QUANTUM

16 July 2025

SMARTPROVISIONING

R81.10

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

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

Certifications

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

Check Point R81.10

For more about this release, see the R81.10 home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

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

Revision History

Date	Description
7 April 2025	Updated: ■ *"Configuring Provisioning Profiles for Security Gateways" on page 49* ■ *"Security Profiles for Check Point Appliance Security Gateways" on page 33*
23 October 2023	Updated *"VPN with One or More LSM Profiles" on page 118*
07 August 2023	Updated *"Activating SmartProvisioning on CO Gateways" on page 114*
30 June 2023	Added *"Getting Started with SmartProvisioning" on page 13*
25 June 2023	Updated *"Creating a VPN Community for SmartLSM Security Gateways" on page 116*
13 February 2023	Updated *"SmartProvisioning Objects" on page 11*x.
14 June 2022	In the HTML version, added glossary terms in the text
21 November 2021	Updated *"Configuring Internet Connection Types" on page 80*
07 November 2021	Updated: ■ *"Creating a VPN Community for SmartLSM Security Gateways" on page 116* - added a note that in Star community, the "Center Gateways" section does not support Quantum Spark appliances
05 July 2021	First release of this document

Table of Contents

Introduction to SmartProvisioning

SmartProvisioning lets you manage multiple gateways from one Security Management Server or Multi-Domain Security Management. SmartProvisioning defines, manages, and provisions (remotely configures) large-scale deployments of Check Point Security Gateways:

- SmartProvisioning helps you manage the load on the Security Gateways. The policy is not installed on all Security Gateways simultaneously, but the gateways fetch the policy at different time intervals.
- The SmartProvisioning management concept is based on profiles, which help you manage your gateways more efficiently. With these profiles, you can define the gateway settings once and then assign each profile to multiple gateways, as needed. For example, when you select which blades to enable in the LSM Profile, the selected blades are enabled on all gateways which are assigned to the Profile.
- SmartProvisioning supports two types of profiles: Security Profiles, which define the security settings, and Provisioning Profiles, which define the device settings. SmartProvisioning is efficient for use in large enterprises with many branch offices, where the branch offices have identical or similar characteristics. You can use a relatively small number of Security Profiles or Provisioning Profiles to manage a much larger number of gateways.

Note - SmartProvisioning is not available for members of SmartLSM cluster.

A list of Supported Features

- Central management of security policies, gateway provisioning, remote gateway boot, and Dynamic Object value configurations
- Automatic Profile Fetch for large deployment management and provisioning
- All Firewall features supported by DAIP gateways, including DAIP and static IP address gateways
- Easy creation and maintenance of VPN tunnels between SmartLSM Security Gateways and CO gateways, including generation of IKE certificates for VPN, from third-party CA Servers or Check Point CA
- Automatic calculation of anti-spoofing information for SmartLSM Security Gateways
- Log tracking for gateways based on unique, static IDs; with local logging for reduced logging load
- High level and in-depth status monitoring
- Complete management of licenses and packages, Client Authentication, Session Authentication and User Authentication

- Command Line Interface to manage SmartLSM Security Gateways
- Support of Check Point 1100, 1200R, 1400 and 1500 Appliances

SmartProvisioning Objects

SmartProvisioning manages SmartLSM Security Gateways and enables provisioning management for Check Point Security Gateways.

Gateways

SmartProvisioning manages and provisions different types of gateways.

- **SmartLSM Security Gateways**: Remote gateways which provide firewall security to local networks, and the Security Policies are managed from a central Security Management Server or Domain Management Server. When remote gateways are defined through SmartLSM Security Profiles, a single system administrator or a smaller team can manage the security of all your networks. You can assign a Provisioning Profile to SmartLSM Security Gateways to manage device settings.
- **CO Gateways**: Standard Security Gateways that act as central Corporate Office headquarters for the SmartLSM Security Gateways. The CO gateway is the hub of a Star VPN, and the satellites are SmartLSM Security Gateways. The SmartLSM Security Gateways are represented in the VPN Community object by the applicable Security Profile object. The CO gateway has a static IP address, which ensures continued communications with SmartLSM Security Gateways that have dynamic IP addresses.
- **Provisioned Gateways**: Non-SmartLSM gateways with an assigned provisioning profile. A provisioning profile defines the device settings, such as interfaces, routing and DNS.

  Note - You cannot use SmartProvisioning with externally managed gateways.

  Important - SmartProvisioning does not support VSX Gateways and VSX Clusters.

Profiles

SmartProvisioning uses different types of profiles to manage and provision the gateways:

- **SmartLSM Security Profiles**

  Defines a Check Point Security Policy and other security-based settings for a type of SmartLSM Security Gateway. A SmartLSM Security Profile can hold the configuration for multiple SmartLSM Security Gateways. All SmartLSM Security Gateways must have a SmartLSM Security Profile. You configure and manage SmartLSM Security Profiles in SmartConsole.

- **Provisioning Profiles**:

  Defines the device settings. Among others, it sets the interfaces, routing and DNS settings. CO gateways, SmartLSM Security Gateways, and non-SmartLSM gateways can have Provisioning Profiles, if they are Check Point supported Security Gateways. You configure and manage the Provisioning Profiles in SmartProvisioning. Configuration options and features for Provisioning Profiles differ according to the device type.

Profile Fetching

All gateways managed by SmartProvisioning fetch their assigned profiles from the Security Management Server or Domain Management Server. Define the SmartLSM Security Profiles and Security Policies in SmartConsole. Define Provisioning Profiles in SmartProvisioning when you prepare the gateway settings on the SmartProvisioning database. The profile definition procedures do not push the profile to any specific gateway.

Managed gateways fetch their profiles periodically. Each gateway randomly selects a time slot within the fetch interval.

When a fetched profile differs from the previous profile, the gateway is updated with the changes. Updated Security Management Server or Domain Management Server Security Policies are automatically installed on SmartLSM Security Gateways, and gateways with Provisioning Profiles are updated with management changes.

In addition to the profile settings, the properties of the gateway are used to localize the profile changes for each gateway. One profile can update potentially thousands of gateways, each with the new common properties, while it maintains its own local settings.

VPNs and SmartLSM Security Gateways

Your SmartLSM Security Gateways in a virtual private network (VPN) secures communications within your organization.

SmartProvisioning supports the inclusion of SmartLSM Security Profiles as members in Star VPN Communities (as satellites). When a Star VPN Community contains a SmartLSM Security Profile as a satellite, the settings of the community apply both to the Corporate Office (CO) gateway and to the SmartLSM Security Gateways.

You can establish a VPN tunnel from a SmartLSM Security Gateway to a static IP address CO gateway (similar to the way that DAIP gateways establish VPN tunnels to static IP gateways). A CO gateway recognizes and authenticates an incoming VPN tunnel as a tunnel from a SmartLSM Security Gateway, with the IKE Certificate of the SmartLSM Security Gateway. The CO gateway treats the peer SmartLSM Security Gateway as if it were a DAIP gateway, whose properties are defined by the SmartLSM Security Profile to which the gateway is assigned. A CO gateway can also initiate a VPN tunnel to a SmartLSM Security Gateway.

You can establish a VPN tunnel for SmartLSM-to-SmartLSM, or SmartLSM-to-other gateway configurations, through the CO gateway.

Getting Started with SmartProvisioning

1. In SmartConsole, configure the SmartProvisioning permission in the applicable Permission Profiles, so the applicable administrators could work with SmartProvisioning.

   See *"Configuring Administrators in SmartProvisioning" on page 15*

2. Enable SmartProvisioning on the Security Management Server.

   See *"Activating SmartProvisioning on the Security Management Server" on page 17*.

3. Enable SmartProvisioning on all Security Gateways, which you wish to manage with SmartProvisioning.

   See *"Activating SmartProvisioning on a Security Gateway" on page 18*.

4. Connect with SmartConsole to you Management Server.

5. In SmartConsole, create the required **SmartLSM Security Profiles** for your Security Gateways.

   See *"Creating SmartLSM Security Profiles" on page 33*.

   This way you can enable or disable a Software Blade on all Security Gateways that use this profile with one change and one policy installation.

6. In the SmartConsole top left corner, click **Menu** > click **SmartProvisioning**.

7. If you wish to manage configuration of Security Gateways with a profile, in SmartProvisioning, create the required **SmartLSM Provisioning Profiles** for your Security Gateways.

   This way you can configure some operating system settings on all Security Gateways that use this profile with one change and one policy push.

   - For regular Security Gateways, you can configure DNS, Hosts, and Domain Name.

     See *"Configuring Provisioning Profiles for Security Gateways" on page 49*.

   - For Quantum Spark Appliances, you can configure DNS, Hosts, Domain Name, Firmware, RADIUS, Hotspot, and a Configuration Script.

     See the *"Configuring Provisioning Profiles for Small Office Appliances Gateways" on page 56*.

8. Create the required device objects for your Security Gateways.

- For regular Security Gateways, see *"Creating Check Point Security Gateways in SmartProvisioning" on page 36*.
- For Quantum Spark Appliances, see *"Creating a Small Office Appliance Gateway in SmartProvisioning" on page 41*.

  Optional: Use the *"SmartProvisioning Wizard" on page 63*.

Note - You can always assign or remove a SmartLSM Provisioning Profile in the Security Gateway object properties.

9. Open each Security Gateway object and make sure the settings are correct for your environment.

   See:

   - *"Provisioning Settings for Security Gateways Configured in SmartConsole" on page 65*.
   - *"Provisioning Settings for Security Gateways Configured in SmartProvisioning" on page 70*.
   - *"Small Office Appliance Settings" on page 76*.

10. **Optional:** If your Security Gateway must participate in a Site to Site VPN, see *"VPNs and SmartLSM Security Gateways" on page 114*.
11. In SmartProvisioning, push the settings to the applicable profiles and devices:

    - From the left panel, click **Profiles** > select a profile > from the top **Actions** menu, select **Push Settings and Actions**.
    - From the left panel, click **Devices** > right-click a device object > click **Actions** > click **Push Settings and Actions** > right-click a device object > click **Actions** > click **Push Policy**.

Configuring Administrators in SmartProvisioning

From the SmartConsole Menu, select **SmartProvisioning** to define SmartProvisioning Administrators and set Administrator Collaborations.

Defining SmartProvisioning Administrators

Login administrator permissions to the SmartProvisioning Console are defined in SmartConsole or in the Check Point Configuration Tool. In SmartConsole, you can further define specific administrator permissions, such as provisioning devices with SmartProvisioning.

1. Open SmartConsole.
2. Go to **Manage & Settings > Permissions & Administrators > Administrators**.
3. Click **New** or **Edit** an existing administrator.

   The Administrator properties window opens.
4. Go to **Permissions** > **Permission Profile**, and from the drop-down list, select **New**.

   The **New Profile** window opens.
5. In **Overview** > **Permissions**, select **Customized**.
6. In **Gateways**, make sure that **SmartLSM Gateways Database** has **Write** permissions, and set other permissions.

   Other Permissions

Option	Write	Read	Cleared
SmartLSM Gateway Database	Add, edit, delete, assign provisioning profiles to gateways	Assign provisioning profiles to gateways	Provisioning features are unavailable
System Backup, System Restore and **Open Shell**	Edit all gateway network settings	View gateway network settings	Gateway network settings are unavailable

7. Click **OK**.

   The changes in permissions are applied the next time the administrator logs in.

Administrator Collaboration

Multiple administrators can work on the SmartProvisioning GUI client on the same Security Management Server at the same time. To avoid configuration conflicts, every administrator has their own username, and works in a session that is independent of the other administrators.

When an administrator logs in to the SmartProvisioning GUI client, a new editing session starts. The changes made during the session are only available to that administrator. If another administrator tries to change the edited objects, this error message shows: **Failed to update <*object_name*>. Could not access file for write operation**.

To make your changes available to other administrators and for the SmartLSM and SmartProvisioning appliances, you must publish the SmartConsole session. When you publish a SmartConsole session, a new database version is created.

To be able to perform certain actions on the managed appliances, such as **Push Policy** or **Push Settings and Actions**, you are prompted to publish all unpublished changes in the current session. When the administrator performs these actions, unpublished changes from other sessions are not included.

Publishing a session

In the **SmartProvisioning** toolbar, click **Publish**. A window opens which includes the publish date and name of administrator.

Best Practice - In this window, we recommend that you add a brief description of the changes that you made in the session. This is useful for auditing and troubleshooting purposes.

Note - When there are unpublished changes in the session, the **Publish** button is colored in yellow.

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

For more information on the R80 session architecture, see the *Check Point R80.10 Security Management Architecture Overview*.

Enabling SmartProvisioning

This section describes how to activate SmartProvisioning on a Security Management Server, on a Security Gateway, and on a Corporate Office (CO) gateway.

Activating SmartProvisioning on the Security Management Server

Before you can use SmartProvisioning, you must enable it on the Security Management Server.

Procedure

1. Obtain a SmartProvisioning license. This license is required to activate SmartProvisioning functionality.
2. Add the license to the Security Management Server or Domain Management Server, with `cpconfig` or SmartUpdate.

   You can also use the `cplic` command to add the license.

For Multi-Domain Server, perform these steps also:

1. Enable the Provisioning Blade on the Multi-Domain Server object:
   a. Connect with SmartConsole to the Security Management Server or the applicable Domain Management Server.
   b. In the **Gateways & Servers** view, double-click the Multi-Domain Server object.
   c. In the **General Properties** page, go to the **Management** tab, and select **Provisioning**.
   d. Click **OK**.
2. Enable SmartProvisioning on the Multi-Domain Server CLI:
   a. Log in to the Expert mode
   b. Go to the context of the applicable Domain Management Server. Run `mdsenv <Domain IP address or name>`.
   c. Run `LSMenabler on`

   This message is displayed: `Check Point services should be restarted. Restart now (y/n) [y] ?`

   Enter **y** to restart the Check Point services.

Activating SmartProvisioning on a Security Gateway

To manage a gateway with SmartProvisioning, you must first activate SmartProvisioning on the gateway.

Procedure

1. From the CLI, run these commands in Expert mode:

   ```
   LSMenabler -r on
   ```

   ```
   cpstop
   ```

   ```
   cpstart
   ```

2. Run `cpconfig`
3. Go to the **ROBO Interfaces** page and define an **External** interface.

Note - Small Office Appliance gateways do not require activation of provisioning. This section is relevant for all other gateway types..

SmartProvisioning User Interface

This section describes the SmartProvisioning User Interface and how to work with it.

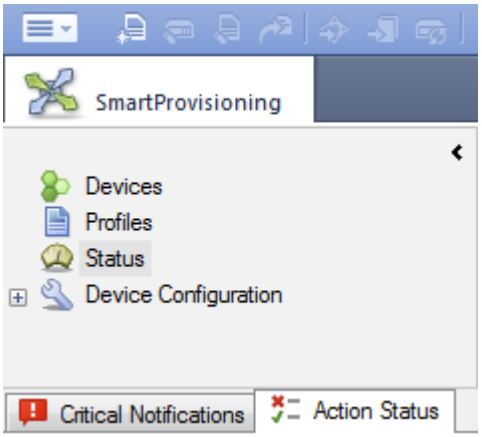
Main Window Panes

The main SmartProvisioning window has a tree pane with separate nodes, each with its own purpose:

- **Devices** workspace - Use this workspace to manage gateways and other device objects, such as clusters.
- **Profiles** workspace - Use this workspace to manage Provisioning Profiles. Click **Profiles** in the tree.
- **Status** - Shows dynamic status of devices. Click **Status** in the tree (see *"Status View" below*).
- **Device Configuration** - Displays information about the gateway configuration in the assigned Provisioning Profiles.

Status View

The information in the Status View pane depends on whether you select **Action Status** or **Critical Notifications**.



Action Status

You can see the Action Status for each action you do on a device:

- **Name**: The name of the action.
- **Action type**: The type of action. See *"SmartProvisioning Menus and Toolbar" on page 21*r .
- **Start Time**: The time the action began on the selected gateway.

- **Status**: The current status of the action, dynamically updated.
- **Details**: Relevant notes.
- **Results:** Click the Result link to open the **Run Script** window and see the results of this script.

Critical Notifications

For each device that has a critical status or error, you can view the gateway status, its Security Policy (if the device is a SmartLSM Security Gateway), and its Provisioning Profile (if it is assigned to a Provisioning Profile).

Gateway Status Indicators

Indicator	Description
OK	Gateway is up and performing correctly
Waiting	SmartProvisioning is waiting for status from the Security Management Server or Domain Management Server
Unknown	Status of gateway is unknown
Not Responding	Gateway has not communicated with Security Management Server or Domain Management Server
Needs Attention	Gateway has an issue and needs to be examined
Untrusted	SIC Trust is not established between gateway and Security Management Server or Domain Management Server

Policy Status Indicators

Indicator	Description
OK	Gateway is up and performing correctly
Waiting	SmartProvisioning is waiting for status from Security Management Server or Domain Management Server
Unknown	Status of gateway is unknown
Not installed	Security Policy is not installed on this gateway

Indicator	Description
Not updated	Installed Security Policy has been changed; gateway should fetch new policy from Security Management Server or Domain Management Server
May be out of date	Security Policy was not retrieved within the fetch interval

Provisioning Profile Indicators

Indicator	Description
OK	SmartProvisioning Agent is installed and operating
Needs Attention	Device has an issue and needs to be examined
Agent is in local mode	Device is in maintenance mode (see *"Maintenance Mode for SmartLSM Security Gateways" on page 112*)
Uninitialized	Device has not yet received any provisioning configurations
Unknown	Status of provisioning is unknown

SmartProvisioning Menus and Toolbar

This section is a reference for the menus and toolbar buttons in SmartProvisioning. The available menu commands depend on the list that is displayed in the work space.

To access menu options, click the **Launch Menu** button on the toolbar and then access the specified menu.

For example, the **File** > **New** command enables you to create new SmartLSM Security Gateways when the **Devices** work space is displayed. When the **Profiles** work space is displayed, **File** > **New** enables you to create a new Provisioning Profile.

The table below lists the menus and explains their commands. Some of the commands have toolbar buttons that you can use to access the same functionality.

Menus and Their Commands

Menu	Command	Description	For further information
File	New	Define new SmartLSM Security Gateway/Cluster or Provisioning Profile	See: ■ *"Creating Check Point Security Gateways in SmartProvisioning" on page 36* ■ *"Security Profiles for Small Office Appliance Gateways" on page 41* ■ *"Configuring SmartLSM Cluster Objects in SmartProvisioning" on page 128* ■ *Creating Provisioning Profiles*
	Export to file	Export objects list to file	See *"Export to File" on page 26*
	Exit	Close SmartProvisioning	
Edit	Edit gateway	Edit selected gateway	See *"Common Gateway Management" on page 93*
	Delete SmartLSM Gateway	Delete selected gateway; only for devices with SmartLSM Security Profiles	See *"Deleting Security Gateway Objects" on page 94*
	Profile Details	Edit selected Provisioning Profile	See *"Configuring Provisioning Profiles" on page 49*
	Find	Find specific object in visible list	See *"Find" on page 24*
View	Toolbar	Show/Hide Toolbar	
	Status bar	Show/Hide Status View pane	See *"Main Window Panes" on page 19*

Menu	Command	Description	For further information
	Status View	Show/Hide Status View pane	See *"Status View" on page 19*
	Menu Bar	Show/Hide Menu Bar above Toolbar	
	Clear All Filters	Clears all the configured filters	See *"Filtering Columns in Devices and Devices Configuration." on page 26*
	Show/Hide columns	Open the Show/Hide Columns window and select the data to be displayed in the work space	See *"Show/Hide Columns" on page 25*
Manage	Custom Commands	Add/Edit user-defined executables to run on remote gateways	See *"Executing Commands" on page 96*
	Select SSH Application	Provide pathname to SSH application for remote management of devices	See *"SSH Applications" on page 27*
Actions	Push Settings and Actions	Immediate execute of Backup and fetch of profile settings	See *"Applying Changes" on page 112*
	Get Actual Settings	Fetch configuration settings from device to management server	See *"Configuring Interfaces" on page 95*
	Push Policy	Push values resolved in SmartProvisioning to SmartLSM Security Gateway	See *"Immediate SmartLSM Security Gateway Actions" on page 98*
	Push Dynamic Objects	Push values resolved in SmartProvisioning to SmartLSM Security Gateway	See *"Dynamic Objects" on page 133*

Menu	Command	Description	For further information
	Stop Gateway	Stop Check Point services on selected gateway	See *"Controlling Remote Gateways" on page 93*
	Start Gateway	Start Check Point services on selected gateway	
	Restart Gateway	Restart Check Point services on selected gateway	
	Reboot Gateway	Reboot the device	
	Get Status Details	Open Gateway Status Details	See *"Viewing Status of Remote Security Gateways" on page 110*
	Packages	Software management	See *"Managing Software on SmartLSM Security Gateways" on page 106*
	Updated Selected Corporate Office Gateway	Update selected CO (available *when CO gateway is selected*)	
	Backup	Create a backup image	See *"Immediate Backup of Security Gateways" on page 111*
Window	Access SmartEvent		
Help	View version information and open online help		

Working with SmartProvisioning Menus and Options

This section describes SmartProvisioning customizations and general functions.

