Important Information

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

**Latest Documentation**
The latest version of this document is at:

To learn more, visit the Check Point Support Center ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 June 2015</td>
<td>Updated <em>Showing the SMP License</em> (on page 26)</td>
</tr>
<tr>
<td>31 May 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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

Please help us by sending your comments ([mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Management Portal R12 Administration Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Management Portal R12 Administration Guide)).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to SMP</td>
<td>9</td>
</tr>
<tr>
<td>Overview of the SMP</td>
<td>9</td>
</tr>
<tr>
<td>Logging in to the SMP</td>
<td>9</td>
</tr>
<tr>
<td>Managing Gateways with Plans</td>
<td>10</td>
</tr>
<tr>
<td>Managing the Gateway Settings from the SMP</td>
<td>10</td>
</tr>
<tr>
<td>Using Software Blades and Services</td>
<td>10</td>
</tr>
<tr>
<td>Understanding the SMP Server</td>
<td>11</td>
</tr>
<tr>
<td>Implementing SMP</td>
<td>12</td>
</tr>
<tr>
<td>Creating a New Plan</td>
<td>12</td>
</tr>
<tr>
<td>Using Software Blades</td>
<td>13</td>
</tr>
<tr>
<td>Backing Up Gateway Settings to an FTP Server</td>
<td>13</td>
</tr>
<tr>
<td>Creating New Users</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Outgoing Mail Settings for Service Domains</td>
<td>14</td>
</tr>
<tr>
<td>SMP Scenarios and Workflows</td>
<td>15</td>
</tr>
<tr>
<td>Creating VPN Communities</td>
<td>15</td>
</tr>
<tr>
<td>Configuring DNS Settings for the SMP Server</td>
<td>16</td>
</tr>
<tr>
<td>Adding Gateways</td>
<td>17</td>
</tr>
<tr>
<td>Managing Gateways behind NAT</td>
<td>18</td>
</tr>
<tr>
<td>Gateway Maintenance</td>
<td>18</td>
</tr>
<tr>
<td>Upgrading a Gateway Remotely</td>
<td>18</td>
</tr>
<tr>
<td>Sending Security Reports</td>
<td>19</td>
</tr>
<tr>
<td>Configuring Dynamic DNS for Gateways</td>
<td>20</td>
</tr>
<tr>
<td>Configuring General SMP Settings</td>
<td>21</td>
</tr>
<tr>
<td>Using the SMP WebUI</td>
<td>21</td>
</tr>
<tr>
<td>Showing the SMP Status</td>
<td>21</td>
</tr>
<tr>
<td>Showing Active User Sessions for Service Domains</td>
<td>22</td>
</tr>
<tr>
<td>Showing the Gateway Map View</td>
<td>22</td>
</tr>
<tr>
<td>Configuring Settings for the SMP Server</td>
<td>23</td>
</tr>
<tr>
<td>Configuring General Settings for the SMP</td>
<td>23</td>
</tr>
<tr>
<td>Configuring SMP Logging</td>
<td>24</td>
</tr>
<tr>
<td>Configuring the SMP WebUI to Use a Web Proxy Server</td>
<td>24</td>
</tr>
<tr>
<td>Configuring Outgoing Mail Settings for the SMP</td>
<td>25</td>
</tr>
<tr>
<td>Showing the SMP License</td>
<td>26</td>
</tr>
<tr>
<td>Configuring SMP Backup Settings</td>
<td>27</td>
</tr>
<tr>
<td>Starting the SMP Backup</td>
<td>28</td>
</tr>
<tr>
<td>Configuring the SMP Internal Certificate Authority</td>
<td>28</td>
</tr>
<tr>
<td>Configuring SMP Notifications</td>
<td>29</td>
</tr>
<tr>
<td>Configuring Management Access Control</td>
<td>29</td>
</tr>
<tr>
<td>Managing Gateways</td>
<td>31</td>
</tr>
<tr>
<td>Showing and Editing Gateways</td>
<td>31</td>
</tr>
<tr>
<td>Configuring General Settings</td>
<td>32</td>
</tr>
<tr>
<td>Setting the Gateway Location</td>
<td>33</td>
</tr>
<tr>
<td>Configuring Gateway Owners</td>
<td>34</td>
</tr>
<tr>
<td>Showing Gateway Status</td>
<td>35</td>
</tr>
<tr>
<td>Showing Gateway Logs</td>
<td>36</td>
</tr>
</tbody>
</table>
Managing VPN Communities

Overview

VPN Community Types

Diagram of VPN Community Types

Understanding Nested Communities

Creating VPN Communities

Showing Communities

Configuring the Community General Settings

Filtering the Communities Table

Deleting Communities

VPN Settings

Configuring VPN Settings

Assigning a Center Gateway

Configuring IKE Settings

Configuring Communities’ Custom Fields

Configuring Communities’ Members Lists

Creating Community Topologies

Viewing Community Histories

Showing a Summary of a Community

Managing VPN Community with an External Gateway

Preparing to Add an External Gateways

Configuring a VPN Community with External Gateways
Introduction to SMP

In This Section:

- Overview of the SMP .................................................................9
- Logging in to the SMP .................................................................9
- Managing Gateways with Plans ..................................................10
- Managing the Gateway Settings from the SMP ..............................10
- Using Software Blades and Services ...........................................10
- Understanding the SMP Server ..................................................11

Overview of the SMP

The SMP (Security Management Portal) is a Check Point product that lets MSPs (Managed Service Providers) and large companies centrally manage small security appliances and give customers value added services.

The SMP provides a scalable and efficient mechanism to centrally configure and monitor SMB gateways. In addition, you can use the SMP to create flexible business models and support different SMB 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 that you have a username and password for your Service Domain.

If you see warning that the certificate for this site is not trusted, you can click Continue and safely use the SMP WebUI.

For a list of supported Internet browsers, go to the SMP Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=33100) for your version.

To log in to the SMP:

1. From the Internet browser,
   - If you are using the Check Point Cloud service, go to https://smbmgmtservice.checkpoint.com/SMC (https://smbmgmtservice.checkpoint.com/SMC)
   - If you are using a local server, go to https://<SMP Server IP address>/SMC or https://<SMP Server domain>/SMC

The Check Point Security Management 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 WebUI opens.

### Managing Gateways with Plans

The SMP uses plans to help you manage gateways that share the same features or security settings. Each gateway that you define in the SMP is assigned to a plan. The default setting is that the gateways use all of the plan settings. Manually unlock the gateway from specified features and Software Blades in the plan to customize the gateway for a customer.

These are some common situations that you can use for different plans:
- Premium customers can 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 reduce the effort to configure the appliances. The SMP lets you easily search for gateways and configure the applicable settings. If it is necessary to configure a single appliance, with one click you can connect to the WebUI.

When you make changes to gateways in the SMP, the changes are applied in a short time frame. After the gateway is connected to the SMP, the gateway contacts the SMP at a regular interval 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 can be a maximum of a five minute interval before the new settings are applied to the gateway.

After you connect a gateway to the SMP, all the settings that are controlled by the SMP are marked with a lock icon. You can configure these settings only from the SMP. You cannot use the gateway WebUI to configure these settings.

### Using Software Blades and Services

The SMP lets you configure Software Blades and Services to help manage the gateway settings.

**Software Blades**

Software Blades let SMBs efficiently manage the unique security requirements for their networks. Each blade is a logical 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 according to the policy that is configured in the SMP. They define these behaviors and settings between the gateway and the SMP:

- Logging and reports
- Gateway maintenance - Firmware and backup
- Dynamic DNS

Understanding the SMP Server

The SMP WebUI 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 R2 64-bit server.

For more about installing the SMP Server, see the *SMP Installation Guide* for your version.
Implementing 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. We recommend that you:

- Create a plan for a common features and security policy settings for a group of gateways
- Create user accounts for the 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 the plan.

- If the plan uses VPN communities, make sure to configure them after you complete the wizard
- For plans that support the Dynamic DNS service, configure the SMP for Dynamic DNS ("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. From the navigation tree, click Home > Plans.
   The Plans window opens.
2. Click New.
   The Create New Plan wizard opens.
3. Enter a Name (cannot be changed after you save) and a Description (optional) for the new plan.
4. Click Next.
   The Supply the following services window opens.
5. Select the services ("Configuring Services" on page 53) for the plan.
6. Click Next.
   The Activate the following Security Software Blades window opens.
7. Select the Software Blades ("Using Software Blades" on page 13) for the plan.
8. Click Next.
9. Click Finish.
   The Edit Plans window opens and shows the General page.
Using Software Blades

These are the Software Blades that you can activate on plans or gateways:

- Firewall - Makes sure that only specified traffic is allowed to enter the internal network
- Application Control and 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 Threat Prevention 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 - 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
- Threat Prevention Anti-Bot - Automatically scans for bot-infected hosts and for communications with a C&C (Command and Control)
- Threat Prevention Policy - Configure the confidence and performance settings for Anti-Virus and Anti-Bot protections

Back up the gateway settings for each 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.

To back up the gateway settings for a plan:

1. From the navigation tree, click Home > Plans.
   The Edit Plans window opens and shows the plans.
2. Click the plan.
   The Plans window opens and shows the General page.
3. Click Services > Periodic Backup.
4. Configure the settings to back up the gateways in this plan ("Periodic Backup" on page 55).
Creating New Users

There is a **New User** wizard in SMP to help you create new users. These are settings that you can define for each user:

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

**To create a user:**

1. From the navigation tree, click **Home > Users**. The **Users Search** window opens.
2. Click **New**. The **Create New User** window opens.
3. Enter the information for the user.
   - **User ID** - The login name for this user
     You can click the generate name button 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 (**"Configuring Roles for Users"** on page 128) 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. From the navigation tree, click **Service Domain > Settings**. The **Settings** window opens for the Service Domain and shows the **General** page.
2. Click **Mail**.
3. In **"Reply To:" Email Address**, enter the email address to which recipients send their 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 that appears in the **From** field of all reports, Service Domain notifications, and custom alerts that the SMP sends.
5. Click **Save**.
Creating VPN Communities

Use a VPN community to create VPN site-to-site connections between a group of gateways. There are two types of VPN communities that are used for different scenarios.

- A Full Mesh VPN Community connects all member gateways to each other. Each gateway has a secure connection with each other gateway. 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.

In order 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 ("Managing VPN Community with an External Gateway" on page 101).

To prepare a gateway to join a VPN community:

1. From the navigation tree, click Home > Gateways.
   The Gateways window opens.
2. Click the gateway.
   The Edit Gateways window opens and shows the General page.
3. Configure the settings for the Internal Network Topology ("Configuring Network Topology for Gateways" on page 58).

To create a VPN community:

1. From the navigation tree, click Home > Communities.
   The Communities window opens and shows the VPN communities.
2. Click New.
   The Create New Community wizard opens.
3. Enter these settings for the community:
   - **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.

5. Click the community.
The Edit **Communities** window opens and shows the **General** page.

6. Configure these settings for the community:
   - General Settings ("Configuring the Community General Settings" on page 95)
   - VPN Settings ("Configuring VPN Settings" on page 97)
   - IKE Settings ("Configuring IKE Settings" on page 98)

7. From the Members window, click **Add Gateway**.
The **Add Gateways Wizard** opens.

8. Complete ("Adding Gateways" on page 17) the wizard and add the gateway to the community.
   Add additional gateways as necessary.

### Configuring DNS Settings for the SMP Server

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

- **Server Edit > Settings** page to configure DNS settings for deployments with one SMP Server
  ("Configuring the Settings for a SMP Server" on page 142)

- **Settings > General** page to configure DNS settings for deployments with multiple SMP Servers
  ("Configuring General Settings for the SMP" on page 23)

**Note** - Make sure that the IP addresses on the Windows interface are configured correctly
("Dynamic DNS - Gateways Cannot Push Actions to the SMP" on page 173).

**To configure the DNS settings for one SMP Server:**

1. From the navigation tree, click **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.
3. From the navigation tree, click **Settings**.
4. In **DNS Name**, enter the DNS name for the SMP Server.
5. Click **Save**.

**To configure the DNS settings for multiple SMP Servers:**

1. From the navigation tree, click **System > Settings**.
   The SMP **Settings** window opens and shows the **General** page.
2. From **SMP System DNS Name**, enter the DNS name for the primary SMP Server.
3. Click **Save**.
4. Do the previous steps again for each SMP Server.
Adding Gateways

These are the ways you can add new gateways:

- Create an individual gateway with the procedure below. During the gateway configuration process, you can assign the gateway to a community. Once configuration is complete, you can assign an owner for the gateway with the procedure Configuring Gateway Owners (on page 34).

- Create a user, with the procedure Creating New Users (on page 14). Then add gateways for the user, with the procedure Adding Gateways for a User (“Managing Gateways for a User” on page 125).

- Create a community with the procedure Adding Communities. Then add gateways to the community, with the procedure Adding Gateways to Communities.

When you create a new gateway, you can also configure a gateway owner. After the gateway is created, an activation email is sent to the owner of the Check Point 600 & 1100 Appliance. This email contains an activation link and the registration key (if manual activation is necessary).

- If the appliance has been 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 has not been 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 Check Point 600 & 1100 Appliance WebUI > Home > Cloud Services page, manually enters the registration key sent in the email, and connects to the SMP.

To add a new Check Point 600 & 1100 Appliance gateway:

1. Click Home > Gateways > New.
   The Create New Gateway window opens.
2. Enter a Name (cannot be changed after you save) or click Generate Name for a system generated name.
3. Select a Plan from the list. By default, the gateway inherits its default settings from this plan.
4. The Registration Key field shows an automatically generated registration key. You can enter a registration key or click the Generate Registration Key button to randomly generate a new registration key.
5. Enter a user name in Owner ID. If necessary, click New to create a new user or Search to look for an existing user.
6. Complete the wizard instructions.
7. Click Finish.
The Home > Gateways > Edit window opens. The navigation tree includes different options. The options you see depend on the plan you selected. An email is sent to the gateway owner specified. The email contains an activation key and information on how to connect to the appliance.

⚠️ Important - When a Check Point 600 & 1100 Appliance is behind a NAT device, you must enable the gateway to communicate with the SMP ("Managing Gateways behind NAT" on page 18).

Managing Gateways behind NAT

When a Check Point 600 & 1100 Appliance gateway is located behind a NAT device, the SMP does not have the correct IP address to communicate with it. Configure the SMP and gateway to use the correct NATed IP addresses. These are the options to manage a gateway behind NAT:

- In the gateway WebUI, enable the appliance to connect to SMP with the Check Point SMB Relay ("Connecting to Gateways behind NAT" on page 69)
- Define NAT port forwarding rules ("Gateway behind NAT" on page 60) to enable communication between the Check Point 600 & 1100 Appliance and the Service Domain

Gateway Maintenance

Upgrading a Gateway Remotely

Use the SMP to manage and upgrade the firmwares for gateways. Upgrade the firmware for:

- All the gateways in a plan
- Each gateway individually

When you upgrade the gateway firmware, the gateway must reboot.

To upgrade gateways in a plan:

1. From the navigation tree, click Home > Plans.
   The Plans window opens.
2. Select the plan.
   The Edit plans window opens and shows the General page.
3. Click Services > Firmware.

To upgrade one gateway:

1. Search for the gateway ("Searching for Gateways" on page 63).
2. Select a gateway from the list.
   The gateway properties page opens on the General node.
3. Click Services > Firmware.
Sending Security Reports

Security reports show the gateway owner a summary of the security and network activity for the time interval. These are the reports that you can send:

- 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. From the navigation tree, click Home > Plans.
   
   The Plans window opens.
2. Select the plan.
   
   The Edit plans window opens and shows the General page.
3. Select Services > Managed Services.
4. Click Send periodic reports.
5. Click Save.
6. Select Services > Reports.
7. Click the time interval that the SMP sends the Security reports.
8. Click Save.

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

1. Search for the gateway ("Searching for Gateways" on page 63).
2. Select a gateway from the list.
   
   The gateway properties page opens on the General node.
3. Select Services > Managed Services.
4. Click Send periodic reports.
5. Click Save.
6. Select Services > Reports.
7. Click the time interval that the SMP sends the Security reports.
8. Click Save.
Configuring Dynamic DNS for Gateways

Dynamic DNS lets users log in to the WebUI 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 SMP Installation Guide*.

To configure Dynamic DNS for gateways:

1. Create a Plan ("Creating a New Plan" on page 12) 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 WebUI .......................................................... 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 that is exclusively used by your company. Settings for the Service Domain are applied to all plans and gateways.

Using the SMP WebUI
These are common buttons and drop-down menus that are used in the SMP WebUI.

<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</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you configure settings for an object, the settings are only applied after you click <strong>Save</strong></td>
</tr>
<tr>
<td>Revert</td>
<td>Changes the object settings to the values when it was previously saved</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the window</td>
</tr>
<tr>
<td>Filter</td>
<td>Opens a new window to filter objects according to the search parameters</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the object</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>Opens the WebUI 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 **Status** window shows basic information about the Service Domain for the SMP.

**To show the Status window:**
1. From the navigation tree, click **Home > Overview**.
   The **Overview** window opens and shows the **Status** tab.
2. To show all the gateways that the SMP manages, click **Show All**.
3. To show gateways according to these filters, from the **Gateways** section click **Show** for applicable filter:
   - **Connected** - Shows gateways that the SMP manages.
   - **Not Connected** - Shows gateways that are not connected to the SMP. The SMP will manage them when they are connected to it.
   - **Disabled** - Shows gateways that are disabled and the SMP not manage them.
4. To show the plans, from 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**

You can show a list of currently active sessions, for users defined in the Service Domain. The following information is displayed for each user session:

- SMP ID for the user
- The date and time when 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. From the navigation tree, click **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 the refresh button.

**Showing the Gateway Map View**

The **Map View** window shows a geographical representation of all the gateways connected to the Service Domain. Each gateway is displayed at its physical location with an icon indicating whether it is connected, disconnected or disabled.

Multiple gateways at a near location are clustered together with a number that indicates the number of gateways. 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** - Some gateways are connected and one or more gateways are disconnected from the SMP
- **Red** - All the gateways are disconnected from the SMP

When you click on a gateway, a summary window opens and shows useful information and links to navigate to related objects.

The location for each gateway is set in the **Location** page of the **Gateway** window (**"Setting the Gateway Location"** on page 33).

The **Map View** window shows a map with the physical location of the gateways that are connected to the Service Domain.
If the window shows the **Map Permission Error** message, click **Continue in trial mode** to use the 30-day trial license for the **Map View** window ("Activating the Map License" on page 173).

**To show the Map View window:**
1. From the navigation tree, click **Home > Map**.
2. Click on the icon for a gateway.
   
   The **Gateway Details** window opens and shows information about the gateway, including:
   - Name - Click this link to open the **General** page for this gateway
   - IP address - Click this link to open the WebUI of the gateway in a new tab
   - Plan - Click this link to open the **General** page for this Plan
   - Owner - Click this link to open the **General** page for this user
   - MAC address

**Configuring Settings for the SMP Server**

**Configuring General Settings for the SMP**

For deployments that use multiple SMP Servers, make sure that you enter the DNS name of the primary server ("Configuring DNS Settings for the SMP Server" on page 16) in **SMP System DNS Name**.

**To configure general settings:**
1. From the navigation tree, click **System > Settings**.
   
   The **SMP Settings** window opens and shows the **General** page.
2. Configure the settings.
3. To generate a report that summarizes the SMP settings, click **Generate Report**.
   
   The Internet browser saves the report as an Excel file.
4. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMP System DNS Name</td>
<td>DNS name of the active or primary server.</td>
</tr>
<tr>
<td>Minimum user password length</td>
<td>Minimum number of characters that new user passwords must contain.</td>
</tr>
<tr>
<td></td>
<td>This value must be between 7-25.</td>
</tr>
<tr>
<td>Default registration key length</td>
<td>Number of characters the SMC uses to generate new Registration Keys.</td>
</tr>
<tr>
<td></td>
<td>This value must be between 8-20.</td>
</tr>
<tr>
<td>Gateways keep-alive interval (seconds)</td>
<td>The time-interval for keep-alive transmissions to the gateways</td>
</tr>
</tbody>
</table>
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.

To show the Logging page:

1. From the navigation tree, click **System > Settings**.
   The SMP Settings window opens and shows the General page.
2. Click **Logging**.

To configure the minimum severity level for the logs:

1. From **Log Level**, select the option for the minimum severity of logs.
2. Click **Save**.

To configure the SMP Server as a Syslog client for system logs:

1. From **Log Level**, select the option for the minimum severity of logs that are sent to the Syslog server.
2. Click **Forward logs to an external Syslog Server**.
3. In **Syslog Server**, enter the IP address of the Syslog server.
4. In **Syslog Port**, enter the port that is used to send Syslog messages.
5. Click **Save**.

To configure log file storage for SMP system logs:

1. Click **Purge old logs**.
2. In **Older than**, enter the number of days that log files are saved in the SMP.
3. From **Action**, select what the SMP does to log files that are older than the configured setting: **Delete** or **Archive**.
4. Click **Save**.

Configuring the SMP WebUI to Use a Web Proxy Server

If your network requires a Web proxy server in order to access the Internet, you must configure the SMP WebUI to use the Web proxy server.

To configure the WebUI to use a Web proxy server:

1. From the navigation tree, click **System > Settings**.
   The SMP Settings window opens and shows the General page.
2. Click **HTTP Proxy**.
3. Click **Use a proxy server**.
4. Complete the settings.
5. Click **Save**.
6. Restart the SMP.
a) Log in to the SMP Server.
b) From the Windows Start menu, select **Administrative Tools > Services**.
c) Restart the Apache-Catalina service.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a proxy server</td>
<td>Select this option if your company uses a proxy server to connect to the Internet</td>
</tr>
<tr>
<td>Proxy host</td>
<td>Enter the domain or IP address of the proxy server host</td>
</tr>
<tr>
<td>Proxy port</td>
<td>Enter the proxy server port</td>
</tr>
<tr>
<td>Proxy user</td>
<td>If the proxy server requires authentication, enter the appropriate user name</td>
</tr>
<tr>
<td>Proxy password</td>
<td>If the proxy server requires authentication, enter the appropriate password</td>
</tr>
</tbody>
</table>

### Configuring Outgoing Mail Settings for the SMP

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

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

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

1. From the navigation tree, click **System > Settings**. The SMP **Settings** window opens and shows the **General** page.
2. Click **Mail Settings**.
3. Configure the settings.
4. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>Enter the IP address or domain for the outgoing mail server</td>
</tr>
<tr>
<td>&quot;Reply To:&quot; Email Address</td>
<td>The email address to which users can send their replies. This address appears in all SMP system notifications sent by the SMP.</td>
</tr>
<tr>
<td>&quot;Reply To:&quot; Friendly Name</td>
<td>The name that appears in the From field of all SMP system notifications.</td>
</tr>
<tr>
<td>Use authenticated SMTP</td>
<td>Select this option if the SMTP server requires authentication.</td>
</tr>
<tr>
<td>User and Password</td>
<td>Authentication credentials for the SMTP server.</td>
</tr>
</tbody>
</table>
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 ("Managing Licenses without the WebUI" on page 150).

