address.

**To remove a user from the Users tab:**
Select the user and click **Remove**.

**To preview the notification:**
1. Click **Preview**.
   The **Preview** tab reappears and shows the report with your changes.
2. If you are satisfied with the notification, click **OK**.

### Using Custom Alerts

You can configure the SMP to automatically generate alerts when it receives specified log messages. Alerts can be sent as an email message and a log message, or as a log message.

#### Using SMP System Custom Alerts

To use SMP custom alerts, you must configure mail settings for the SMP.

**To add or edit custom alerts:**

1. Go to **System > Settings**.
   The **System > Settings** window opens and shows the **General** page.
2. Click **Custom Alerts**.
3. Configure the alert:
   - To add a new alert, click **New**.
   - To edit an existing alert, click the alert name.
4. Complete the fields.
5. Configure the alert action:
   - If you selected **Log Only** in the **Action** drop-down list, continue at Log Only Alerts (on page 145).
   - If you selected **Send Email** in the **Action** drop-down list, continue at Send Email Alerts (on page 146).

---

**Custom Alerts Details Window**

**To configure the details for a new custom alert:**

1. Complete the fields listed in the table below.
   **Note** - Only logs that match the **Filter** and fulfill the **Recurrences** conditions generate the alert.
2. Click **OK**.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the alert name with no spaces.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this option to enable the alert.</td>
</tr>
<tr>
<td>Description</td>
<td>The description appears in the custom alert log message.</td>
</tr>
</tbody>
</table>

### Filter

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ID</td>
<td>Select the only Log ID that generates the alert.</td>
</tr>
<tr>
<td>Min. Severity</td>
<td>Select the minimum severity for logs to generate the alert.</td>
</tr>
<tr>
<td>Free Text</td>
<td>Enter a string that logs must contain to generate the alert.</td>
</tr>
</tbody>
</table>

### Recurrences

- **At least** - The alert is generated when the number of logs is greater than the value for the time interval (too many logs).
- **Less than** - The alert is generated when the number of logs is less than the value for the time interval (too few logs).

### Matching events are received from

- **From the same source** - The logs must originate from the same source to generate the alert.
- **From any** - The logs can originate from any source to generate the alert.

### Alert Action

- **Send Email** - Send an email to the SMP administrators specified in the Administrators tab. Also, write a log message to the General Logs table.
- **Log Only** - Write a log message to the General Logs table.

### Log Only Alerts

**To generate Log Only Alerts:**

1. Go to **System > Settings**.
   - The System > Settings window opens and shows the General page.
2. Click **Custom Alerts**.
3. Configure the alert:
   - To add a new alert, click **New**.
   - To edit an existing alert, click the alert name.
4. Complete the fields.
5. Configure the alert action.
6. Click **OK**.
   - The dialog box closes.
7. Click **Save**.
Send Email Alerts

To send email alerts:
1. Do the first 5 steps in the procedure Using SMP Server Custom Alerts (on page 144).
2. Click the Edit tab.
   The Edit tab shows.
3. For Subject, enter the text for the alert’s Subject line.
4. For BCC, enter the email addresses that receive a copy of the alert.
5. In the script text box, edit the template.
   Or
   Load an alert template.

To load an alert template:
1. Click Browse to browse to the file with the report template, or enter the filename in the File text box. The file can be a *.txt or *.html file.
2. Click Load File.

To reset the HTML script to its default settings:
Click Default.

To select the SMP administrators:
1. Click Administrators.
2. Click Add.
3. Select the administrators.
4. Click Done.

To send an email to an administrator:
Click the administrator’s email address.

To remove an administrator from the Administrators tab:
1. Select the administrator.
2. Click Remove.

To select users:
1. Click Users.
2. Click Add.
   The Add User Wizard opens and shows Select Method.
3. To select an existing user, enter the User ID.
   Note - The User ID must already be defined in the system.
4. Click Next.
   The Completed window shows.

To search for users:
1. Select Search for users.
2. Click Next.
The **Search for Users** window opens.