Find

Opening the **Find** window:

1. Go to the Launch Menu, and select **Edit** > **Find**.
2. **In the Look in field, select a column header to search for the string in a specific data type**
   - **All Fields**
   - **Name**
   - **IP/ID**: Format of IP address; tracking ID for logs
   - **Product**: Check Point product, platform, or operating system
   - **Version**
   - **Provisioning Profile**
   - **Last Applied Settings**
   - **Security Profile**
   - **Gateway Status**: Use a valid status string (see *"Status View" on page 19*).
   - **Policy Status**: Use a valid status string (see *"Status View" on page 19*).
   - **Provisioning Status**: Use a valid status string (see *"Status View" on page 19*).

Show/Hide Columns

Customizing the **Devices** list columns

1. Go to the Launch Menu and select **View** > **Show/Hide Columns**.
2. In the **Show/Hide Columns** window, select the columns to display.
3. Clear the columns that you do not want to display.
4. Click **OK**.
5. To hide a column, right-click the column header and select **Hide Column**.

Filter

Filtering the Devices workspace list

1. Select the **Devices** workspace.
2. In **Look for**, enter the filter text.
3. From the **In** drop-down list, select the filter category that you want.

You can select one of the filter categories

- **All**: The filter number or text is applied to all the filter categories. (Default)
- **Name**: name of the gateway and icon which indicates its type (Security Management Server, Domain Management Server, SmartLSM Security Gateway, Check Point host, Mobile Access).
- **IP/ID**: unique ID in the form of an IP address, used to track logs generated from a Gateway, even if it changed its external IP address.
- **Product**: Name of the Check Point platform used for the Security Gateway.
- **Version**: Check Point software version for the Security Gateway.
- **Provisioning Profile**: Name of the Provisioning Profile.
  This field is blank if the Security Gateway is not enabled for provisioning.
- **Last Applied Settings**: Date and time that the Security Gateway definition was last changed.
- **Security Profile**: Name of the last installed Security Profile.
- **Gateway Status**: Current status of the Security Gateway.
- **Policy Status**: Current status of the Security Policy.
- **Provisioning Status**: Current status of the provisioning settings.

Filtering Columns in Devices and Devices Configuration.

1. In the tree, select **Devices** or the **Device Configuration** display.
2. Right-click the column heading and select **Filter** > **Add/Edit Filter**.

   The **Advanced Filter** window opens.
3. Configure the filter settings for that column.
4. Click **OK**.
5. To clear the filter settings, right-click the column heading and select **Filter** > **Clear Filter**.

Export to File

If you prefer to track your managed devices in other programs, you can export the SmartProvisioning objects list.

Exporting SmartProvisioning data to a file

1. From the Launch Menu, select **File** > **Export to File**.
2. Click **Export To**.

The **Export to File** window opens.

3. Provide a name for the file and select a type: MS Excel, Web, CSV, Text, or All (to create your own extension).
4. Click **Save**.
5. Select the file options that you want:
   - **Show Headers**: Select to include the column headers.
   - **Use the following Delimiter**: Select **Tab** as a delimiter between data, or select **Other** and specify the delimiter you want. (This is disabled for MS Excel and Web page file types.)
6. Click **OK**.

   The file is created. A dialog box opens, with the message

   File '<pathname>' created successfully
7. Click **Open File** to view the exported file in a relevant application.

SSH Applications

SSH applications let you connect to devices remotely.

Selecting a Default SSH Application For the First Time

If you did not yet open an SSH application, you can provide the path from within SmartProvisioning. The first time you select an SSH application, select a default application from the **Launch Menu** > **Manage** > **Select SSH Application**. Each subsequent time that you want to open an SSH terminal, you can right-click the required device and select **Launch SSH Terminal**.

Select an SSH application for the first time

1. Select **Manage** > **Select SSH Application**.
2. **Select your SSH Client**.
3. In the **SSH Client Connection Attributes** section, select a predefined application template, such as **PuTTY** or **SecureCRT**, or select **Custom** to create your own. Make sure that the **Connection Attributes** match the syntax required for your selected SSH terminal application, where <IP> refers to the device's IP address.
4. When the required syntax for the specific application appears in the **Connection Attributes** field. Click **OK**.

Launching an SSH Application from Devices

After you selected a default SSH application for the first time, you can launch it from any supported device.

Launch the default SSH application from a device

1. Right-click a device.
2. Select **Launch SSH Terminal**.

   The SSH terminal opens and automatically calls the object's IP address from its last known IP address.

Web Management

You can use the Web management portal to manage Security Gateways. This is especially useful with remote gateways that need individual changes, or system administration management.

Using the Portal to manage a Security Gateway

1. Right-click a Security Gateway and select **Launch Device Management Portal**.

   A web browser opens to:

   `https://<IP_address>` - for Gaia devices.

   `https://<IP_address>:4434` - for Small Office Appliance devices.
2. Log in with the administrator user name and password.

   The features available from the Portal enable you to manage networking, routing, servers, and many other local device configurations.

SmartLSM Security Profiles

A SmartLSM Security Gateway has a SmartLSM Security Profile (created in SmartConsole), which fetches a Check Point Security Policy from the Security Management Server or Domain Management Server. This Security Policy determines the settings of the firewall.

Before you can add a SmartLSM Security Gateway to SmartProvisioning, you must:

1. Configure a Security Policy in SmartConsole.
2. Have at least one SmartLSM Security Profile with an installed Security Policy.

This section describes how to create a Security Policy for a SmartLSM Security Gateway managed by SmartProvisioning.

Best Practice - We recommend that you define a separate Security Policy for every SmartLSM Security Profile. In the **Installation Targets** section of the Security Policy, add only the SmartLSM Security Profile object.

For more information about how to create Security Policies, see the *R81.10 Security Management Administration Guide*.

Guidelines for Basic SmartLSM Security Policies

You can use this procedure as a guideline for the creation of a Security Policy for a SmartLSM Security Profile. The Security Policy rules depend on the needs of your environment and the requirements of the SmartLSM Security Gateways that reference the SmartLSM Security Profile.

Note - This procedure uses Dynamic Objects. For more details, see *"Dynamic Objects" on page 133*.

To define a Security Policy for a SmartLSM Security Profile object:

1. Use the **LocalMachine** dynamic object to represent any SmartLSM Security Gateway.
2. Use the **InternalNet**, **DMZnet**, and **AuxiliaryNet** dynamic objects to represent the respective networks, behind any SmartLSM Security Gateway.
3. Add rules based on the needs of your organization and the requirements for the SmartLSM Security Gateways, with Dynamic Objects whenever possible.

   Dynamic Objects make the SmartLSM Security Profile applicable to numerous gateways.

4. To allow **Push** actions from SmartProvisioning, add a rule that allows an incoming **FW1_CPRID** service from the Security Management Server or Domain Management Server to **LocalMachine**.
5. Install the Policy on the SmartLSM Security Profile object.

   This action prepares the Security Policy on the Security Management Server or Domain Management Server to be fetched by the SmartLSM Security Gateways that reference this SmartLSM Security Profile.

Creating Security Policies for the Security Management Server and SmartLSM Security Gateways

You must define explicit rules to allow management traffic between SmartLSM Security Gateways and the Security Management Server or Domain Management Server. These rules are part of the Security Policy installed on the gateway that protects the Security Management Server or Domain Management Server.

Because SmartLSM Security Gateways can have Dynamic IP addresses, you must use "ANY" to represent all possible SmartLSM Security Gateways addresses.

Note - For each rule listed in the table below, the **Action** is **Accept**.

When the **Source** or **Destination** is **Server**, use your Security Management Server or Domain Management Server.

Rules for Traffic between SmartProvisioning Gateway and Management Server

Source	Destination	Service	Type of Allowed Traffic
Any	Server	FW1	Firewall control
Server	Any	FW1	Firewall control
Any	Server	CPD	CPD control
Server	Any	CPD	CPD control
Any	Server	FW1_ica_pull	Pulling certificates
Server	Any	FW1_ica_push	Pushing certificates

Source	Destination	Service	Type of Allowed Traffic
Server	Any	FW1_ CPRID	Check Point Remote Installation Protocol, for Push actions
Any	Server	FW1_ CPRID	Check Point Remote Installation Protocol. For firmware updates, from the Gateway to the Security Management Server
Any	Server	FW1_log	Logs
Server	Any	CPD_ amon	Status monitoring
Any	Server	FW1_ica_ services	IPsec VPN

Creating Security Policies for VPNs

To create a VPN tunnel from a SmartLSM Security Gateway to a CO gateway, create a Security Policy for this encrypted traffic. As in the basic Security Policy (see *"Guidelines for Basic SmartLSM Security Policies" on page 29*), use Dynamic Objects. This localizes the policy for each SmartLSM Security Gateway that references the SmartLSM Security Profile.

To create a VPN Security Policy for a SmartLSM Security Profile:

1. Define a Star VPN Community.

   Configure all the relevant authentication and encryption properties for it. To learn more, see the *R81.10 Site to Site VPN Administration Guide*.

2. Add the CO gateway as a **Central Gateway**.

   Make sure the CO gateway is configured with a static IP address.

3. Add the SmartLSM Security Profile that represents the SmartLSM Security Gateways as a **Satellite Gateway**.

4. Add rules that allow relevant VPN traffic.

Example

Telnet Through VPN Traffic Rule. This rule allows encrypted telnet traffic that matches the community criteria.

Source	Destination	Service	VPN	Action	Install On	Any
Any	Any	Telnet	Community	Accept	Any	Any

1. Add a rule to allow **Push** actions from SmartProvisioning: allow **FW1_CPRID** service from the Security Management Server or the Domain Management Server to **LocalMachine**.
2. Install the Security Policy on the SmartLSM Security Profile object.
3. Update the CO gateway with the new or changed SmartLSM Security Profiles. In SmartProvisioning, click **Update Corporate Office Gateway**.

Security Profiles for Check Point Appliance Security Gateways

this section describes how to create a SmartLSM Security Profiles which fetch a Check Point Security Policy from the Security Management Server or Domain Management Server, how to add a Check Point Appliance / Open Server Security Gateway to SmartProvisioning, and how to handle messages on SmartLSM Security Gateway.

Creating SmartLSM Security Profiles

A SmartLSM Security Gateway must have a SmartLSM Security Profile, which fetches a Check Point Security Policy from the Security Management Server or Domain Management Server. This Security Policy determines the settings of the firewall.

Before you can add a SmartLSM Security Gateway to SmartProvisioning, you must create the Security Policies and Security Profiles for them in SmartConsole.

This procedure describes how to create a SmartLSM Security Profile for Security Gateways. After you create a Security Profile, you can assign the gateway objects to it.

Do these steps again for each SmartLSM Security Profile. Make a new profile for each type of appliance or server:

Creating a SmartLSM Security Profile

1. In SmartConsole, go to **Menu > Manage policies and layers > Policies > New**.
2. Create a Security Policy and save it.
3. In the Global Toolbar, go to **New Object** > **LSM Profile**, and select the type of profile you wish to create.

   The **SmartLSM Security Profile** window opens.
4. Configure the Profile properties.

   To open the online help for each view of this window, click **Help**.

   Note - In an High Availability environment, click **Add** > the **Add Masters** window opens. From the **Available Management Stations** column, select all servers and click **Add**. Then click **OK**.
5. Click **OK**.
6. Install Policy on the LSM Security Profile you created.

a. Click **Install Policy**.

   The **Install Policy** window opens.

b. Select the SmartLSM Security Profile object.

c. Click **Install**.

Creating a SmartLSM Security Cluster Profile

When you make a new SmartLSM cluster profile, define prefixes and suffixes for the profile name to form the full cluster name. This makes it easy to identify which SmartLSM profile is assigned to a cluster.

You define these common parameters in a SmartLSM cluster Security Profile

- Cluster members.
- Cluster member physical interfaces.
- Interface network objective (Cluster, Sync and so on).
- Cluster interface names.
- Cluster and member interface IP addresses and net masks.
- When you create a SmartLSM cluster Security Profile, define complete IP addresses. These addresses are placeholders and you can override them when you create SmartLSM cluster objects in SmartProvisioning.
- **Cluster and member name components** - Use a common component for the cluster and cluster member names, and another component, to reflect the relative function in the cluster. The common component is in the Profile. The other component is defined in SmartProvisioning for the specific cluster, as a prefix or a suffix to the common component. For example, you can have two two-member clusters, named First_ cluster and Second_cluster. You can then name the respective members First_ member1, First_member2, Second_member1 and Second_member2. In this example, you define the names _cluster, _member1 and _member2 at the Profile level. Then, when you define individual clusters, you need to define only the names First and Second as name prefixes.

  You can manage SmartProvisioning Clusters by a Security Management Server or by a Domain Management Server.

Note - SmartProvisioning is not available for the members of a SmartProvisioning cluster, even if the member gateway runs the SecurePlatform OS.

Creating a SmartLSM Security Cluster Profile

1. In SmartConsole, go to the Objects bar and select **New** > **More** > **LSM Profile**.
2. Select the cluster:
   - Check Point Appliance/Open Server Cluster
   - Small Office Appliance Cluster

   The **Cluster Profile** window opens.
3. On the **General Properties** page, do these steps:
   a. Enter the profile **Name**.
   The profile name becomes the middle section of all SmartLSM cluster names that you define with this profile.
   b. If your clusters use a third-party clustering platform (such as IPSO or Crossbeam), in the **Network Security** tab, clear **ClusterXL**.

   Note - When you use third party cluster platforms, create a different SmartLSM Profile for each platform type.

   c. In the **Network Security** tab, make sure that **IPSec VPN** is selected, if clusters which use this profile are part of a VPN community.
4. On the **Cluster Members** page, add members to the Profile. These member names become the middle section of all member names defined with this Profile.
5. Configure the applicable parameters on the **ClusterXL** or **3rd Party Configuration** page.
6. On the **Topology** page, click **Edit Topology**.
7. Double-click the **New Object** column to configure each interface.

   Use these guidelines

   - Make sure that the number of interfaces and their network objectives match those of the physical SmartLSM clusters.
   - For interfaces with Private or Sync network objectives, do not enter information in the Cluster column.

- Every SmartLSM cluster mapped to this Profile retains the host parts (by net mask) of the member IP addresses, and the name of the cluster (virtual) interface.
  - The network parts of the members' IP addresses and the entire cluster IP addresses are only used as a template here. You define the relevant network for each interface of each SmartLSM Security Gateway later in SmartProvisioning.
  - Make sure that the host ID for the external interface of the SmartLSM cluster profile is the same as the external interface of the cluster.
- The network parts of the members IP addresses must be identical for the same interface name, even though they are only place holders.
- Profile member interface names can be overridden for the actual SmartLSM cluster. However, they are usually the same for all clusters (eth0, eth1 and so on), so it is convenient to use the actual names here as well.

8. Optional: change the **Fetch Policy** interval on the **Fetch Policy** page.

   Select a Scheduled Event or create a new one.
9. Configure other parameters as required. You define VPN domains for cluster objects using SmartProvisioning.
10. Click **OK** to confirm the settings, and save the Policy Package.
11. Install policies to the cluster Profile.

Creating Check Point Security Gateways in SmartProvisioning

This procedure describes how to add a Check Point Appliance/Open Server Security Gateway to SmartProvisioning.

Before you begin, you must have at least one SmartLSM Security Profile.

Adding a SmartLSM Security Gateway to SmartProvisioning

1. In the navigation tree, click **Devices**.
2. From the Launch Menu, select **File > New > Check Point Appliance / Open Server Gateway**.

   The wizard opens in a new window. Follow the steps to define the gateway.
3. Enter a name for the gateway and optional comments. Click **Next**.

This name is for SmartProvisioning management purposes and can be different from the name of the gateway device.

4. In the **More Information** page, configure these settings:
   a. **OS**: Select the Operating System of the gateway.
   b. **SmartLSM Gateway**: Select the version that is installed on the gateway.
   c. **Security Profile**: Select a SmartLSM Security Profile object created in SmartConsole.
   d. **Enable Provisioning**: Select to assign Provisioning Profiles to this gateway.

      Clear this option if you are sure that Provisioning Profiles can have a negative impact on the gateway.

      - **No Provisioning Profile** - Select to enable provisioning for this gateway, and leave the actual assignment of Provisioning Profile for later.
      - **Provisioning Profile** - Select a Provisioning Profile to assign to this gateway.
5. Click **Next**.
6. In the **SmartLSM Security Gateway Communication Properties** page, define an *Activation Key* in the **Authentication** section.

   An activation key sets up a Secure Internal Communication (SIC) Trust between the Security Gateway and the Security Management Server or Domain Management Server. This is the same activation key that you provide in the **SIC** tab of the Check Point Configuration Tool (**cpconfig**) on the Security Gateway.

   In the **Authentication** section, select one of these options:

   - **Initiate trusted communication securely by using a one-time password**.

     Enter a password, and then enter it again in the **Confirm one-time password** field.

- **Initiated trusted communication with an auto-generated one-time password**.
  a. Click **Generate**.

     The **Generated Activation Key** window opens, and displays the key in clear text.

  b. Save the key so you can enter it on the Security Gateway for SIC initialization).

  c. Click **Accept**.

7. In the **Trusted Communication Initiation** pane, select one of these options:
   - If you do not know the IP address of the SmartLSM Security Gateway, select **Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time**.
   - If you know the IP address of this SmartLSM Security Gateway, select **Initiate trusted communication now using the following IP address** and enter the IP address in the field. When you complete this step, the SIC certificate is pushed to the Security Gateway.
8. Click **Next**.
9. If you want a CA certificate from the Internal Check Point CA, select **I wish to create a VPN Certificate from the Internal CA**.

   If you want a CA certificate from a third-party (for example, if your organization already has certificates from an external CA for other devices), clear this check box and request the certificate from the appropriate CA server after you complete the wizard.
10. To continue the gateway configuration, select the **Edit SmartLSM Security Gateway properties after creation**.
11. Click **Finish**.

Handling SmartLSM Security Gateway Messages

This section explains how to handle messages that may appear after you finish the wizard to add a Check Point Appliance / Open Server or UTM Security Gateway, during the SmartProvisioning processing of the gateway object.

Activation Key is Missing

If you did not generate or select an Activation Key for SIC setup during the wizard, a message appears:

'Activation Key' for the Gateway SIC setup is missing.
Do you want to continue?