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

To show the SMP system license:

1. Click System > Settings.
   The Settings window opens and shows the General page.
2. Click License Management.
   The License Management page opens.
3. Click View License.

To add a license:

1. Click View License.
2. Click Add License.
3. The Add SMP License wizard opens.
4. Configure these settings:
   - IP address - Enter the IP address of the SMP Server
   - Expiration date - Enter the date that the SMP license expires
   - Signature - Copy and paste the string for the license
   - SKU - Copy and paste the SKU for the license.
5. Click Finish.
   The wizard closes.
6. Click Apply License.
   The settings for the license are applied to the SMP.
7. Click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the SMP Server</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Date that the SMP license expires</td>
</tr>
<tr>
<td>Signature</td>
<td>Hash signature for the license</td>
</tr>
<tr>
<td>Number of Gateways</td>
<td>Maximum number of gateways that the SMP can manage</td>
</tr>
<tr>
<td>SKU</td>
<td>SKU for the license</td>
</tr>
</tbody>
</table>
Configuring SMP Backup Settings

System backup settings are used for both automatic and manual SMP configuration backup. Save the back-up file according to the deployment of the SMP Server:

- For SMP Servers that are located in the Check Point cloud, it is necessary to 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. From the navigation tree, click **System > Settings**. The **Settings** window opens and shows the **General** page.
2. Click **System Backup**.
3. To enable automatic backups, click **Perform** and select the appropriate option:
   - Daily
   - Weekly
   - Monthly
4. Complete the settings.
5. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Storage</td>
<td></td>
</tr>
<tr>
<td>Upload backup file to FTP</td>
<td>Choose this option to upload the backup file to an FTP server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>FTP server</strong> - Enter the IP address or DNS name, and then the port number</td>
</tr>
<tr>
<td></td>
<td>- <strong>Path on server</strong> - Enter the path to the directory where the SMP backup file is saved</td>
</tr>
<tr>
<td></td>
<td>- <strong>Username</strong> and <strong>Password</strong> - Enter the authentication credentials for the FTP server</td>
</tr>
<tr>
<td>Save the file</td>
<td>Choose this option to save the backup file to a location on your network.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use the following path</strong> - Type the path to the directory where the SMP backup file should be saved. This can be a UNC or local path.</td>
</tr>
<tr>
<td>File name</td>
<td></td>
</tr>
<tr>
<td>Automatically generate filename</td>
<td>Choose this option to automatically generate a name for the backup file</td>
</tr>
<tr>
<td></td>
<td>- <strong>Filename prefix</strong> - The filename is generated in this format: prefix_yyyyMMddHHmmss</td>
</tr>
</tbody>
</table>
Configuring General SMP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use static filename</td>
<td>• Enter the <strong>Filename</strong> for the backup file</td>
</tr>
<tr>
<td></td>
<td>• <strong>Overwrite file if already exists</strong> - When this option is selected</td>
</tr>
<tr>
<td></td>
<td>the new backup file overwrites the previous one.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you do not select this option, if there is a backup file with</td>
</tr>
<tr>
<td></td>
<td>the same name, the backup operation stops.</td>
</tr>
</tbody>
</table>

Starting the SMP Backup

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

1. From the navigation tree, click **System > Settings**. The **Settings** window opens and shows the **General** page.
2. Click **System Backup > Status**.
3. Click **Run Now**. A confirmation window opens.
4. Click **OK**.
5. To refresh the fields, click **Refresh**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Run</td>
<td>The date at which the last backup operation ran</td>
</tr>
<tr>
<td>State</td>
<td>Shows the status of the backup operation</td>
</tr>
</tbody>
</table>

Configuring the SMP Internal Certificate Authority

Once you have initialized the internal CA, you can configure settings for the following:

- The CA root certificate
- Gateways' certificates
- Online revocation checking

**To configure certificate settings:**

1. From the navigation tree, click **System > Settings**. The **Settings** window opens and shows the **General** page.
2. Click **Certificate Authority**.
3. Complete the settings.
4. Click **Save**.
5. Click **Reinitialize CA**.
6. To export the certificate to a file, click **Export X.509**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Certificate</td>
<td>The root certificate expires every Enter the number of months after the CA's initialization that the CA root certificate expires.</td>
</tr>
</tbody>
</table>
Configuring General SMP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically renew</td>
<td>Enter the when the root certificate is automatically renewed. This setting is the number of months before the CA root certificate's expiration date.</td>
</tr>
<tr>
<td></td>
<td>When the root certificate is renewed, the CA is reinitialized. All the certificates for the gateways are automatically renewed.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Date and time when the CA's root certificate expires.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>The CA certificate's fingerprint, which is a unique string that identifies the certificate.</td>
</tr>
<tr>
<td>Gateway Certificate</td>
<td>The gateway certificate expires every Enter the number of months after the CA's sends a certificate to the gateway that this certificate expires.</td>
</tr>
<tr>
<td></td>
<td>Automatically renew Enter the when the gateway certificate is automatically renewed. This setting is the number of months before the gateway certificate's expiration date.</td>
</tr>
<tr>
<td>Online Revocation Checking</td>
<td>Revocation answer is valid for When gateways authenticate to each other, each gateway performs online revocation by checking with the SMS to verify that the other gateway's certificate has not been revoked. To enhance VPN performance, the gateway then caches this answer. Type the number of hours after a gateway has performed online revocation checking that the gateway should store the answer in cache. After this period has expired, the revocation answer is purged from the cache.</td>
</tr>
</tbody>
</table>

Configuring SMP Notifications

Configure the notifications for the:

- SMP Server ("Configuring SMP System Notifications" on page 161)
- Service Domains ("Configuring Service Domain Notifications" on page 163)

Configuring Management Access Control

The Management Access Control page 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 WebUI.

**Note** - The localhost address (127.0.0.1) is always allowed and you cannot block it.
To define the only IP addresses that are allowed to log in to the SMP WebUI:
1. From the navigation tree, click **System > Settings**.
   The **Settings** window opens and shows the **General** page.
2. Click **Management Access Control**.
3. Click **Allow web access (HTTPS) to the SMP from the following IP addresses and subnets**.
4. For each allowed address:
   a) Click **New**.
   b) From **Source Type**, select **IP Address** or **Network**.
   c) Enter the IP address and for a Network also enter the subnet mask.
   d) Click **Finish**.
5. Click **Save**.

To allow all IP addresses to log in to the SMP WebUI:
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**.
Managing Gateways

In This Section:

- Showing and Editing Gateways ................................................................. 31
- Locking and Unlocking Settings ................................................................. 62
- Searching for Gateways ............................................................................. 63
- Exporting Gateway Information ............................................................... 66
- Sending Email to Gateway Owners .......................................................... 67
- Deleting Gateways ...................................................................................... 67
- Accessing Local Gateways ......................................................................... 68

A gateway is the SMP object that represents the appliance you are managing for a customer.

Showing and Editing Gateways

From the Home > Gateways > Search Results page you can:

- Add a new Check Point 600 & 1100 Appliance gateway ("Adding Gateways" on page 17)
- Search for a specified gateway ("Searching for Gateways" on page 63)
- Delete a gateway ("Deleting Gateways" on page 67)
- Export gateway information to Excel ("Exporting Gateway Information" on page 66)
- Send emails to gateway owners ("Sending Email to Gateway Owners" on page 67)
- Reset all settings of a gateway to its plan simultaneously
- See or edit the details of a gateway
- Access a gateway ("Connecting to Gateways" on page 68)

To see or edit the properties of a gateway:

1. From the navigation tree, click Home > Gateways.
   The Gateways window opens and shows the gateways for the Service Domain.
2. Click on a gateway link in the Name column.
   The Home > Gateways > Edit page opens with the General node selected.
3. Select the applicable node to see or edit it:
   - Configuring General Settings (on page 32)
   - Configuring gateway Owners (on page 34)
   - Showing gateway Statuses ("Showing Gateway Status" on page 35)
   - Showing Gateway Logs (on page 36)
   - Using CLI Scripts (on page 61)
   - Security Software Blades ("Configuring Security Software Blades" on page 41)
   - Configuring Services (on page 53)
   - Configuring VPN Settings ("Configuring VPN Settings (Gateway)" on page 57)
   - Configuring Setup Settings (on page 59)
To connect to a local gateway in the Gateways window:
1. Click the IP Address for the local gateway.
2. If a security warning message is shown, confirm it and continue.
   A browser page opens and shows the progress of the SMP connecting to the gateway.
   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 MAC address of the gateway.
   To make sure that the gateway you are securely connecting to is the correct gateway, check that the MAC address in the middle part of the string matches the one of the gateway. You can find the MAC address of the gateway in the General tab of the gateway.
3. If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, you can click OK and override that connection. If you click Cancel, your login attempt is canceled.
   When logged in, you can update the local Check Point 600 & 1100 Appliance as necessary.

To connect to a local gateway in the Edit Gateways window:
From the Edit Gateways window, click Access gateway.

Configuring General Settings

To configure general settings for a gateway:
1. In the SMP menu, click Home > Gateways.
   The Home > Gateways > Search Results page opens.
2. Select a gateway from the list.
   The gateway properties page opens on the General node.
3. Configure the necessary fields.
4. To set the physical location of the gateway on the map, do one of these options:
   • In Search, enter the location of the gateway
   • In the map, click the location of the gateway
5. Click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the appliance.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this option to enable the gateway.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, the gateway is disabled and cannot connect to the SMP.</td>
</tr>
<tr>
<td></td>
<td>This field only appears in the Home &gt; Gateways &gt; Edit page.</td>
</tr>
<tr>
<td>Managed by SMP</td>
<td>When selected, the SMP manages this gateway.</td>
</tr>
<tr>
<td>Gateway Type</td>
<td>Shows the appliance type. For example, Small Office Appliance.</td>
</tr>
</tbody>
</table>
### Field Description

**Plan**
Select a plan for this gateway. The plan specifies the settings (services, blades) for the gateway. By default, a gateway inherits its settings from the plan. For information on unlocking the gateway settings from the plan, see Locking and Unlocking Settings (on page 62).
Click Go to open the plan.

**MAC Address**
Shows the unique physical identifier of the appliance. The format is XX:XX:XX:XX:XX:XX, where X is a numeral from 1-9, or a letter from A-F.
The MAC address is assigned to the appliance's WAN port. It is used as a key in the UserCenter. You see this MAC address in your account details next the appliance's SKU. The MAC address of the appliance is located on a label beneath the appliance or on the barcode label on the appliance's package.
**Note:** If you do not fill in this field, it is filled in automatically when the gateway connects to the SMP for the first time.

**Static IP**
For gateways that are NOT managed by the SMP, enter the static IP address of the gateway.

**Last connected IP address**
Shows the last connected IP address of the gateway.

**Registration Key**
The key used to authenticate to the SMP.
You can enter a registration key or click the Generate Registration Key button next to the field to the randomly generate a new Registration Key.
**Note:** You can control the length of randomly generated Registration Keys using the procedure Configuring General Settings for the SMP (on page 23).

**Activation Key**
Shows the activation key that is used by the appliance to connect to the SMP. It is sent to the gateway owner in an email.

### Setting the Gateway Location

The **Location** page lets you set the physical location of the gateway. After the gateway is created, the location is empty.

If the window shows the **Map Permission Error** message, click **Continue in trial mode** to use the 30-day trial license for the **Map View** window ("Activating the Map License" on page 173).
To set the gateway location:
1. In the navigation tree, click **Location**.
2. In the **Search an address** field, enter the gateway location.
   The map shows the gateway.
3. Click **Save**.

Configuring Gateway Owners

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

When you set a new gateway owner and save the configuration, an activation email is sent to the owner of the Check Point 600 & 1100 Appliance. This email contains an activation link and the registration key (if manual activation is necessary).

- If the appliance has been 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 has not been 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 Check Point 600 & 1100 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. In the navigation tree, click **Owner**.
2. Click **Set**.
   The **Add User** wizard opens.
3. To add an existing user:
   a) In **User ID**, enter the user’s User ID.
   
      **Note**: The User ID must already be defined in the system.
   b) Click **Next** and then **Done**.
4. To search for users:
   a) Select **Search for users**.
   b) Click **Next**.
   c) Enter the search criteria and select the options from the drop-down lists.
   d) Click **Next**.
The Add User window opens with a list of users that meet the specified search criteria.

e) Select the check box next to the applicable user.
   
   **Note:** You cannot assign a specific gateway to more than one user.

f) Click Next.
   
The Completed window opens.

g) Click Done.

5. To create a new user, see Creating New Users (on page 14).

6. Click Save.

To remove an owner from a gateway:

1. In the navigation tree, click the **Owner** node.
   
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 database. The association between the gateway and the user is deleted.

Showing Gateway Status

You can see the current status of a gateway and this information:

- The connection details and status of the gateway
- The last time the gateway was modified

To see the status of a gateway:

In **Home > Gateways > Edit** of a gateway, click **Status**.

The Status page opens.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>The date and time at which 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 is using.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>The status of the connection between the gateway and the SMP (Connected/Not Connected).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update Time</td>
<td>The time and date when the gateway status last changed. This field is shown 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. This field is shown only when the gateway is connected to the SMP.</td>
</tr>
<tr>
<td>Connection Address</td>
<td>The current IP address of the gateway. This field is shown only when the gateway is connected to the SMP.</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. This field is shown only when the gateway is connected to the SMP.</td>
</tr>
<tr>
<td>Error Details</td>
<td>Details are shown 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, continue scrolling down the page. The log table is automatically refreshed.

> **Note** - To see Gateway logs, make sure **Store gateway logs** is selected in **Services > Managed Services**.

**To show gateway logs:**

In **Home > Gateways > Edit** of a gateway, click **Logs**.

A table with log entries is shown.

**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 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.

Configuring Device Settings
The Device Settings section lets you configure these settings for gateways or a plan:
- NTP (on page 37)
- Time Zone (on page 38)
- DNS (on page 39)
- Gateway Administrators (on page 40)
These features are only supported on R77.20 and higher gateways.

NTP
Configure the SMP to synchronize the time settings for the specified plans and gateways with an NTP server.
This feature is only supported on R77.20 and higher gateways.

To configure the NTP settings of a plan:
1. In Home > Plans > Edit of a plan, click Device Settings > NTP.
2. Make sure Manage in SMP is selected.
3. Enter the host name or IP address for the Primary and Second NTP Server.
4. From Update Interval, enter the time interval in minutes that SMP contacts the NTP server to update the time settings.
5. Optional: Configure the settings to authenticate to the NTP server.
   a) Click NTP Authentication.
   b) Enter the Shared Secret and Shared Secret Identifier.
6. Click Save.

To override the NTP settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click Device Settings > NTP.
2. If the NTP settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Configure the NTP settings (see above).
5. Click **Save**.

To connect to the appliance:

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > NTP**.
2. Click **Access Gateway: Date and Time**.

   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the **Date and Time** page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   ![Note](image)

   If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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. In **Home > Plans > Edit** of a plan, click **Device Settings > Time Zone**.
2. Make sure **Manage in SMP** is selected.
3. From the **Local Time Zone** list, select the correct time zone option.
4. Select **Automatically adjust clock for daylight saving changes** to enable automatic daylight saving changes.
5. Click **Save**.

To override the Time Zone settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > Time Zone**.
2. If the Time Zone settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Configure the Time Zone settings (see above).
5. Click **Save**.

To connect to the appliance:

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > Time Zone**.
2. Click **Access Gateway: Date and Time**.

   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the **Date and Time** page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   ![Note](image)

   If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 choose to define up to three DNS servers which are applied to all Internet connections or use the DNS configuration provided by the active Internet connection (Primary).

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

Use the DNS configuration from the Internet connection to allow a more dynamic definition of DNS servers. The gateways use the DNS settings of the currently active Internet connection.

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 is resolving
- DNS queries that do not contain a domain name are automatically appended with the domain name

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. In Home > Plans > Edit of a plan, click Device Settings > DNS.
2. Make sure Manage in SMP is selected.
3. Configure the DNS Settings:
   - To configure the DNS servers, click Configure DNS servers, and then enter the IP addresses for the DNS servers.
   - To use the Internet connection DNS settings, click Use DNS servers configured for the active Internet connection(s).
4. Configure the DNS Proxy settings:
   - To configure the gateways to provide DNS resolving services to internal hosts, click Enable DNS Proxy.
   - To use the DNS Proxy gateways to treat the local network objects as a hosts list, click Resolve Network Objects.
5. Enter the Domain Name that is appended to DNS queries.
6. Click Save.

To override the DNS settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click Device Settings > DNS.
2. If the DNS settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the DNS settings and let the administrator of the gateway manage them exclusively, clear Manage in SMP.
4. Configure the DNS settings (see above).
5. Click Save.
To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Device Settings > DNS.
2. Click Access Gateway: DNS.

   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the DNS page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can click OK to override that connection or Cancel to stop the current login attempt.

Gateway Administrators

The Gateway Administrators window 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. In Home > Plans > Edit of a plan, click Device Settings > Gateway Administrator.
2. Make sure Manage in SMP is selected.
3. To create a new Gateway Administrator:
   a) Click New.

      The Add Gateway Administrator window opens.
   b) Enter the Name and Password.
   c) Select the Permission for the administrator.
   d) Click Finish.
4. To delete a Gateway administrator:
   a) Select the administrator.
   b) Click Delete.

      A confirmation window opens.
   c) Click OK.

      The administrator is deleted.
5. Click Save.
To override the Gateway administrator settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click Device Settings > Gateway Administrator.
2. If the Gateway administrator settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Configure the Gateway administrator settings (see above).
5. Click Save.

To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Device Settings > Gateway Administrator.
2. Click Access Gateway: Administrators.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Administrators page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 (on page 41)
- Application Control and URL Filtering (on page 42)
- IPS (on page 43)
- Traditional Anti-Virus (on page 44)
- Anti-Spam (on page 45)
- QoS (on page 46)
- Remote Access (on page 47)
- Site to Site VPN (on page 48)
- User Awareness (on page 49)
- Threat Prevention Anti-Virus (on page 49)
- Threat Prevention Anti-Bot (on page 50)
- Threat Prevention Policy (on page 51)
For each, you can set Blade Control to On or Off. 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 specific rules.
You can override the Firewall Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Firewall Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).
To configure the Firewall settings of a plan:

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > Firewall**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Strict**: Traffic that is not specified as Allowed in the Firewall Rule Base, is Blocked. Configure the Rule Base in gateway WebUI.
   - **Standard**: Traffic coming in to the internal network is Blocked, unless the Firewall Rule Base allows it. Traffic to the Internet, on all services, is Allowed. Traffic between internal networks and between trusted wireless networks is Allowed.
4. Select to log **Blocked Traffic**, **Accepted Traffic**, or both.
5. Click **Save**.

To override the Firewall settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Firewall**.
2. If the Firewall settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** and **Log** options (see above).
5. Click **Save**.

To connect to the appliance:

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Firewall**.
2. Click **Access Gateway:Firewall**.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Firewall Policy page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.
   
   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Application Control and URL Filtering**

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

You can override the Application Control and URL Filtering Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Application Control and URL Filtering Software Blade from the plan. For more information, see **Locking and Unlocking Settings** (on page 62).

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

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > Application and URLs**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**, to block applications and URLs that are known to be insecure:
   - **Block security risk categories**: spyware, phishing, botnet, spam, anonymizer, and hacking
   - **Block torrents and P2P applications**: torrent trackers, BitTorrent and Gnutella protocols, file storage and sharing, media sharing, Facebook file sharing
   - **Block inappropriate content**: weapons, violence, sex, gambling, hate, illegal activities, and illegal drugs

4. Click **Save**.

**To override the Application Control and URL Filtering settings set by a plan in a gateway:**

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Application and URLs**.
2. If the Application Control and URL Filtering settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** options (see above).
5. Click **Save**.

**To connect to the appliance:**

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Application and URLs**.
2. Click **Access Gateway: Application Control**.
   
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Firewall Policy page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 to use on the gateways.

You can override the IPS Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the IPS Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

**To configure the IPS Software Blade settings of a plan:**

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > IPS**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Strict**: Use the IPS profile that has most of the protection categories enabled.
   - **Typical**: Use the IPS profile that blocks the most dangerous threats.
   - **Custom**: You can change the policy of which protection groups (by confidence level, severity, performance, and impact) are enabled or disabled.
4. Set the mode:
   - To implement IPS protections on the gateways, clear **Detect-only mode**.
   - To monitor IPS rule matches, click **Detect-only mode**.

5. Click **Save**.

To override the IPS settings set by a plan in a gateway:

1. In Home > Gateways Edit of a plan, click **Security Software Blades > IPS**.
2. If the IPS settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** and **Mode** options (see above).
5. Click **Save**.

To connect to the appliance:

1. In Home > Gateways Edit of a plan, click **Security Software Blades > IPS**.
2. Click **Access Gateway:IPS**.
   
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the IPS page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the Traditional Anti-Virus Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

Gateways that are R77.20 and higher automatically use the Threat Prevention Anti-Virus Software Blade (**"Threat Prevention Anti-Virus"** on page 49). 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. In Home > Plans > Edit of a plan, click **Security Software Blades > Traditional Anti-Virus**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Scan incoming files**: Files coming in to the gateway on the selected protocols are scanned.
   - **Scan outgoing files**: Files that users send out are scanned. (This option is cleared by default.)
   - **Scan files between networks**: Files going between internal networks, or from the DMZ to internal, are scanned. You can filter this internal scanning to scan only the files that use selected protocols.
4. Set **Tracking**: **Log, Alert** (as defined in the System Settings), **None**.