3. Complete the fields with the information in User Search Fields.

4. Click Next.
   The **Add User** window opens.

5. Select the user(s).

6. Click Next.
   The **Completed** window opens.

### To create a new user:

1. Select **Create a new user**.

2. Click Next.
   The **Create New User Wizard** opens and shows **Create New User: Step 1**.

3. Complete the fields with the information in User Details Fields.

4. Click Next.
   The **Create New User: Step 2** window opens.

5. Complete the fields with the information in User Details Fields.

6. Click Next.
   The **Create New User: Step 3** window opens.

7. Click Finish.
   The **Create New User Wizard** closes.
   The **Add User Wizard** opens and shows the **Completed** window.

8. Click Done.

### To send email to a user:

Click the user’s email address.

### To remove a user from the Users tab:

1. Select the user.

2. Click Remove.

### To preview the alert:

Click Preview.

### When you are ready to finish:

1. If you are satisfied with the alert, click **OK**.
   The window closes.

2. Click **Save**.

### Viewing and Deleting Custom Alerts

### To view or delete custom alerts:

1. Go to **System > Settings**.

2. Click **Custom Alerts**.
To delete an alert:
1. Select the alert.
2. Click Delete.
   A confirmation message appears.
3. Click OK.
   The alert is deleted.
4. Click Save.

Using Service Domain Custom Alerts

Before you use Service Domain custom alerts, you must configure mail settings for the SMP Service Domains.

To show the Custom Alerts for Service Domains:
1. Go to Service Domain > Settings.
   The Settings window opens and shows the General tab.
2. Click Custom Alerts.

Adding and Editing Custom Alerts

To add or edit custom alerts
1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click Custom Alerts.
3. To add a new alert, click New.
4. To edit an existing alert, click the alert.
5. Complete the fields using the information in Custom Alerts Details Fields.
6. Complete the alert settings.

To generate Log Only Alerts:
1. Go to System > Settings.
   The System > Settings window opens and shows the General page.
2. Click Custom Alerts.
3. Configure the alert:
   • To add a new alert, click New.
   • To edit an existing alert, click the alert name.
4. Complete the fields.
5. Configure the alert action.
6. Click OK.
   The dialog box closes.
7. Click Save.

To send email alerts:
1. Do the first 5 steps in the procedure Using SMP Server Custom Alerts (on page 144).
2. Click the **Edit** tab. 
   The **Edit** tab shows.
3. For **Subject**, enter the text for the alert’s Subject line. 
4. For **BCC**, enter the email addresses that receive a copy of the alert.
5. In the script text box, edit the template. 
   Or 
   Load an alert template.

**To load an alert template:**
1. Click **Browse** to browse to the file with the report template, or enter the filename in the **File** text box. The file can be a *.txt or *.html file.
2. Click **Load File**.

**To reset the HTML script to its default settings:**
Click **Default**.

**To select the SMP administrators:**
1. Click **Administrators**.
2. Click **Add**.
3. Select the administrators.
4. Click **Done**.

**To send an email to an administrator:**
Click the administrator’s email address.

**To remove an administrator from the Administrators tab:**
1. Select the administrator.
2. Click **Remove**.

**To select users:**
1. Click **Users**.
2. Click **Add**.
   The **Add User Wizard** opens and shows **Select Method**.
3. To select an existing user, enter the User ID. 
   **Note** - The User ID must already be defined in the system.
4. Click **Next**.
   The **Completed** window shows.

**To search for users:**
1. Select **Search for users**.
2. Click **Next**.
   The **Search for Users** window opens.
3. Complete the fields with the information in User Search Fields.
4. Click **Next**.
   The **Add User** window opens.
5. Select the user(s).
6. Click Next.
   The Completed window opens.

To create a new user:
1. Select Create a new user.
2. Click Next.
   The Create New User Wizard opens and shows Create New User: Step 1.
3. Complete the fields with the information in User Details Fields.
4. Click Next.
   The Create New User: Step 2 window opens.
5. Complete the fields with the information in User Details Fields.
6. Click Next.
   The Create New User: Step 3 window opens.
7. Click Finish.
   The Create New User Wizard closes.
   The Add User Wizard opens and shows the Completed window.
8. Click Done.

To send email to a user:
Click the user’s email address.

To remove a user from the Users tab:
1. Select the user.
2. Click Remove.

To preview the alert:
Click Preview.

When you are ready to finish:
1. If you are satisfied with the alert, click OK.
   The window closes.
2. Click Save.