Click **Yes** to define the gateway now and handle the SIC setup later; or click **No** and then **Back** to return to the **Communication Properties** page.

To handle the SIC setup after the gateway is added:

1. Right-click the required gateway **Edit Gateway**.
2. In the **General** tab > **Secure Internal Communication**, click **Communication**.

   The **Communication** window opens, with the same fields as the **Communication Properties** page of the wizard.
3. Generate or provide an Activation Key.
4. Click **Close** to close the **Communication** window.
5. Click **OK**.
6. Open the Check Point Configuration tool on the Security Gateway and click **Reset SIC**.

Operation Timed Out

When you add a new SmartLSM Security Gateway, SmartProvisioning connects between the Security Management Server or Domain Management Server and the SmartLSM Security Gateway, to match and initialize SIC and VPN certificates.

If the **Operation Timed Out** message shows, the most common cause is that SmartProvisioning cannot reach the Security Management Server or Domain Management Server or the SmartLSM Security Gateway. The gateway is still added to SmartProvisioning, but you must check the certificates status.

To view trust status:

1. Double-click the gateway in the work space.

   The **SmartLSM Security Gateway** window opens
2. In the **General** tab > **Secure Internal Communication**, click **Communication**.
3. Check the value of **Certificate state**. If the value is not **Initialized**, pull the SIC certificate from the Security Management Server or Domain Management Server.

Complete the Initialization Process

If you generated an Activation Key or provided an Activation Key file, but were not able to provide the IP address of the SmartLSM Security Gateway, this message shows:

To complete the initialization process, use the Check Point Configuration tool on the SmartLSM Security Gateway, to pull the certificate from the Security Management Server.

Note - For Multi-Domain Security Management, this message says **Domain Management Server** in place of **Security Management Server**.

To complete the initialization process:

1. Click **OK**.
2. Open the Check Point Configuration tool (**cpconfig**):

   From the CLI on a Gaia, SecurePlatform, or Linux based Security Gateway, run `cpconfig`
3. According to the specific SIC or Communication options, reset and initialize the SIC with the Activation Key of the Security Management Server or Domain Management Server.
4. Restart Check Point services on the SmartLSM Security Gateway.

Security Profiles for Small Office Appliance Gateways

For more about how to use SmartProvisioning with Check Point Small Office Appliance, visit the *Check Point Support Center* and search for the relevant appliance to you.

Creating a Small Office Appliance Gateway in SmartProvisioning

Make sure you have a SmartLSM Security Profile for Small Office Appliance gateways defined in SmartConsole before you create a gateway in SmartProvisioning (see *"Creating SmartLSM Security Profiles" on page 33*).

Procedure

1. In the navigation tree, click **Devices**.
2. From the Launch Menu, select **File** > **New** > **Small Office Appliance Gateway**.

   The **SmartLSM Security Gateway General Properties** page opens.
3. Enter a **Name** for the SmartLSM Security Gateway and optional comments. The name cannot contain spaces or non-alphanumeric characters.
4. Click **Next**.
5. In the **More Information** page, configure these settings:
   a. **Hardware** - Select the gateway hardware.
   b. **SmartLSM gateway** - Select the firmware version of the installed Small Office Appliance.
   c. **Security Profile** - Select the SmartLSM Security Profile to which the Security Gateway is assigned.

d. Select **Enable Provisioning** to enable gateway management with provisioning configurations.

- Select **No Provisioning Profile** to enable provisioning without assigning a specific profile.
- Select **Provisioning Profile** to assign a provisioning profile to this gateway. Select the provisioning profile from the drop-down list.

6. Click **Next**.

   The **SmartLSM Gateway Communication Properties** page opens.

7. In the **Authentication** section, select one of these options:

   - **Initiate trusted communication securely by using a one-time password**.

     Enter a password, and then enter it again in the **Confirm one-time password** field.

   - **Initiated trusted communication with an auto-generated one-time password**.

     a. Click **Generate**.

        The **Generated Activation Key** window opens and displays the key in clear text.

     b. Save this key to enter it later on the Security Gateway for SIC initialization.

     c. Click **Accept**.

8. In the **Trusted Communication Initiation** section:

   - If you do not know the IP address of the SmartLSM Security Gateway, select **Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time**.
   - If you know the IP address of the SmartLSM Security Gateway, select **Initiate trusted communication now using the following IP address**, and enter the IP address in the field. When you complete this step, the SIC certificate is pushed to the Security Gateway.

   Note - The Activation Key sets up Secure Internal Communication (SIC) Trust between the SmartLSM Security Gateway and the Security Management Server. With this SmartLSM wizard, you create the key on the Security Management Server (the SIC certificate and the IKE certificate for the selected gateway are created when you finish this wizard). The certificate is pulled by the gateway when it first connects to the Security Management Server after it is configured with the gateway First Time Configuration Wizard.

9. Click **Next**.

10. Select how to create a VPN certificate:
    - To create a VPN certificate from the Internal Check Point CA, select **I wish to create a VPN Certificate from the Internal CA**.
    - To create a VPN certificate from a third party CA (for example, if your organization already has certificates from an external CA for other devices), clear this checkbox and request the certificate from the appropriate CA server.
11. Select **Edit SmartLSM gateway properties after creation** to work with the newly created object.
12. Click **Finish** to complete the SmartLSM Security Gateway creation.

Configuring DNS in a Provisioning Profile for Small Office Appliances

You can configure DNS servers on a Provisioning Profile, which will provide the configuration for all Small Office Appliances assigned to this profile.

Configuring the DNS server Provisioning Profile for Small Office Appliances

1. Open the **Security Gateway Provisioning Profile** window, and select the **DNS** tab.

   By default, you can apply the **Manage DNS settings locally on the device** option.
2. If you want to manage the DNS setting centrally, select **Manage DNS settings centrally from this application**.
3. Click **Advanced**. The **Profile Settings** window is displayed.
4. Select one of these override profile settings:
   - **Allowed**
   - **Denied**
   - **Mandatory**

   For more information about override profile settings, see .
5. To manually configure the IP address for the DNS servers:
   a. Select **Set DNS server configuration**.
   b. Enter the IP addresses for the DNS servers.
6. To automatically configure the IP address for the DNS server, select **Use DNS configurations provided by the active Internet connection**.
7. To use the Small Office Appliance as your default DNS proxy, select **Enable DNS Proxy - resolves local DNS requests**.

Configuring Firmware in a Provisioning Profile for Small Office Appliances

When you configure firmware settings on a Provisioning Profile, you give the configuration for all Small Office Appliances assigned to this profile.

The Security Gateway version must match its SmartLSM profile's version as defined in SmartConsole for correct policy behavior. In some instances, it is necessary to define exceptions for the default SmartLSM security profile that replaces the security profiles you have now, after installation of the firmware image. For example, if you do not want all gateways to use the specified default SmartLSM profile after installation, you can customize different security profiles to replace known security profiles.

Example scenario

- The default SmartLSM profile after installation is configured to use a SmartLSM profile called "NewLSM".
- After firmware installation, you want the "NewLSM" profile to be installed on all Security Gateways **except** for gateways that currently use the "GroupA_LSM" profile.
- You want to replace the "GroupA_LSM" profile with a profile called "GroupA_ NewLSM".

In such a scenario, you add an **exception** that replaces the "GroupA_LSM" profile with the "GroupA_NewLSM" profile.

Options for installing the firmware

- Immediately - Downloads and installs the firmware immediately after you save these settings in the next synchronization with a Security Gateway assigned to this profile.
- According to time ranges - You can define download and installation time ranges for the firmware image. You can limit the download and installation time to a specified list of time ranges in the week. They start at the nearest time range after firmware settings are applied. For example, if the firmware installation settings are applied on Sunday and there are two time ranges:
  - One range is set to Friday 00:00 to Saturday 00:00
  - One range is set to Wednesday 23:00 to Thursday 06:0

    The firmware will be installed between Wednesday 23:00 and Thursday 06:00.

    If the Security Gateway does not succeed to download or install the firmware during the nearest time range, it tries again in the next time range.

Configuring firmware installation settings on a Provisioning Profile for Small Office Appliances

1. Open the **Security Gateway Profile** window, and select the **Firmware** tab.
2. Select **Manage firmware centrally from this application**.
3. Click **Advanced**. The **Profile Settings** window is displayed.
4. Select one of these override profile settings:
   - **Allowed**
   - **Denied**
   - **Mandatory**

   For more information about override profile settings, see .
5. In **Firmware image**, click **Select** to select a firmware image that was uploaded through SmartUpdate (see *"Uploading Packages to the Repository" on page 107*).
6. In **Default SmartLSM Profile after installation**, select the new SmartLSM profile of the Security Gateway (the Security Gateway version must match its SmartLSM profile's version as defined in SmartConsole for correct policy behavior). The Security Gateway will replace its SmartLSM profile after successful firmware installation and only if the new firmware version is different from the version you have now.
7. If necessary, click **Exceptions** to select a new SmartLSM profile for Security Gateways with a specified SmartLSM profile.
   - **Add/Edit** - Click **Add** or **Edit** to open the **Exceptions** window to define or change an exception for a SmartLSM profile replacement.
     - **Current SmartLSM Profile** - Select a SmartLSM profile from the list. Make sure you installed policy for the SmartLSM profile in SmartConsole.
     - **SmartLSM Profile after installation** - Select a SmartLSM profile to replace the SmartLSM profile after the firmware image installation. A SmartLSM profile is shown only if the version is the same as the selected firmware version. Make sure you installed policy for the SmartLSM profile in SmartConsole.
   - **Remove** - Click to remove a SmartLSM profile **exception** setting.
8. Select one of these options to install the firmware:

a. **Immediately**

b. **According to these time ranges** - Select to use the Security Gateway time or local time.

- **Add/Edit** - Click Add or Edit to open the Time Range window to define or change the weekdays and times for download and installation of the firmware image. Select the days and times. Click **OK**.
- **Remove** - Select a range from the list and click **Remove** to delete a time range.
- **Download image immediately** - Click this option to download the firmware image immediately but install the image during one of the set time ranges.

9. Click **Show profile settings** - to see the settings of the Provisioning Profile that this gateway references.
10. Click **OK**.

Configuring RADIUS in a Provisioning Profile for Small Office Appliances

You can configure the RADIUS server (Remote Authentication Dial In User Service) that provides authentication, authorization, and accounting for your gateways. You can configure RADIUS in the provisioning profile once for all gateways that reference this profile. The RADIUS server or group must already be defined as a SmartConsole object.

Procedure

1. Open the **Small Office Appliances Profile** window, and select the **RADIUS** tab.

   Manage RADIUS settings locally on the device is a default selection.

2. If you select **Manage RADIUS settings centrally from this application**, click **Advanced** to set the central management options. See for more information.
3. Optionally: select **RADIUS is activated on device** option, click **Add** and choose a RADIUS server to assign to this Provisioning Profile. Change their order with buttons **Up** and **Down**.
4. In the **Allow administrators from specific RADIUS groups only (comma separated):** line, type the names of the relevant administrators and separate them by comma.

   Note - The **RADIUS Servers** lists show all the servers that are defined in SmartConsole as RADIUS servers.

5. Click **OK**.

Configuring HotSpot in a Provisioning Profile for Small Office Appliances

You can configure a HotSpot in a Provisioning Profile, to provision the same HotSpot on all gateways that reference the profile. If your gateway provides wireless connectivity, a HotSpot provides improved remote internet access.

Note - Some HotSpots use RADIUS servers for Authentication, Authorization, and Accounting. If this is true of yours, be sure to configure the HotSpot in the Provisioning Profile; see *"Configuring RADIUS in a Provisioning Profile for Small Office Appliances" on page 59*.

Procedure

1. Open the **Small Office Appliances Profile** window, and select the **HotSpot** tab.

   Manage HotSpot settings locally on the device is a default selection.

2. If you select **Manage HotSpot settings centrally from this application**, click **Advanced** to set the central management options. See for more information.

3. In the **HotSpot is activated on device** field, specify the following:

   Portal Title. Change the default name, if necessary.

   Portal message. Enter free text that you need.

   Select the **Terms of use** and **Require authentication** > **Allow users from specific group** and enter free text in the relevant fields.

4. Click **OK**.

Configuring Configuration Script in a Provisioning Profile for Small Office Appliances

You can configure a Configuration Script in a Provisioning Profile, to provision the same Configuration Script on all gateways that reference the profile. You can view and edit a configuration script to configure settings that are not included in the WebUI. Any changes that you make to the configuration script are enforced when the Small Office Appliances fetch their SmartProvisioning settings.

Procedure

1. Open the **Small Office Appliances Profile** window, and go to the **Configuration Script** tab.

2. Select one of these options:

- **Manage Configuration Script settings locally on the device** - Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioning gateway object. If you select this option, the gateway window shows: settings are defined to be managed locally on the device.
- **Manage Configuration Script settings centrally from this application** - Each gateway that references this profile gets its configuration settings from the Provisioning Profile or from the SmartProvisioninggateway object. If you select this option:
  a. Click **Advanced** and select one of these override profile settings:
     - **Allowed** - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
     - **Denied** - Each gateway takes the settings from the profile, with no option to override the profile settings.
     - **Mandatory** - Each gateway is managed without a Provisioning Profile.
  b. Enter the Configuration Script in the **Configuration Script** box.

3. Click **OK**.

Configuring Provisioning Profiles

With SmartProvisioning, you can use a Provisioning Profile to configure the same settings on similar devices. A Provisioning Profile can provision any or all of the network configurations. You can determine which settings are provisioned and which are set up locally.

After you created a Provisioning Profile, assign it to the applicable gateways. When each gateway device fetches its Provisioning Profile, the device's configuration is updated with the settings in the profile.

For example, you can create a Provisioning Profile for a number of gateways that are in one branch office. They are on the same LAN, therefore you can provision their DNS servers with central management (configure once, set on all). However, this office has multiple domains, so you do not want the Provisioning Profile to determine their domain. You set the Domain settings to local management.

Provisioning Profiles function similarly to SmartLSM Security Profiles. The main differences between Provisioning Profiles and SmartLSM Security Profiles are described in this table:

Category	Provisioning Profile	SmartLSM Security Profile
Provides	Central management of servers, network, and so on, of Check Point gateways	Installation of Security Policy for SmartLSM Security Gateways
Necessary for	No gateway	SmartLSM Security Gateways
Managed by	SmartProvisioning	SmartConsole

Gateways that are provisioning-enabled have more management features, such as multiple automatic backups (see *"Security Gateway Actions on SmartLSM Security Gateways" on page 110*).

Configuring Provisioning Profiles for Security Gateways

You can create Provisioning Profiles in SmartProvisioning. Each Provisioning Profile can automate the steps required to manage configurations of gateways that have the same operating system, hardware, and Check Point software version.

Before you begin this procedure, make sure that your administrator username has Write permissions for Provisioning Profiles (see *"Defining SmartProvisioning Administrators" on page 15*).

Creating a Provisioning Profile

1. In the tree in the main window, click **Profiles**.

   Profiles is shown in the work space.

2. From the Launch Menu, select **File** > **New** > **Provisioning Profile**.

   The **New Provisioning Profile Wizard** opens.

3. Enter a name for the profile.

4. From the **Select Type** drop-down list, select the platform or operating system that this profile supports.

   Each Provisioning Profile can support only one operating system.

5. Click **Next**.

6. If you want to configure the settings of the Provisioning Profile now, select **Edit Provisioning Profile properties after creation**.

7. Click **Finish**.

8. Click **Publish** from the top toolbar.

Configuring Provisioning Profile Settings

A Provisioning Profile can provision any or all of the network configurations to the gateways. Each Provisioning Profile holds settings that are provisioned onto the gateways assigned to this profile. You can determine which settings are provisioned and which are set up locally.

For example, you can create a Provisioning Profile for a number of gateways that are in one branch office. They are on the same LAN, therefore you can provision their DNS servers with central management (configure once, set on all). However, this office has multiple domains, so you do not want the Provisioning Profile to determine their domain. You set the domain settings to local management.

Configuring a Provisioning Profile Settings

1. In the **Profiles List**, right-click a profile and select **Edit Provisioning Profile**.

2. **Configure DNS Settings**

a. Select management settings for gateways that reference the profile:

- **Manage settings locally on the device**: Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioninggateway object. If you select this option, the Gateway window shows: **settings are defined to be managed locally on the device**.
- **Manage settings centrally from this application**: Each gateway that references this profile gets its configuration for this setting from the Provisioning Profile or from the SmartProvisioninggateway object.

b. If you selected to manage settings centrally, click **Advanced**.

The **Profile Settings** window opens.

c. Select an option for **Overriding profile settings on device level is**:

- **Allowed** - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
- **Denied** - Each gateway takes the settings from the profile, with no option to override the profile settings.
- **Mandatory** - Each gateway is managed without a Provisioning Profile.

d. Provide the IP address of the **First**, **Second**, and **Third** DNS servers of the network.

e. Click **OK**.

3. **Configure Hosts settings**

a. Select management settings for gateways that reference the profile:

- **Manage settings locally on the device**: Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioninggateway object. If you select this option, the Gateway window shows: **settings are defined to be managed locally on the device**.
- **Manage settings centrally from this application**: Each gateway that references this profile gets its configuration for this setting from the Provisioning Profile or from the SmartProvisioninggateway object.

Best Practice - Central Host management is useful for gateways on the same LAN or network, such as Security Gateways with High Availability.

b. If you selected to manage settings centrally, click **Advanced**.

The **Profile Settings** window opens.

c. Select an option for **Overriding profile settings on device level is**:

- **Allowed** - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
- **Denied** - Each gateway takes the settings from the profile, with no option to override the profile settings.
- **Mandatory** - Each gateway is managed without a Provisioning Profile.

d. Click **New**.

e. Enter the **Host name** and the **IP address**.

Click **OK** to return to the **Hosts** tab.

f. Repeat for all required hosts.

Every gateway assigned to this Provisioning Profile will receive this Host list.

4. **Configure Domain Name settings:**

a. Select management settings for gateways that reference the profile:

- **Manage settings locally on the device**: Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioninggateway object. If you select this option, the Gateway window shows: **settings are defined to be managed locally on the device**.
- **Manage settings centrally from this application**: Each gateway that references this profile gets its configuration for this setting from the Provisioning Profile or from the SmartProvisioninggateway object.

Best Practice - Central **Domain Name** management is useful for gateways that share a domain. This way, you only have to configure it once for all the gateways.

b. If you selected to manage settings centrally, click **Advanced**.

The **Profile Settings** window opens.

c. Select an option for **Overriding profile settings on device level is**:

- **Allowed** - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
- **Denied** - Each gateway takes the settings from the profile, with no option to override the profile settings.
- **Mandatory** - Each gateway is managed without a Provisioning Profile

d. Click **OK**.

e. Enter the **Domain Name**.

f. Click **OK**.

5. **Configure Backup Settings (relevant for IP Appliances and UTM-1/Power-1/SSecurePlatform gateways)**

a. Select management settings for gateways that reference the profile:

- **Manage settings locally on the device**: Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioninggateway object. If you select this option, the Gateway window shows: **settings are defined to be managed locally on the device**.
- **Manage settings centrally from this application**: Each gateway that references this profile gets its configuration for this setting from the Provisioning Profile or from the SmartProvisioninggateway object.

b. If you selected to manage settings centrally, click **Advanced**.

The **Profile Settings** window opens.

c. Select an option for **Overriding profile settings on device level is**:

- **Allowed** - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
- **Denied** - Each gateway takes the settings from the profile, with no option to override the profile settings.
- **Mandatory** - Each gateway is managed without a Provisioning Profile.

d. Click **OK**.

e. Select **Enable Backup**.

f. In the **Start at** field, select the hour (on European 24-hour units) and minute for the backup to start.

g. Select the backup frequency:

- Select the **day of the month** radio button and select a date.
- Select the weekdays radio button and select the required day.

h. If you want the backup to include the log files, select **Include Check point products log files in the backup**.