5. Set the mode:
   - To implement Traditional Anti-Virus on the gateways, clear **Detect-only mode**.
   - To monitor Traditional Anti-Virus rule matches, click **Detect-only mode**.

6. Click **Save**.

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

1. In **Home** > **Gateways** > **Edit** of a gateway, click **Security Software Blades** > **Traditional Anti-Virus**.

2. If the Anti-Virus settings are locked to a plan, click **Manage in SMP**.

3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.

4. Set the **Policy**, **Tracking**, and **Mode** options (see above).

5. Click **Save**.

**To connect to the appliance:**

1. In **Home** > **Gateways** > **Edit** of a gateway, click **Security Software Blades** > **Traditional Anti-Virus**.

2. Click **Access Gateway**: **Traditional Anti-Virus**.
   
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Anti-Virus page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the Anti-Spam Software Blade from the plan. For more information, see **Locking and Unlocking Settings** (on page 62).

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

1. In **Home** > **Plans** > **Edit** of a plan, click **Security Software Blades** > **Anti-Spam**.

2. Make sure **Manage in SMP** is selected.

3. Click **Filter spam based on email content**.

4. Set the **Policy**:
   - **Block spam emails**
   - **Flag spam email subject**
   - **Flag spam email header**

5. Set **Tracking**: **Log, Alert** (as defined in the System Settings), **None**.
6. Set the mode:
   - To implement Anti-Virus on the gateways, clear **Detect-only mode**.
   - To monitor Anti-Virus rule matches, click **Detect-only mode**.

7. Click **Save**.

To override the Anti-Spam settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Anti-Spam**.
2. If the Anti-Spam settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Click **Filter spam based on email content**.
5. Set the **Policy**, **Tracking**, and **Mode** options (see above).
6. Click **Save**.

To connect to the appliance:

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Anti-Spam**.
2. Click **Access Gateway:Anti-Spam**.
   
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Anti-Spam page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   📝 **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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, define Quality of Service, to give more bandwidth to the more important traffic in your environment.

You can override the QoS Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the QoS Software Blade from the plan. For more information, see **Locking and Unlocking Settings** (on page 62).

To configure the QoS Software Blade settings of a plan:

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > QoS**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Ensure low latency for delay sensitive services**: Give more bandwidth for traffic that uses services that cannot function if the packets do not arrive on time. 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.
   
   - ** Guarantee % of the bandwidth to**: Set a minimum ratio of the bandwidth for traffic that is not preferred, in the VPN or for all traffic.
• **Limit bandwidth consuming applications**: 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.

4. Click **Save**.

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

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > QoS**.
2. If the QoS settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** options (see above).
5. Click **Save**.

**To connect to the appliance:**

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > QoS**.
2. Click **Access Gateway: QoS**.

   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the QoS page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 on computers, handheld devices, and laptops.

You can override the Remote Access VPN Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Remote Access VPN Software Blade from the plan. For more information, see **Locking and Unlocking Settings** (on page 62).

**To configure the Remote Access VPN Software Blade settings of a plan:**

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > Remote Access**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Allow traffic from Remote Access users (by default)**: This setting enables your employees to log in to the network from a remote site. It does not give access without authentication.
   - **Log traffic from Remote Access users - (by default)**
4. Click **Save**.
To override the Remote Access VPN settings set by a plan in a gateway:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Remote Access VPN.
2. If the Remote Access VPN settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Set the Policy options (see above).
5. Click Save.

To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Remote Access VPN.

A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Remote Access page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the Site to Site VPN Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62)

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

1. In Home > Plans > Edit of a plan, click Security Software Blades > Site to Site VPN.
2. Make sure Manage in SMP is selected.
3. Set the Policy:
   - Allow traffic from remote VPN sites (by default): This setting enables VPN traffic.
   - Log VPN sites traffic (by default)
4. Click Save.

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

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Site to Site VPN.
2. If the Site to Site VPN settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Set the Policy options (see above).
5. Click Save.
To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Site to Site VPN.
2. Click Access Gateway:Site to Site.

   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Site to Site VPN Blade Control page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the User Awareness Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62)

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

1. In Home > Plans > Edit of a plan, click Security Software Blades > User Awareness.
2. Make sure Manage in SMP and On are selected.
3. Click Save.

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

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > User Awareness.
2. If the User Awareness settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Make necessary changes.
5. Click Save.

To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > User Awareness.

   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the User Awareness page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 gateway 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 Threat Prevention Anti-Virus Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Threat Prevention Anti-Virus Software Blade from the plan ("Locking and Unlocking Settings" on page 62).

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 ("Traditional Anti-Virus" on page 44).

To configure the Threat Prevention Anti-Virus Software Blade settings of a plan:
1. In Home > Plans > Edit of a plan, click Security Software Blades > Threat Prevention Anti-Virus.
2. Make sure Manage in SMP and On are selected.
3. Set the mode:
   - To implement Anti-Virus protections on the gateways, clear Detect-only mode.
   - To monitor Anti-Virus protection matches, click Detect-only mode.
4. Click Save.

To override the Threat Prevention Anti-Virus settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Threat Prevention Anti-Virus.
2. If the User Awareness settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Make necessary changes to the mode (see above).
5. Click Save.

To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Threat Prevention Anti-Virus.
2. Click Access Gateway: Threat Prevention Anti-Virus.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Threat Prevention Anti-Virus page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.
   
   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can click OK to override that connection or Cancel to stop the current login attempt.

Threat Prevention Anti-Bot

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

You can override the Threat Prevention Anti-Bot Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Threat Prevention Anti-Bot Software Blade from the plan ("Locking and Unlocking Settings" on page 62).

This feature is only supported on R77.20 and higher gateways.
To configure the Threat Prevention Anti-Bot Software Blade settings of a plan:

1. In Home > Plans > Edit of a plan, click Security Software Blades > Threat Prevention Anti-Bot.
2. Make sure Manage in SMP and On are selected.
3. Set the mode:
   - To implement Anti-Bot protections on the gateways, clear Detect-only mode.
   - To monitor Anti-Bot protection matches, click Detect-only mode.
4. Click Save.

To override the User Awareness settings set by a plan in a gateway:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Threat Prevention Anti-Bot.
2. If the User Awareness settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Click Save.

To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Threat Prevention Anti-Bot.

A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Threat Prevention Anti-Bot page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 and Anti-Bot 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. For more information about protections, see the Check Point ThreatWiki. You can access it from a link on the Threat Prevention > Engine Settings page on the gateway.

Set protection activation according to these criteria:

- **Confidence level** - The confidence level is how confident the Software Blade is that recognized attacks are actually bot traffic. Some attack types are more subtle than others and legitimate traffic can sometimes be mistakenly recognized as a threat. The confidence level value shows how well protections can correctly recognize a specified attack. 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 according to the defined tracking option (none, logged, or logged with an alert).
• **Prevent** - Blocks identified bot traffic from passing through the gateway.
• **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 Anti-Bot 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 if necessary. You must first unlock the Threat Prevention Policy from the plan ("Locking and Unlocking Settings" on page 62).

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

**To configure the Threat Prevention Policy settings of a plan:**

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > Threat Prevention Policy**.
2. Make sure **Manage in SMP** and **On** are selected.
   - Select the **High**, **Medium**, and **Low confidence** settings
   - Select the **Performance impact** setting
   - Select the **Tracking options** setting
4. Click **Save**.

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

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Threat Prevention Policy**.
2. If the User Awareness settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Make necessary changes.
5. Click **Save**.

**To connect to the appliance:**

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Threat Prevention Policy**.
2. Click **Access Gateway:Threat Prevention Policy**.
   
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Threat Prevention Policy page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 (on page 53)
- Firmware ("Firmware for Gateways and Plans" on page 54)
- Backup ("Periodic Backup" on page 55)
- Reports (on page 55)
- Report Recipients (on page 56)
- Dynamic DNS (on page 57) - Only in gateways

**Managed Services**

All gateways subscribed to the plan take their managed services settings from the plan, by default.

If necessary, you can override the inherited managed services settings for a specific gateway, by configuring these settings in the gateway. You must first unlock the managed services from the plan. For more information, see Locking and Unlocking Settings (on page 62).

**To configure the managed services settings of a plan:**

1. In Home > Plans > Edit of a plan, click the Services > Managed Services node.
   
   The Managed Services window opens.
2. Select or clear the necessary services.
3. Click Save.

<table>
<thead>
<tr>
<th>Managed Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store gateway logs</td>
<td>Send logs from the gateways to the SMP with SmartLog</td>
</tr>
<tr>
<td>Send periodic reports</td>
<td>Send Check Point Executive reports that contain security and network analysis details from the SMP to the gateway owners</td>
</tr>
<tr>
<td>Firmware upgrades</td>
<td>Controls the gateways firmware upgrades</td>
</tr>
<tr>
<td>Periodic backup</td>
<td>Schedule periodic backups of the appliance settings</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>Gateways will use Dynamic DNS services</td>
</tr>
</tbody>
</table>

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

1. In Home > Gateways > Edit of a gateway, click the Services > Managed Services node.
   
   The Managed Services window opens.
2. If necessary, click Unlock from plan to unlock the node from plan.
   
   The fields are enabled.
3. Select or clear the necessary services.
4. Click Save.
**Firmware for Gateways and Plans**

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

- Firmware to use for the gateways
- Scheduling firmware updates

All gateways subscribed to the plan will take their firmware settings from the plan, by default. If necessary, you can override the inherited firmware settings for a specific gateway, by configuring these settings in the gateway. You must first unlock the firmware service from the plan. For more information, see Locking and Unlocking Settings (on page 52).

Automatic firmware updates require the gateway to reboot. If necessary, you can limit automatic firmware updates to certain days and hours, using the following procedure.

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

---

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

1. In **Home > Plans > Edit** of a plan, click the **Services > Firmware** node. The **Firmware** window opens.
2. Select one of these options:
   - **Specific firmware version** - Select one of the firmware options from the list or **Do Not Upgrade** (the gateway does not get a firmware update, it keeps the firmware installed on it).
   - **Check Point latest** - The gateway will download the latest firmware version available from Check Point.
   - **The firmware is managed locally on the device** - The gateway will not download firmware.
3. Select one of these options to define when the firmware is downloaded to the gateway:
   - **Upgrade immediately** - Automatically downloads the software and upgrades immediately.
   - **Daily** - Select the **time of day** range that the firmware should be downloaded every day.
   - **Weekly** - Select the **day of week** and **time of day** range that the firmware should be downloaded every week.
   - **Monthly** - Select the **day of month** and **time of day** range that the firmware should be downloaded every month.
4. Click **Save**.

**To override firmware settings for a gateway:**

1. In **Home > Gateways > Edit** of a gateway, click the **Services > Firmware** node. The **Firmware** window opens.
2. Click **Unlock from plan** to unlock the node from plan. The fields are enabled.
3. Select the firmware and schedule options (see above).
4. Click **Save**.
Periodic Backup

All gateways subscribed to the plan take their backup settings from the plan, by default. The backup file backs up the settings for each gateway in a separate ZIP file.

The naming convention of the file is:

<GW name>_<firmware version>_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.

If necessary, you can override the inherited backup settings for a specific gateway, by configuring these settings in the gateway. You must first unlock the managed services from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the backup settings of a plan:

1. In Home > Plans > Edit of a plan, click Services > Periodic Backup.
   The Periodic Backup window opens.
2. Set the necessary fields.
3. Click Save.

<table>
<thead>
<tr>
<th>Periodic Backup</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File storage details</td>
<td>Enter the FTP Path, Username, and Password to back up gateway settings</td>
</tr>
<tr>
<td>Daily</td>
<td>Weekly</td>
</tr>
</tbody>
</table>

To override the backup settings set by a plan in a gateway:

1. In Home > Gateways > Edit of a gateway, click the Services > Backup node.
2. In the navigation tree, click the Services > Backup node.
   The Periodic Backup window opens.
3. If necessary, click Unlock from plan to unlock the node from plan.
   The fields are enabled.
4. Set the necessary fields.
5. Click Save.

Reports

All gateways subscribed to the plan take their report settings from the plan, by default.

You can override the reports settings set by a plan for a specified gateway if necessary. You must first unlock the reports service from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the report settings of a plan:

1. In Home > Plans > Edit of a plan, click the Services > Reports node.
   The Security Reports window opens.
2. Set the applicable options.
3. Click Save.
### Reports

<table>
<thead>
<tr>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>Weekly</td>
</tr>
<tr>
<td>Report’s language</td>
<td>Select the language for the report</td>
</tr>
</tbody>
</table>

To override the report settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click the **Services > Reports** node.
   The **Security Reports** window opens.
2. If necessary, click **Unlock from plan** to unlock the node from plan.
   The fields are enabled.
3. Set the applicable options.
4. Click **Save**.

---

### Report Recipients

All gateways subscribed to the plan take their report recipient settings from the plan, by default. You can override the reports settings set by a plan for a specified gateway if necessary. You must first unlock the reports service from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the report settings of a plan:

1. In **Home > Plans > Edit** of a plan, click the **Services > Report Recipients** node.
   The **Report Recipients** window opens.
2. Set the applicable options.
3. Click **Save**.

<table>
<thead>
<tr>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send to owner</td>
<td>Send the security report to the gateway owner</td>
</tr>
<tr>
<td>Additional emails</td>
<td>Enter email addresses separated by a semicolon to receive the security report</td>
</tr>
</tbody>
</table>

To override the report settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click the **Services > Report Recipients** node.
   The **Report Recipients** window opens.
2. If necessary, click **Unlock from plan** to unlock the node from plan.
   The fields are enabled.
3. Set the applicable options.
4. Click **Save**.
**Dynamic DNS**

You can add DNS aliases to the primary domain name.

**To add a DNS alias:**
1. In Home > Gateways > Edit of a gateway, click Services > Dynamic DNS.
   The Dynamic DNS window opens.
2. Click New.
3. Enter the DNS alias.
4. Repeat steps 2-3 to add more DNS aliases.
5. 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 VPN Settings (Gateway)**

You can configure these VPN settings:
- Community ("VPN Community Settings" on page 57)
- Internal Network Topology ("Configuring Network Topology for Gateways" on page 58)

**VPN Community Settings**

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

You can override the VPN community settings set by a plan for a specified gateway if necessary. You must first unlock the community settings from the plan. For more information, see Locking and Unlocking Settings (on page 62).

For a gateway to get the community settings configured here, make sure that the Site to Site VPN blade has been turned on in the appliance.

**To configure community settings:**
1. For a plan - In Home > Plans > Edit of a plan, click VPN > Community.
   The Community window opens.
2. For a gateway - If you are editing community settings through the gateway and it is necessary, click Unlock from plan.
3. Click Join a community.
4. Select a community from the Community list.
   To see or change the VPN Community settings, click Go.
   If the selected community is a Star Community, the Member Type will show Normal or Center.
   You cannot configure this property in the plan, because only one gateway can be the center of a Star. When you configure a plan, all gateways are Normal Members. To change a gateway to be the Center, configure the gateway properties.
5. For a gateway only - Click **Use DNS name** to use a DNS name instead of an IP address. You cannot configure this property in a plan, because a DNS name is a concrete and unique name, so it cannot be assigned with the same value to all gateways under the same plan.

6. Click **Save**.

**Authentication Method**

Use the Authentication Method window to show 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:**

In the gateway navigation tree, click **VPN > Authentication Method**.

The **Authentication Method** page opens and shows the following settings for the gateway.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>The gateway uses a <strong>Certificate</strong> to authenticate for VPN traffic</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - For externally managed gateways, the window shows only this field</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>The CA for the gateway is the SMP <strong>Internal CA</strong></td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>Select and copy this field to paste the DN in an external Management server</td>
</tr>
</tbody>
</table>

**To manage the certificates for the gateway:**

1. In the **Authentication Method** window, click **Manage Certificate**.
   
The **Export Wizard** window opens.

2. Select one of these options:
   
   - **Revoke and renew the certificate**
   
   - **Export the certificate**

3. Click **Next**.

4. When you are exporting 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, and you want to expose some of the networks behind this gateway to the other members of the VPN community, 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, which are exposed to the virtual private network.

**To manually configure network topology settings:**

1. In the gateway navigation tree, click **VPN > Internal Network Topology**.
   
The **Internal Network Topology** page opens.
2. Do the following for each network behind the gateway:
   a) Click New.
      The Internal Network Edit window opens.
   b) Complete the fields using the information in the table below.
   c) Click Finish.
      The network information appears in the Manually configured networks area.
3. To edit a network's settings, click on the network's name.
   The Internal Network Edit dialog box appears.
4. To delete a network's settings, do the following:
   a) Select the check box next to the network and click Delete.
      A confirmation message appears.
   b) Click OK.
      The network's settings are deleted.
5. Click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>Enter the name for the internal network</td>
</tr>
<tr>
<td>Network Address</td>
<td>Enter the IP address for the internal network</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Select the netmask for the internal network</td>
</tr>
</tbody>
</table>

Configuring Setup Settings

Use the Setup page to define SMP access.

- **Administrators Access** (on page 59): Add IP addresses to this table, to let SMP administrators access appliances over HTTPS and SSH.

- **Gateways behind NAT** ("Gateway behind NAT" on page 60): A gateway that connects to the Internet behind a NAT device does not have a publicly accessible IP address. To enable some features, SMP must access the gateway. To configure SMP for gateway IP address access, configure port forwarding for the required ports (default: local admin access =4434, push to gateway =18209) on the NAT device. Then, enter the ports here.

**Administrators Access**

Add IP addresses or a network to this table, to let SMP administrators 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 for a specified gateway if necessary. You must first unlock the administrator access settings from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure administrator access for a plan:

1. In Home > Plans > Edit of a plan, click Setup > Administrators Access.
   The Administrators Access window opens.
2. Click **New**.
   The **Administrator Access** page opens.
3. Select the **Source Type** (Network or IP Address).
4. Enter the **IP Address**.
5. For a network source type, enter a **Subnet Mask**.
6. Click **Finish**.
   The details are shown in a table in the Administrators Access window.
7. Click **Save**.

**To override administrator access set by a plan for a gateway:**

1. In **Home > Gateways > Edit** of a gateway, click **Setup > Administrators Access**.
   The **Administrators Access** page opens.
2. If necessary, click **Unlock from plan** to unlock the node from plan.
   The fields are enabled.
3. Click **New**.
   The Administrator Access window opens.
4. Configure the options (see above).
5. 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 for a specified gateway if necessary. You must first unlock the Gateway behind NAT settings from the plan. For more information, see Locking and Unlocking Settings (on page 62).

Instead of configuring the NAT port forwarding rules, you can log in to the gateway and configure it to connect to the SMP ("Connecting to Gateways behind NAT" on page 69).

**To configure the SMP for gateway IP address access of a plan:**

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

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

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

2. Paste the Web URL from the gateway.
3. 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 will fail.

For more about the supported clish commands, see the Check Point 1100 and 600 Appliances CLI and Advanced Routing Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=26395).

You can override the CLI script settings set by a plan for a specified gateway if necessary. You must first unlock the CLI script from the plan. For more information, see Locking and Unlocking Settings (on page 62).

If there were any errors reported by the gateway when running the CLI script, they are shown 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. From the navigation tree, click Home > Plans. The Plans window opens.
2. Click the plan to change. The Edit Plans window opens and shows the General page.
3. Click CLI Scripts > CLI Script 1 - 5.
4. Click Manage in SMP.
5. Enter the CLI commands that you want 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. In Home > Gateways > Edit of a gateway, click CLI Script > CLI Script 1 - 5.
2. If the CLI script is locked to a plan, click Unlock from plan.
3. Select Manage in SMP.
4. Enter the CLI commands that you want the script to run.
5. To disable the CLI script, clear Manage in SMP.
6. 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 in this window.

To edit the custom fields information for a gateway:
1. In Home > Gateways > Edit of a gateway, click Custom Fields.
   The Custom Fields page opens.
2. Edit the appropriate fields.
3. Click Save.

Locking and Unlocking Settings
By default, a gateway that is managed by the SMP inherits its settings from the plan to which it is subscribed. If necessary, you can override some of these inherited settings.

In the Home > Gateways > Edit page's navigation tree, 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
You can unlocking the gateway from a plan and override the inherited settings.

To unlock a gateway from a plan:
In the Home > Gateways > Edit window, click the applicable gateway.
1. Click Unlock from Plan.
2. Make the necessary changes.
3. Click Save.
Locking Gateways to a Plan

You can reset an individual gateway to the values specified in the plan, by locking it to a plan.

**To lock a node to a plan:**

1. In the Home > Gateways > Edit window, click the applicable gateway.
2. Click Lock to Plan.
   - The gateway is locked and cannot be edited. The settings are taken from the plan.
3. Click Save.

Searching for Gateways

You can filter the gateways list for a gateway that matches specified criteria.