Viewing and Deleting Custom Alerts

To view or delete custom alerts
1. Go to Service Domain > Settings.
   The Settings page opens and shows the General tab.
2. Click Custom Alerts.

To delete an alert:
1. Select the check box next to the alert.
2. Click Delete.
A confirmation message appears.

3. Click **OK**.
   The alert is deleted.

4. Click **Save**.
Troubleshooting the SMP

In This Section:
- Activating the Map License ................................................................. 152
- Dynamic DNS - Gateways Cannot Push Actions to the SMP ............... 152
- Using Internet Explorer to Access Gateways ...................................... 153

Activating the Map License

The SMP Map View window includes a 30-day temporary license. You must activate the temporary license for each SMP session. The functionality of the Map window is the same with the temporary and permanent license. The same license is used for the SMP and gateway Map View windows.

After you add the permanent license to the SMP, you can activate the license for the Map View window.

To activate the permanent Map license:

1. Go to Home > Map.
   The window opens and shows the Map Permission Error message.
2. Click activation request.
   An email message opens with the necessary details to activate the Map license. The To address in the email is: smbmgmt.service@checkpoint.com
3. Optional - In SMP DNS name, enter additional DNS settings.
4. Send the email to Check Point.
   It can take time for Check Point to add apply the Map license for your SMP account.

To use the temporary Map license:

1. From the Map View window, click Continue in trial mode.
   The temporary license is only valid for 30 days.
2. Optional - To activate the permanent license, click Resolve.
   The SMP shows the Map Permission Error message.

Dynamic DNS - Gateways Cannot Push Actions to the SMP

For deployments that use Dynamic DNS for the gateways, Windows may not use the correct IP address to communicate with the gateways. For example, actions that the SMP pushes to the gateway, such as Security Reports, are not sent.

When there are multiple IP addresses on an interface, Windows 2008 Server automatically selects which one connects to the gateways. The SMP must use the external IP address to connect to the gateways.

- Make sure that the external IP address is closer to the default Gateway IP address than the Dynamic DNS IP address.
- We recommend that the external IP address is on the same subnet as the default Gateway. The Dynamic DNS IP address uses a different subnet.

For more about how Windows uses multiple IP addresses on one interface, go to Microsoft kb969029 https://support.microsoft.com/en-us/kb/969029.

**Note** - The previous link is to the Microsoft Support web site. Check Point is not responsible for the information on that web site.

### Using Internet Explorer to Access Gateways

The default security settings for Internet Explorer do not allow it to connect to the gateway Portal. When you try to access the gateway, the browser shows a window with this error message: **Request Refused SMP Portal.**

Install the SMP certificate for the gateway as a self-signed certificate in Internet Explorer to configure it to access the gateway Portal.
Appendix: Regular Expressions

In This Appendix

SMP Regular Expressions ................................................................. 154
Regular Expression Syntax ............................................................. 154

SMP Regular Expressions

Use regular expressions to configure the settings for roles (on page 110).

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Backslash</td>
<td>escape metacharacters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>non-printable characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>character types</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square Brackets</td>
<td>character class definition</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis</td>
<td>sub-pattern, to use metacharacters on the enclosed string</td>
</tr>
<tr>
<td>{min[,max]}</td>
<td>Curly Brackets</td>
<td>min/max quantifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n} - exactly n occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,m} - from n to m occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,} - at least n occurrences</td>
</tr>
<tr>
<td>.</td>
<td>Dot</td>
<td>match any character</td>
</tr>
<tr>
<td>?</td>
<td>Question Mark</td>
<td>zero or one occurrences {equals {0,1}}</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>zero or more occurrences of preceding character</td>
</tr>
<tr>
<td>+</td>
<td>Plus Sign</td>
<td>one or more occurrences {equals {1,}}</td>
</tr>
<tr>
<td></td>
<td>Vertical Bar</td>
<td>alternative</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex</td>
<td>anchor pattern to beginning of buffer {usually a word}</td>
</tr>
<tr>
<td>$</td>
<td>Dollar</td>
<td>anchor pattern to end of buffer {usually a word}</td>
</tr>
<tr>
<td>-</td>
<td>hyphen</td>
<td>range in character class</td>
</tr>
</tbody>
</table>