Such backups are generally much larger than without the logs, so clear this checkbox if you do not need the logs. Log files are not relevant for IP Appliances, so clear this checkbox for IPSO-Based gateways.

You can configure backup to be stored on a different machine than the SmartProvisioning server. This option is relevant only if all gateways which are assigned to this Provisioning Profile are on the same network, with access to the server which stores the backups.

i. If you want the backups to be saved on another server, click **Backup Target**.

The **Backup Target** window opens.

j. Select the server type to hold the backups, or select **Locally on Device**, which enables each gateway of this profile to hold its own backup file.

k. Provide the **IP address** or **Hostname** of the selected server.

l. For SCP servers, also provide the **Username** and **Password**.

m. Click **OK**.

Example for Backup schedule - If you want to make sure that all gateways are backed up with no downtime, you can create one Provisioning Profile that backs up primary gateways at midnight on the weekend and another Provisioning Profile that backs up secondary gateways at six in the morning on every fifth day of the month.

This table maps the profile settings selections to the Gateway window options:

Profile managed	Profile Override	Gateway Window Display and options
Locally	Not relevant	**Settings are defined to be managed locally on the device.** **To change this, refer to the attached Provisioning Profile***profile_name*. (controls are unavailable)

Profile managed	Profile Override	Gateway Window Display and options
Centrally	Override denied	**Overriding profile settings is denied**. **To change this, refer to the attached Provisioning Profile***profile_name* (controls are Read-Only, configured by profile)
Centrally	Override allowed	Select override method: ■ **Manage settings locally on the device**: Local management. Override provisioning configurations with local settings. ■ **Use profile settings**: Enforce profile settings on this gateway. ■ **Use the following settings**: Manage these settings on this gateway individually with the values given here.
Centrally	Override mandatory	**Overriding profile settings is mandatory: configure settings here**. **To change this, refer to Provisioning Profile***profile_name* (Each gateway is configured separately) ■ **Manage settings locally on the device:** Manage these settings on this gateway locally. ■ **Use the following settings**: Manage these settings on this gateway individually with the values given here.

For example, you set Hosts configuration to **Central** and **Allowed**. The **Hosts** tab on the gateway enables you to manage the Host List of a gateway if you:

- Define the Host List locally on the device (even if it has an assigned Provisioning Profile)
- Define Provision gateways with the Host List of the Provisioning Profile
- Define a New Host List (in the Gateway window) that overrides the Provisioning Profile on this gateway

Warning - If you select **Use the following settings** and do not enter values for a specified topic, the current settings on the device are deleted.

Viewing General Properties of Provisioning Profiles

Right-click a Provisioning Profile and select **Edit Provisioning Profile**.

The **Security Gateway Provisioning Profile** window opens, depending on the operating system for which you created the profile. The **General** tab is a Read-Only view of the **Profile name** and **OS**. You cannot change these profile properties after it is created.

The operating system of a Provisioning Profile determines which gateways you can assign to the profile.

Configuring Provisioning Profiles for Small Office Appliances Gateways

This chapter explains how to create provisioning profiles for Small Office Appliance Gateways.

Configuring DNS in a Provisioning Profile for Small Office Appliances

You can configure DNS servers on a Provisioning Profile, which will provide the configuration for all Small Office Appliances assigned to this profile.

Configuring the DNS server Provisioning Profile for Small Office Appliances

1. Open the **Security Gateway Provisioning Profile** window, and select the **DNS** tab.

   By default, you can apply the **Manage DNS settings locally on the device** option.
2. If you want to manage the DNS setting centrally, select **Manage DNS settings centrally from this application**.
3. Click **Advanced**. The **Profile Settings** window is displayed.
4. Select one of these override profile settings:
   - **Allowed**
   - **Denied**
   - **Mandatory**

   For more information about override profile settings, see .
5. To manually configure the IP address for the DNS servers:
   a. Select **Set DNS server configuration**.
   b. Enter the IP addresses for the DNS servers.
6. To automatically configure the IP address for the DNS server, select **Use DNS configurations provided by the active Internet connection**.

7. To use the Small Office Appliance as your default DNS proxy, select **Enable DNS Proxy - resolves local DNS requests**.

Configuring Firmware in a Provisioning Profile for Small Office Appliances

When you configure firmware settings on a Provisioning Profile, you give the configuration for all Small Office Appliances assigned to this profile.

The Security Gateway version must match its SmartLSM profile's version as defined in SmartConsole for correct policy behavior. In some instances, it is necessary to define exceptions for the default SmartLSM security profile that replaces the security profiles you have now, after installation of the firmware image. For example, if you do not want all gateways to use the specified default SmartLSM profile after installation, you can customize different security profiles to replace known security profiles.

Example scenario

- The default SmartLSM profile after installation is configured to use a SmartLSM profile called "NewLSM".
- After firmware installation, you want the "NewLSM" profile to be installed on all Security Gateways **except** for gateways that currently use the "GroupA_LSM" profile.
- You want to replace the "GroupA_LSM" profile with a profile called "GroupA_NewLSM".

In such a scenario, you add an **exception** that replaces the "GroupA_LSM" profile with the "GroupA_NewLSM" profile.

Options for installing the firmware

- Immediately - Downloads and installs the firmware immediately after you save these settings in the next synchronization with a Security Gateway assigned to this profile.
- According to time ranges - You can define download and installation time ranges for the firmware image. You can limit the download and installation time to a specified list of time ranges in the week. They start at the nearest time range after firmware settings are applied. For example, if the firmware installation settings are applied on Sunday and there are two time ranges:

- One range is set to Friday 00:00 to Saturday 00:00
- One range is set to Wednesday 23:00 to Thursday 06:0

  The firmware will be installed between Wednesday 23:00 and Thursday 06:00.

  If the Security Gateway does not succeed to download or install the firmware during the nearest time range, it tries again in the next time range.

Configuring firmware installation settings on a Provisioning Profile for Small Office Appliances

1. Open the **Security Gateway Profile** window, and select the **Firmware** tab.
2. Select **Manage firmware centrally from this application**.
3. Click **Advanced**. The **Profile Settings** window is displayed.
4. Select one of these override profile settings:
   - **Allowed**
   - **Denied**
   - **Mandatory**

   For more information about override profile settings, see .
5. In **Firmware image**, click **Select** to select a firmware image that was uploaded through SmartUpdate (see *"Uploading Packages to the Repository" on page 107*).
6. In **Default SmartLSM Profile after installation**, select the new SmartLSM profile of the Security Gateway (the Security Gateway version must match its SmartLSM profile's version as defined in SmartConsole for correct policy behavior). The Security Gateway will replace its SmartLSM profile after successful firmware installation and only if the new firmware version is different from the version you have now.
7. If necessary, click **Exceptions** to select a new SmartLSM profile for Security Gateways with a specified SmartLSM profile.
   - **Add/Edit** - Click **Add** or **Edit** to open the **Exceptions** window to define or change an exception for a SmartLSM profile replacement.
     - **Current SmartLSM Profile** - Select a SmartLSM profile from the list. Make sure you installed policy for the SmartLSM profile in SmartConsole.
     - **SmartLSM Profile after installation** - Select a SmartLSM profile to replace the SmartLSM profile after the firmware image installation. A SmartLSM profile is shown only if the version is the same as the selected firmware version. Make sure you installed policy for the SmartLSM profile in SmartConsole.
   - **Remove** - Click to remove a SmartLSM profile **exception** setting.
8. Select one of these options to install the firmware:

a. **Immediately**

b. **According to these time ranges** - Select to use the Security Gateway time or local time.

- **Add/Edit** - Click Add or Edit to open the Time Range window to define or change the weekdays and times for download and installation of the firmware image. Select the days and times. Click **OK**.
- **Remove** - Select a range from the list and click **Remove** to delete a time range.
- **Download image immediately** - Click this option to download the firmware image immediately but install the image during one of the set time ranges.

9. Click **Show profile settings** - to see the settings of the Provisioning Profile that this gateway references.
10. Click **OK**.

Configuring RADIUS in a Provisioning Profile for Small Office Appliances

You can configure the RADIUS server (Remote Authentication Dial In User Service) that provides authentication, authorization, and accounting for your gateways. You can configure RADIUS in the provisioning profile once for all gateways that reference this profile. The RADIUS server or group must already be defined as a SmartConsole object.

Procedure

1. Open the **Small Office Appliances Profile** window, and select the **RADIUS** tab.

   Manage RADIUS settings locally on the device is a default selection.

2. If you select **Manage RADIUS settings centrally from this application**, click **Advanced** to set the central management options. See for more information.
3. Optionally: select **RADIUS is activated on device** option, click **Add** and choose a RADIUS server to assign to this Provisioning Profile. Change their order with buttons **Up** and **Down**.
4. In the **Allow administrators from specific RADIUS groups only (comma separated):** line, type the names of the relevant administrators and separate them by comma.

   Note - The **RADIUS Servers** lists show all the servers that are defined in SmartConsole as RADIUS servers.

5. Click **OK**.

Configuring HotSpot in a Provisioning Profile for Small Office Appliances

You can configure a HotSpot in a Provisioning Profile, to provision the same HotSpot on all gateways that reference the profile. If your gateway provides wireless connectivity, a HotSpot provides improved remote internet access.

Note - Some HotSpots use RADIUS servers for Authentication, Authorization, and Accounting. If this is true of yours, be sure to configure the HotSpot in the Provisioning Profile; see *"Configuring RADIUS in a Provisioning Profile for Small Office Appliances" on the previous page*.

Procedure

1. Open the **Small Office Appliances Profile** window, and select the **HotSpot** tab.

   Manage HotSpot settings locally on the device is a default selection.

2. If you select **Manage HotSpot settings centrally from this application**, click **Advanced** to set the central management options. See for more information.

3. In the **HotSpot is activated on device** field, specify the following:

   Portal Title. Change the default name, if necessary.

   Portal message. Enter free text that you need.

   Select the **Terms of use** and **Require authentication** > **Allow users from specific group** and enter free text in the relevant fields.

4. Click **OK**.

Configuring Configuration Script in a Provisioning Profile for Small Office Appliances

You can configure a Configuration Script in a Provisioning Profile, to provision the same Configuration Script on all gateways that reference the profile. You can view and edit a configuration script to configure settings that are not included in the WebUI. Any changes that you make to the configuration script are enforced when the Small Office Appliances fetch their SmartProvisioning settings.

Procedure

1. Open the **Small Office Appliances Profile** window, and go to the **Configuration Script** tab.

2. Select one of these options:

- **Manage Configuration Script settings locally on the device** - Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioning gateway object. If you select this option, the gateway window shows: settings are defined to be managed locally on the device.
- **Manage Configuration Script settings centrally from this application** - Each gateway that references this profile gets its configuration settings from the Provisioning Profile or from the SmartProvisioninggateway object. If you select this option:
  a. Click **Advanced** and select one of these override profile settings:
     - **Allowed** - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
     - **Denied** - Each gateway takes the settings from the profile, with no option to override the profile settings.
     - **Mandatory** - Each gateway is managed without a Provisioning Profile.
  b. Enter the Configuration Script in the **Configuration Script** box.

3. Click **OK**.

Assigning Provisioning Profiles to Gateways

After you create a Provisioning Profile, you can assign gateways to be automatically managed by a provisioning profile.

Make sure the software version and operating system of the Provisioning Profile correspond to the software version and operating system of the Security Gateway.

Procedure:

1. In the tree in the main window, click **Devices**.

   The **Devices** work space appears in the work space.

2. Double-click a gateway.

   The Gateway window opens, with the **General** settings displayed.

3. Make sure **Enable Provisioning** is selected.

4. Select **Provisioning Profile**.

5. From the drop-down menu, select the required Provisioning Profile, or click **New** and create a new Provisioning Profile.

SmartProvisioning Wizard

When you open SmartProvisioning, you access the **SmartProvisioning Wizard** through the **Status** workspace > **Getting Started**. Before you use the wizard, make sure that SmartProvisioning is disabled on the applicable devices.

SmartProvisioning can run one or more of these operations on provisioned devices:

- Verify each device has the software needed to support provisioning.
- Fetch each device's current configuration settings.
- Associate the selected devices with a Provisioning Profile.

Using the SmartProvisioning Wizard

Before you use the SmartProvisioning Wizard, make sure that all gateways have security policies installed on them.

Procedure

1. Make sure that the **Devices** section shows the applicable gateways.
2. From the navigation tree, click **Status**.
3. In the **Getting Started** section, click **SmartProvisioning Wizard**.
4. Click **Next**.

   The **Choose Devices** window opens.
5. Select the device type.

   You can run the wizard on only one appliance or device type at a time.

   The window shows the list of appliances and devices that you can assign to a Provisioning Profile.
6. Select the appliances and devices to assign to a specified profile.
7. Click **Next**.

   The **Choose Operations** window opens.
8. To assign the gateways to a profile:
   a. Select **Associate devices with a Provisioning Profile**.
   b. Select the Provisioning Profile or click **New** and create a Provisioning Profile for the devices.
9. Click **Next**.

The **Summary** window opens appears.

10. Click **Finish**.

Configuring Provisioning Settings on Security Gateways

This section describes how to configure the Provisioning settings for Security Gateways assigned with a Provisioning Profile, and Provisioning settings for Small Office Appliances.

Provisioning Settings for Security Gateways Configured in SmartConsole

This section describes how to configure the Provisioning settings that are common to all the Security Gateways **that you created in SmartConsole**.

Before you begin, make sure that your administrator user name has Write permissions for SmartLSM Gateway Database (see *"Defining SmartProvisioning Administrators" on page 15*).

From the **Devices** pane, double-click the Security Gateway object.

The window opens and shows the **General** tab.

Assigning a Provisioning Profile

1. Click the **General** tab.
2. In the **Provisioning** section, select **Enable Provisioning**.
3. Click **Provisioning Profile**.
4. From the drop-down menu, select the required Provisioning Profile, or click **New** and create a new Provisioning Profile.
5. Click **OK**.
6. Click **Publish** from the top toolbar.

Configuring Interfaces

You can configure the interfaces of the individual Security Gateway, or view how they are managed with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the interface settings, or configure them locally on the Security Gateway.

Configure interfaces with SmartProvisioning

1. Click the **Interfaces** tab.
2. Click **Use the following settings**.

3. Click **Add** and select the applicable interface type.
4. Configure the interface settings.
5. Click **OK** to close the interface properties.
6. Click **OK** to close the Security Gateway object properties.
7. Click **Publish** from the top toolbar.

Configure interfaces on the Security Gateway

1. Click the **Interfaces** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Routing

You can configure the routing settings of individual Security Gateways in the Devices pane in SmartProvisioning. You cannot configure these settings in a Provisioning Profile. You must configure the interfaces before the routes, because there are different types of routing configurations for different interfaces.

You can also configure the routing settings on the local appliance or server.

Configuring and Managing the routing settings with SmartProvisioning

Configure the routing settings with SmartProvisioning

1. Click the **Routing** tab.
2. Click **Use the following settings**.
3. Click **Add**.
4. Select a route type:
   - **Network Route** - Configure internal network routes (see *"Configuring Network Route" on the next page*).
   - **Host Route** - Configure access to a specific host (see *"Configuring Host Route" on the next page*).
   - **Default Route** - Configure the default route to access external destinations (see *"Configuring Default Route" on page 68*).

   A different **Routing** window opens for each type.
5. Enter the data.

Click **OK**.

Some of the options are different for different appliances.

6. Click **OK**.
7. Click **Publish** from the top toolbar.

Configure the routing settings on the Security Gateway

1. Click the **Routing** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Network Route

Configure these settings for the internal network routes:

- **Destination IP Address** - Destination IP address for this route (for example, the IP address of the CO Security Gateway or the Security Management Server/Domain Management Server).
- **Destination Netmask** - Net mask of the destination network.
- **Interface** - Select a pre-configured interface for this route.
- **Gateway** - IP address of the Security Gateway, which provides access to this route (for the Gaia gateways also assign a priority).
- **Next Hop Type** - For Gaia and the IP Appliances:
  - **Normal** - Allow traffic to the Security Gateway.
  - **Reject** - Block traffic where the gateway is the destination, and acknowledge.
  - **Black Hole** - Block traffic without acknowledgment.

Configuring Host Route

Configure these settings for host routes:

- **Destination IP Address** - IP address of the destination host.
- **Interface** - Select a pre-configured interface for this route.
- **Gateway** - IP address of the gateway providing access to this host.

- **Metric** - Distance in hops to the destination. If the host is on your local site, this must be a very low number. If the host is not behind routers, the metric must be zero.

Configuring Default Route

Configure these settings for default routes to external destinations:

- **Gateway** - IP address of the gateway providing access to the default external route.
- **Metric** - Distance in hops to the gateway (this value must be as accurate as possible: too low a value can cause lost communications with looping; too high a value may cause security issues). You can define only one default route per gateway.

Configuring DNS Servers

You can configure the DNS servers of the individual Security Gateway, or view how they are managed with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the DNS settings, or configure on the local appliance or server.

Configure DNS servers with SmartProvisioning

1. Click the **DNS** tab.
2. Click **Use the following settings**.
3. Enter the IP addresses of the **First**, **Second**, and **Third** DNS servers.
4. Click **OK**.
5. Click **Publish** from the top toolbar.

Configure the DNS servers on the Security Gateway

1. Click the **DNS** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Hosts

You can set up the host list of the individual Security Gateway, or view how it is managed centrally with the assigned Provisioning Profile.

You can use SmartProvisioning to manage the host list, or configure it on the local appliance or server.

Configure the host list with SmartProvisioning

1. Click the **Hosts** tab.
2. Click **Use the following settings**.
3. Click **New**.
4. Provide the **Hostname** and **IP address**.
5. Click **OK**.
6. Click **Publish** from the top toolbar.

Configure the host list on the Security Gateway

1. Click the **Hosts** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Domain Name

You can set up the domain of the individual Security Gateway, or view how it is managed centrally with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the domain settings, or configure on the local appliance or server.

Configure domain settings with SmartProvisioning

1. Click the **Domain Name** tab.
2. Click **Use the following settings**.
3. Enter the **Domain name**.
4. Click **OK**.
5. Click **Publish** from the top toolbar.

Configure the domain settings on the Security Gateway

1. Click the **Domain Name** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Host Name

You can see or change the host name of the individual Security Gateway in SmartProvisioning. You cannot use a Provisioning Profile to change the host name.

You can select to use SmartProvisioning to manage the host name settings, or configure on the local appliance or server.

Configure host name with SmartProvisioning

1. Click the **Host Name** tab.
2. Click **Use the following settings**.
3. Enter the **Hostname** of the gateway.
4. Click **OK**.
5. Click **Publish** from the top toolbar.

Configure the host name on the Security Gateway

1. Click the **Host Name** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Provisioning Settings for Security Gateways Configured in SmartProvisioning

This section describes how to configure the Provisioning settings that are common to all the Security Gateways **that you created in SmartProvisioning**.

Before you begin, make sure that your administrator user name has Write permissions for SmartLSM Gateway Database (see *"Defining SmartProvisioning Administrators" on page 15*).

From the **Devices** pane, double-click the Security Gateway object.

The window opens and shows the **General** tab.

Assigning a Provisioning Profile

1. Click the **General** tab.
2. In the **Provisioning** section, select **Enable Provisioning**.
3. Click **Provisioning Profile**.

4. From the drop-down menu, select the required Provisioning Profile, or click **New** and create a new Provisioning Profile.
5. Click **OK**.
6. Click **Publish** from the top toolbar.

Configuring Interfaces

You can configure the interfaces of the individual Security Gateway, or view how they are managed with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the interface settings, or configure them locally on the Security Gateway.