**To search for gateways:**

1. Click Home > Gateways.
   - The Home > Gateways > Search Results page opens.
2. Click Filter.
   - The Search for gateways window opens.
3. To perform an advanced search, click Advanced Search Mode.
   - **Note:** You can revert to a simple search, by clicking Simple Search Mode.
4. Enter the applicable search criteria using the information in Gateway Search Fields (on page 64), and select the options from the drop-down lists using the information in Drop-down List Options (on page 65).
   - To indicate wildcards (for an unlimited number of characters), type an asterisk (*). For example, if you want to search for all gateways whose name starts with gw, type gw* in the appropriate search input field.
5. Select Filter.
   - The Home > Gateways > Search Results page opens and shows the gateways that meet the specified search criteria. The Status column indicates whether the gateway is currently connected ( ), not connected ( ), or disabled ( ).
These are the available 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>
</tbody>
</table>
| Status         | Select the current status of the gateway. This can be any of the following:  
  - **Any** - The status of the gateway is not important.  
  - **Connected** - The gateway is connected.  
  - **Downloading** - The gateway is currently downloading data from the SMS.  
  - **Client login failed** - The gateway’s attempt to authenticate to the SMP failed.  
  - **Disabled** - The gateway is disabled. | Connected |
| Management     | Select the gateway’s management type. This can be any of the following:  
  - **Any** - The gateway’s management type is not important.  
  - **Internal** - The gateway is remotely managed by the SMP.  
  - **Local** - The gateway is locally managed. | Internal |
<p>| Plan           | Select the plan configured for the gateway.            | Silver  |
| Description    | Enter a description for the gateway.                   | Appliance used in NY office |
| Domain Names   | Enter the DNS alias for the gateway.                    | johnsmith |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>What to enter</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<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>Static IP</td>
<td>Enter the static IP address of the gateway.</td>
<td>62.90.10.1</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>

These are the drop-down list options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is</td>
<td>Searches for gateways that match the data in the field.</td>
</tr>
<tr>
<td></td>
<td>For example, if you type “gw352” in the Name text box, the search will return only gw352.</td>
</tr>
<tr>
<td>not</td>
<td>Searches for gateways that do not match the data in the field.</td>
</tr>
<tr>
<td></td>
<td>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>contains</td>
<td>Searches for gateways that contain the data in the field.</td>
</tr>
<tr>
<td>none</td>
<td>Searches for gateways that do not have this feature.</td>
</tr>
<tr>
<td></td>
<td>For example, if for Owner you select none, the search will return all gateways without an owner.</td>
</tr>
<tr>
<td>from file</td>
<td>Loads a file containing MAC addresses and searches according to its content.</td>
</tr>
<tr>
<td>more</td>
<td>Searches for gateways with more nodes than the selected number.</td>
</tr>
<tr>
<td>less</td>
<td>Searches for gateways with fewer nodes than the selected number.</td>
</tr>
<tr>
<td>unlimited</td>
<td>Searches for gateways with an unlimited number of nodes.</td>
</tr>
<tr>
<td>don't care</td>
<td>Searches for gateways where the desired date/time can be anytime or non-existent.</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>anytime</td>
<td>Searches for gateways where the desired date/time can be anytime, but must be existent. For example, if for <strong>Expiration Date</strong> you select <strong>anytime</strong>, 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 <strong>Expiration Date</strong> you select <strong>last 7 days</strong>, 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 <strong>Creation Time</strong> you select <strong>last month</strong>, 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 criteria to Microsoft Excel format. The exported information includes the gateway type, assigned plan, product key, gateway settings, owner’s email address, and more.
To export gateway information to Microsoft Excel:

1. Click Home > Gateways.
   The Home > Gateways > Search Results page opens.
2. Select the check boxes of the applicable gateways or Filter ("Searching for Gateways" on page 63) 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

You can send email to one or more gateway owners.

To send an email to gateway owners:

1. Search for owners of gateways ("Searching for Gateways" on page 63).
   You can also click Home > Gateways to show all the gateways.
2. Select one or more of the gateways with the necessary owners.
3. Click Actions > Mail to owner.
   The General Mail window opens and shows the Preview tab.
4. To edit the email:
   a) Click the Edit tab.
   b) Change the email.
   c) Click the Preview tab.
5. Click Send Email.

Deleting Gateways

To delete a gateway in the Home > Gateways > Search Results page:

1. Select the check box next to the applicable gateway.
2. Click Delete.
   A confirmation message appears.
3. 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 Home >Gateways >Edit page:

1. Click Delete.
   A confirmation message appears.
2. Click OK.
   The gateway is deleted.
   The gateway's certificate is revoked and listed in the Certificate Revocation List as revoked.

   **Note:** Deleting a gateway does not delete the user ("Deleting Users" on page 125) 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 are using Internet Explorer, install the SMP certificate before you access the gateway ("Using Internet Explorer to Access Gateways" on page 174).

Connecting to Gateways

After you connect to the gateway, these identification details are shown:

- 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 Home >Gateways >Edit window:

1. Click Access Gateway.
2. If a security warning message is shown, confirm it and continue.
   A browser page opens and shows the progress of the SMP connecting to the gateway.

   **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 MAC address of the gateway.

   To make sure that the gateway you are securely connecting to is the correct gateway, check that the MAC address in the middle part of the string matches the one of the gateway. You can find the MAC address of the gateway in the **General** tab of the gateway.

3. If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can click OK to override that connection or Cancel to stop the login attempt.
   Update the local Check Point 600 & 1100 Appliance as necessary.
Connecting to Gateways behind NAT

When a gateway is behind a NAT device, by default the SMP cannot access the local WebUI. It is necessary to 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. From the navigation tree, 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.
   It is necessary to paste this URL in the SMP WebUI.
8. Click Apply.
   The gateway is ready to allow the SMP to access it.

To configure the SMP to access the gateway behind NAT:

1. Log in to the SMP.
2. From the navigation tree, click Gateways.
3. Click the gateway.
   The Gateways Edit window opens and shows the General page.
4. Click Setup > Gateways behind NAT.
5. If the gateway is locked to a plan, click Unlock from plan.
7. Paste the URL in the field.
8. Click Save.
Using Plans for Gateways

In This Section:

Editing Plans .......................................................................................................................... 70
Filtering the Plans Table ....................................................................................................... 90
Deleting Plans ........................................................................................................................ 91

A plan is a template of gateway features. Each gateway is assigned to a plan, and by default, inherits its settings from the plan. When necessary, 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 them in the WebUI for a gateway that is centrally managed.

Editing Plans

You can see or change the properties of plans in the Home > Plans window.

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 show the plans:

1. From the navigation tree, click Home > Plans.
   The Plans window opens.
2. Click the plan to change.
   The Edit Plans window opens and shows the General page ("Configuring General Settings (Plan)" on page 70).
3. Configure the settings for the plan.
4. Click Save.

Configuring General Settings (Plan)

To configure the managed services settings of a plan:

1. In Home > Plans > Edit of a plan, click General.
   The General page opens.
2. To disable the plan, clear Enabled.
3. 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.

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 will fail.

For more about the supported clish commands, see the *Check Point 1100 and 600 Appliances CLI and Advanced Routing Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=26395).

You can override the CLI script settings set by a plan for a specified gateway if necessary. You must first unlock the CLI script from the plan. For more information, see Locking and Unlocking Settings (on page 62).

If there were any errors reported by the gateway when running the CLI script, they are shown 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. From the navigation tree, click Home > Plans. The Plans window opens.
2. Click the plan to change. The Edit Plans window opens and shows the General page.
3. Click CLI Scripts > CLI Script 1 - 5.
4. Click Manage in SMP.
5. Enter the CLI commands that you want 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. In Home > Gateways > Edit of a gateway, click CLI Script > CLI Script 1 - 5.
2. If the CLI script is locked to a plan, click Unlock from plan.
3. Select Manage in SMP.
4. Enter the CLI commands that you want the script to run.
5. To disable the CLI script, clear Manage in SMP.
6. Click Save.
   The gateway runs the CLI script, and the script in the plan is not run.

**Configuring Device Settings**

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

- NTP (on page 37)
- Time Zone (on page 38)
- DNS (on page 39)
- Gateway Administrators (on page 40)

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

Configure the SMP to synchronize the time settings for the specified plans and gateways with an NTP server.

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

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

1. In Home > Plans > Edit of a plan, click Device Settings > NTP.
2. Make sure Manage in SMP is selected.
3. Enter the host name or IP address for the Primary and Second NTP Server.
4. From Update Interval, enter the time interval in minutes that SMP contacts the NTP server to update the time settings.
5. **Optional:** Configure the settings to authenticate to the NTP server.
   
a) Click NTP Authentication.
   
b) Enter the Shared Secret and Shared Secret Identifier.
6. Click Save.

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

1. In Home > Gateways > Edit of a gateway, click Device Settings > NTP.
2. If the NTP settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Configure the NTP settings (see above).
5. Click Save.

**To connect to the appliance:**

1. In Home > Gateways > Edit of a gateway, click Device Settings > NTP.
2. Click Access Gateway: Date and Time.
   
A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Date and Time page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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. In Home > Plans > Edit of a plan, click Device Settings > Time Zone.
2. Make sure Manage in SMP is selected.
3. From the Local Time Zone list, select the correct time zone option.
4. Select **Automatically adjust clock for daylight saving changes** to enable automatic daylight saving changes.

5. Click **Save**.

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

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > Time Zone**.
2. If the Time Zone settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Configure the Time Zone settings (see above).
5. Click **Save**.

**To connect to the appliance:**

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > Time Zone**.
2. Click **Access Gateway: Date and Time**.

A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the **Date and Time** page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

**Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 choose to define up to three DNS servers which are applied to all Internet connections or use the DNS configuration provided by the active Internet connection (Primary).

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

Use the DNS configuration from the Internet connection to allow a more dynamic definition of DNS servers. The gateways use the DNS settings of the currently active Internet connection.

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 is resolving
- DNS queries that do not contain a domain name are automatically appended with the domain name

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. In Home > Plans > Edit of a plan, click Device Settings > DNS.
2. Make sure Manage in SMP is selected.
3. Configure the DNS Settings:
   - To configure the DNS servers, click Configure DNS servers, and then enter the IP addresses for the DNS servers.
   - To use the Internet connection DNS settings, click Use DNS servers configured for the active Internet connection(s).
4. Configure the DNS Proxy settings:
   - To configure the gateways to provide DNS resolving services to internal hosts, click Enable DNS Proxy.
   - To use the DNS Proxy gateways to treat the local network objects as a hosts list, click Resolve Network Objects.
5. Enter the Domain Name that is appended to DNS queries.
6. Click Save.

To override the DNS settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click Device Settings > DNS.
2. If the DNS settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the DNS settings and let the administrator of the gateway manage them exclusively, clear Manage in SMP.
4. Configure the DNS settings (see above).
5. Click Save.

To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Device Settings > DNS.
2. Click Access Gateway: DNS.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the DNS page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.
   
   
   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can click OK to override that connection or Cancel to stop the current login attempt.

Gateway Administrators
The Gateway Administrators window 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. In **Home > Plans > Edit** of a plan, click **Device Settings > Gateway Administrator**.
2. Make sure **Manage in SMP** is selected.
3. To create a new Gateway Administrator:
   a) Click **New**.
      - The **Add Gateway Administrator** window opens.
   b) Enter the **Name** and **Password**.
   c) Select the **Permission** for the administrator.
   d) Click **Finish**.
4. To delete a Gateway administrator:
   a) Select the administrator.
   b) Click **Delete**.
      - A confirmation window opens.
   c) Click **OK**.
      - The administrator is deleted.
5. Click **Save**.

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

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > Gateway Administrator**.
2. If the Gateway administrator settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Configure the Gateway administrator settings (see above).
5. Click **Save**.

**To connect to the appliance:**

1. In **Home > Gateways > Edit** of a gateway, click **Device Settings > Gateway Administrator**.
2. Click **Access Gateway: Administrators**.
   - A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the **Administrators** page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 (on page 41)
- Application Control and URL Filtering (on page 42)
- IPS (on page 43)
- Traditional Anti-Virus (on page 44)
- Anti-Spam (on page 45)
- QoS (on page 46)
- Remote Access (on page 47)
- Site to Site VPN (on page 48)
- User Awareness (on page 49)
- Threat Prevention Anti-Virus (on page 49)
- Threat Prevention Anti-Bot (on page 50)
- Threat Prevention Policy (on page 51)

For each, you can set **Blade Control** to **On** or **Off**. 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 specific rules.

You can override the Firewall Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Firewall Software Blade from the plan. For more information, see **Locking and Unlocking Settings** (on page 62).

To configure the Firewall settings of a plan:

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > Firewall**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Strict**: Traffic that is not specified as Allowed in the Firewall Rule Base, is Blocked. Configure the Rule Base in gateway WebUI.
   - **Standard**: Traffic coming in to the internal network is Blocked, unless the Firewall Rule Base allows it. Traffic to the Internet, on all services, is Allowed. Traffic between internal networks and between trusted wireless networks is Allowed.
4. Select to log **Blocked Traffic**, **Accepted Traffic**, or both.
5. Click **Save**.

To override the Firewall settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Firewall**.
2. If the Firewall settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** and **Log** options (see above).
5. Click **Save**.

**To connect to the appliance:**

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Firewall**.
2. Click **Access Gateway:Firewall**.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Firewall Policy page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can click **OK** to override that connection or **Cancel** to stop the current login attempt.

**Application Control and URL Filtering**

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

You can override the Application Control and URL Filtering Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Application Control and URL Filtering Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

**To configure the Application Control and URL Filtering Software Blade settings of a plan:**

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > Application and URLs**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**, to block applications and URLs that are known to be insecure:
   - **Block security risk categories**: spyware, phishing, botnet, spam, anonymizer, and hacking
   - **Block torrents and P2P applications**: torrent trackers, BitTorrent and Gnutella protocols, file storage and sharing, media sharing, Facebook file sharing
   - **Block inappropriate content**: weapons, violence, sex, gambling, hate, illegal activities, and illegal drugs
4. Click **Save**.

**To override the Application Control and URL Filtering settings set by a plan in a gateway:**

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > Application and URLs**.
2. If the Application Control and URL Filtering settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** options (see above).
5. Click **Save**.
To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Application and URLs.
2. Click Access Gateway:Application Control.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Firewall Policy page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   **Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 to use on the gateways.

You can override the IPS Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the IPS Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the IPS Software Blade settings of a plan:
1. In Home > Plans > Edit of a plan, click Security Software Blades > IPS.
2. Make sure Manage in SMP is selected.
3. Set the Policy:
   - **Strict**: Use the IPS profile that has most of the protection categories enabled.
   - **Typical**: Use the IPS profile that blocks the most dangerous threats.
   - **Custom**: You can change the policy of which protection groups (by confidence level, severity, performance, and impact) are enabled or disabled.
4. Set the mode:
   - To implement IPS protections on the gateways, clear Detect-only mode.
   - To monitor IPS rule matches, click Detect-only mode.
5. Click Save.

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

To connect to the appliance:
1. In Home > Gateways Edit of a plan, click Security Software Blades > IPS.
2. Click Access Gateway:IPS.
A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the IPS page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the Traditional Anti-Virus Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

Gateways that are R77.20 and higher automatically use the Threat Prevention Anti-Virus Software Blade ("Threat Prevention Anti-Virus" on page 49). 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. In Home > Plans > Edit of a plan, click Security Software Blades > Traditional Anti-Virus.
2. Make sure Manage in SMP is selected.
3. Set the Policy:
   - Scan incoming files: Files coming in to the gateway on the selected protocols are scanned.
   - Scan outgoing files: Files that users send out are scanned. (This option is cleared by default.)
   - Scan files between networks: Files going between internal networks, or from the DMZ to internal, are scanned. You can filter this internal scanning to scan only the files that use selected protocols.
4. Set Tracking: Log, Alert (as defined in the System Settings), None.
5. Set the mode:
   - To implement Traditional Anti-Virus on the gateways, clear Detect-only mode.
   - To monitor Traditional Anti-Virus rule matches, click Detect-only mode.
6. Click Save.

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

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Traditional Anti-Virus.
2. If the Anti-Virus settings are locked to a plan, click Manage in SMP.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Set the Policy, Tracking, and Mode options (see above).
5. Click Save.
To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Traditional Anti-Virus.
2. Click Access Gateway:Traditional Anti-Virus.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Anti-Virus page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the Anti-Spam Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the Anti-Spam Software Blade settings of a plan:
1. In Home > Plans > Edit of a plan, click Security Software Blades > Anti-Spam.
2. Make sure Manage in SMP is selected.
3. Click Filter spam based on email content.
4. Set the Policy:
   - Block spam emails
   - Flag spam email subject
   - Flag spam email header
5. Set Tracking: Log, Alert (as defined in the System Settings), None.
6. Set the mode:
   - To implement Anti-Virus on the gateways, clear Detect-only mode.
   - To monitor Anti-Virus rule matches, click Detect-only mode.
7. Click Save.

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

To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Anti-Spam.
2. Click Access Gateway:Anti-Spam.
A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Anti-Spam page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

**Note** - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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, define Quality of Service, to give more bandwidth to the more important traffic in your environment.

You can override the QoS Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the QoS Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the QoS Software Blade settings of a plan:

1. In **Home > Plans > Edit** of a plan, click **Security Software Blades > QoS**.
2. Make sure **Manage in SMP** is selected.
3. Set the **Policy**:
   - **Ensure low latency for delay sensitive services**: Give more bandwidth for traffic that uses services that cannot function if the packets do not arrive on time. 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.
   - **Guarantee _% of the bandwidth to**: Set a minimum ratio of the bandwidth for traffic that is not preferred, in the VPN or for all traffic.
   - **Limit bandwidth consuming applications**: 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 services in the WebUI of the gateway.

4. Click **Save**.

To override the QoS settings set by a plan in a gateway:

1. In **Home > Gateways > Edit** of a gateway, click **Security Software Blades > QoS**.
2. If the QoS settings are locked to a plan, click **Unlock from plan**.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear **Manage in SMP**.
4. Set the **Policy** options (see above).
5. Click **Save**.
To connect to the appliance:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > QoS.
2. Click Access Gateway:QoS.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the QoS page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   
   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 on computers, handheld devices, and laptops.

You can override the Remote Access VPN Software Blade settings in a plan for a specified gateway if necessary. You must first unlock the Remote Access VPN Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the Remote Access VPN Software Blade settings of a plan:
2. Make sure Manage in SMP is selected.
3. Set the Policy:
   - Allow traffic from Remote Access users (by default): This setting enables your employees to log in to the network from a remote site. It does not give access without authentication.
   - Log traffic from Remote Access users - (by default)
4. Click Save.

To override the Remote Access VPN settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Remote Access VPN.
2. If the Remote Access VPN settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Set the Policy options (see above).
5. Click Save.
To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Remote Access VPN.


A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Remote Access page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the Site to Site VPN Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62)

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

1. In Home > Plans > Edit of a plan, click Security Software Blades > Site to Site VPN.

2. Make sure Manage in SMP is selected.

3. Set the Policy:
   - Allow traffic from remote VPN sites (by default): This setting enables VPN traffic.
   - Log VPN sites traffic (by default)

4. Click Save.

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

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Site to Site VPN.

2. If the Site to Site VPN settings are locked to a plan, click Unlock from plan.

3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.

4. Set the Policy options (see above).

5. Click Save.

To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > Site to Site VPN.

2. Click Access Gateway:Site to Site.

A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the Site to Site VPN Blade Control page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 if necessary. You must first unlock the User Awareness Software Blade from the plan. For more information, see Locking and Unlocking Settings (on page 62)

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

1. In Home > Plans > Edit of a plan, click Security Software Blades > User Awareness.
2. Make sure Manage in SMP and On are selected.
3. Click Save.

To override the User Awareness settings set by a plan in a gateway:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > User Awareness.
2. If the User Awareness settings are locked to a plan, click Unlock from plan.
3. To stop remote management of the blade and let the administrator of the gateway manage the blade settings exclusively, clear Manage in SMP.
4. Make necessary changes.
5. Click Save.

To connect to the appliance:

1. In Home > Gateways > Edit of a gateway, click Security Software Blades > User Awareness.
   A browser page opens and shows the progress of the SMP connecting to the gateway. The Check Point 600 & 1100 Appliance opens on the User Awareness page. The SMP administrator can now update the local Check Point 600 & 1100 Appliance.

   Note - If a local administrator is already logged in to the Check Point 600 & 1100 Appliance, a message is shown. You can 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 (on page 53)
- Firmware ("Firmware for Gateways and Plans" on page 54)
- Backup ("Periodic Backup" on page 55)
- Reports (on page 55)
- Report Recipients (on page 56)
- Dynamic DNS (on page 57) - Only in gateways
Managed Services

All gateways subscribed to the plan take their managed services settings from the plan, by default.

If necessary, you can override the inherited managed services settings for a specific gateway, by configuring these settings in the gateway. You must first unlock the managed services from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the managed services settings of a plan:
1. In Home > Plans > Edit of a plan, click the Services > Managed Services node.
   The Managed Services window opens.
2. Select or clear the necessary services.
3. Click Save.

<table>
<thead>
<tr>
<th>Managed Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store gateway logs</td>
<td>Send logs from the gateways to the SMP with SmartLog</td>
</tr>
<tr>
<td>Send periodic reports</td>
<td>Send Check Point Executive reports that contain security and network analysis details from the SMP to the gateway owners</td>
</tr>
<tr>
<td>Firmware upgrades</td>
<td>Controls the gateways firmware upgrades</td>
</tr>
<tr>
<td>Periodic backup</td>
<td>Schedule periodic backups of the appliance settings</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>Gateways will use Dynamic DNS services</td>
</tr>
</tbody>
</table>

To override managed services for a gateway:
1. In Home > Gateways > Edit of a gateway, click the Services > Managed Services node.
   The Managed Services window opens.
2. If necessary, click Unlock from plan to unlock the node from plan.
   The fields are enabled.
3. Select or clear the necessary services.
4. Click Save.

Firmware for Gateways and Plans

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

- Firmware to use for the gateways
- Scheduling firmware updates

All gateways subscribed to the plan will take their firmware settings from the plan, by default.

If necessary, you can override the inherited firmware settings for a specific gateway, by configuring these settings in the gateway. You must first unlock the firmware service from the plan. For more information, see Locking and Unlocking Settings (on page 62).
Automatic firmware updates require the gateway to reboot. If necessary, you can limit automatic firmware updates to certain days and hours, using the following procedure.

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

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

1. In **Home > Plans > Edit** of a plan, click the **Services > Firmware** node.
   The **Firmware** window opens.
2. Select one of these options:
   - **Specific firmware version** - Select one of the firmware options from the list or **Do_Not_Upgrade** (the gateway does not get a firmware update, it keeps the firmware installed on it).
   - **Check Point latest** - The gateway will download the latest firmware version available from Check Point.
   - **The firmware is managed locally on the device** - The gateway will not download firmware.
3. Select one of these options to define when the firmware is downloaded to the gateway:
   - **Upgrade immediately** - Automatically downloads the software and upgrades immediately.
   - **Daily** - Select the **time of day** range that the firmware should be downloaded every day.
   - **Weekly** - Select the **day of week** and **time of day** range that the firmware should be downloaded every week.
   - **Monthly** - Select the **day of month** and **time of day** range that the firmware should be downloaded every month.
4. Click **Save**.

**To override firmware settings for a gateway:**

1. In **Home > Gateways > Edit** of a gateway, click the **Services > Firmware** node.
   The **Firmware** window opens.
2. Click **Unlock from plan** to unlock the node from plan.
   The fields are enabled.
3. Select the firmware and schedule options (see above).
4. Click **Save**.