Configure interfaces with SmartProvisioning

1. Click the **Interfaces** tab.
2. Click **Use the following settings**.
3. Click **Add** and select the applicable interface type.
4. Configure the interface settings.
5. Click **OK** to close the interface properties.
6. Click **OK** to close the Security Gateway object properties.
7. Click **Publish** from the top toolbar.

Configure interfaces on the Security Gateway

1. Click the **Interfaces** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Routing

You can configure the routing settings of individual Security Gateways in the Devices pane in SmartProvisioning. You cannot configure these settings in a Provisioning Profile. You must configure the interfaces before the routes, because there are different types of routing configurations for different interfaces.

You can also configure the routing settings on the local appliance or server.

Configuring and Managing the routing settings with SmartProvisioning

Configure the routing settings with SmartProvisioning

1. Click the **Routing** tab.
2. Click **Use the following settings**.
3. Click **Add**.
4. Select a route type:
   - **Network Route** - Configure internal network routes (see *"Configuring Network Route" below*).
   - **Host Route** - Configure access to a specific host (see *"Configuring Host Route" on the next page*).
   - **Default Route** - Configure the default route to access external destinations (see *"Configuring Default Route" on the next page*).

   A different **Routing** window opens for each type.
5. Enter the data.

   Click **OK**.

   Some of the options are different for different appliances.
6. Click **OK**.
7. Click **Publish** from the top toolbar.

Configure the routing settings on the Security Gateway

1. Click the **Routing** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Network Route

Configure these settings for the internal network routes:

- **Destination IP Address** - Destination IP address for this route (for example, the IP address of the CO Security Gateway or the Security Management Server/Domain Management Server).
- **Destination Netmask** - Net mask of the destination network.
- **Interface** - Select a pre-configured interface for this route.

- **Gateway** - IP address of the Security Gateway, which provides access to this route (for the Gaia gateways also assign a priority).
- **Next Hop Type** - For Gaia and the IP Appliances:
  - **Normal** - Allow traffic to the Security Gateway.
  - **Reject** - Block traffic where the gateway is the destination, and acknowledge.
  - **Black Hole** - Block traffic without acknowledgment.

Configuring Host Route

Configure these settings for host routes:

- **Destination IP Address** - IP address of the destination host.
- **Interface** - Select a pre-configured interface for this route.
- **Gateway** - IP address of the gateway providing access to this host.
- **Metric** - Distance in hops to the destination. If the host is on your local site, this must be a very low number. If the host is not behind routers, the metric must be zero.

Configuring Default Route

Configure these settings for default routes to external destinations:

- **Gateway** - IP address of the gateway providing access to the default external route.
- **Metric** - Distance in hops to the gateway (this value must be as accurate as possible: too low a value can cause lost communications with looping; too high a value may cause security issues). You can define only one default route per gateway.

Configuring DNS Servers

You can configure the DNS servers of the individual Security Gateway, or view how they are managed with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the DNS settings, or configure on the local appliance or server.

Configure DNS servers with SmartProvisioning

1. Click the **DNS** tab.
2. Click **Use the following settings**.
3. Enter the IP addresses of the **First**, **Second**, and **Third** DNS servers.
4. Click **OK**.

5. Click **Publish** from the top toolbar.

Configure the DNS servers on the Security Gateway

1. Click the **DNS** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Hosts

You can set up the host list of the individual Security Gateway, or view how it is managed centrally with the assigned Provisioning Profile.

You can use SmartProvisioning to manage the host list, or configure it on the local appliance or server.

Configure the host list with SmartProvisioning

1. Click the **Hosts** tab.
2. Click **Use the following settings**.
3. Click **New**.
4. Provide the **Hostname** and **IP address**.
5. Click **OK**.
6. Click **Publish** from the top toolbar.

Configure the host list on the Security Gateway

1. Click the **Hosts** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Domain Name

You can set up the domain of the individual Security Gateway, or view how it is managed centrally with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the domain settings, or configure on the local appliance or server.

Configure domain settings with SmartProvisioning

1. Click the **Domain Name** tab.
2. Click **Use the following settings**.
3. Enter the **Domain name**.
4. Click **OK**.
5. Click **Publish** from the top toolbar.

Configure the domain settings on the Security Gateway

1. Click the **Domain Name** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Host Name

You can see or change the host name of the individual Security Gateway in SmartProvisioning. You cannot use a Provisioning Profile to change the host name.

You can select to use SmartProvisioning to manage the host name settings, or configure on the local appliance or server.

Configure host name with SmartProvisioning

1. Click the **Host Name** tab.
2. Click **Use the following settings**.
3. Enter the **Hostname** of the gateway.
4. Click **OK**.
5. Click **Publish** from the top toolbar.

Configure the host name on the Security Gateway

1. Click the **Host Name** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Configuring Backup

You can configure backup of the individual Security Gateway, or view how they are managed with the assigned Provisioning Profile.

You can select to use SmartProvisioning to manage the backup settings, or configure them locally on the Security Gateway.

Configure backup with SmartProvisioning

1. Click the **Backup** tab.
2. Click **Use the following settings**.
3. Select **Enable Backup**.
4. Configure the backup settings.
5. Click **OK** to close the Security Gateway object properties.
6. Click **Publish** from the top toolbar.

Configure backup on the Security Gateway

1. Click the **Backup** tab.
2. Click **Manage settings locally on the device**.
3. Click **OK**.
4. Click **Publish** from the top toolbar.

Small Office Appliance Settings

For more about the Small Office Appliance settings, visit the *Check Point Support Center* and search for the appliance relevant to you.

Configuring DNS

Procedure

1. From the **Devices** window, double-click the Small Office Appliance object.

   The Security Gateway window opens.
2. Select the **DNS** tab.
3. Select **Use the following settings**.

The DNS settings open.

4. To manually configure the IP addresses:
   a. Select **Set DNS server configuration**.
   b. Enter the IP addresses for each DNS server which is used.
5. To use the DNS server of the ISP provider, select **Use DNS configurations provided by the active Internet connection**.
6. To use the Small Office Appliance as your default DNS proxy, select **Enable DNS Proxy - resolves local DNS requests**.
7. Click **OK**.

Configuring Interfaces

Configure the Small Office Appliance interfaces in the **Interfaces** tab in the Security Gateway window, then add a VLAN and configure a LAN Switch.

Configuring Interfaces in the Interfaces tab

1. From the **Devices** window, double-click the Small Office Appliance object.

   The **Security Gateway** window opens.
2. Select the **Interfaces** tab.
3. Select **Use the following settings**.

   The interface settings open.
4. Select the interface and click **Edit**.

   The **Edit** window opens.
5. From the IP Assignment section, configure the IP address of the interface:
   a. Select **Static IP**.
   b. Enter the **IP Address** and **Subnet Mask** for the interface.
6. Select **Enable Hotspot authentication** to allow
7. **To configure the DHCP settings for the interface**
   a. In the DHCP section, select **Enabled**.
   b. In **DHCP IP range**, enter the range of IP addresses that can be assigned to the DHCP clients.

c. In **Exclude IP range**, enter the range of IP addresses that are not assigned to the DHCP clients.

d. To configure an IP Relay agent, select **Relay**.

e. Enter the IP address for the IP Relay agent.

8. To configure the advanced parameters for the interface:
   a. To assign a MAC address to the interface, select **Override MAC Address**.
   b. Enter the new MAC address value.
   c. From **Link speed/Duplex**, select the bandwidth for the interface.
9. Click **OK**.

   The **Edit** window closes.
10. Optional: In the **Switch** section > **LAN Switch is active**, click **Activate** to configure a LAN switch (see *"Configuring a LAN Switch" on the next page*).
11. To configure the MTU (Maximum Transmission Unit) for all the interfaces that are not part of the LAN switch:
    - In the **Advanced** section, enter the new MTU value.
12. To enable the configured connection, select the interface and click **Enable**.

Adding a VLAN

You can add a new VLAN to a configured interface.

Create a VLAN (according to the IEEE 802.1q Standard) on one of the interfaces

1. From the **Devices** window, double-click the Small Office Appliance object.

   The Security Gateway window opens.
2. Select the **Interfaces** tab.
3. Click **New > New VLAN**.

   The Add VLAN window opens.
4. From **Interface**, select the interface to which the new VLAN is added.
5. Enter these parameters from the new VLAN:
   - **VLAN number**
   - **IP address**
   - **Subnet Mask**

6. To configure the DHCP settings for the new VLAN:
    a. From the DHCP section, select **Enabled**.
    b. In **DHCP IP range**, enter the range of IP addresses that can be assigned to the DHCP clients.
    c. In **DHCP Exclude IP range**, enter the range of IP addresses that are not assigned to the DHCP clients.
    d. To configure an IP Relay agent for the new VLAN, select **Relay**.
    e. Enter the IP address for the IP relay.
7. Click **OK**.

    The new VLAN is added to the interface.

Configuring a LAN Switch

Configure the Small Office Appliance as a LAN switch in the **Interfaces** tab in the Security Gateway window.

Title for collapsed Step 3-A

1. From the **Devices** window, double-click the Small Office Appliance.

    The Security Gateway window opens.
2. Select the **Interfaces** tab.
3. From the Switch section, click **Activate**.

    The Edit Switch window opens.
4. In the IP Assignment section, enter the **IP address** and **Subnet Mask** of the LAN switch.
5. To add an interface to the LAN switch:
    a. In the **Interfaces** section, select an interface from the **Available Interfaces** list.
    b. Click **Add**.
6. **To configure the DHCP settings for the LAN switch**
    a. From the DHCP section, select **Enabled**.
    b. In **DHCP IP range**, enter the range of IP addresses that can be assigned to the DHCP clients.

c. In **DHCP Exclude IP range**, enter the range of IP addresses that are not assigned to the DHCP clients.

d. To configure an IP Relay agent for the new VLAN, select **Relay**.

e. Enter the IP address for the IP Relay agent.

7. To assign a MAC address to the interface, in the Advanced section select **Override MAC Address** and enter the MAC address.
8. Click **OK**.

   The Edit Switch window closes and the switch is configured and activated.
9. The Switch section allows you to manage the LAN switch.
   - To disable the interfaces in the LAN switch, clear **Enable Interfaces**.
   - To deactivate the LAN switch, click **Deactivate**.

   Note - When the LAN switch is deactivated, the settings of all interfaces in the LAN switch are erased.
10. Click **OK**.

Configuring Internet Connection Types

You must configure a primary Internet connection, and you can configure a secondary one. When High Availability is activated, if there is a failover on the primary Internet connection, then the Small Office Appliance starts to use the secondary Internet connection.

These are the Internet connections:

- **Static IP** - A fixed (non-dynamic) IP address.

  Configuring a Static Internet Connection

  You can configure an Internet connection with a static IP address.

  1. From the **Devices** window, double-click the Small Office Appliance network object.

     The Security Gateway window opens.
  2. Select the **Internet** tab.
  3. Select **Use the following settings**. The Internet connection settings open.

4. Configure the primary Internet connection type:
   a. Select **Enable Primary Internet Connection**.
   b. Select whether the primary Internet connection is on the **WAN** or **DMZ**.
   c. From **Connection Type**, select **Static IP**.
5. Click **Configure**.

   The Primary Internet Configuration window for the Static IP Internet connection type opens.
6. In the IP Settings section, enter these IP address parameters:
   - **IP Address**
   - **Subnet Mask**
   - **Default Gateway**
7. In the DNS section, enter the IP addresses for the DNS servers.
8. In the WAN Port Settings section, enter these interface settings:
   - To configure the MTU (Maximum Transmission Unit) for the Internet connection, enter the new **MTU** value.

     Note - For a DMZ interface, the MTU value is applied to all LAN ports.
   - To assign a MAC address to the Internet connection, select **Override MAC Address** and enter the MAC address.
   - To configure the bandwidth for the Internet connection, select the appropriate option from **Link speed/Duplex**.
9. From the **Advanced** section, you can select **Use ICMP to monitor connection status** (see *"Configuring ICMP" on page 87*).
10. Click **OK**.

- **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network.

  Configuring a DHCP Internet Connection

  You can configure an Internet connection that uses DHCP to automatically assign IP addresses.

  1. From the **Devices** window, double-click the Small Office Appliance network object.

     The Security Gateway window opens.

2. Select the **Internet** tab.
3. Select **Use the following settings**. The Internet connection settings open.
4. Configure the primary Internet connection type:
   a. Select **Enable Primary Internet Connection**.
   b. Select whether the primary Internet connection is on the **WAN** or **DMZ**.
   c. From **Connection Type**, select **Obtain IP Address Automatically (DHCP)**.
5. Click **Configure**.

   The Primary Internet Configuration window for the DHCP Internet connection type opens.
6. In the WAN Port Settings section, enter these interface settings:
   - To configure the MTU (Maximum Transmission Unit) for the Internet connection, enter the new **MTU** value.

     Note - For a DMZ interface, the MTU value is applied to all LAN ports. .
   - To assign a MAC address to the Internet connection, select **Override MAC Address** and enter the MAC address.
   - To configure the bandwidth for the Internet connection, select the appropriate option from **Link speed/Duplex**.
7. From the **Advanced** section, you can select **Use ICMP to monitor connection status** (see *"Configuring ICMP" on page 87*).
8. Click **OK**.

- **PPPoE** - A network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.

  Note - It is not possible to configure internet connection over DSL for 1100, 1430, 1450 appliances using SmartProvisioning.

  Configuring a PPPoE Internet Connection

  You can configure an Internet connection that uses PPPoE protocol.

Basic Configuration

1. From the **Devices** window, double-click the Small Office Appliance network object.

   The Security Gateway window opens.

2. Select the **Internet** tab.
3. Select **Use the following settings**. The Internet connection settings open.
4. Configure the primary Internet connection type:
   a. Select **Enable Primary Internet Connection**.
   b. Select whether the primary Internet connection is on the **WAN** or **DMZ**.
   c. From **Connection Type**, select **Point-to-Point Protocol over Ethernet (PPPoE)**.
5. Click **Configure**.

   The General tab of the Primary Internet Configuration window for the PPPoE Internet connection type opens.

6. Enter these settings for your Internet Service Provider:
   - **User Name**
   - **Password**
7. In the WAN Port Settings section, enter these interface settings:
   - To configure the MTU (Maximum Transmission Unit) for the Internet connection, enter the new **MTU** value.

   Note - For a DMZ interface, the MTU value is applied to all LAN ports.

   - To assign a MAC address to the Internet connection, select **Override MAC Address** and enter the MAC address.
   - To configure the bandwidth for the Internet connection, select the appropriate option from **Link speed/Duplex**.
8. Click **OK**.

PPPoE Advanced Settings

You can configure the advanced settings for a PPPoE Internet connection. The advanced settings allow you to configure:

- IP settings for the tunnel
- How the Internet connection is started and maintained

1. From the **Primary Internet Configuration** window for PPPoE, select **Advanced**.

   The **Advanced PPPoE** window opens.

2. In the **Local Tunnel IP Assignment** section, enter these settings for the PPPoE tunnel:
   - **Obtain IP Address Automatically** - The IP address for the PPPoE tunnel is automatically configured (default setting).
   - **Use the Following IP Address** - Enter the static IP address that is used for the PPPoE tunnel.
3. In the **Connection Method** section, configure how the Small Office Appliance uses the PPPoE Internet connection:
   - **Auto Connect** - The Small Office Appliance automatically establishes a PPPoE connection to the Internet.
   - **Connect on Demand** - The Small Office Appliance Gateway establishes a PPPoE connection to the Internet when required.
   - **Disconnect Idle Time** - Enter the number of maximum number of idle minutes before the PPPoE Internet connection is disconnected.
4. In the **Monitor Connections** section, enter the PPPoE Echo requests settings:
   - **Monitor Connection Status Every** - Enter how often, in seconds, that PPPoE Echo requests are sent to the server.
   - **Assume Connection is Down After** - Enter the maximum number of failed PPPoE Echo requests before the PPPoE server is considered down.
   - From the **Advanced** section, you can select **Use ICMP to monitor connection status** (see *"Configuring ICMP" on page 87*).
5. Click **OK**.

- **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) is a method for implementation of virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
- **L2TP** - Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself. It relies on an encryption protocol that it passes within the tunnel to provide privacy.

Configuring an Internet connection that uses PPTP or L2TP protocol

1. From the **Devices** window, double-click the Small Office Appliance network object.

   The Security Gateway window opens.

2. Select the **Internet** tab.
3. Select **Use the following settings**. The Internet connection settings open.
4. Configure the primary Internet connection type:
   a. Select **Enable Primary Internet Connection**.
   b. Select whether the primary Internet connection is on the **WAN** or **DMZ**.
   c. From **Connection Type**, select **Point-to-Point Tunneling Protocol over Ethernet (PPTP)** or **Layer 2 Tunneling Protocol (L2TP)**.
5. Click **Configure**.

   The General tab of the Primary Internet Configuration window for the Internet connection type opens.

6. Enter these settings for your Internet Service Provider:
   - **Server Host Name or IP Address**
   - **ISP Login User Name**
   - **ISP Login Password**
7. In the WAN Port Settings section, enter these interface settings:
   - To configure the MTU (Maximum Transmission Unit) for the Internet connection, enter the new **MTU** value.

     Note - For a DMZ interface, the MTU value is applied to all LAN ports. .
   - To assign a MAC address to the Internet connection, select **Override MAC Address** and enter the MAC address.
   - To configure the bandwidth for the Internet connection, select the appropriate option from **Link speed/Duplex**.
8. Click **OK**.

PPTP or L2TP Advanced Settings

You can configure the advanced settings for a PPTP or L2TP Internet connection. The advanced settings allow you to configure:

- IP settings for the tunnel and the WAN
- How the Internet connection is started and maintained

1. From the **Primary Internet Configuration** window for PPTP or L2TP, select **Advanced**.

   The Advanced settings open.

2. In the **Local Tunnel IP Assignment** section, enter the settings for the tunnel:
   - **Obtain IP Address Automatically** - The IP address for the tunnel is automatically configured (default setting).
   - **Use the Following IP Address** - Enter the static IP address that is used for the tunnel.
3. In the **WAN IP Assignment** section, enter the IP address settings for the WAN:
   - **Obtain IP Address Automatically** - The IP address for the WAN is automatically configured (default setting).
   - **Use the Following IP Address** - Configure these settings for the WAN IP address:
     - **IP Address**
     - **Subnet Mask**
     - **Default Gateway**
4. In the **Connection Method** section, configure how Small Office Appliance uses the PPTP or L2TP Internet connection:
   - **Auto Connect** - Small Office Appliance automatically establishes a PPTP or L2TP connection to the Internet.
   - **Connect on Demand** - Small Office Appliance establishes a PPTP or L2TP connection to the Internet when required.
   - **Disconnect Idle Time** - Enter the number of maximum number of idle minutes before the PPTP or L2TP Internet connection is disconnected.

5. In the **Monitor Connections** section, enter the Echo request settings:
   - **Monitor Connection Status Every** - Enter how often (in seconds) that Echo requests are sent to the server.
   - **Assume Connection is Down After** - Enter the maximum number of failed Echo requests before the server is considered down.
   - From the **Advanced** section, you can select **Use ICMP to monitor connection status** (see *"Configuring ICMP" below*).
6. Click **OK**.

When you have enabled both Internet connections, you can configure High Availability to revert back to the primary Internet connection.

You can configure the ICMP (Internet Control Message Protocol) settings for the Internet connection. You can specify servers that receive ICMP requests to monitor the status of the Internet connection. If you enabled High Availability, the Small Office Appliance can activate the other Internet connection when necessary.

Configuring ICMP

1. From the **Devices** window, double-click the Small Office Appliance.

   The Security Gateway window opens.
2. Select the **Internet** tab.
3. From the required Internet connection, click **Configure**.

   The Internet Configuration window is opens.
4. From the Advanced section or tab, select **Use ICMP to monitor connection status**.
5. Click **Configure**.

   The ICMP Settings window opens.
6. To monitor a server:
   a. Click **Add**.
   b. Enter the host name or IP address of the server.
   c. Repeat these steps for all the servers that are monitored.
   d. Select **Send ICMP requests to the following servers**.
7. To monitor the default gateway, select **Send ICMP requests to default gateway**.
8. Enter these ICMP connection monitoring settings:

a. **Interval Between** - Enter the number of seconds between each ICMP request.

b. **Failover After** - Enter the maximum number of failed ICMP requests. When High Availability is active, after an ICMP failover the other Internet connection becomes active.

c. **Resume Requests After** - Enter the number of seconds after an ICMP failover that ICMP requests are resumed.

9. Click **OK**.

Configuring Routing Settings

You must configure Small Office Appliance interfaces before you configure the routing settings. The routing configurations are not the same for all interfaces.

You cannot add a default route from the **Routing** tab. The default route of the system is the same as the default gateway that is configured for the Internet connection (see *"Configuring Internet Connection Types" on page 80*). If Internet Connection High Availability is active, the default route automatically changes to the default gateway of the other Internet connection. When there is no active Internet connection and no default route is active, this message is displayed:

```
Note: There is no default route since no Internet connection is
enabled.
```

You can configure Small Office Appliance to automatically select the interface or gateway that is used for a route. You cannot select the **Automatic** option for both the interface and the gateway.

Configuring a Network Route

You can use SmartProvisioning to configure network routes for Small Office Appliances. Use a network route to configure routing for an internal network.

1. In the **Devices** window, double-click the Small Office Appliance.

   The Security Gateway window opens.

2. Select the **Routing** tab.

3. Select **Use the following settings**.

   The Routing settings open.

4. Click **Add** and select **Network Route**.

   The Routing window opens.

5. In **Destination IP Address**, enter the IP address of the network.

6. In **Destination Netmask**, enter the netmask for the destination IP address.

7. From **Interface**, select a configured interface for the route.
8. In **Gateway**, enter the IP address of the gateway that provides access to the route.
9. In **Metric**, enter the number of hops to the destination.

   Note - This value must be accurate. A metric that is too low can cause lost communications because of looping. A metric that is too high can cause security issues.
10. Click **OK**.

Configuring a Host Route

You can use SmartProvisioning to configure host routes for Small Office Appliances. A host route configures access to a specific host.

1. In the **Devices** window, double-click the Small Office Appliance object.

   The Security Gateway window opens.
2. Select the **Routing** tab.
3. Select **Use the following settings**.

   The Routing settings open.
4. Click **Add** and select **Host Route**.

   The Routing window opens.
5. In **Destination IP Address**, enter the IP address of the host.
6. From **Interface**, select a configured interface for the route.
7. In **Gateway**, enter the IP address of the gateway that provides access to the host.
8. In **Metric**, enter number of hops to the destination host.

   Note - If the host is on your local site, the metric must be a low number. If the host is not behind routers, the metric must be zero.
9. Click **OK**.

Configuring Firmware Installation Settings

You can use SmartProvisioning to manage the firmware installation settings for Small Office Appliances.

You can select the firmware image to install on your Security Gateway. The firmware images that are shown in the list were uploaded through SmartUpdate. If firmware installation fails, the Security Gateway reverts to its state before installation. The list shows the details of the firmware image. These include the Name, Vendor, Major Version, Minor Version, Build Number, and Description.

You can install the firmware with one of these options:

- Immediately - Downloads and installs the firmware immediately after saving these settings in the next synchronization with a Security Gateway assigned to this profile.
- According to time ranges - You can define download and installation time ranges for the firmware image. You can limit the download and installation time to a specified list of time ranges in the week. They will start at the nearest time range after the firmware settings are applied. For example, if the firmware installation settings are applied on Sunday and there are two time ranges:
  - One range is set to Friday 00:00 to Saturday 00:00
  - One range is set to Wednesday 23:00 to Thursday 06:0

    The firmware will be installed between Wednesday 23:00 and Thursday 06:00.

    If that the Security Gateway fails to download and or install the firmware during the nearest time range, it tries again in the next time range.

Configuring Procedure

1. In the **Devices** window, double-click the Small Office Appliance object.

   The Security Gateway window opens.
2. Select the **Firmware** tab.
3. Select **Use the following settings**.

   The Firmware settings open.
4. In **Firmware image**, click **Select** to select a firmware image that was uploaded through SmartUpdate.
5. In **SmartLSM Profile after installation**, select a related SmartLSM profile from the list that can be installed for the selected firmware image and its supported versions.
6. Select one of the options to install the firmware:

a. **Immediately**

b. **According to these time ranges** - Select to use the Security Gateway time or local time.

- **Add/Edit** - Click Add or Edit to open the Time Range window to define or change the weekdays and times for download and installation of the firmware image. Select the days and times.
- Click **OK**.
- **Remove** - Select a range from the list and click **Remove** to delete a time range.
- **Download image immediately** - Click this option to download the firmware image immediately but install the image during one of the set time ranges.

7. Click **Show profile settings** - to see the settings of the Provisioning Profile that this gateway references.
8. Click **OK**.

Configuring a RADIUS Server

You can configure the RADIUS server (Remote Authentication Dial In User Service) that provides authentication, authorization, and accounting for Small Office Appliance gateways. You can configure RADIUS in the Provisioning Profile once for all gateways assigned to this profile. The RADIUS server must be already defined as a SmartConsole object.

You can configure your appliance to contact more than one RADIUS server. If the first server in the list is unreachable, the next RADIUS server in the list is contacted to authenticate with. If the list is empty, the RADIUS option is turned off on the Security Gateway.

Procedure

1. In the **Devices** window, double-click the Small Office Appliance object.

   The Security Gateway window opens.
2. Select the **RADIUS** tab.
3. Select **Use the following settings**.
4. Click **Add** to add RADIUS servers that were defined in SmartConsole, select a RADIUS server from the list.
5. Click **OK**.
6. To remove a server, select a server in the list and click **Remove**.
7. Use **Up/Down** to set the priority used for contacting RADIUS servers.

8. Click **Allow administrators from specific RADIUS groups only (comma separated)** to allow authentication from specified groups as defined on the RADIUS server. Only administrators which belong to those groups can get access.
9. Click **OK**.

Common Gateway Management

SmartProvisioning can manage SmartLSM Security Gateways, Provisioned Gateways, and CO gateways on Security Gateway devices of any supported platform and operating system.

This chapter explains concepts and procedures that are common to all SmartProvisioning managed gateways.

Before you begin, make sure that your administrator user name has Write permissions for SmartLSM Gateway Database (see *"Defining SmartProvisioning Administrators" on page 15*).

Immediate Gateway Actions

At any point during configuration or management of a gateway, you can do a number of immediate actions on the gateway. Some actions are for Provisioned gateways only, some are applicable only for SmartLSM Security Gateways, and some only for SmartLSM Security Gateways on non-Edge devices.

Accessing Actions

This section describes how to use the features available from the **Actions** menu.

To open the **Actions** menu, do one of the following:

- From the main menu, click **Actions**.
- Right-click a **Provisioning Profile** and select **Actions**.
- Right-click a gateway and select **Actions**.
- In a Gateway window, click **Actions**.

Controlling Remote Gateways

You can manage remote gateways with SmartProvisioning. You can start, stop, and restart the Check Point Security Gateway services, and you can reboot devices. This is true for all types of SmartProvisioning gateways.

Remote Actions on Check Point Services and Gateways

Updating Corporate Office Security Gateways

The CO gateway is the center of the Star VPN Community, in which SmartLSM Security Gateways are the satellites. It is important to update the CO Security Gateway when SmartLSM Security Gateways are added, deleted, or modified (such as the generation of a new IKE key, a Push Policy action, or a Push Dynamic Objects action).

To update a CO gateway:

1. Click the **Update Corporate Office Gateway** toolbar button: 
2. From the **Corporate Office Gateway** drop-down list, select the CO Security Gateway.
3. Click **OK**.

After you create the SmartLSM Security Gateway object, update the Corporate Office Security Gateway. If the VPN option was selected in the VPN Properties page, the Certificate Authority issues a certificate to the appliance. This certificate is installed on the appliance the first time that the SmartLSM Security Gateway connects to the Security Management Server.

Deleting Security Gateway Objects

If you delete a SmartLSM Security Gateway as a SmartProvisioning object, this revokes all certificates of the Security Gateway.

To delete a SmartLSM Security Gateway:

In the SmartProvisioning work space, right-click the gateway and select **Delete SmartLSM Security Gateway**.

You can delete provisioned gateways in SmartConsole.

Editing Gateway Properties

Opening the Gateway window

The Edit window for gateways is different for each type, but is opened in the same way.

1. In the tree, click **Devices**.
2. Do one of these actions:
   - In the **Devices** work space, double-click the gateway you want to edit.
   - In the **Devices** work space, right-click the gateway and select **Edit Gateway**.
   - Click the **Edit Gateway** toolbar button.

Note - Gateway windows for non-SmartLSM Security Gateways (without a SmartLSM Security Profile) show only the **General** tab, until you select **Enable Provisioning**. Then they show all tabs.

Gateway Comments

You can view the properties that define a gateway in the **General** tab of the **Gateway** window. You can also edit some of the properties.

- You cannot change the **Name** of the gateway after you add it to SmartProvisioning.
- The **Comments** field displays comments that were added when the gateway object was created in SmartConsole. If the gateway is a SmartLSM Security Gateway, you can edit the comments here. If the gateway is a Provisioned gateway or a CO gateway, this field is Read-Only.

Changing Assigned Provisioning Profile

You can manage SmartProvisioning gateways with Provisioning Profiles. At any time, you can change the Provisioning Profile that is assigned to a gateway.

To change the assigned Provisioning Profile:

1. Open the Gateway window and select the **General** tab.
2. Make sure the **Enable Provisioning** is selected.
3. Select **Provisioning Profile**, and select a profile from the drop-down list.
4. Click **OK**.

Configuring Interfaces

You can manage the interfaces of the individual gateway through SmartProvisioning. This is not available for Provisioning Profiles, because the interface configuration is different for each device.

Note - SmartLSM Security Gateways: In the **Gateway Topology** page, if **All IP addresses behind the gateway based on Topology information** is selected, the VPN Domain is based on the interfaces configured in this procedure.

Changes to the interface configuration of a SmartLSM Security Gateway always affect its VPN Domain. This is true even if Provisioning is disabled or the **Manage settings locally** option is selected in the **Interfaces** page.

Adding an interface to the gateway's configuration

1. Click **Actions** > **Get Actual Settings**.

   Note - For IP Appliances:
   The interface configuration for these appliances is complex. To prevent mistakes, you must first select **Get Actual Settings**, to upload the existing interfaces. IP Appliance interfaces are available for management (add, edit, delete) only after this action is done.
   For other gateways, this step is optional.

2. In SmartProvisioning, open the Gateway window and select the **Interfaces** tab.

- To manage the interfaces locally on the device, select **Manage settings locally on the device**. This way, changes in SmartProvisioning do not affect the device.
- To configure interfaces through SmartProvisioning, which overrides the local settings, select **Use the following settings**.

The configuration options are different for **Security Gateway** or **Small Office Appliance**.

If **Use the following settings** is selected, the Interface configuration options are available.

3. Click **Add**.

   A menu of interface types opens. Select an interface type. This menu is different for Security Gateways, Small Office Appliance, and IP Appliances. The window that opens is different for each selected interface.

4. Enter the required data.
5. Click **OK**.

Applying interface configuration changes

1. The device is updated with new configurations on a time interval. To immediately apply these settings to the gateway, select **Actions** > **Push Settings and Actions**.
2. To update the CO gateway with the new VPN Domain, click on **Update Corporate Office Gateway**.

Executing Commands

You can run the executables or shell commands on a managed Security Gateway with **Custom Commands**.

For example, if you want to check the connection between the SmartProvisioning console and a gateway, you can create a command that pings the selected gateway: **Executable** = **ping**; **Parameter** = <**IP**>. When you execute this command on a gateway, the terminal window of the console opens and runs the Ping command.

Preparing a custom command

1. Select **Manage** > **Custom Commands**.
2. Click **Add**.

   The **Add New Custom Command** Window opens.

3. Provide a name for your command.

4. Provide the command or pathname of the executable.
5. If parameters are needed, provide them here.
6. If the parameters include the local IP address or host name, click **Variables** and select **Object IP Address** or **Object Name**.
7. Click **OK**.

   The new custom command is added to the **Custom Commands** list.
8. Select the commands that you want to use.

Executing a prepared custom command

1. Right-click a gateway in the **Devices** work space.

   Custom Commands is added to the standard right-click menu.
2. Select **Custom Commands** and then the command that you want to execute.

Managing SmartLSM Security Gateways

This section describes how to manage SmartLSM Security Gateways.

Immediate SmartLSM Security Gateway Actions

At any point during the configuration or management of a SmartLSM Security Gateway, you can perform immediate actions on the gateway.

Applying Dynamic Object Values

SmartLSM Security Profiles implement a Security Policy, with rules for source/destination IP addresses, and localize these rules for each SmartLSM Security Gateway assigned to the profile. SmartProvisioning manages **Dynamic Objects** (see *"Dynamic Objects" on page 133*) only for SmartLSM Security Gateways.

Example

The Security Policy assigned to the SmartLSM Security Profile has a rule to drop traffic from IP addresses on a StormCenter. The Security Profile is assigned to ten SmartLSM Security Gateways. Some of the SmartLSM Security Gateways assigned to this profile must use one StormCenter site, and others use a different one. You do not have to create a new rule for each gateway. You can create one rule in the main policy, and use the **CPDShield** dynamic object to define the source (StormCenter list of IP addresses to block).

In SmartProvisioning, on each SmartLSM Security Gateway assigned to this profile, you resolve the CPDShield dynamic object to the real IP address of a StormCenter (double-click a SmartLSM Security Gateway and open **Dynamic Objects** > **Add**).

After you resolve the dynamic object to a real IP address value, it is not applied immediately to the selected SmartLSM Security Gateway. You can wait for the gateway to fetch its profile, but if you want the value to be applied immediately, you can push the resolved values of dynamic objects to the SmartLSM Security Gateway.

To apply new values to dynamic objects of a SmartLSM Security Gateway:

Right-click the gateway and select **Actions** > **Push Dynamic Objects**.

Getting Updated Security Policy

If you change the Security Policy assigned to a SmartLSM Security Profile in SmartConsole, and install it on gateways, it is not applied to SmartLSM Security Gateways. Each SmartLSM Security Gateway fetches its SmartLSM Security Profile on a different time interval, and then gets the updated Security Policy.

You can apply the changes immediately by pushing the policy on the SmartLSM Security Gateway. To do this, right-click the Security Gateway and **Actions** > **Push Policy**.

Common SmartLSM Security Gateway Configurations

This chapter explains management concepts and procedures that are common to all SmartLSM Security Gateways.

You must have Write permissions for **SmartLSM Gateway Database**.

The edit window is different for each type of SmartLSM Security Gateway, but is opened in the same ways.

Opening the SmartLSM Security Gateway window

1. In the tree, click **Devices**.
2. Do one of the these actions:
   - Click the **Edit Gateway** toolbar button.
   - In the **Devices** work space, double-click the gateway you want to edit.
   - In the **Devices** work space, right-click the gateway and select **Edit Gateway**.
   - From the **Edit** menu, when the gateway is selected in the work space, click **Edit Gateway**.

Changing Assigned SmartLSM Security Profile

You can change the SmartLSM Security Profile that you assign to a SmartLSM Security Gateway.

Note - If the assigned SmartLSM Security Profile was changed in SmartConsole, do this procedure to make sure that the changes are applied immediately.

To apply a change in SmartLSM Security Profile:

1. In SmartConsole, edit the Security Policy as needed and install it on the SmartLSM Security Profile.
2. In SmartProvisioning, open the **Gateway** window, and select the **General** tab.
3. From the **Security Profile** drop-down list, select the SmartLSM Security Profile.
4. Click **Actions** > **Push Policy**.

Managing SIC Trust on SmartLSM Security Gateways

Verifying SIC Trust on SmartLSM Security Gateways

You can view and edit the status of the Secure Internal Communication Trust between the Security Management Server or Domain Management Server and the SmartLSM Security Gateway. SIC Trust is established after a certificate is issued by the management server and delivered to the SmartLSM Security Gateway.

To check the SIC Trust of a SmartLSM Security Gateway:

1. Double-click a SmartLSM Security Gateway.
2. In the **General** tab, find the **Secure Internal Communication** > **DN** field.

   This is the SmartLSM Security Gateway's Distinguished Name (SIC name)

   syntax: `CN=gw-name, O=Management-domain-name`

   If it is empty, change the SIC certificate state.
3. Click **Communication**.
4. Check the value of the **Certificate state** field. This field shows the status of the SIC trust between this SmartLSM Security Gateway's and the Security Management Server or Domain Management Server.
   - **Initialized** - Indicates that the SmartLSM Security Gateway has a valid SIC certificate (it is possible that the Security Gateway is not connected).
   - **Uninitialized** - Indicates that the SmartLSM Security Gateway does not have a valid SIC certificate (because it was never initialized, or its certificate was revoked).

Initializing SIC Trust on SmartLSM Security Gateways

If the **Certificate state** is set to **Uninitialized**, and the IP address of the SmartLSM Gateways & Servers is entered, you can initialize the SIC trust now. Perform this procedure if the **Generate** button is available.

To initialize a SIC trust:

1. Click **Generate** to generate a one-time password, or provide a one-time password.
2. Click **Initialize**. A new SIC certificate is created for this SmartLSM Security Gateway, and its certificate state becomes **Initialized**.

Pulling SIC from Security Management Server

If no **IP address** is entered, you must pull the SIC certificate from the Security Management Server or Domain Management Server with the Check Point Configuration tool (cpconfig).

To initialize a SIC trust if the Security Management Server or Domain Management Server cannot find the gateway:

1. Open **cpconfig** > **Secure Internal Communication (SIC)** on the Security Management Server or Domain Management Server and on the SmartLSM Security Gateway.
2. Copy the SIC password.
3. On the gateway, provide the password of the Security Management Server or Domain Management Server.
4. Restart Check Point services on the gateway.

Resetting Trust on SmartLSM Security Gateways

You may want to reset an established SIC Trust if you replaced the gateway host machine, or if you lost the Activation Key.

From the time that you reset SIC until trust is re-established, the internal communications between the Check Point applications, the management server, and the managed devices is down. This procedure revokes the current certificate and provides a new one. Therefore, it is recommended that you continue only if you are sure that SIC must be reset. After you complete this procedure, quickly re-initialize SIC trust.

To reset a SIC trust:

1. In the **Communication** window, click **Reset**

   A message asks for confirmation: **Are you sure you want to reset SIC?**

If you reset the SIC certificate now (revoke current license and get a new one), internal communications between Check Point applications, Security Management Server/Domain Management Server, and managed devices can be adversely affected. Continue only if you are sure this must be done.

2. If you are ready to reset SIC now, click **Yes**.
3. On the SmartLSM Security Gateway, open the **Check Point Configuration tool** > **Secure Internal Communication** tab, and click **Reset**.
4. Reboot the SmartLSM Security Gateway.

Tracking Details for SmartLSM Security Gateways

The **Details** tab of the Gateway window provides identification information for log tracking and cluster usage.

You can edit the ID of the gateway device and add detailed notes for easier network management.