**Periodic Backup**

All gateways subscribed to the plan take their backup settings from the plan, by default. The backup file backs up the settings for each gateway in a separate ZIP file.

The naming convention of the file is:

<GW 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.
If necessary, you can override the inherited backup settings for a specific gateway, by configuring these settings in the gateway. You must first unlock the managed services from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the backup settings of a plan:
1. In Home > Plans > Edit of a plan, click Services > Periodic Backup. The Periodic Backup window opens.
2. Set the necessary fields.
3. Click Save.

<table>
<thead>
<tr>
<th>Periodic Backup</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File storage details</td>
<td>Enter the FTP Path, Username, and Password to back up gateway settings</td>
</tr>
<tr>
<td>Daily</td>
<td>Weekly</td>
</tr>
</tbody>
</table>

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

Reports
All gateways subscribed to the plan take their report settings from the plan, by default. You can override the reports settings set by a plan for a specified gateway if necessary. You must first unlock the reports service from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure the report settings of a plan:
1. In Home > Plans > Edit of a plan, click the Services > Reports node. The Security Reports window opens.
2. Set the applicable options.
3. Click Save.

<table>
<thead>
<tr>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>Weekly</td>
</tr>
<tr>
<td>Report's language</td>
<td>Select the language for the report</td>
</tr>
</tbody>
</table>

To override the report settings set by a plan in a gateway:
1. In Home > Gateways > Edit of a gateway, click the Services > Reports node. The Security Reports window opens.
2. If necessary, click **Unlock from plan** to unlock the node from plan. The fields are enabled.
3. Set the applicable options.
4. Click **Save**.

### Configuring VPN Settings

You can configure these VPN settings:

- Community ("VPN Community Settings" on page 57)

#### VPN Community Settings

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

You can override the VPN community settings set by a plan for a specified gateway if necessary. You must first unlock the community settings from the plan. For more information, see Locking and Unlocking Settings (on page 62).

For a gateway to get the community settings configured here, make sure that the **Site to Site VPN blade** has been turned on in the appliance.

#### To configure community settings:

1. For a plan - In **Home > Plans > Edit** of a plan, click **VPN > Community**. The **Community** window opens.
2. For a gateway - If you are editing community settings through the gateway and it is necessary, click **Unlock from plan**.
3. Click **Join a community**.
4. Select a community from the **Community list**.
   - To see or change the VPN Community settings, click **Go**.
   - If the selected community is a Star Community, the **Member Type** will show **Normal** or **Center**. You cannot configure this property in the plan, because only one gateway can be the center of a Star. When you configure a plan, all gateways are Normal Members. To change a gateway to be the Center, configure the gateway properties.
5. For a gateway only - Click **Use DNS name** to use a DNS name instead of an IP address. You cannot configure this property in a plan, because a DNS name is a concrete and unique name, so it cannot be assigned with the same value to all gateways under the same plan.
6. Click **Save**.

### Configuring Setup Settings

Use the **Setup** page to define SMP access.

- **Administrators Access** (on page 59): Add IP addresses to this table, to let SMP administrators access appliances over HTTPS and SSH.

- **Gateways behind NAT** ("Gateway behind NAT" on page 60): A gateway that connects to the Internet behind a NAT device does not have a publicly accessible IP address. To enable some features, SMP must access the gateway. To configure SMP for gateway IP address access, configure port forwarding for the required ports (default: local admin access =4434, push to gateway =18209) on the NAT device. Then, enter the ports here.
Administrators Access

Add IP addresses or a network to this table, to let SMP administrators 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 for a specified gateway if necessary. You must first unlock the administrator access settings from the plan. For more information, see Locking and Unlocking Settings (on page 62).

To configure administrator access for a plan:
3. Select the Source Type (Network or IP Address).
4. Enter the IP Address.
5. For a network source type, enter a Subnet Mask.
6. Click Finish. The details are shown in a table in the Administrators Access window.
7. Click Save.

To override administrator access set by a plan for a gateway:
2. If necessary, click Unlock from plan to unlock the node from plan. The fields are enabled.
4. Configure the options (see above).
5. 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 for a specified gateway if necessary. You must first unlock the Gateway behind NAT settings from the plan. For more information, see Locking and Unlocking Settings (on page 62).
Instead of configuring the NAT port forwarding rules, you can log in to the gateway and configure it to connect to the SMP ("Connecting to Gateways behind NAT" on page 69).

To configure the SMP for gateway IP address access of a plan:
1. Configure port forwarding for the required ports (default: local admin access =4434, push to gateway =18191) on the NAT device.
2. In Home > Plans > Edit of a plan, click Setup > Gateway behind NAT. The Gateway behind NAT page opens.
3. Enter the port numbers in Local admin access port and Push actions to gateway on port.
4. Click Save.

To override the gateway behind NAT settings set by a plan for a gateway:
1. Configure port forwarding for the required ports (default: local admin access =4434, push to gateway =18191) on the NAT device.
2. In Home > Gateways > Edit of a gateway, click Setup > Gateway behind NAT. The Gateway behind NAT page opens.
3. If necessary, click Unlock from plan to unlock the gateway from the plan.
4. Enter the port numbers in Local admin access port and Push actions to gateway on port.
5. Click Save.

To configure the gateway to connect to SMP with the Check Point SMB Relay:
2. Paste the Web URL from the gateway.
3. Click Save.

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. From the navigation tree, click Home > Plans. The Plans window opens.
2. Click the plan to change.
   The Edit Plans window opens and shows the General page.
3. Click History.

Filtering the Plans Table
If you have many plans, you can filter the Plans to easily find the one you want.

To filter the Plans:
1. From the navigation tree, click Home > Plans. The Plans window opens.
2. Click Filter. The Filter Plans window opens.
3. Enter filter criteria.
   You can use the asterisk (*) as an "any character, any number of times" wildcard.
   - **Name and Description** - {is | not | contains} <text>
   - **Creation Date and Modification Date** - {anytime | today | yesterday | last 7 days | last month | this month | on or after <date>| before <date>| between <date> <date>}

4. Click **Filter**.
   The window shows the filtered Plans.

**Deleting Plans**

You cannot delete a plan if it is currently in use by some gateways. You can disable plans ("Editing Plans" on page 70), so make sure the plan must be deleted.

**To delete a plan:**

1. From the navigation tree, click **Home > Plans**.
   The **Plans** window opens.
2. Select one or more plans.
3. Click **Delete**.
   A confirmation message shows.
4. Click **OK**.
   All selected plans are deleted.
Managing VPN Communities

In This Section:

Overview ................................................................. 92
VPN Community Types .............................................. 92
Creating VPN Communities ......................................... 95
Showing Communities ................................................ 95
Configuring the Community General Settings .................. 95
Filtering the Communities Table .................................... 96
Deleting Communities .................................................. 96
VPN Settings ............................................................ 97
Configuring Communities’ Custom Fields ......................... 99
Configuring Communities’ Members Lists ........................ 99
Creating Community Topologies .................................... 100
Viewing Community Histories ....................................... 100
Showing a Summary of a Community ............................... 100
Managing VPN Community with an External Gateway ......... 101

This chapter explains how to manage communities.

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.

It is also possible to configure a VPN community with gateways that are not managed by the SMP (“Managing VPN Community with an External Gateway” on page 101).

VPN Community Types

These are the VPN communities that 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 any need for intermediaries or “center” gateways. A fully meshed topology allows the highest performance, lowest transmission delay, and the best fault tolerance possible.

- Star
  A star community is composed of two types of members, center and satellite (also called hub and spoke), where:
  - The center gateway can communicate with each satellite gateway
  - Satellite gateways cannot communicate with each other
- **Nested**
  
  You can create advanced VPN topologies by nesting communities. For example, you can create a meshed community in which the members are star communities, a star community in which the members are meshed communities, and so on.

**Diagram of VPN Community Types**

![Diagram of VPN Community Types](image)
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. While gateways A and B are members of both communities X and Z, VPN tunnels between these gateways are established using the parameters of community Z rather than X, because Z is the innermost common community. VPN tunnels between gateways A and C are established using the parameters of community X, since X is the innermost common community of A and C.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VPN community X</td>
</tr>
<tr>
<td>2</td>
<td>VPN community Y</td>
</tr>
<tr>
<td>3</td>
<td>VPN community Z</td>
</tr>
<tr>
<td>4</td>
<td>Gateway D</td>
</tr>
<tr>
<td>5</td>
<td>Gateway C</td>
</tr>
<tr>
<td>6</td>
<td>Gateways A and B</td>
</tr>
</tbody>
</table>

VPN routing in nested communities is performed according to the nested community's type, fully meshed or star. In a nested fully meshed community, the gateways communicate directly with each other and with gateways in their parent community. In the example above, if community Y is fully meshed, then gateway C can communicate directly with other gateways in the community, as well as with gateway D, which is a member of the parent community, X.
Creating VPN Communities

To create a new VPN community:
1. From the navigation menu, click Home > Communities.
   The Communities window opens and shows the VPN 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 Communities window opens and shows the General page.

Showing Communities

To show the SMP communities:
From the navigation menu, click Home > Communities.
The Communities window opens and shows the communities.

<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>These are the 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>These are the values for the status of the community:</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>If necessary, shows the error for the community</td>
</tr>
</tbody>
</table>

Configuring the Community General Settings

To configure the General settings for a community:
1. From the navigation menu, click Home > Communities.
   The Communities window opens and shows the communities.
2. Click the community.
   The Edit Communities window opens and shows the General page.
3. Configure the General community settings.
4. Click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Optional: Enter a description of the community</td>
</tr>
<tr>
<td>Parent Community</td>
<td>To create a nested community, select the parent for this community</td>
</tr>
</tbody>
</table>

Filtering the Communities Table

To filter the communities window:

1. From the Communities window, click Filter. The Select communities window opens.
2. 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.
3. Click Apply.

Deleting Communities

You cannot delete a community that has gateways. You must remove the community’s gateways before deleting it. You can also remove gateways from a community ("Configuring Communities' Members Lists" on page 99).

To delete a community:

1. From the navigation menu, click 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.
VPN Settings

Configuring VPN Settings

For a star VPN, satellite members cannot communicate with each other. 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. From the navigation menu, click Home > Communities.
   The Communities window opens and shows the communities.
2. Click the community.
   The Edit Communities window opens and shows the General page.
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 ("Assigning a Center Gateway" on page 97).
6. To make sure that VPN tunnels between gateways in the community are always open, click Permanent VPN.
7. To disable Hide NAT for connections between the gateways in this community, click Disable NAT.

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. From the navigation menu, click Home > Communities.
   The Communities window opens and shows the communities.
2. Click the community.
   The Edit Communities window opens and shows the General page.
3. Click VPN Settings.

To assign the center gateway for a Star VPN community:

1. From the VPN Settings window of the community, in the Topology section click Choose.
   The Add Gateway wizard opens.
2. In the Select Method window, click one of these options to locate the center gateway.
   - Name - Enter the name of the gateway
   - MAC Address - Enter the MAC address of the gateway
   - Search for gateways - Opens a window to search for a gateway
3. Click Next.
4. If you are searching for the gateway:
   a) Enter the search values ("Searching for Gateways" on page 63).
   b) Click **Next**.
   c) Select the gateway.
   d) Click **Next**.

5. The **Done** window shows that the gateway is the center of the Star community, click **Done**.

Configuring IKE Settings

**To configure IKE settings for the community.**

1. From the navigation menu, click **Home > Communities**.
   The **Communities** window opens and shows the communities.
2. Click the community.
   The Edit **Communities** window opens and shows the **General** page.
3. Click **VPN Settings > IKE Settings**.
4. Configure the IKE settings.
5. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IKE Phase-1</strong></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><strong>IKE Phase-2</strong></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>
Configuring Communities' Custom Fields

If custom community fields are defined for the Service Domain, you can configure the custom fields as described in the following procedure. You can also define custom fields for Service Domains ("Configuring Custom Fields for Service Domains" on page 116).

**To configure a community's custom fields:**

1. From the navigation menu, click **Home > Communities**.
   The **Communities** window opens and shows the communities.
2. Click the community.
   The Edit **Communities** window opens and shows the **General** page.
3. Click **Custom Fields**.
4. Complete 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. SMP supports different types of VPN communities ("VPN Community Types" on page 92).

**To show the gateway members of a community:**

1. From the navigation menu, click **Home > Communities**.
   The **Communities** window opens and shows the communities.
2. Click the community.
   The Edit **Communities** window opens and shows the **General** page.
3. Click the **Members** tab.
   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 Wizard** opens.
2. Complete ("Adding Gateways" on page 17) the wizard and add the gateway to the community.

**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. 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. From the navigation menu, click **Home > Communities**.
   The **Communities** window opens and shows the communities.
2. Click the community.
3. Click **Actions > Generate Topology**.
   A confirmation message appears.
4. Click **OK**.

Viewing Community Histories

**To show history for a community:**

1. From the navigation menu, click **Home > Communities**.
   The **Communities** window opens and shows the communities.
2. Click the community.
   The Edit **Communities** window opens and shows the **General** page.
3. Click **History**.
   The **History** window shows the date and time when the community was:
   - First created
   - Most recently modified

Showing a Summary of a Community

You can show a summary of a community and email it.

**To show the summary for a community:**

1. From the navigation menu, click **Home > Communities**.
   The **Communities** window opens and shows the communities.
2. Click the community.
   The Edit **Communities** window opens and shows the **General** page.
Managing VPN Communities

3. Click View > Summary.
The Community Details Summary window opens.
4. To email the summary:
   a) In To, enter the email addresses.
   b) 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, it is necessary to install the applicable CAs to decrypt the VPN traffic. Similar procedures are required for the SMP and the external 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 Management server.
2. Create objects for the externally managed gateways.
3. For the SMP and Management server:
   a) Export the CA to file.
   b) Import the CA from the other Management server.
4. If necessary for the external gateways, install the security policy.

Preparing to Add an External Gateways

Before you add an external gateway to a VPN community, make sure that these items are ready:

- VPN community in the SMP is configured ("Configuring the Community General Settings" on page 95)
- Credentials to log in to the external Management server with Administrator permissions
- Static IP address for each external gateway

Note - It is possible for the VPN community in the external Management servers can to include Check Point 600 & 1100 Appliance gateways with dynamic IP addresses ("Adding Gateways to SmartDashboard (Dynamic IP Address)" on page 110). The specific settings depend on your external Management server.

Configuring a VPN Community with External Gateways

This is a high-level work flow that describes the process to create a VPN community with externally gateways.

1. In the external 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 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

Use the Members tab in the Communities Edit window to manage SMP and external gateways for the VPN community.

**To add the external gateway in the SMP:**

1. From the navigation menu, click **Home > Communities**. The Communities window opens and shows the communities.
2. Click the community. The Edit Communities window opens and shows the General page.
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.
7. Configure these settings:
   a) Enter the Name of the external gateway.
      **Note** - It is not necessary to use the same name for the external gateway in the SMP as in the external Management server.
   b) Clear Managed by SMP.
   c) Enter the Static IP for the external gateway.
8. 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 are only able to communicate after the SMP and external Management server exchange CAs.

**To import the external Management CA to the SMP:**

1. From the navigation tree, click **Service Domain > Settings**. The 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.
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.

### 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 management servers:

- **SMP** - Check Point 600 & 1100 Appliance gateways
- **SmartDashboard** - VPN community and VPN Security Gateway

#### High-level Workflow

1. Add Check Point 600 & 1100 Appliance 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 Check Point 600 & 1100 Appliance 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. It is also possible to add gateways that use a dynamic IP address ("Adding Gateways to SmartDashboard (Dynamic IP Address)" on page 110).

To add a gateway to SmartDashboard as an Externally Managed VPN gateway 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. Configure these **General Properties** settings:
   - **Name** - The SMP gateway name
   - **IPv4 Address** - IP address of the external interface
   - **Hardware** - Select **1100 Appliance**
   - From **Network Security**, click **IPsec VPN**
4. From the navigation tree, click **Topology**.
5. Configure these **Topology** settings:
   - Click **Manually defined on the Security Management server, based on the below Topology Table**
   - Click **All IP Addresses behind Gateway are based on the below Topology Table**

6. Make sure the external interface is configured correctly:
   a) Double-click the external interface.
   b) Review these settings:
      - Name - Name of external interface
      - Network Type - **External (leads out to the Internet)**
      - Static IP address and Net Mask - Same settings as the external interface on the gateway
   c) Click **OK**.

7. Configure each internal interface:
   a) Double-click the internal interface or click **New**.
   b) Configure these settings:
      - Name - Name of internal interface
      - Network Type - **Internal (leads to the local network)**
      - Static IP Address and Net Mask - IPv4 address and subnet mask for the interface
      - Topology - **Network defined by the interface IP and Net Mask**
   c) Click **OK**.

8. Click **OK**.
   The Check Point 600 & 1100 Appliance 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 Check Point 600 & 1100 Appliance 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 Check Point 600 & 1100 Appliance 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. Configure these settings:
   - Perform key exchange encryption with - AES-256
   - (Phase 1) Perform data integrity with - SHA1
   - Perform IPsec data encryption with - AES 128
   - (Phase 2) Perform data integrity with - SHA1

7. Click OK.

8. From the navigation tree, click Advanced Settings > Advanced VPN Properties.

9. Configure these settings:
   - Use Diffie-Hellman group - Group 2 (1024 bit)
   - Renegotiate IKE security associations every 1440 minutes
   - Renegotiate IPsec security associations every 3600 seconds
   - Select Disable NAT inside the VPN community.

10. 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 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

In the SMP use the Gateways Edit window to add and manage the VPN Security Gateway.

To add the VPN Security Gateway to the SMP:

1. Log in to the SMP.
2. From the navigation menu, click Home > Gateways.
   The Gateways window opens and shows the gateways.
3. Click New.
   The Create New Gateway window opens.
4. Configure these settings:
   a) Enter the Name of the VPN Security Gateway.
      
      Note - It is not necessary to use the same name for the external Security Gateway in the SMP as in SmartDashboard.
   b) Clear Managed by SMP.
   c) Enter the Static IP for the VPN Security Gateway.
5. Click Finish.
   The gateway object is created and shows the General page.
6. Configure the topology for each internal interface that is included in the encryption domain of the VPN Security Gateway:
   a) Click **New**.
      The **Internal Network Edit** window opens.
   b) Configure these settings:
      - Network Name - Enter the Interface name
      - Network Address - Enter the IPv4 address
      - Network Mask - Select the subnet mask
   c) Click **Save**.
   d) Perform these steps again 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. From the navigation tree, click **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 Check Point 600 & 1100 Appliance gateways are the satellite gateways.

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. From the navigation tree, click **Home > Communities**.
   The **Communities** window opens and shows the VPN 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 **Communities** window opens and shows the **General** page.

6. Click **VPN Settings**.

7. Add the **VPN Security Gateway** as the center gateway for the community:
   a) From **VPN Type**, select **Star**.
   b) From Center Gateway, click **Choose**.
   c) Enter the gateway **Name** or click **Search for Gateways** (*Searching for Gateways* on page 63).
   d) Click **Next**, and then click **Done**.

8. Configure these settings for the VPN community:
   a) Click **Disable NAT**.
   b) In **Encryption Method** select **IKEv1**.
   c) **Optional:** Click **No communication between satellites** to configure the VPN Security Gateway as the only encryption domain.

9. From the navigation menu, click **VPN Settings > IKE Settings**.

10. Configure these **IKE Phase 1** settings:
    - Encryption - **AES-256**
    - Authentication - **SHA1**
    - Diffie Hellman Group - **Group 2**
    - Renegotiate every - **1440**

11. 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 Gateway pair**

12. Click **Save**.

**To add the satellite gateways to the VPN community.**

1. In the **VPN Communities Edit** window, click the **Members** tab.

2. Add the satellite gateways. Perform these steps for each gateway:
   a) Click **Add Gateway**.
      The **Add Gateways** window opens.
   b) Enter the gateway **Name** or click **Search for Gateways**.
   c) Select the satellite gateway.
   d) Click **Next**.
   e) Click **Done**.
Exporting the SMP CA

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

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

To export the SMP CA:

1. From the navigation tree, click **System > Settings**.
   The **Settings** window opens and shows the **General** page.
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMP VPN</td>
<td>Any</td>
<td>Any</td>
<td>SMP_VPN</td>
<td>FTP- port</td>
<td>VPN Security Gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SMTP</td>
<td></td>
</tr>
</tbody>
</table>

Adding Gateways to SmartDashboard (Dynamic IP Address)

Create new objects for the Check Point 600 & 1100 Appliance 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 are able to log in to the SMP when you are adding this gateway.

Before you add the gateway, make sure that you imported the SMP CA to SmartDashboard ("Importing the CA to SmartDashboard and Updating the Policy" on page 109). It is necessary to assign the SMP CA to the gateway.

This procedure is for gateways that use a dynamic external IP address. It is also possible to add gateways that use a static IP address ("Adding Gateways to SmartDashboard (Static IP Address)" on page 103).

To get the DN for a gateway in the SMP:
1. From the navigation tree, click Home > Gateways.
2. Click the gateway.
   The Gateways Edit window opens and shows the General page.
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. Configure these General Properties settings:
   • Name - The SMP gateway name
   • IPv4 Address - Click Dynamic Address
     A warning window opens. Click Yes.
   • Hardware - Select 1100 Appliance
   • From Network Security, click IPsec VPN
4. From the navigation tree, click **Topology**.

5. Configure these **Topology** settings:
   - Click **Manually defined on the Security Management server, based on the below Topology Table**
   - Click **All IP Addresses behind Gateway are based on the below Topology Table**

6. Make sure the external interface is configured correctly:
   a) Double-click the external interface.
   b) Review these settings:
      - Name - Name of external interface
      - Network Type - **External (leads out to the Internet)**
      - Make sure **Dynamic IP** is selected
   c) Click **OK**.

7. Configure each internal interface:
   a) Double-click the external interface or click **New**.
   b) Configure these settings:
      - Name - Name of internal interface
      - Network Type - **Internal (leads to the local network)**
      - Static IP Address and Net Mask - IPv4 address and subnet mask for the interface
      - Topology - **Network defined by the interface IP and Net Mask**
   c) Click **OK**.