- **SmartLSM ID**: Unique ID, in the form of an IP address, per-SmartLSM Security Gateway. When the SmartLSM Security Gateway sends logs to a Log Server, the logs are stored by an Origin IP, which is this SmartLSM ID. This allows consistent tracking of the SmartLSM Security Gateway's logs, even if its external IP address changes. This ID cannot be edited.
- **Device ID**: Often used to hold a SmartLSM Security Gateway's MAC address. This field accepts free text. Use this field to note the machine ID, in the best format for the environment and the SmartLSM Security Gateway.
- **Domain Details**: Often used to contain environment details of the SmartLSM site, which can be especially useful if the SmartProvisioning administrators are not familiar with the remote office.

Configuring Log Servers for SmartLSM Security Gateway

When you create a SmartLSM Security Profile for Security Gateway gateways in SmartConsole, you can also configure the log servers. In SmartProvisioning you can edit the log server configuration. You can select different log servers for a selected gateway, but the servers must already be defined in SmartConsole.

Changing log servers of SmartLSM Security Gateways

1. From the **Devices** pane, double-click the Security Gateway.

   The window opens and shows the **General** tab.
2. Click the **Advanced** tab.
3. Clear **As defined in SmartLSM Profile**.
4. Select the log servers for this SmartLSM Security Gateway:
   - **Send logs to** - Select the primary log server for this gateway.
   - **When unreachable, send logs to** - Select the alternative log server.

SmartLSM Security Gateway Licenses

You have a License Repository with the licenses that you acquired for your environment. You can manage the licenses of the SmartLSM Security Gateways through SmartProvisioning.

Uploading Licenses to the Repository

SmartLSM Security Gateway licenses are available for SmartProvisioning management if they are in the License Repository on the Security Management Server or Domain Management Server.

To upload licenses to the repository:

1. Open SmartUpdate and go to **Licenses and Contracts** > **Add License**
2. Select a source location.
3. Browse to the file.
4. Click **Open**.

   The license is added to the License Repository.

Attaching License to SmartLSM Security Gateways

To attach a license to a SmartLSM Security Gateway:

1. Open the **SmartLSM Security Gateway** window, and select the **Licenses** tab.
2. Click **Add**.

A list shows with the licenses in your License Repository which are not attached to any gateway. If an original license is used on another SmartLSM Security Gateway, you will not see the corresponding upgraded license in the License Repository.

3. Select the licenses to appear in this gateway's **Licenses** window. You can select more than one license at a time.
4. Click **OK**.

   The license attached to this gateway is added to the **Licenses** list.
5. In the Gateway window, Click **OK**.

   The license operations, attachment or detachment, are performed immediately. The **License Operation** message appears:

   Attaching/Detaching Licenses. Please wait...

License State and Type

The state of the license depends on whether the license is associated with the Security Gateway in the License Repository, and whether the license is installed on the remote Security Gateway.

- **Unattached**: Not associated with the Security Gateway in the License Repository, and not installed on the remote Security Gateway.
- **Engaged**: Associated with the Security Gateway in the License Repository, but not installed on the remote Security Gateway.
- **Attached**: Associated with the Security Gateway in the License Repository, *and* installed on the remote Security Gateway.

The type of license depends on the IP address enabled in the license. If the IP address is of this gateway, the license type is *Local*. If the IP address is of the Security Management Server or Domain Management Server, the license type is *Central*.

Handling License Attachment Issues

- If there are unattached licenses that belong to the SmartLSM Security Gateway, a message is displayed in the **Licenses** tab. In general, this situation occurs after you run the License Upgrade Tool. Click **Add these licenses to the list**. The upgraded and unattached licenses are disabled.
- To remove an existing license from the **Licenses** list, select it and click **Remove**. The license will be detached from the SmartLSM Security Gateway after you click **OK**.
- You cannot have an upgrade license attached to a SmartLSM Security Gateway while the corresponding original license is detached and exists in the License Repository.

- If you try to remove the original license from the gateway, while the upgrade license is listed, you will receive a warning that if you proceed, both licenses will be removed. If you click **OK**, both licenses are removed from the gateway.
- If you try to remove the upgrade license from the gateway, while the original license is listed, a notification shows, which indicates that you can remove only the upgrade license or both licenses.
- If both the original and the upgrade license are in the **License Repository,** and you try to add the upgrade license to the gateway, a notification shows, which indicates that if you proceed, both licenses will be added to the gateway.

Configuring Topology for SmartLSM Security Gateways

You can manage the topology of SmartLSM Security Gateways through SmartProvisioning. View and change the internal and external interfaces of each gateway to fit its local environment.

Configuring the topology of a SmartLSM Security Gateways

1. From the **Devices** pane, double-click the Security Gateway.

   The window opens and shows the **General** tab.

2. Click the **Topology** tab.
3. Select the option that best describes the VPN Domain of this SmartLSM Security Gateway:
   - **Not defined** - No VPN is defined for this gateway. To enable this Gateway to participate in a VPN, select a different option.
   - **Only the external interfaces** - The external IP addresses of the SmartLSM Security Gateway is the entire VPN domain. The CO gateway connects to the remote office nodes only through the SmartLSM Security Gateway. The nodes are usually connected and secured by NAT.
   - **All IP Addresses behind the Gateway based on Topology information** - SmartProvisioning automatically calculates the encryption domain based on the IP address and net mask of the SmartLSM Security Gateway's internal interfaces.
   - **Manually defined**: You can define the VPN domain manually. The range table is enabled.

Configuring a VPN Domain

Complex networks behind SmartLSM Security Gateways cannot be properly configured as VPN domains by the automatic calculation option (**All IP Addresses behind the Gateway based on Topology information**). If the SmartLSM Security Gateway topology consists of one type (Meshed or Star) and does not include subsequent firewalls, you may select the automatic option. Otherwise, it is recommended that you select **Manually defined**.

To manually configure a VPN domain:

1. In the **Topology** tab, click **Manually defined**.
2. Click **Add**.

   The **IP Address Range Configuration** window opens.
3. Enter the range of IP addresses that define a network behind this gateway.
4. Click **OK**.
5. Repeat these steps and add IP address ranges for the VPNs that connect to the CO gateway.
6. Select **Actions** > **Push Policy**.

   You are prompted to save the data and then SmartProvisioning validates the topology you defined.

   If successfully validated, the topology is immediately pushed to the gateway.
7. Update the CO gateway.

   The IP addresses in this range are now part of the VPN domain that is secured by the SmartLSM Security Gateway and that tunnels to the CO gateway.

   To complete the VPN configurations, see *"Configuring VPNs on SmartLSM Security Gateways" on page 115*.

Managing Software on SmartLSM Security Gateways

You can manage the software installed on SmartLSM Security Gateways and standard Security Gateways. The Package commands are available from the **Actions** menu and the Package toolbar buttons.

These commands are not available for Small Office Appliances . To centrally manage the firmware of Small Office Appliances, use the **Firmware** tab. (see *"Configuring firmware installation settings on a Provisioning Profile for Small Office Appliances" on page 58*)

Uploading Packages to the Repository

Upload Security Gateway software packages to the SmartProvisioning Package Repository on the Security Management Server or Domain Management Server.

Procedure

1. Open SmartUpdate:

   In SmartConsole, click **Menu** > **Manage licenses and packages**.

2. From the menu bar, select **Packages** > **Add** and select a source:

   - **From Download Center** - Enter your user name and password for the Check Point Download/User Center. When your credentials are authenticated, the **Get Packages from Download Center** window opens, which displays the packages that are available to you. Select the ones you want and click **Download**.
   - **From CD/DVD** - Insert the CD or DVD with the package into the appliance or server. Browse to the DVD with the TGZ files that you are adding to the repository, and then click **OK**.
   - **File** - Browse to the TGZ files that you are adding to the repository, and then click **OK**. The software package is added to the Package Repository.

Viewing Installed Software

You can view the Check Point software packages installed on a gateway. Such packages include Security Gateway upgrades, Check Point Hotfixes that are relevant for the installed version, and Check Point HFAs.

Procedure

1. From the **Devices** pane, double-click the Security Gateway.

   The window opens and shows the **General** tab.

2. Click the **Packages** tab.

   The operating system of the Security Gateway, and all installed Check Point packages are listed.

Verifying Pre-Install

Before you install a Check Point software package on a Security Gateway, you can test if the package is compatible with the selected Security Gateway.

Procedure

1. In the **Devices** work space, select a Security Gateway.
2. From the menu bar, select **Actions** > **Packages** > **Pre-Install Verifier**.

   A message appears: **Getting targets for install. Please wait...**

   If there are packages in the Package Repository (see *"Uploading Packages to the Repository" on the previous page*) the **Verify Installation** window opens.
3. Select a listed package and click **Verify**.

   In the **Status View** > **Action Status**, see the verification phases in the **Details** column:

   - Checks connection between Security Gateway and Security Management Server or Domain Management Server.
   - Checks for sufficient disk space on the Security Gateway.
   - Checks that the package is not already installed.
   - Checks compatibility of package with operating system and currently installed packages.

   If the package is verified for the selected Security Gateway, the **Status** column shows **Completed**, and the **Details** column shows:

   '<package>' is compatible with installed packages

Upgrading Packages with SmartProvisioning

Use the **Upgrade to Management Version** features to upgrade devices for a new version of the Security Gateway software.

Procedure

1. In the work space, select the Security Gateway.
2. From the menu bar, select **Actions** > **Packages** > **Upgrade to Management Version**.

   If there are packages in the Package Repository (see *"Uploading Packages to the Repository" on the previous page*) installed packages are upgraded to the latest available version.

   If required packages are missing, they are listed in the **Missing Packages** window.

   Use SmartUpdate to add the missing packages, and rerun **Upgrade to Management Version**.

Distributing Packages with SmartProvisioning

Use the **Distribute Packages** feature to distribute Check Point Hotfixes and HFAs to the Security Gateways that can be enhanced by installing the package.

Procedure

1. In the work space, select the Security Gateway.
2. Verify that the package you want to distribute is available and appropriate for the selected Security Gateway (see *"Verifying Pre-Install" on page 107*).
3. From the menu bar, select **Actions** > **Packages** > **Distribute Packages**.

   A warning opens, which explains that using **Distribute Packages**, rather than **Upgrade All**, may lead to a mismatch between versions and malfunctions.

   To prevent this issue, make sure to use *Distribute* for Hotfix and HFA installations, not for upgrading to a new version.
4. If you want to continue with this procedure, click **OK**.

   If there are packages in the Package Repository (see *"Uploading Packages to the Repository" on page 107*), the **Distribute Package** window opens.
5. Select a package from the list.
6. In the **Choose action** section, select an action:
   - **Distribute and install packages** - Download selected packages from the Package Repository and install them on the selected gateway.
   - **Only distribute packages** - Download selected packages from the Package Repository to the selected Security Gateway, but do not install them yet.
   - **Install previously distributed packages** - Install packages that were previously distributed to the selected Security Gateway.
7. If you want the Security Gateway to automatically reboot after the installation, if the installation requires this, select **Allow reboot if required**.
8. Select **Backup image for automatic revert** (available only for Security Gateways). Clear this option only if disk space is a real issue.

   The image creation can take some time.
9. If **Change to a new profile after install** is enabled, you must select an appropriate SmartLSM Security Profile for the Security Gateway from the drop-down list.

   This field is enabled, and required, only if the change is necessary.
10. Click **Start**.

Security Gateway Actions on SmartLSM Security Gateways

You can execute immediate actions on SmartLSM Security Gateways and Provisioned Security Gateways.

You can run these actions on individual Security Gateways, or on a Provisioning Profile, which effectively runs the action on all Security Gateways assigned to this profile.

Before you begin, make sure that your administrator has permissions to **Run Scripts**.

Viewing Status of Remote Security Gateways

You can get an instant view of the status of a Security Gateway: traffic, interfaces, performance, CPU, memory, and so on.

To view status details of a selected Security Gateway:

1. Make sure an administrator is logged into the Security Gateway.
2. Select **Actions** > **Get Status Details**.

Running Scripts

You can execute complex gateway commands with your own scripts on any provisioned gateway.

Before you begin, make sure that your administrator has permissions to run scripts.

Running Scripts on Individual Security Gateways

Procedure

1. Right-click a [SmartLSM] Security Gateway and select **Actions** > **Run Script**.
2. In the **Run Script** window, provide your script.
   - If you have the script in a file, select **Load Script** and then browse to the file.
   - You can type a script into the text box, or paste it in from another source.
3. Click **Run Script**.

   The script is pushed to the gateway and runs immediately. See the **Action Status** tab of the **Status** pane to view the details of the push and execution.

The **Result** pane displays the results of the script, **0** for success and **other value** for failure.

4. To save the script to a file, click **Save Script**.

Running Scripts by Profiles

The Run Script feature lets you use a Security Gateway Provisioning Profile to run scripts on multiple Security Gateways.

Procedure

1. In the tree in the main window, select **Profiles**.
2. Select a Provisioning Profile and from the menu bar select **Actions** > **Run Script**.
3. In the Run Script window, provide your script.
   - If you have the script in a file, select **Load script** and then browse to the file.
   - You can type a script into the text box, or paste it in from another source.
4. Click **Run Script**. The script is pushed to all the gateways that use this profile.

   See the **Action Status** tab of the Status pane to view details of the push and execution.

   The **Result** pane displays the results of the script, **0** for success and **other value** for failure.
5. To save the script to a file, click **Save Script**.

Immediate Backup of Security Gateways

You can create a backup image of Security Gateways and SmartLSM Security Gateways. You can do this with the Action command on the Security Gateway, or use a Provisioning Profile to create a backup image on all gateways assigned to the profile.

You can select to store backups on the Security Gateway, or on another backup server. If you select another server, make sure you have the IP address or host name of that server, and if needed, a user name and password with Read/Write permissions.

To execute an immediate backup of a Security Gateway:

1. Right-click a **[SmartLSM] Security Gateway** or a Provisioning Profile, and select **Actions** > **Backup**.
2. If you want the backup to include Check Point logs, select **Include Check Point products log files in the backup**.

3. Provide details of the device on which the backup will be stored, or select **Locally on device**, to store the backup file on each device.
4. Click **OK**.
5. Select **Actions** > **Push Settings and Actions**.

   The backup is created and pushed to the Security Gateway or defined server. See the documentation of the target's operating system for Restore Backup instructions.

Applying Changes

If you make a change to a Security Gateway Provisioning Profile, or use the **Actions** > **Backup** command, no change or action is immediately applied to the Security Gateways.

Profile changes are applied to the Security Gateways assigned to them when the Security Gateways fetch their profiles on interval. At this time, the Security Gateways get the commands to pull the scripts from SmartProvisioning and execute them, or to create backup images.

However, you sometimes need to apply profile changes and actions immediately. For example, if you run a script that configures a new server behind a SmartLSM Security Gateway, you want to apply this configuration as quickly as possible, to include the server in the Security Gateway's VPN with the CO Security Gateway.

To apply profile changes and actions immediately:

Right-click the Provisioning Profile and select **Actions** > **Push Settings and Actions**.

Maintenance Mode for SmartLSM Security Gateways

Enable **Maintenance Mode** on a Security Gateway when you test changes to its object configuration or Provisioning Profile. In this mode, changes are pushed from the SmartProvisioning console to the Security Management Server or Domain Management Server, but they are not pushed to the gateway.

Example

A SmartLSM Security Gateway on your SmartProvisioning management has operational issues. The SmartLSM Security Gateway is in a remote office which is too far away for you to manage yourself, so you ask the local system administrator to handle the issue.

However, you do not want the gateway to lose the configurations that you already made to it from your central SmartProvisioning console. Therefore, enable **Maintenance Mode** on this gateway.

The local administrator fixes the issue. You disable Maintenance Mode, which switches the SmartLSM Security Gateway back to centralized configuration through the SmartProvisioning console.

Note - When you disable **Maintenance Mode**, the central SmartProvisioning configurations override any local changes. If the local administrator discovers that changes need to be made on this gateway, make sure you have the data before you switch back.

To enable Maintenance Mode:

Right-click a Security Gateway, and select **Actions** > **Turn on maintenance mode**.

Notes:

- Changes to the Provisioning Profile do not affect the gateway as long as **Maintenance Mode** is on.
- If you turn off Maintenance Mode, all local changes are overridden by central configurations.

VPNs and SmartLSM Security Gateways

Secured communication between your CO gateway and the SmartLSM Security Gateways depends on correct configuration of the Virtual Private Network.

You can define how the VPN domain of a selected SmartLSM Security Gateway is encrypted. You can change the keys as needed and perform other VPN maintenance and change management operations. Before you can configure the IKE certificate, you must have already defined Certificate Authority servers as objects in SmartConsole. See the *R81.10 Security Management Administration Guide*.

Note - After you change the CO gateway configuration, it can be necessary to create a new certificate. This is especially important when there are topology changes.

Activating SmartProvisioning on CO Gateways

A Corporate Office (CO) gateway represents the center of a Star VPN Community. The satellites can be SmartLSM Security Gateways or Security Profiles.

Procedure on a Security Gateway / Security Cluster in the Gateway mode

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the **Expert** mode.
3. Activate SmartProvisioning:

   ```
   LSMenabler on
   ```

Procedure on a VSX Gateway / VSX Cluster

1. Connect to the command line on the VSX Gateway / each VSX Cluster Member.
2. Log in to the **Expert** mode.
3. Activate SmartProvisioning in the context of VS0:
   a. `vsenv 0`
   b. `LSMenabler on`
4. Activate SmartProvisioning in the context of each applicable Virtual System:

a. `vsx stat -v`

b. `vsenv <VS ID>`

c. `LSMenabler on`

Configuring VPNs on SmartLSM Security Gateways

Configuring the VPN encryption of a selected SmartLSM Security Gateway

1. Open the SmartLSM Security Gateway window and select the **Topology** tab.
2. Define a VPN domain (see *"Configuring Topology for SmartLSM Security Gateways" on page 105*).
3. Select the **VPN** tab.

   If, when you created this SmartLSM Security Gateway in the gateway creation wizard, you cleared the **I wish to create a VPN Certificate from the Internal CA** option, you can select **VPN Not supported**. No IKE certificate is generated. You can change this setting at any time.

   For this SmartLSM Security Gateway to participate in a VPN, continue with the next steps.
4. Select **Use Certificate Authority Certificate**.

   If you selected **I wish to create a VPN Certificate from the Internal CA** in the wizard, this option is automatically selected and cannot be edited.
5. From the **Certificate Authority Name** drop-down list, select a CA server object that was previously defined in SmartConsole.
   - If you cleared **I wish to create a VPN Certificate from the Internal CA** in the wizard, you can select a third-party CA from this list.
   - If you selected **I wish to create a VPN Certificate from the Internal CA** in the wizard, the Check Point Internal CA is selected and cannot be edited.
6. If you select a third-party CA in **Certificate Authority Name**, enter a **Key Identifier** or **Authorization Code**, as instructed by the CA.
7. If this SmartLSM Security Gateway does not yet have an initiated IKE certificate, click **Generate**.

   To generate a new IKE certificate, click **Reset**.

The SmartLSM Security Gateway's Distinguished Name (DN) of the certificate is automatically provided and cannot be edited.

8. To apply a new IKE certificate, update the CO gateway (see *"Updating Corporate Office Security Gateways" on page 93*).

Creating a VPN Community for SmartLSM Security Gateways

This section explains how to create the VPN itself in SmartConsole. Before doing so, you must first configure, in SmartProvisioning, the SmartLSM Security Gateways to support VPN participation.

Creating a VPN tunnel between a SmartLSM Security Gateway and a CO gateway

1. Open SmartConsole.
2. Define a VPN Star Community: **Security Policies** > **Access Control** > **Policy** > **Access Tools** > **VPN Communities** > **New** > **Star Community**.
3. In **Gateways** > **Center Gateways**, click **Add**, and select the applicable Security Gateway / Cluster objects.

   Important - This field does not support:
   - VSX Gateways and VSX Clusters.
   - Maestro Security Groups.
   - Quantum Spark appliances that run Gaia Embedded OS.