8. From the navigation tree, click **IPsec VPN**.

9. Click **Matching Criteria**.
   The **Certificate Matching Criteria** window opens.

10. From **Gateway must present a certificate issued by CA**, select the SMP CA.

11. Click **DN**.

12. Enter or paste the **DN** (Distinguished Name) for the gateway.

13. Click **OK**.

14. In the Gateway Properties window, click **OK**.
   The Check Point 600 & 1100 Appliance gateway with a dynamic IP address is added to SmartDashboard.
Managing Service Domains

In This Section:

- Adding Service Domains ................................................................. 112
- Showing Service Domains ............................................................... 113
- Editing the General Page ................................................................. 113
- Deleting Service Domains ............................................................... 114
- Showing Service Domain Histories .................................................. 114
- Configuring the Settings for an SMP Service Domain ....................... 114

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. Configure the settings.
4. Click Finish.
   The new Service Domain opens and shows the General page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Service Domain name | The name of the SMP virtual Service Domain  
                       You cannot change this name after you create the Service Domain |
| Description     | Description of the SMP virtual Service Domain |
| Company         | Company that uses this Service Domain |
| Contact         | Contact for this Service Domain |
| Email           | Contact's email address  
                       **Note:** You cannot use the SMP to send emails to this address |
Managing Service Domains

Showing Service Domains

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

To show the Service Domains:

From the navigation tree, click System > Service Domains.

The Service Domains window opens.

Editing the General Page

If the portal is disabled, all users defined in the portal cannot log in, and all gateways defined in the portal are disabled.

To edit the General page of a Service Domain:

1. From the navigation tree, click System > Service Domain.
   The Service Domains window opens.
2. Click the Service Domain.
   The Edit Service Domains window opens and shows the General tab.
3. To enable the Service Domain, click Enabled.
4. Change the settings.
5. Click Save.

These are the Service Domain fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the SMP virtual Service Domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This field appears only in the System &gt; Service Domains &gt; Edit page. It is read-only.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the SMP virtual Service Domain.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this option to enable the Service Domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - If the Service Domain is disabled, all users defined in the Service Domain will not be allowed to log in, and all gateways defined in the Service Domain will be considered disabled.</td>
</tr>
<tr>
<td></td>
<td>This field appears only in the System &gt; Service Domains &gt; Edit page.</td>
</tr>
<tr>
<td>Company</td>
<td>Enter the name of the company for which this Service Domain is used.</td>
</tr>
<tr>
<td>Contact</td>
<td>Enter the name of the contact for this Service Domain.</td>
</tr>
<tr>
<td>Email</td>
<td>Enter the contact's email address.</td>
</tr>
</tbody>
</table>
Deleting Service Domains

To delete a Service Domains:

1. From the navigation tree, click System > Service Domains.
   The System > Service Domains page appears and shows the Service Domains.
2. Select the Service Domain.
3. Click Delete.
   A confirmation window opens.
4. Type your administrator password in the field.
5. Click OK.
   The Service Domain is deleted.

Showing Service Domain Histories

To show the history for a Service Domain:

1. From the navigation tree, click System > Service Domains.
   The Service Domains window opens.
2. Click the Service Domain.
   The Edit Service Domain window 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. From the navigation tree, click Service Domain > Settings.
   The Settings window opens for the Service Domain 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. From the navigation tree, click Service Domain > Settings.
   The Settings window opens and shows the General page.
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 control the system logging mechanism:
- Configure the severity of the logs that are generated
- Forward them 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. From the navigation menu, click **Service Domain > Settings**.
   The Settings window opens and shows the General page.
2. Click **Logging**.
3. In the Log Level drop-down list, select the minimum severity that generates logs.
4. To configure the server as a Syslog client for logs from the Service Domain:
   a) Click **Forward logs to an external Syslog Server**.
   b) In **Syslog Server**, enter the IP address of the Syslog server.
   c) In **Syslog Port**, enter the port number that is used to send the logs.
5. To delete old logs:
   a) Click **Purge old logs**.
   b) In **Older than**, enter the maximum number of days that logs are saved.
   c) In **Action**, select:
      - **Delete** - Old logs are deleted from the server
      - **Archive** - Old logs are archived on the server
6. Click **Save**.
Configuring DNS Settings for Service Domains

If you want to enable the Dynamic DNS service, you must configure the DNS settings.

**To configure the DNS settings:**

1. From the navigation tree, click **Service Domain > Settings**.
   
The Settings window opens for the Service Domain and shows the **General** page.

2. Click **DNS**.
   
The **DNS** fields appear.

3. Configure the DNS settings.
   
   **Note:** This is the DNS server for the SMP. It is not the DNS server that is used for Dynamic DNS.

4. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Suffix</td>
<td>Enter the DNS suffix for the SMP domain registration.</td>
</tr>
<tr>
<td>Dynamic IP Time to Live</td>
<td>Enter the number of seconds that a dynamic IP address remains in the DNS server’s cache after resolution. A longer amount of time reduces the load on the server. A shorter amount of time makes sure there is less downtime when you change IP addresses.</td>
</tr>
<tr>
<td>Static IP Time to Live</td>
<td>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 amount of time reduces the load on the server.</td>
</tr>
</tbody>
</table>

Configuring Custom Fields for Service Domains

Use custom fields to record additional information for a user, gateway, or community. You can configure custom fields for these objects:

- Users
- Gateways
- VPN Communities

**To configure custom fields for a Service Domain:**

1. From the navigation tree, click **Service Domain > Settings**.
   
The Settings window opens for the Service Domain and shows the **General** page.

2. Click **Custom Fields**.

3. To add a custom field:
   
   a) Click **User**, **Gateway**, or **Community custom fields**.
   
   b) Click **New**.
   
   The custom field is shown.
c) Enter the name field. For example, Billing Code or Shipping Date.
d) Click Save.

4. To delete a custom field:
   a) Select the custom field.
   b) Click Delete.
   c) Click Save.

Showing Firmware for Service Domains
You can view a list of firmwares that are available in a specific Service Domain. SMP administrators can manage the firmware images that are available ("Managing Firmwares for Gateways" on page 138).

To show firmwares for a Service Domain:
1. From the navigation tree, click Service Domain > Settings.
   The Settings window opens and shows the General page.
2. From the Service Domain navigation tree, 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 permanent connection error occurs, it is possible to configure how long gateways wait before they attempt to reconnect to the server.

To manage gateways reconnection settings for a Service Domain:
1. From the navigation tree, click Service Domain > Settings.
   The Settings window opens for the Service Domain and shows the General page.
2. From the Service Domain navigation tree, 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. From the navigation tree, click Service Domain > Advanced.
   The Custom Email Template Images window 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:** Enter the alternate text for the image, if the image cannot be shown.
   a) In **Display Description** enter the alternate text.
   b) 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. From the navigation tree, click **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 window opens and shows the **General** page.
3. Change the settings.
4. Click **Save.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Comment about the image file</td>
</tr>
<tr>
<td>Display Description</td>
<td>Alternate text for the image, if the image cannot be shown</td>
</tr>
<tr>
<td>Usage in reports</td>
<td>HTML tags and content that you paste into the SMP template</td>
</tr>
</tbody>
</table>
History (Custom Images)

To show the History page for Custom Images:

1. From the navigation tree, click 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 window opens and shows the General page.

3. From the navigation tree, click History.
   The History page opens and shows when the image was Created and Last Modified.
Managing Service Domain Users

In This Section:

- Showing Users ................................................................. 120
- Searching for Users .......................................................... 120
- Editing Users ....................................................................... 122
- Sending Emails to Users .................................................... 124
- Showing Logs (Users) .......................................................... 124
- Exporting Users ................................................................... 125
- Deleting Users ..................................................................... 125
- Managing Gateways for a User ............................................ 125

Showing Users

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

- **User ID** column shows the login name for a user
- **Role** ("Configuring Roles for Users" on page 128) shows the privileges for the user
- **Status** column shows if users are logged in to the SMP:
  - Green - The user is logged in
  - Red - The user is logged out
  - Gray - The user does not have a password or is deactivated for SMP

To show the SMP users:
From the navigation tree, click Home > Users.

Searching for Users

The Search Users window contains many search fields that you can use to show only the specified users. The window also lets you:

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

To search for users:
1. From the navigation tree, click Home > Users.
2. Click Filter.
   The Users Search window opens.
3. Enter the search settings.
4. Click Apply.
   The Search Results window opens and shows the users.
5. To export the table of users to Excel:
   a) Select one or more users.
   b) 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 for the user
   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 shows the users that match the search.
5. In the Search window, click Clear to reset the search fields and options.

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

To email a summary of user data:
1. From the navigation tree, click Home > Users.
   The Users window opens.
2. Click the User ID.
   The Edit window opens for the user and shows the General page.
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. From the navigation tree, click Home > Users.
   The Users window opens.
2. Click the User ID.
   The Edit window opens for the user and shows the General page.
3. Change the settings for the user.
4. Click Save.
   The changes for the user are saved.

<table>
<thead>
<tr>
<th>Page</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Email address, change Role, change password</td>
</tr>
<tr>
<td>Expiration</td>
<td>Time that account remains active</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact information for the user</td>
</tr>
<tr>
<td>Status</td>
<td>List of SMP sessions</td>
</tr>
</tbody>
</table>

General Settings (User)

To change the email address or Role for the user:

1. In the General page, in Email, enter the new email address.
   SMP sends emails for the user to this address.
2. From Role, select the role or the user.
3. 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.
   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. In the **Expiration** page, click **User will expire in**.
2. From the drop-down menu, select one of the time settings:
   - Hours
   - Days
   - Months
3. Enter the number of hours, days, or months when the account will deactivate.
4. In **Start From**, click on of these options:
   - **First login** - The time frame when the account will deactivate, starts from the first time that the user logged in to SMP
   - **Specified date** - The time frame when the account will deactivate, starts from the configured time
5. 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. Edit the appropriate fields.
2. Click **Save**.

Status Settings (User)
The **Status** window shows if the user is logged into SMP and details about the SMP session.
The **Status** option in the navigation tree shows if the user is logged in to the SMP:
- Green - The user is logged in
- Red - The user is 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>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>

**Sending Emails to Users**

You can send email to one or more SMP users.

**To send an email to users:**

1. Search for users that you are exporting ("Searching for Users" on page 120).
   You can also 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:
   a) Click the **Edit** tab.
   b) Change the email.
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. From the navigation tree, click **Home > Users**.
   The Users window opens.
2. Click the **User ID**.
   The Edit window opens for the user and shows the General page.
3. Click **View > Today's system logs**.
   The System Logs window opens and shows the user logs.
4. To filter the logs:
   a) Click **Actions > Filter**.
   The Filter the Logs window opens.
b) Change the filter settings.
c) 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 that you are exporting ("Searching for Users" on page 120).
   You can also 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. From the navigation tree, click **Home > Users**.
   The **Users** window opens.
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. From the navigation tree, click **Home > Users**.
   The **Users** window opens.
2. Click the **User ID**.
   The **Edit** window opens for the user and shows the **General** page.
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** ("Adding a Gateway (Name)" on page 126) of the gateway
   - **MAC Address** ("Adding a Gateway (MAC Address)" on page 126)
- Search for a gateway ("Adding a Gateway (Search)" on page 127)
- Create a new gateway ("Adding a New Gateway" on page 127)

6. Click **Next**.
   The applicable window opens.

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

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

**Adding a Gateway (MAC Address)**

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

1. From the **Gateways** tab, click **Add**.
   The **Add Gateways** wizard opens.
2. In the **Select Method** window, click **MAC address**.
3. In **MAC Address**, enter the gateway MAC address.
4. Click **Next**.
   The **Completed** window opens, and the gateway is added to the user.
5. Click **Done**.
Adding a Gateway (Search)

To search for the gateway and add it to a user:
1. From the Gateways tab, click Add.
   The Add Gateways wizard opens.
2. In the Select Method window, click Search.
3. Click Next.
   The Search for gateways window opens.
4. Use the search fields to filter the gateways.
5. Click Next.
   The Add Gateways opens and shows the applicable gateways.
6. Select one or more gateways.
7. Click Next.
   The Completed window opens, and the gateway is added to the user.
8. Click Done.

Adding a New Gateway

To create a new gateway and add it to a user:
1. From the Gateways tab, click Add.
   The Add Gateways wizard opens.
2. In the Select Method window, click Name.
3. Click Create a new Gateway.
4. From the drop-down menu, select the gateway type.
5. Click Next.
   The Create New Gateway: Step 1 window opens.
6. Enter the data for the gateway.
7. Click Next.
   The Create New Gateway: Step 2 window opens.
8. Enter the MAC Address and Registration Key for the gateway.
9. Click Next.
   The Completed window opens, and the gateway is added to the user.
10. Click Done.
Configuring Roles for Users

In This Section:

Overview of Roles ................................................................. 128
Using Predefined Roles ......................................................... 128
Creating New Roles .............................................................. 129
Showing Roles ...................................................................... 129
Deleting Roles ........................................................############ 130
Editing Roles ......................................................................... 130
Configuring Advanced Role Settings ...................................... 132
Resetting Predefined Roles to Default Settings ......................... 133

Users are assigned roles that specify which actions they can and cannot perform in the Service Domain. For example:

* A role can only allow a user to configure the gateway settings in the Service Domain
* A role can allow a user full read-write permission for all objects in the Service Domain

Roles allow you to create granular permissions for SMP system administrators. The SMP includes different pre-defined roles that you can use for your company.

Overview of Roles

Roles define privileges for users and the changes that they are allowed to make in the SMP. These are some 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>
</table>
| Power User     | • Show SMP objects  
                 • Change gateways, plans and End Users  
                 • Cannot change other users and roles  
                 • Send emails  
                 • Show Service Domain logs |
| Read Only User | • Show SMP objects  
                 • Show Service Domain logs |
| Super User     | • Change SMP objects  
                 • Send emails  
                 • Show Service Domain logs |
| Support User   | • Show SMP objects  
                 • Create and configure gateways and End Users  
                 • Change SMP objects  
                 • Send emails  
                 • Show Service Domain logs |

### Creating New Roles

There is a **New User** wizard in SMP to help you can create new users.

**To add a new role**

1. From the navigation tree, click **Service Domain > Roles**.  
   The **Roles** window opens.
2. Click **New**.  
   The **Create New Role: Step 1** window opens.
3. Enter the **Name** for the role.
4. Click **New**.  
   The new role is created. The **Edit** role window opens and shows the **General** page.

### Showing Roles

The **Roles** window shows some of the roles for SMP users in the database.

**To show the roles:**

From the navigation tree, click **Service Domain > Roles**.
Deleting Roles

You can delete roles except for the predefined roles.

Note: You cannot delete a role when it is assigned to users.

To delete one or more roles:
1. Select one or more roles.
2. Click Delete.
   A confirmation window opens.
3. Click OK.
   The role is deleted.

Editing Roles

Define the access control policy for each role to configure the permissions for users that are assigned to the role.

The SMP applies rules for roles in sequential order. If rule 2 blocks an action, and that same action is allowed in rule 4, users cannot do that action.

Configuring Rules for Roles

These are the fields that you use to configure a role:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td>• Allow - Allow users with this role to do the specified operations</td>
</tr>
<tr>
<td></td>
<td>• 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 (&quot;Using String Operators for Roles&quot; on page 131)</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. From the navigation tree, click Service Domain > Roles.
   The Roles window opens.
2. Click the role.
   The Edit window opens for the role and shows the General page.
3. Click Access Control Policy.
4. Create or edit a rule:
   • To create a new rule, click New
   • 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

The following represents a list of 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: &lt;br&gt; 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: &lt;br&gt; uid != CurrentUser.uid</td>
</tr>
<tr>
<td>&amp;&amp;</td>
<td>Concatenates condition string elements. The rule must match all of the condition string elements.</td>
<td>element &amp;&amp; element</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Alternates between condition string elements. The rule must match at least one of the condition string elements.</td>
</tr>
<tr>
<td>Contains</td>
<td>Shows that the element is a member of the array.</td>
<td>Contains(array, element)</td>
<td>Rule applies for communities that contain the current user's gateways: &lt;br&gt; Contains(communities, CurrentUser.gateways)</td>
</tr>
<tr>
<td>Intersects</td>
<td>Shows that the two arrays intersect.</td>
<td>Intersects(array1, array2)</td>
<td>Rule applies for gateways that the current user owns: &lt;br&gt; Intersects(gateways, CurrentUser.gateways)</td>
</tr>
</tbody>
</table>
### Configuring Roles for Users

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
</table>
| `!`      | Negates condition string elements. | `! element` | Rule applies only for gateways that do not belong to the current user:  
`!Intersects(gateways, CurrentUser.gateways)` |
| **Length** | Shows the length of an array or the number of characters in a string. | `Length(array|element)` | Rule applies only if the gateway belongs to a community:  
`Length(CurrentUser.gateways)!=0` |
| **Matches** | Compares the value of a condition string element to a regular expression. | `Matches(element, regular-expression)` | Rule applies when the gateway name starts with "gw"  
`Matches(name, "gw.+")` |

### Deleting Role Rules

**To delete a role rule**

1. From the navigation tree, click **Service Domain > Roles**.  
The **Roles** window opens.
2. Click a role.
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. From the navigation tree, click **Service Domain > Roles**.
2. Click a role.  
The **Edit** window opens and shows the **General** page.
3. Click **Advanced**.  
The **Advanced** window opens.
4. To configure additional permissions for the role, in the **Additional Permissions** section, configure the settings.
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 that this role can use to connect to the SMP.
4. Click Save.

To delete a range of IP addresses for a role:
1. In the Restrictions section, select a 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>User Privilege when Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access SMP WebUI</td>
<td>Log in to the SMC</td>
</tr>
<tr>
<td>Enable Lost Password Recovery</td>
<td>Recover lost passwords for other users</td>
</tr>
<tr>
<td>Access API</td>
<td>Access the SMP API</td>
</tr>
<tr>
<td>View Logs</td>
<td>Open logs for this SMP Service Domain</td>
</tr>
<tr>
<td>Send Email</td>
<td>Send emails from the SMP</td>
</tr>
</tbody>
</table>

Resetting Predefined Roles to Default Settings

To reset a predefined role to its default settings
1. From the navigation tree, click Service Domain > Roles.
   The Roles window opens.
2. Click the role.
   The Edit window opens for the role and shows the General page.
3. Click Revert.
   The role is reset to its default settings.
Configuring SMP Administrators

In This Section:
- Showing Administrators ................................................................. 134
- Adding SMP Administrators ............................................................. 134
- Editing SMP Administrators ............................................................ 135
- Deleting SMP Administrators ........................................................... 136
- Configuring SMP Administrator Account Expiration ......................... 136
- Configuring SMP Administrators' Contact Details ............................... 136
- Showing SMP Administrator Statuses ............................................... 137

This chapter explains how to manage SMP administrators.

These tasks are relevant for SMP administrators only.

Showing Administrators

The Status column indicates whether the administrator is currently logged on to the SMP (green icon) or not (red icon).

To show the SMP administrators:
From the navigation tree, click System > Administrators.

Adding SMP Administrators

To add an SMP administrator:
1. From the navigation tree, click System > Administrators.
2. Click New.
   The Create New Administrator window opens.
3. Enter the following settings for the administrator:
   - 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 - Enter the administrator 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. From the navigation tree, click **System > Administrators**.
2. Click the SMP administrator.
   
   **Note:** If you are a Read-Only administrator, you can only click on your User ID.
   
   The Edit administrators window opens and shows the **General** page.
3. Configure the settings for the administrator.
4. Click **Save**.

To change the password for an administrator:

1. In the **General** page, click **Change**.
   
   The Change Password window opens.
2. Enter the new password.
3. Click **OK**.
   
   The password is changed.
   
   Click **Save**.

You can also configure:

- SMP Administrator Account Expiration ("Configuring SMP Administrator Account Expiration" on page 136)
- Administrators' Contact Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td></td>
</tr>
<tr>
<td>Last name</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Email address that SMP uses to send messages</td>
</tr>
<tr>
<td>Additional emails</td>
<td>SMP also sends emails to these addresses</td>
</tr>
<tr>
<td>Access rights</td>
<td>Select <strong>Administrator</strong> for permissions to edit all the SMP settings, or <strong>Read Only Administrator</strong> for permissions to only see all the windows</td>
</tr>
<tr>
<td>Password</td>
<td>Click <strong>Change</strong> to change the administrator password</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Deleting SMP Administrators

To delete an SMP administrator in the System > Administrators page:
1. From the navigation tree, click System > Administrators.
2. Select the SMP administrator.
3. Click Delete.
   A confirmation message opens.
4. Click OK.
   The SMP administrator is deleted.

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. From the navigation tree, click System > Administrators.
2. Click the SMP administrator.
   The Edit administrators window opens and shows the General page.
3. From the Administrators navigation tree, click Expiration.
   The Expiration page opens.
4. In the Expiration page, click 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 - The time frame when the account will deactivate, starts from the first time that the user logged in to SMP
   - Specified date - The time frame when the account will deactivate, starts from the configured time
8. Click Save.

Configuring SMP Administrators' Contact Details

To configure contact details for an SMP administrator:
1. From the navigation tree, click System > Administrators.
2. Click the SMP administrator.
   The Edit administrators window opens and shows the General page.
3. From the Administrators navigation tree, click Contact.
   The Contact page opens.
4. Enter the information in the applicable fields.
5. Click Save.

Showing SMP Administrator Statuses

The Status option in the navigation tree shows if the administrator is logged in to the SMP WebUI:

- Green - The administrator is logged in
- Red - The administrator is logged out
- Gray - The administrator does not have a password or is deactivated for SMP

To view the status of an SMP administrator:

1. From the navigation tree, click **System > Administrators**.
2. Click the SMP administrator.
   
   The Edit administrators window opens and shows the General page.
3. From the Administrators navigation tree, click **Status**.
   
   The Status page opens.

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>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 .................................................................................................................. 138
- Adding Firmware to the SMP System ......................................................................................... 138
- Deleting Firmware from the SMP System .................................................................................. 138
- Managing Firmware .................................................................................................................... 139
- Showing Firmware Histories ...................................................................................................... 139
- Showing Firmware for Service Domains .................................................................................... 139

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:**

From the navigation tree, click **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. From the navigation tree, click **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 some gateways or plans.

**To delete a SMP firmware from the server:**

1. From the navigation tree, select **System > Firmware**.

2. Select the firmware image.
3. Click **Delete**.
   A confirmation message opens.
4. Click **OK**.
   The firmware is deleted.

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. From the navigation tree, click **System > Firmware**.
2. Click the firmware.
   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. From the navigation tree, click **System > Firmware**.
2. Click the firmware.
   The **Edit Firmware** window opens and shows the **General** page.
3. From the firmware navigation tree, click **History**.
   The **History** page opens.

Showing Firmware for Service Domains

You can view a list of firmwares that are available in a specific Service Domain. SMP administrators can manage the firmware images that are available ("Managing Firmwares for Gateways" on page 138).

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

1. From the navigation tree, click **Service Domain > Settings**.
   The **Settings** window opens and shows the **General** page.
2. From the Service Domain navigation tree, 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 .................................................. 140
- Showing and Editing SMP Servers ................................................................. 141
- Adding Security Management Servers ............................................................ 147
- Deleting an SMP Server ................................................................................ 148
- Showing the Security Management Server Settings ......................................... 148
- Managing Licenses without the WebUI .............................................................. 150

This chapter explains how to manage SMP Servers.

Understanding the SMP Server Architecture

SMP Server
The SMP Server is the Windows Server on which the SMP is installed. This server uses these software to implement the SMP solution:

- Security Management Portal
- Active Directory
- Check Point Security Management Server

SMP Server has two modules that are critical parts of the infrastructure that manages the gateways:

- CMLS - Creates a secure connection between the SMP and the gateways
- J MLS - Processes data that is sent by the CMLS and the gateways

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

SMP WebUI
The SMP WebUI is an Internet browser based application that helps you configure and manage the different SMP components, users, gateways, and system settings. SMP administrators use a secure HTTPS connection to log in to the WebUI.

The SMP WebUI is hosted on an Apache Tomcat application server.
Sample SMP Architecture Workflow

This is a sample workflow to help explain how the components of the SMP architecture manage the gateways.

1. From the SMP WebUI, the administrators configures the settings for a gateway and clicks Save.
2. The data and settings for the gateway are saved to the AD database.
3. The gateway contacts the CMLS at a regular time interval and asks if there are new settings. The default time interval is 5 minutes.
4. The CMLS asks the J MLS if the settings for the gateway are changed.
5. The J MLS queries the AD database and finds that there are new settings for the gateway.
6. The J MLS creates an update package for the gateway that contains the delta based on the gateway and plan settings.
7. The J MLS sends the package to the CMLS.
8. The CMLS sends the package to the gateway.
9. The gateway installs that package and updates the settings.

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>![Icon]</td>
<td>Module is up</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Module is down</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Module is disabled</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Module is up with errors</td>
</tr>
</tbody>
</table>

To show the SMP server modules:

1. From the navigation tree, click 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 ("Showing the General Page" on page 141) page in the Configure tab.

Showing the General Page

To show the General page for a SMP Server:

1. From the navigation tree, click 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.
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 ("Configuring DNS Settings for the SMP Server" on page 16).

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</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancing Weight (Log Server)</td>
<td>200</td>
<td>2/3 of the gateway logs are sent to this server</td>
</tr>
<tr>
<td>Load Balancing Weight (Log Server)</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. From the navigation tree, click **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.

3. From the navigation tree, click **Settings**.

4. Configure the settings.

5. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Addresses</strong></td>
<td></td>
</tr>
<tr>
<td>SMP Address</td>
<td>The IP address for the SMP Server.</td>
</tr>
<tr>
<td>SMP NAT Address</td>
<td>Optional - Enter the NAT IP address for the server. When this field is empty, the server uses the SMP Address.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>Optional - Enter the DNS name for the SMP Server. When this field is empty, the server uses the SMP NAT Address.</td>
</tr>
</tbody>
</table>

**Load Balancing**

<table>
<thead>
<tr>
<th>Load Balancing Weight (Log Server)</th>
<th>Enter the value to increase or decrease the percentage of gateway logs that are sent to this server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The default value of 100 distributes gateway logs equally to all servers.</td>
</tr>
</tbody>
</table>
### Showing the Managed Modules

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

1. From the navigation tree, click **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.
3. From the navigation tree, click **Managed Modules**.
   These are the default processes that are shown:
   - SMP - Main process of the SMP
   - J MLS - 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. From the navigation tree, click **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.
3. From the navigation tree, click **SMS Module > SMS Settings**.
4. Configure the settings and the IP addresses for the server ("Configuring the IP Address for an SMS Module" on page 144).
5. Click **Save**.

### Table: Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancing Weight</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a short description of the server.</td>
</tr>
<tr>
<td>Server Relative Weight</td>
<td>Enter the load balancing capacity relative to the other servers. The default setting is 1.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>- A server with a <strong>Server Relative Weight</strong> of 2 can handle twice as many gateways as a server with a setting of 1.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enabled</td>
<td>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. <strong>Note</strong> - Disable the SMS for a SMP Server that is not connected to the network.</td>
</tr>
</tbody>
</table>

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

You must configure the IP address settings for the SMS 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, when they 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. From the navigation tree, click **SMS Module > SMS Settings** (*Configuring the SMS Module* on page 143).
2. To add an IP address:
   a) Click **New**.
      
      The **Edit Server Address** window opens.
   b) Complete the fields.
   c) Click **Finish**.
3. To edit the IP address:
   a) Click the IP address.
      
      The **Edit Server Address** window opens.
   b) Complete the fields.
   c) Click **Finish**.
4. To delete an IP address:
   a) Select the IP address.
   b) Click **Delete**.
      
      A confirmation message opens.
   c) Click **OK**.
5. Click **Save**.
Configuring Advanced Settings

**To configure advanced server settings:**

1. From the navigation tree, click **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.
3. Click **Advanced**.
4. Configure the settings.
5. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Address</td>
<td>If the interface for the SMS module is located behind a NAT device, enter the IP address or DNS name of the NAT device.</td>
</tr>
<tr>
<td>Default Service Domain</td>
<td>Select the default Service Domain to associate with this IP address. All gateways that use the gateway ID to connect to this IP address are connected to this Service Domain.</td>
</tr>
<tr>
<td>Console Port (TCP)</td>
<td>Enter the console port for the Security Management Server. This port is used to access the server from a browser to view its updated status. The default is 9283.</td>
</tr>
<tr>
<td>Concurrent downloads limit</td>
<td>Enter the maximum number of items (such as a security policy or firmware) that the Security Management Server sends to gateways at the same time. Use this setting to limit the bandwidth the SMP uses to update the gateways. The default setting is 50.</td>
</tr>
</tbody>
</table>

Showing Security Management Server Status

You can show the current status of an SMP Server.

These are the modules that can be used in SMP:

- DRM - Indicates the DNS Resolving Module’s status.

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

1. From the navigation tree, click **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.
3. Click **Status**.
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 name of the SMS</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time at which the SMS was added to the SMP</td>
</tr>
<tr>
<td>Last Modified</td>
<td>The date and time at which the SMS was last modified</td>
</tr>
<tr>
<td>Server is</td>
<td>The status of the SMS.</td>
</tr>
<tr>
<td></td>
<td>The SMS can have the following statuses:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Up</strong>. The SMS is working.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>. The SMS is not working, or it 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 working, but errors have occurred.</td>
</tr>
<tr>
<td>Version</td>
<td>The SMS's version number</td>
</tr>
<tr>
<td>Address</td>
<td>The SMS's IP address and port number in the format: &lt;SMS IP&gt;:&lt;Port Number&gt;</td>
</tr>
<tr>
<td>NAT IP</td>
<td>The IP address of the NAT device behind which the SMS is located.</td>
</tr>
<tr>
<td></td>
<td>If the SMS is not located behind a NAT device, this field displays N/A.</td>
</tr>
<tr>
<td>Certificate will expire on</td>
<td>The date on which the SMS's certificate will expire, 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 <strong>View</strong>.</td>
</tr>
<tr>
<td>Modules</td>
<td>For each module that is enabled in the server, this area indicates the module's status in this SMS. The possible statuses are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ON</strong> - The service is enabled in the SMS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OFF</strong> - The service is disabled in the SMS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>FAIL</strong> - 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>The possible statuses are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong> - The primary database is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standby</strong> - 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>The possible statuses are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong> - The secondary database is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standby</strong> - The secondary database is disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>N/A</strong> - No secondary database is configured.</td>
</tr>
</tbody>
</table>
Showing Security Management Server Diagnostics

You can view diagnostic information for an SMP Server. This information is only available for servers that are currently working.

To view diagnostics for an SMP Server:

1. From the navigation tree, click **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.
3. Click the **Diagnostics** tab.

<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 that the server is using</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 that the server is using</td>
</tr>
<tr>
<td>Virtual Total</td>
<td>The total amount of virtual memory that is available on the server</td>
</tr>
</tbody>
</table>

Adding Security Management Servers

To add a new Security Management Server:

1. Click **System > SMS Servers**.
   - A list of Security Management Servers is shown.
2. Click **New Server**.
   - The **Create New Server Wizard** opens the **Create New Server: Step 1** dialog box.
3. Complete the fields using the information in the table.
4. Click **Next**.
   - The **Create New Server: Step 2** dialog box opens.
5. Click **Finish**.

To create new server wizard fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Enter the name of the Security Management Server. You cannot change this field after saving the server for the first time.</td>
</tr>
</tbody>
</table>
Deleting an SMP Server

To delete an SMP Server:

1. From the navigation tree, click **System > SMP Servers**. The SMP Server window opens and shows a list of servers.
2. In the row, click **Delete**. 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 are applied to all the SMP Servers that are 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. Configure the settings.
4. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a short description of the server.</td>
</tr>
<tr>
<td>Setup Interval</td>
<td>Enter how often (in seconds) the gateways poll the SMP for a new configuration. The default setting is 600 seconds.</td>
</tr>
<tr>
<td>Security Lease Time</td>
<td>Select the amount of time that the encryption key between the SMP and the gateways is valid. The default setting is 1 day.</td>
</tr>
</tbody>
</table>
Managing SMP Servers

Security Management Portal Administration Guide

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBM (Load Balancing Module)</td>
<td>Enable load balancing between SMP Servers.</td>
</tr>
<tr>
<td>Migration Threshold</td>
<td>When LBM is enabled, select the threshold percentage for load balancing.</td>
</tr>
<tr>
<td>Servers Sync Interval</td>
<td>When LBM is enabled, enter how often (in seconds) the servers compare loads.</td>
</tr>
<tr>
<td></td>
<td>The default is 10 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Using a lower interval improves load balancing accuracy, but it also increases the communication between the servers. We recommend that you use a low interval (1-15 seconds).</td>
</tr>
<tr>
<td>CVM (Content Vectoring Module)</td>
<td>Not relevant for version R12 and higher.</td>
</tr>
<tr>
<td>DRM (DNS Resolving Module)</td>
<td>Enable the Dynamic DNS service for the SMP Server.</td>
</tr>
</tbody>
</table>

Configuring the Log Policy

You can add an unlimited number of logging rules.

**To configure the log policy for the Security Management 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. Click **Log Policy**.
4. The **Log Policy** page opens.
5. Configure the settings.
   - To add a new rule, click **New**.
   - To edit a rule, click the rule name in the **Protocol** column.
6. Click **Finish**.
   The **Log Policy** table shows the logging rule.
7. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select the type of logging destination. If you choose local, the Server URL field is disabled.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Enter the log server's address.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select the minimal message severity to send to the logging destination.</td>
</tr>
</tbody>
</table>
Managing SMP Servers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>Select the message origin (Management Server or Gateway), according to which filtering should be performed. Select * if you don't want to filter according to the message origin.</td>
</tr>
</tbody>
</table>

**Deleting Logging Policy Rules**

To delete a logging policy rule:

1. In the Log Policy ("Configuring the Log Policy" on page 149) 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. 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. Click **History**.
   
   The History page opens and shows when the Security Management Server was Created and Last Modified.

**Managing Licenses without the WebUI**

Sometimes it is necessary to add SMP licenses without the SMP WebUI. For example, deployments with multiple SMP Servers, you cannot use the WebUI 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 WebUI, 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 > 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 WebUI, 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 ............................................................. 152
- Exporting SMP Data ............................................................................................ 152
- Importing SMP Data .......................................................................................... 155

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 ("Exporting SMP Data" on page 152) to an XML file and then import the data ("Importing SMP Data" on page 155). 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:
From the navigation tree, click 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 WebUI

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

When you are exporting 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 WebUI:

1. Click 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 is 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|[g|i|[p]r][u]|y][-] destination_file [SMC_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>
<tbody>
<tr>
<td>a</td>
<td>Exports all data</td>
</tr>
<tr>
<td></td>
<td>This command overrides all other commands.</td>
</tr>
<tr>
<td>d</td>
<td>Exports SMP administrators.</td>
</tr>
<tr>
<td>Flag</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>f</td>
<td>Exports firmware.</td>
</tr>
<tr>
<td>g</td>
<td>Exports gateways.</td>
</tr>
<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 will be encrypted.</td>
</tr>
</tbody>
</table>

**destination_file**
The path to the destination file. If the file already exists, it will be overwritten.

**SMC_IP_address**
The IP address of the SMC from which data should be exported.

**username**
The username for accessing the SMC.

**password**
The password for accessing the SMC.

**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 used the Service Domain flag, specify from which Service Domain the data should be exported.
Importing SMP Data

You can choose to import only data that does not currently exist in the database, or to import all data and replace the existing data with the imported data.

Importing Data with the SMP WebUI

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 WebUI:

1. Click 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:
   
   importer source_file {f|n} [SMC_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 you don't want to overwrite existing data, enter this command:
   
   importer n SMP_data.xml
   
   The data is imported from the specified file. If you choose to receive confirmation messages, then confirmation messages open as needed.

   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 overwrite the data that is 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 regarding data that already exists in the SMP database.</td>
</tr>
<tr>
<td>SMC_IP_address</td>
<td>The IP address of the SMC to which data should be imported.</td>
</tr>
<tr>
<td>username</td>
<td>The username for accessing the SMC.</td>
</tr>
<tr>
<td>password</td>
<td>The password for accessing the SMC.</td>
</tr>
<tr>
<td>Service Domain_name</td>
<td>If more than one SMP virtual Service Domain is configured, you can specify the target Service Domain to which the data should be imported. Data will be imported from the first Service Domain in the source file into the specified Service Domain.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a target Service Domain, all of the data in the source file will be imported to the relevant Service Domains.</td>
</tr>
</tbody>
</table>

   Note - By default, the original Service Domain names will be used.
Monitoring the SMP

In This Section:
Showing Logs .................................................................................................................................................. 157

This chapter explains how to monitor the Service Domain activity and show logs for gateways.

Showing Logs

Showing Gateway Logs

Gateway logs detail all firewall-related events, including the following:
- Logged allowed connections
- Logged dropped connections
- Detected viruses
- Web sites blocked by URL filtering
- Suspected spam

To show the gateway logs:
1. From the navigation tree, click 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 it was not blocked</td>
</tr>
</tbody>
</table>
Showing System Logs

System logs detail the following events:

- Scheduler events
  The Scheduler performs the following 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. From the navigation tree, click 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. From the navigation tree, click **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>📊</td>
<td>Done</td>
<td>Activity completed successfully</td>
</tr>
<tr>
<td>🕒</td>
<td>Canceled</td>
<td>Activity was canceled and did not complete</td>
</tr>
<tr>
<td>🕍</td>
<td>Failed</td>
<td>Activity failed and did not complete</td>
</tr>
<tr>
<td>🔄</td>
<td>In progress</td>
<td>Activity is in progress</td>
</tr>
<tr>
<td>🌀</td>
<td>Waiting</td>
<td>SMP is waiting for a response from the logging service</td>
</tr>
</tbody>
</table>

Filtering Logs

If desired, you can set a filter on general logs and gateway logs to display any of the following:

- Logs from different date ranges
- Logs of different severities or actions
- Logs containing specific text

The filter settings are persistent throughout the user session.

**Setting Filters**

To set a filter:

1. From the **Logs** window, click **Actions > Filter**.
   The **Filter the Logs** window opens.
2. Configure the settings for the log filter.
3. Click **Apply**.
<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>• <strong>This Service Domain</strong> - Show logs for this Service Domain only</td>
</tr>
<tr>
<td></td>
<td>• <strong>All Service Domains</strong> - Show logs for all Service Domains</td>
</tr>
<tr>
<td>Start Date</td>
<td>Select the earliest date for the logs that the window shows.</td>
</tr>
<tr>
<td>End Date</td>
<td>Select the latest date for the logs that the window shows.</td>
</tr>
<tr>
<td>Origin</td>
<td>Filter the source that generates the logs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Is</strong> - Show only logs that match this <strong>Origin</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not</strong> - Show only logs that do NOT match this <strong>Origin</strong></td>
</tr>
<tr>
<td>User</td>
<td>Filter the username that generates the logs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Is</strong> - Show only logs that match this <strong>User</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not</strong> - Show only logs that do NOT match this <strong>User</strong></td>
</tr>
<tr>
<td>Free Text</td>
<td>Filter the logs for any column that matches the string. You can use regular expressions (on page 175).</td>
</tr>
<tr>
<td>Min. Severity</td>
<td>Select the lowest severity for the logs that the window shows.</td>
</tr>
<tr>
<td>Limit results to</td>
<td>Set the highest number of logs that the window shows.</td>
</tr>
</tbody>
</table>
Using Reports, Notifications, and Custom Alerts

In This Section:

Using SMP Notifications ................................................................. 161
Using Custom Alerts ....................................................................... 168

This chapter explains how to use the following:

- 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 WebUI 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. ("Configuring Outgoing Mail Settings for the SMP" on page 25)

Note - This task is relevant for SMP administrators only.

Configuring System Administrator Notifications

You can configure SMP to send notifications to SMP system administrators upon certain events.

To configure SMP system notifications:

1. Click System > Settings.
   
   The Settings window opens and shows the General page.

2. Click Notifications.

3. Configure which notifications are sent to administrators.

4. To edit the notification emails sent to administrators, click Customize.

5. Click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Send Notifications When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify administrator added/changed</td>
<td>• A new account is created for the administrator</td>
</tr>
<tr>
<td></td>
<td>• The administrator password, role, or email is changed</td>
</tr>
</tbody>
</table>
### 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. From the navigation tree, click System > Service Domains. The Service Domains window opens.
2. Click the Service Domain. The Edit window opens and shows the General tab.
3. Click Notification.
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. Click System > Settings. The Settings window opens and shows the General page.
2. Click Notifications > Reports.
3. To send reports of portal statistics, select one or more of these options:
   - Send short Service Domain statics report
   - Send extended Service Domain statistics report
4. To edit the reports that are sent to administrators, click Customize.
5. Click Save.
Configuring Service Domain Notifications

You can specify which types of notifications that are sent for a Service Domain.

In order to use Service Domain notifications, you must configure mail settings for the Service Domain ("Configuring Outgoing Mail Settings for Service Domains" on page 14).

**Configuring User Notifications**

To configure user notifications:

1. From the navigation tree, click **Service Domain > Settings**.
   The **Settings** window opens for the Service Domain and shows the **General** page.
2. Click **Notifications > Users**.
3. Configure the user notifications.
4. To edit the notification emails that are sent, click **Customize**.
5. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Notify user of creation of new account or of change in account | Select this option to automatically send notifications to users for these events:  
  - A new account with access permissions is created  
  - Their password or email is modified     |
| Send daily user report                             | Select this option to automatically send a daily report to SMP administrators. The report includes:  
  - Gateways added to this Service Domain today  
  - Gateways deleted from this Service Domain today  
  - Gateways in this Service Domain that connected today for the first time  
  The report is sent at 12:00 AM each day.     |

**Configuring Gateway Notifications**

To configure gateway notifications:

1. From the navigation tree, click **Service Domain > Settings**.
   The **Settings** window opens for the Service Domain and shows the **General** page.
2. Click **Notifications > Gateways**.
3. Configure the gateway notifications.
4. To edit the notification emails that are sent, click **Customize**.
5. Click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify owner X days before subscription expiration</td>
<td>Automatically send notifications before the subscription expires.</td>
</tr>
</tbody>
</table>
### Using Reports, Notifications, and Custom Alerts

#### Security Management Portal Administration Guide R12

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify owner of subscription expiration</td>
<td>Automatically send notifications on the day that their subscription expires.</td>
</tr>
<tr>
<td>Notify owner of gateway added/changed</td>
<td>Automatically send notifications for these events:</td>
</tr>
<tr>
<td></td>
<td>• A new gateway is added for them</td>
</tr>
<tr>
<td></td>
<td>• Registration Key or server group is modified on one of their gateways</td>
</tr>
<tr>
<td>Notify administrator of gateways that have not connected for</td>
<td>Automatically send notifications to SMP administrators when gateways in this Service Domain have not connected to the Service Center for the specified amount of time.</td>
</tr>
<tr>
<td>Notify owner when user login failed at least</td>
<td>Automatically send notifications to gateway owners, if there is the specified number of failed gateway login attempts within the number of minutes.</td>
</tr>
<tr>
<td>Send periodic gateway reports</td>
<td>Automatically send security reports each week to the gateway owners.</td>
</tr>
</tbody>
</table>

#### Configuring Community Notifications

**To configure community notifications:**

1. From the navigation tree, click **Service Domain > Settings**. The **Settings** window opens for the Service Domain and shows the **General** page.
2. Click **Notifications > Community**.
3. To automatically send notifications to community administrators (community members with Community Manager permissions) when changes occur in the community, click **Send notifications about changes in communities**.
   - Community administrators will receive notifications when one of the following events occurs:
     • A user or member is added to the community.
     • A user or member is removed from the community.
4. To edit the notification emails that are sent, click **Customize**.
5. Click **Save**.

#### Configuring Firmware Notifications

When you enable firmware notifications, the SMP automatically sends notifications to Service Domain administrators when there are new firmware updates.

**To configure firmware notifications:**

1. From the navigation tree, click **Service Domain > Settings**. The **Settings** window opens for the Service Domain and shows the **General** page.
2. Click **Notifications > Firmware**.
3. Select or clear **Send notifications about firmware added**.
4. To edit the notification emails that are sent, click **Customize**.
5. Click **Save**.
Configuring Virus/Spam Notifications

When you enable the virus and spam notification, the SMP automatically sends notifications to gateway owners for each 24-hour period in which the server detected viruses or spam in their outgoing mail.

To configure virus and spam notifications:
1. From the navigation tree, click Service Domain > Settings. The Settings window opens for the Service Domain and shows the General page.
2. Click Notifications > Viruses / Spam.
3. Select or clear Send notifications about viruses / spam sent from your computers.
4. To edit the notification emails that are sent, click Customize.
5. Click Save.

Configuring Summary Messages

To configure summary messages:
1. From the navigation tree, click Service Domain > Settings. The Settings window opens for the Service Domain and shows the General page.
2. Click Notifications > Summary Messages.
3. To edit the notification emails that are sent, click Customize.
4. Click Save.

Configuring Summary Reports (Service Domains)

To configure summary reports:
1. From the navigation tree, click 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

1. Next to the desired notification, click **Customize**.
   
The **Message Template** dialog box appears displaying the **Preview** tab. This tab displays a preview of the selected notification type.

2. Click the **Edit** tab.
   
The **Edit** tab appears.

3. In the **Subject** field, type the text that should appear in the notification's Subject line.

4. In the **BCC** field, type the email addresses people who are not SMP administrators, who should receive a copy of the notification.
   
   These addresses will appear in the notification's BCC (Blind Carbon Copy) field.

5. Edit the notification template, by doing one of the following:
   
   - In the script text box, edit the template.
   - To load a notification template:
     
     (i) Click **Browse** to browse to the file containing the report template, or type the filename in the **File** text box.
     
        The file can be a *.txt or *.html file.
     
     (ii) Click **Load File**.
     
        The file is loaded to the script text box.

6. To reset the HTML script to its default settings, click **Default**.

7. To select the SMP administrators who should receive a copy of the notification, do the following:
   
   a) Click the **Administrators** tab.
   
      The **Administrators** tab appears.
   
   b) Click **Add**.
   
      The **Select Administrators** dialog box opens.
   
   c) Select the desired administrators.
   
   d) Click **Done**.
   
      The specified administrator(s) appear in the **Administrators** tab.
   
      The administrator(s) will appear in the notification's BCC field.
   
   e) To send an email to an administrator, click on the administrator's email address.
   
   f) To remove an administrator from the **Administrators** tab, select the administrator and click **Remove**.
   
      The administrator is removed from the **Administrators** tab.

8. To select users who should receive a copy of the notification, do the following:
   
   
   **Note:** This option is only relevant when configuring Service Domain notifications.

   a) Click the **Users** tab.
   
      The **Users** tab appears.
b) Click Add.
   The Add User Wizard appears displaying the Select Method dialog box.

c) To select an existing user, do the following:
   (i) In the User ID field, type the user’s User ID.

   Note: The User ID must already be defined in the system.
   (ii) Click Next.
   The Completed dialog box appears.

d) To search for users, do the following:
   (i) Select Search for users.
   (ii) Click Next.
   The Search for Users dialog box appears.
   (iii) Complete the fields with the desired search criteria using the information in User Search Fields, and select the options from the drop-down lists.
   (iv) Click Next.
   The Add User dialog box appears with a list of users that meet the specified search criteria.
   (v) Select one or more check boxes next to the desired user(s).
   (vi) Click Next.
   The Completed dialog box appears.

e) To create a new user, do the following:
   (i) Select Create a new user.
   (ii) Click Next.
   The Create New User Wizard opens displaying the Create New User: Step 1 dialog box.
   (iii) Complete the fields using the information in User Details Fields.
   (iv) Click Next.
   The Create New User: Step 2 dialog box appears.
   (v) Complete the fields using the information in User Details Fields.
   (vi) Click Next.
   The Create New User: Step 3 dialog box appears.
   (vii) Click Finish.
   The Create New User Wizard closes.
   The Add User Wizard reappears displaying the Completed dialog box.

f) Click Done.
   The specified user(s) appear in the Users tab.
   The user(s) will appear in the notification’s BCC field.

g) To send an email to a user, click on the user’s email address.
h) To remove a user from the Users tab, select the user and click Remove. The user is removed from the Users tab.

9. To preview the notification, click Preview. The Preview tab reappears displaying the report with your changes.

10. If you are satisfied with the notification, click OK.

Using Custom Alerts

You can configure the SMC to automatically generate alerts upon the receipt of specific log messages. Alerts can be sent either as an email message and a log message, or as a log message.

Using SMP System Custom Alerts

In order to use SMP custom alerts, you must configure mail settings for the SMP ("Configuring Outgoing Mail Settings for the SMP" on page 25).

To add or edit custom alerts:

1. From the navigation tree, click System > Settings. The System > Settings window 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’s 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.
   - If you selected Send Email in the Action drop-down list, continue at Send Email Alerts.

Custom Alerts Details Window

To configure the details for a new custom alert:

1. Complete the fields with the correct settings. Only logs that match the Filter and fulfill the Recurrences conditions generate the alert.
2. Click OK.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the alert’s 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>
<tr>
<td>Filter</td>
<td></td>
</tr>
<tr>
<td>Log ID</td>
<td>Select the only Log ID that generates the alert.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</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 in order to generate the alert.</td>
</tr>
<tr>
<td>Recurrences</td>
<td>This section lets you set alerts to generate when there are more than or less than the configured value.</td>
</tr>
</tbody>
</table>
| Trigger alert if             | • At least - The alert is generated when the number of logs is greater than the value during the time interval (too many logs).  
|                              | • Less than - The alert is generated when the number of logs is less than the value during the time interval (too few logs).  |
| matching events are received | Number of logs that match the Filter fields.                                 |
| 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.   |
| over a period of             | Enter the time interval (in minutes) for Recurrences fields.                 |
| Alert Action                 |                                                                            |
| 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**

1. Click **OK**.  
The dialog box closes.
2. Click **Save**.

**Send Email Alerts**

1. Click the **Edit** tab.  
The **Edit** tab appears.
2. In the **Subject** field, type the text that should appear in the alert's Subject line.
3. In the **BCC** field, type the email addresses people who are not SMP administrators, who should receive a copy of the alert.  
These addresses will appear in the alert's BCC (Blind Carbon Copy) field.
4. Edit the alert template, by doing one of the following:  
   • In the script text box, edit the template.  
   • To load an alert template:  
     (i) Click **Browse** to browse to the file containing the report template, or type the filename in the **File** text box.
The file can be a *.txt or *.html file.

(ii) Click **Load File**.

The file is loaded to the script text box.

5. To reset the HTML script to its default settings, click **Default**.

6. To select the SMP administrators who should receive a copy of the alert, do the following:
   a) Click the **Administrators** tab.
      The **Administrators** tab appears.
   b) Click **Add**.
      The **Select Administrators** dialog box opens.
   c) Select the desired administrators.
   d) Click **Done**.
      The specified administrator(s) appear in the **Administrators** tab.
      The administrator(s) will appear in the alert's BCC field.
   e) To send an email to an administrator, click on the administrator's email address.
   f) To remove an administrator from the **Administrators** tab, select the administrator and click **Remove**.
      The administrator is removed from the **Administrators** tab.

7. To select users who should receive a copy of the alert, do the following:
   a) Click the **Users** tab.
      The **Users** tab appears.
   b) Click **Add**.
      The **Add User Wizard** appears displaying the **Select Method** dialog box.
   c) To select an existing user, do the following:
      (i) In the **User ID** field, type the user's User ID.
      Note: The User ID must already be defined in the system.
      (ii) Click **Next**.
      The **Completed** dialog box appears.
   d) To search for users, do the following:
      (i) Select **Search for users**.
      (ii) Click **Next**.
      The **Search for Users** dialog box appears.
      (iii) Complete the fields with the desired search criteria using the information in User Search Fields, and select the options from the drop-down lists.
      (iv) Click **Next**.
      The **Add User** dialog box appears with a list of users that meet the specified search criteria.
Using Reports, Notifications, and Custom Alerts

(v) Select one or more check boxes next to the desired user(s).
(vi) Click Next.

The Completed dialog box appears.

e) To create a new user, do the following:
   (i) Select Create a new user.
   (ii) Click Next.

The Create New User Wizard opens displaying the Create New User: Step 1 dialog box.
(iii) Complete the fields using the information in User Details Fields.
(iv) Click Next.

The Create New User: Step 2 dialog box appears.
(v) Complete the fields using the information in User Details Fields.
(vi) Click Next.

The Create New User: Step 3 dialog box appears.
(vii) Click Finish.

The Create New User Wizard closes.

The Add User Wizard reappears displaying the Completed dialog box.

f) Click Done.

The specified user(s) appear in the Users tab.

The user(s) will appear in the alert's BCC field.

g) To send an email to a user, click on the user's email address.

h) To remove a user from the Users tab, select the user and click Remove.

The user is removed from the Users tab.

8. To preview the alert, click Preview.

The Preview tab reappears displaying the report with your changes.

9. If you are satisfied with the alert, click OK.

The dialog box closes.

10. Click Save.

Viewing and Deleting Custom Alerts

To view or delete custom alerts:

1. From the navigation tree, click System > Settings.

   The System > Settings window and shows the General page.

2. Click Custom Alerts.

3. To delete an alert:
   a) Select the alert.
   b) Click Delete.

   A confirmation message appears.

   A confirmation message appears.
c) Click OK.

The alert is deleted.

d) Click Save.

Using Service Domain Custom Alerts

Before you use Service Domain custom alerts, you must configure mail settings for the SMP Service Domains ("Custom Alerts Details Window" on page 168).

To show the Custom Alerts window for Service Domains:

1. From the navigation tree, click Service Domain > Settings.

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

2. Click Custom Alerts.

Adding and Editing Custom Alerts

To add or edit custom alerts

1. From the navigation tree, click Service Domain Settings.

   The Settings window opens and shows the General page.

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:
   - If you selected Log Only in the Action drop-down list, continue at Log Only Alerts.
   - If you selected Send Email in the Action drop-down list, continue at Send Email Alerts.

Viewing and Deleting Custom Alerts

To view or delete custom alerts

1. In the SMC menu, click Settings > General.

   The Settings > General page appears with the General node selected.

2. In the navigation tree, click the Custom Alerts node.

   The Custom Alerts fields appear.

3. To delete an alert, do the following:
   a) Select the check box next to the desired alert.
   b) Click Delete.

      A confirmation message appears.
   c) Click OK.

      The alert is deleted.
   d) Click Save.
Troubleshooting the SMP

In This Section:
- Activating the Map License ................................................................. 173
- Dynamic DNS - Gateways Cannot Push Actions to the SMP .................. 173
- Using Internet Explorer to Access Gateways ........................................ 174

Activating the Map License

The SMP Map View window includes a 30-day temporary license. It is necessary to 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, it is possible to activate the license for the Map View window.

To activate the permanent Map license:
1. From the navigation tree, click 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: smbmgmtservice@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, it is possible that Windows does 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 actually sent.

When there are multiple IP addresses on an interface, Windows 2008 Server automatically chooses 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 WebUI. When you attempt to access the gateway, the browser shows a window with this error message: Request Refused SMP WebUI.

Install the SMP certificate for the gateway (*Authentication Method* on page 58) as a self-signed certificate in Internet Explorer to configure it to access the gateway WebUI.
Regular Expressions

In This Appendix

SMP Regular Expressions ................................................................. 175
Regular Expression Syntax ............................................................. 175
Using Non-Printable Characters ....................................................... 176
Using Character Types ................................................................. 176

SMP Regular Expressions

Use regular expressions to configure the settings for roles ("Editing Roles" on page 130).

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>subpattern, 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></td>
<td>Vertical Bar</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>
Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\a</td>
<td>alarm; the BEL character (hex 07)</td>
</tr>
<tr>
<td>\cx</td>
<td>&quot;control-x&quot;, where x is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex 1B)</td>
</tr>
<tr>
<td>\f</td>
<td>formfeed (hex 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>newline (hex 0A)</td>
</tr>
<tr>
<td>\r</td>
<td>carriage return (hex 0D)</td>
</tr>
<tr>
<td>\t</td>
<td>tab (hex 09)</td>
</tr>
<tr>
<td>\ddd</td>
<td>character with octal code ddd</td>
</tr>
<tr>
<td>\xhh</td>
<td>character with hex code hh</td>
</tr>
</tbody>
</table>

Using Character Types

To specify types of characters in patterns, escape the reserved character.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>any decimal digit [0-9]</td>
</tr>
<tr>
<td>\D</td>
<td>any character that is not a decimal digit</td>
</tr>
<tr>
<td>\s</td>
<td>any whitespace character</td>
</tr>
<tr>
<td>\S</td>
<td>any character that is not whitespace</td>
</tr>
<tr>
<td>\w</td>
<td>any word character (underscore or alphanumeric character)</td>
</tr>
<tr>
<td>\W</td>
<td>any non-word character (not underscore or alphanumeric)</td>
</tr>
</tbody>
</table>
Index

A
Accessing Local Gateways • 68
Activating the Map License • 173
Active Directory Database • 140
Adding a Gateway [MAC Address] • 126
Adding a Gateway [Name] • 126
Adding a Gateway [Search] • 127
Adding a New Gateway • 127
Adding and Editing Custom Alerts • 172
Adding External Gateways to the SMP • 102
Adding Firmware to the SMP System • 138
Adding Gateways • 17
Adding Gateways to SmartDashboard (Dynamic IP Address) • 110
Adding Gateways to SmartDashboard (Static IP Address) • 103
Adding Security Management Servers • 147
Adding Service Domains • 112
Adding SMP Administrators • 134
Adding the VPN Security Gateway to the SMP • 106
Administrators Access • 59, 89
Anti-Spam • 45, 80
Application Control and URL Filtering • 42, 77
Assigning a Center Gateway • 97
Authentication Method • 58

B
Backing Up Gateway Settings to an FTP Server • 13

C
Configuring a VPN Community with External Gateways • 101
Configuring Advanced Role Settings • 132
Configuring Advanced Settings • 145
Configuring Advanced Settings for Service Domains • 117
Configuring Communities’ Custom Fields • 99
Configuring Communities’ Members Lists • 99
Configuring Community Notifications • 164
Configuring Custom Fields for Service Domains • 116
Configuring Device Settings • 37, 71
Configuring DNS Settings for Service Domains • 116
Configuring DNS Settings for the SMP Server • 16
Configuring Dynamic DNS for Gateways • 20
Configuring Firmware Notifications • 164
Configuring Gateway Notifications • 163
Configuring Gateway Owners • 34
Configuring General Settings • 32
Configuring General Settings [Plan] • 70
Configuring General Settings for Service Domains • 114
Configuring General Settings for the SMP • 23
Configuring General SMP Settings • 21
Configuring IKE Settings • 98
Configuring Logging for Service Domains • 115
Configuring Management Access Control • 29
Configuring Network Topology for Gateways • 58
Configuring Outgoing Mail Settings for Service Domains • 14
Configuring Outgoing Mail Settings for the SMP • 25
Configuring Portal Administrator Notifications • 162
Configuring Roles for Users • 128
Configuring Rules for Roles • 130
Configuring Security Software Blades • 41, 76
Configuring Service Domain Notifications • 163
Configuring Service Domain Statistics Reports • 162
Configuring Services • 53, 84
Configuring Settings for the SMP Server • 23
Configuring Setup Settings • 59, 88
Configuring SMP Administrator Account Expiration • 136
Configuring SMP Administrators • 134
Configuring SMP Administrators’ Contact Details • 136
Configuring SMP Backup Settings • 27
Configuring SMP Logging • 24
Configuring SMP Notifications • 29
Configuring SMP System Notifications • 161
Configuring Summary Messages • 165
Configuring Summary Reports (Service Domains) • 165
Configuring System Administrator Notifications • 161
Configuring the Community General Settings • 95
Configuring the IP Address for an SMS Module • 144
Configuring the Log Policy • 149
Configuring the Settings for a SMP Server • 142
Configuring the Settings for an SMP Service Domain • 114
Configuring the SMP Internal Certificate Authority • 28
Configuring the SMP WebUI to Use a Web Proxy Server • 24
Configuring the SMS Module • 143
Configuring the VPN Community (SmartDashboard) • 104
Configuring User Notifications • 163
Configuring Virus/Spam Notifications • 165
Configuring VPN Settings • 88, 97
Configuring VPN Settings [Gateway] • 57
Connecting to Gateways • 68
Connecting to Gateways behind NAT • 69
Contact Settings [User] • 123
Creating a New Plan • 12
Creating and Configuring the VPN Community
   (SMP) • 107
Creating Community Topologies • 100
Creating New Roles • 129
Creating New Users • 14
Creating VPN Communities • 15, 95
Custom Alerts Details Window • 168
Custom Fields Settings [User] • 123
Customizing Notifications • 165

D
Deleting an SMP Server • 148
Deleting Communities • 96
Deleting Firmware from the SMP System • 138
Deleting Gateways • 67
Deleting Logging Policy Rules • 150
Deleting Plans • 91
Deleting Role Rules • 132
Deleting Roles • 130
Deleting Service Domains • 114
Deleting SMP Administrators • 136
Deleting Users • 125
Diagram of VPN Community Types • 93
DNS • 39, 73
Dynamic DNS • 57
Dynamic DNS - Gateways Cannot Push Actions
to the SMP • 173

E
Editing Custom Fields [Gateways] • 62
Editing Plans • 70
Editing Roles • 130
Editing SMP Administrators • 135
Editing the General Page • 113
Editing Users • 122
Emailing a User Summary • 121
Expiration Settings [User] • 123
Exporting Data with the SMP WebUI • 152
Exporting Gateway Information • 66
Exporting SMP Data • 152
Exporting SMP Data from the Command Line • 153
Exporting the Security Management Server CA
   • 106
Exporting the SMP CA • 109
Exporting Users • 125

F
Filtering Logs • 159
Filtering the Communities Table • 96
Filtering the Plans Table • 90
Firewall • 41, 76
Firmware for Gateways and Plans • 54, 85

G
Gateway Administrators • 40, 74
Gateway behind NAT • 60, 89
Gateway Maintenance • 18
General Settings [Custom Image] • 118
General Settings [User] • 122

H
History [Custom Images] • 119

I
Implementing SMP • 12
Important Information • 3
Importing and Exporting SMP Objects • 152
Importing and Exporting the CA • 102
Importing Data with the SMP WebUI • 155
Importing SMP Data • 155
Importing SMP Data from the Command Line • 156
Importing the CA to SmartDashboard and
   Updating the Policy • 109
Importing the Security Management Server CA
   • 107
Introduction to SMP • 9
IPS • 43, 78

L
Locking and Unlocking Settings • 62
Locking Gateways to a Plan • 63
Log Only Alerts • 169
Logging in to the SMP • 9

M
Managed Services • 53, 85
Managing Firmware • 139
Managing Firmwares for Gateways • 138
Managing Gateways • 31
Managing Gateways behind NAT • 18
Managing Gateways for a User • 125
Managing Gateways with Plans • 10
Managing Licenses without the WebUI • 150
Managing Service Domain Users • 120
Managing Service Domains • 112
Managing SMP Servers • 140
Managing the Gateway Settings from the SMP • 10
Managing VPN Communities • 92
Managing VPN Community with an External
   Gateway • 101
Monitoring the SMP • 157
Moving SMP Object and Settings Data • 152

N
NTP • 37, 72
Overview of Roles • 128
Overview of the SMP • 9

Periodic Backup • 55, 86
Preparing to Add an External Gateways • 101

QoS • 46, 81

Regular Expression Syntax • 175
Regular Expressions • 175
Remote Access • 47, 82
Report Recipients • 56
Reports • 55, 87
Resetting Predefined Roles to Default Settings • 133

Sample Configuration with SmartDashboard • 103
Sample SMP Architecture Workflow • 141
Searching for Gateways • 63
Searching for Users • 120
Send Email Alerts • 169
Sending Email to Gateway Owners • 67
Sending Emails to Users • 124
Sending Security Reports • 19
Setting Filters • 159
Setting the Gateway Location • 33
Showing a Summary of a Community • 100
Showing Active User Sessions for Service Domains • 22
Showing Activity Logs • 159
Showing Administrators • 134
Showing and Editing External CAs for Service Domains • 114
Showing and Editing Gateways • 31
Showing and Editing SMP Servers • 141
Showing Communities • 95
Showing Firmware for Service Domains • 117, 139
Showing Firmware Histories • 139
Showing Firmwares • 138
Showing Gateway Logs • 36, 157
Showing Gateway Status • 35
Showing Logs • 157
Showing Logs [Users] • 124
Showing Plan Histories • 90
Showing Roles • 129
Showing Security Management Server Diagnostics • 147
Showing Security Management Server Status • 145
Showing Service Domain Histories • 114
Showing Service Domains • 113
Showing SMP Administrator Statuses • 137
Showing System Logs • 158
Showing the Gateway Map View • 22
Showing the General Page • 141
Showing the General Page for the Security Management Server • 148
Showing the Managed Modules • 143
Showing the Security Management Server Settings • 148
Showing the SMP License • 26
Showing the SMP Server History • 150
Showing the SMP Status • 21
Showing Users • 120
Site to Site VPN • 48, 83
SMP Regular Expressions • 175
SMP Scenarios and Workflows • 15
SMP Server • 140
SMP WebUI • 140
Starting the SMP Backup • 28
Status Settings [User] • 123

Threat Prevention Anti-Bot • 50
Threat Prevention Anti-Virus • 49
Threat Prevention Policy • 51
Time Zone • 38, 72
Traditional Anti-Virus • 44, 79
Troubleshooting the SMP • 173

Understanding Nested Communities • 94
Understanding the SMP Server • 11
Understanding the SMP Server Architecture • 140
Unlocking Gateways from a Plan • 62
Upgrading a Gateway Remotely • 18
Uploading Images for Email Templates • 117
User Awareness • 49, 84
Using Character Types • 176
Using CLI Scripts • 61, 70
Using Custom Alerts • 168
Using Internet Explorer to Access Gateways • 174
Using Non-Printable Characters • 176
Using Plans for Gateways • 70
Using Predefined Roles • 128
Using Reports, Notifications, and Custom Alerts • 161
Using Service Domain Custom Alerts • 172
Using SMP Notifications • 161
Using SMP System Custom Alerts • 168
Using Software Blades • 13
Using Software Blades and Services • 10
Using String Operators for Roles • 131
Using the SMP WebUI • 21
V

Viewing and Deleting Custom Alerts • 171, 172
Viewing Community Histories • 100
VPN Community Settings • 57, 88
VPN Community Types • 92
VPN Settings • 97