   Select **Mesh center gateways** if you want the central Security Gateways to communicate.
4. In **Gateways** > **Satellite Gateways**, click **Add**, select the SmartLSM Security Profile from the displayed list.

   When you select the profile, all SmartLSM Security Gateways assigned to this SmartLSM Security Profile are added to the VPN community. The gateways must be configured with the ability to participate in a VPN community (see *"Configuring VPNs on SmartLSM Security Gateways" on the previous page*).
5. In the **Advanced** tab, specify the **IKE (Phase 1)** properties.
6. In the **Shared Secret** tab, clear **Use only Shared secret for all External Members**.
7. Click **OK**.

8. In **Access Control > Policy**, create a Rule Base which defines the services allowed for the VPN community. See *"Sample VPN Rules for a SmartLSM Security Gateways" below*.
9. Install the Security Policy with this rule on the CO gateway.

   A topology file and a certificate are downloaded to the SmartLSM Security Gateway, listing the members of the VPN community and specifying encryption information.

Steps to perform after you create the VPN tunnel in SmartConsole

1. Update the CO gateway. See *"Updating Corporate Office Security Gateways" on page 93*.
2. Establish the VPN tunnel. Send a test connection with an allowed service (according to the rules created in the Security Policy Rule Base) and use SmartView Monitor to make sure that the test was successfully encrypted, sent, and received. To access SmartView Monitor, go to the **Logs & Monitor** view > **External Apps** > **Tunnel & User Monitoring**.

Sample VPN Rules for a SmartLSM Security Gateways

To create a VPN community for SmartLSM Security Gateways, you must create a step for creating a rule in SmartConsole's Security Policy Rule Base that defines the services for the VPN community (see *"Creating a VPN Community for SmartLSM Security Gateways" on the previous page*).

The Dynamic Objects used in the rules

- **MyComm**: Resolves to the IP address range of the VPN Community.
- **MyCO**: Resolves to the IP address of the CO gateway.
- **CO_VPN**: Resolves to the IP address range of the encryption domain of the CO gateway.
- **Edge_Net**: Resolves to the IP address range of exposed SmartLSM Security Gateways.

Rule for Outgoing Connections

Source	Destination	VPN	Service	Action	Install On
Any	Any	MyCommunity	ftp telnet	Accept	MyCO

VPN Rules for Incoming Connections

Source	Destination	VPN	Service	Action	Install On
Edge_Net	CO_VPN	MyCommunity	ftp telnet	Accept	MyProfile
CO_VPN	Edge_Net	MyCommunity	ftp telnet	Accept	MyProfile

VPN with One or More LSM Profiles

You can configure a VPN star community between two SmartLSM Profiles. The procedures below show a SmartLSM Gateway Profile and SmartLSM Cluster Profile. You can also configure the community with two SmartLSM Cluster Profiles or two SmartLSM Gateway Profiles. All included SmartLSM Gateways and Cluster Profiles must have the IPsec VPN blade enabled.

The configuration steps are:

1. Configuration in SmartConsole.

   In SmartConsole, create network objects that represent the VPN community members and their networks. You must create a star community with **To center and to other satellites through center** as the selected option for **VPN Routing** in the Star Community Properties.

   Procedure

   a. Create and configure a SmartLSM Cluster Profile.

      When you configure the topology, make sure that the interface name exactly matches the name of the physical interface.

   b. Create and configure a SmartLSM Gateway Profile.

   c. Create a Security Gateway object to be the Center Gateway.

      Note - Small Office Appliance cannot be the Center Gateway.

d. Create a new VPN Community:

   i. From the left navigation panel, click **Security Policies**.

   ii. In the top section, click **Access Control**.

   iii. In the bottom section **Access Tools**, click **VPN Communities**.

   iv. Click the **New** icon and select **Star Community**.

   v. Enter a name for the VPN Community.

   vi. In the **Center Gateways** area, click the plus icon to add one or more Security Gateways to be in the center of the VPN community.

   Select **Mesh center gateways** if you want the central Security Gateways to communicate.

   vii. In the **Satellite Gateways** area, click the plus icon select the SmartLSM Cluster Profile and SmartLSM Gateway Profile (or second cluster).

   viii. In **VPN Routing**, select **To center and to other satellites through center**.

   ix. Click **OK**.

e. Create a **Network** object that represents the internal network of each satellite in the VPN community.

   i. From the Objects bar, select **New** > **Network Object** > **Network**.

   ii. In the **Network Address** field, enter the IP address that represents the internal IP address of the satellite. If the satellite is a cluster, enter the internal Virtual IP.

f. Create a **Host** object that represents the external IP address of each satellite in the VPN community.

   i. From the Objects bar, select right-click **New** > **Network Object** > **Gateways and Servers** > **Check Point Host**.

   ii. In the **IP Address** field, enter the IP address that represents the external IP address of the satellite. If the satellite is a cluster, enter the external Virtual IP.

g. Create a **Group** object that represents the networks for each satellite object:

   i. From the Objects bar, select **New** > **Network Object** > **Group** > **New Network Group**.

   ii. Enter a **Name** for the group that is unique for one satellite.

   iii. Click **Add** and select the **Network** object that you created for that satellite's internal network.

   iv. Click **Add** and select the **Host** object that you created for that satellite's external IP address.

h. Create a **Group** object that represents the Center Gateway.

   i. From the Objects bar, select **New** > **Network Object** > **Group** > **New Network Group**.

   ii. Enter a **Name** for the group that is unique for the Center Gateway.

   iii. Click **Add**, and select the Gateway object.

2. Configuration in Security Management Server CLI.

   Procedure

   Edit the routing table of the Domain Management Server or Security Management Server to enable two SmartLSM Gateways or Cluster Profiles to communicate with each other through the Center Gateway. Do this in the `vpn_route.conf` file in the CLI.

a. Edit the `vpn_route.conf` file in Vi editor.

   - **In a Multi-Domain Security Management environment**

     Edit the file in the context of a Domain Management Server.

     - If satellites are Small Office Appliance Gateways or Clusters, edit this file:
       - For R80.x `/var/opt/CPmds-R81.10/customers/<Name of Domain Management Server>/CPSFWR80CMP-R81.10/conf/vpn_route.conf`
       - For R81.x `/var/opt/CPmds-R81.10/customers/<Name of Domain Management Server>/CPSFWR81CMP-R81.10/conf/vpn_route.conf`
     - If satellites are on a different appliance or open server, edit this file:

       `/opt/CPmds-R81.10/customers/<Name of Domain Management Server>/CPsuite-R81.10/fw1/conf/vpn_route.conf`

   - **In a Security Management Server environment**

     - If satellites are Small Office Appliance Gateways or Clusters, edit this file:
       - For R80.x Small Office Appliance Gateways, edit: `/opt/CPSFWR80CMP-R81.10/conf/vpn_route.conf`
       - For R81.x Small Office Appliance Gateways, edit: `/opt/CPSFWR81CMP-R81.10/conf/vpn_route.conf`
     - If satellites are on a different appliance or open server, edit this file:

       `/opt/CPsuite-R81.10/fw1/conf/vpn_route.conf`

b. Add the required configuration:

- If two SmartLSM Gateways on different LSM Gateway profiles communicate with each other through the Center gateway, configure:

# destination	router	[install on]
<Name of the **Network Group** object that contains internal network of SmartLSM Gateway>	<Name of Center Gateway object>	<Name of second LSM Profile>
<Name of the **Network Group** object that contains internal network of second SmartLSM Gateway>	<Name of Center Gateway object>	<Name of LSM Profile>

- If more than one SmartLSM Gateway in the same LSM Profile communicate with each other through the Center gateway, configure:

# destination	router	[install on]
<Name of the **Network Group** object that contains internal network of SmartLSM Gateway>	<Name of Center Gateway object>	<Name of LSM Profile>

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

d. In SmartConsole, install policy on the SmartLSM Profiles and on the Center Gateway.

3. Completing the configuration in the SmartProvisioning GUI and in the Center Gateway CLI.

Procedure

a. From SmartConsole, open the SmartProvisioning GUI.

b. Create a new SmartLSM Gateway or Cluster based on the type of device you have.

c. Generate a VPN certificate for each Gateway or Cluster Member:

   i. Open the Gateway or Cluster object > **VPN** tab.

   ii. Select **Use Certificate Authority Certificate**.

   iii. Click **Generate**.

   iv. Do these steps again for each Cluster Member.

   Note - If the topology information, including date and time, changes after you generate the certificate, you must generate a new certificate in the **VPN** tab and update the Gateway (**Actions** > **Update Gateway**.

d. In the CLI of the Center Gateway, run:

```
LSMenabler on
```

e. In the SmartProvisioning GUI, right-click the Center Gateway and select **Actions** > **Update Selected Corporate Office Gateway**.

f. In the **Topology** tab of each object, make sure that the topology of the provisioned objects is correct for each device:

   - Make sure that the interfaces have the same IP addresses as the actual gateways.
   - Make sure that the external and internal interfaces are recognized and configured correctly as "External" and "Internal".
   - If the interfaces show without IP addresses, click: **Get Actual Settings**.

g. In the **Topology** tab, configure the VPN domain:

   - For a SmartLSM Gateways Profile, select one of the options.
   - For a SmartLSM Cluster Profile, select **Manually defined** and manually add the encryption domains that you want to include.

h. Click **Push Policy**.

Note - All traffic between the satellites and Center Gateway is encrypted.

Special Considerations for VPN Routing

The VPN routing option **To center and to other satellites through center** is not supported by SmartLSM Security Gateways.

To configure VPN routing to SmartLSM Security Gateways through the center, enable VPN Routing for a hub and spoke configuration, by editing the `vpn_route.conf` file on the Security Management Server.

Example

1. Generate a group that contains the encryption domains of all the satellite SmartLSM Security Gateways, and call it **SmartLSM_domain**.
2. Generate a group that contains all the central gateways, and call it **Center_gws**.
3. In `vpn_route.conf` , add the rule:

Destination	Router	Install On
SmartLSM_domain	Center_gws	SmartLSM_profile

You can have a Star VPN topology for multiple routing gateways, if the gateways are listed under **install on** in the `vpn_route.conf`

For more information, see *Route Based VPN* in the *R81.10 Site to Site VPN Administration Guide*.

SmartLSM Clusters

A *SmartLSM Cluster* is a logical entity that provides high-availability connectivity with at least two devices. Each device serves as an entry point to the same network. In a SmartLSM Cluster, there is no state synchronization between the devices: if the active SmartLSM Cluster member becomes unavailable, users are not automatically connected to another member. The party that initiated the communication must actively intervene to reconnect the users.

To create a SmartLSM Cluster, you need at least two SmartLSM Security Gateways. A gateway can participate in only one SmartLSM Cluster at a time.

To create and configure SmartLSM clusters , do these steps:

1. Create a SmartLSM Security Cluster Profile in SmartConsole. Profiles set common parameters and policies for SmartLSM clusters, which are created with that profile. See *"Creating a SmartLSM Security Cluster Profile" on page 34*.
2. Create a SmartLSM cluster object in SmartProvisioning. In the **Security Profile** field, select the Profile that you created in step 1.
3. Push Policy to the SmartLSM cluster object. See *"Pushing a Policy in SmartProvisioning" on page 131*.

Creating a SmartLSM Security Cluster Profile

When you make a new SmartLSM cluster profile, define prefixes and suffixes for the profile name to form the full cluster name. This makes it easy to identify which SmartLSM profile is assigned to a cluster.

You define these common parameters in a SmartLSM cluster Security Profile:

- Cluster members.
- Cluster member physical interfaces.
- Interface network objective (Cluster, Sync and so on).
- Cluster interface names.
- Cluster and member interface IP addresses and net masks.
- When you create a SmartLSM cluster Security Profile, define complete IP addresses. These addresses are placeholders and you can override them when you create SmartLSM cluster objects in SmartProvisioning.

- **Cluster and member name components** - Use a common component for the cluster and cluster member names, and another component, to reflect the relative function in the cluster. The common component is in the Profile. The other component is defined in SmartProvisioning for the specific cluster, as a prefix or a suffix to the common component. For example, you can have two two-member clusters, named First_cluster and Second_cluster. You can then name the respective members First_member1, First_member2, Second_member1 and Second_member2. In this example, you define the names _cluster, _member1 and _member2 at the Profile level. Then, when you define individual clusters, you need to define only the names First and Second as name prefixes.

You can manage SmartProvisioning Clusters by a Security Management Server or by a Domain Management Server.

Note - SmartProvisioning is not available for the members of a SmartProvisioning cluster, even if the member gateway runs the SecurePlatform OS.

Procedure

1. In SmartConsole, go to the Objects bar and select **New** > **More** > **LSM Profile**.
2. Select the cluster:
   - Check Point Appliance/Open Server Cluster
   - Small Office Appliance Cluster

   The **Cluster Profile** window opens.
3. On the **General Properties** page, do these steps:
   a. Enter the profile **Name**.
   The profile name becomes the middle section of all SmartLSM cluster names that you define with this profile.
   b. If your clusters use a third-party clustering platform (such as IPSO or Crossbeam), in the **Network Security** tab, clear **ClusterXL**.

      Note - When you use third party cluster platforms, create a different SmartLSM Profile for each platform type.

   c. In the **Network Security** tab, make sure that **IPSec VPN** is selected, if clusters which use this profile are part of a VPN community.
4. On the **Cluster Members** page, add members to the Profile. These member names become the middle section of all member names defined with this Profile.
5. Configure the applicable parameters on the **ClusterXL** or **3rd Party Configuration** page.
6. In the **Topology** page, click **Edit Topology**.

7. Double-click the **New Object** column to configure each interface.

   Use these guidelines:

   - Make sure that the number of interfaces and their network objectives match those of the physical SmartLSM clusters.
   - For interfaces with Private or Sync network objectives, do not enter information in the Cluster column.
   - Every SmartLSM cluster mapped to this Profile retains the host parts (by net mask) of the member IP addresses, and the name of the cluster (virtual) interface.
     - The network parts of the members' IP addresses and the entire cluster IP addresses are only used as a template here. You define the relevant network for each interface of each SmartLSM Security Gateway later in SmartProvisioning.
     - Make sure that the host ID for the external interface of the SmartLSM cluster profile is the same as the external interface of the cluster.
   - The network parts of the members IP addresses must be identical for the same interface name, even though they are only place holders.
   - Profile member interface names can be overridden for the actual SmartLSM cluster. However, they are usually the same for all clusters (eth0, eth1 and so on), so it is convenient to use the actual names here as well.

8. In the **Fetch Policy** page:
   - In a High Availability environment, click **Add** > the **Add Masters** window opens. From the **Available Management Stations** column, select all servers and click **Add**. Then click **OK**.
   - Optional: Change the **Fetch Policy** interval and select a **Scheduled Event** or create a new one.
9. Configure other parameters as required. You define VPN domains for cluster objects using SmartProvisioning.
10. Click **OK** to confirm the settings, and save the Policy Package.
11. Install policies to the cluster Profile.

Configuring SmartLSM Cluster Objects in SmartProvisioning

Before you define a SmartLSM cluster in SmartProvisioning, you must have an applicable SmartLSM Cluster Security Profile in SmartConsole (see *"Creating a SmartLSM Security Cluster Profile" on page 125*). Use SmartProvisioning to create and configure a SmartLSM cluster.

Note - Alternatively, you can use LSMcli commands (possibly, in a script) to define SmartLSM clusters, for example `AddROBO VPN1Cluster`". The LSMcli commands enable you to replace a part of Profile names, which is not possible when you use the SmartProvisioning interface.

Procedure

1. From the **File** menu, select **New** > **Check Point Appliance/Open Server SmartLSM Cluster**.
2. Enter a **Cluster Name Prefix** or **Suffix** or both to add to the cluster Profile and member names.
3. Enter the **Cluster Main IP Address**.
4. Click **Next**.
5. Select the SmartLSM **Cluster Version** and the **SmartLSM Security Cluster Profile**. Click **Next**.
6. Verify the resulting names. Click **Next**.

   The **More Information** window opens. This window shows the interface topology defined on the Cluster Profile object in SmartConsole. The profile topology includes generic (template) IP addresses for any SmartLSM Cluster mapped to this profile. You can override the IP addresses in the list with new values for a specific SmartLSM Cluster.
7. Select each interface and **Edit** it.

   The settings here override Profile settings.
8. For each interface, define:
   - The **Members' Network Override** address (usually the same for all interfaces).
   - Members' interface **Name Override** (must match the name defined in the operating system)
   - The **Cluster IP Address and Net Mask**.

- You can also override the **IP address for each Cluster Member**. For this option to show in the UI, you must set an environment variable in Windows. To do this, first you must close SmartConsole and SmartProvisioning. To set this environment variable, go to the Windows > **Control Panel** > **System and Security** > **System** > **Advanced System Settings** > at the bottom of the window, go to **Environment Variables**. In the **User variable** section, select **New**. In the **New User Variable** window that opens, enter these details:
  - **Variable name:** LSM_USING_IP_OVERRIDE
  - **Variable value:** 1

  After you set the environment variable, reopen SmartConsole and SmartProvisioning and define the IP overrides.

For fields left empty, the values are taken from the Profile. You can define the overrides later on by editing the cluster object. You can also edit the cluster object to override interface topology.

9. Click **Next**.
10. Select each member, and **Initialize** SIC communication. The **Communication** window opens. SIC is initialized only when you complete the wizard.

    Note - Alternatively, you can do this later - edit the member object and, in the **General** tab, click **Communication**.

11. Click **Next**.

    The **Finished SmartLSM Security Cluster Wizard** window opens.

    a. To create a VPN certificate for the cluster, select this option.

       The certificate is created only when you complete the wizard. You can later create VPN certificates for the individual cluster members - edit the member object and, in the VPN tab, click **Generate**.

    b. To configure additional cluster options (such as VPN settings or Dynamic Objects) after the SmartLSM cluster object is created, select this option and click **Finish**.

    SmartProvisioning creates the SmartLSM Cluster object and its members.

    Note - After a SmartLSM Cluster is defined and mapped to a Profile, do not add or remove a member or an interface. Do not change a cluster (virtual) interface name.

12. To retrieve the policy for the first time, from the command line of each SmartLSM Cluster member, run:

```
fw fetch_robo -n -f
```

Note - To edit the cluster properties, double-click the cluster object. To edit the properties of a cluster member, you can double-click the member object or go to the Cluster tab in the cluster properties window.

Creating a SmartLSM Small Office Appliance Cluster

Make sure you have a SmartLSM cluster Security Profile defined in SmartConsole before you create a Small Office Appliance cluster in SmartProvisioning.

Procedure

1. In the navigation tree, click **Devices**.
2. From the Launch Menu, select **File** > **New** > **Small Office Appliance Cluster**.

   The **SmartLSM Security Cluster General Properties** page opens.
3. Enter a unique **Cluster Name Prefix** (Suffix is optional).

   The SmartLSM Security Cluster name is:
   `<prefix>cluster<suffix>`.
4. In **Cluster Main IP Address**, enter the real external virtual IP address for your actual gateway cluster.
5. Click **Next**.
6. Configure these settings:
   a. **Hardware** - Select the gateway hardware version.
   b. **Version** - Select the firmware version for the device.
   c. **Security Profile** - Select the SmartLSM Cluster Profile that was created in SmartConsole.
   d. **Provisioning** - Select **Enable Provisioning** to enable the management of this gateway by provisioning configurations:
   - **No Provisioning Profile** - Select to enable provisioning but not yet assign a specific profile.
   - **Provisioning Profile** - Select to assign to this gateway from the drop-down list.
7. Click **Next**

   The **Cluster Names** page opens.

   The names of the cluster members are shown with the configured prefix.

8. Click **Next**.

   The **More Information** page opens.

9. Click **Edit** to override the settings of the template topology on each of the interfaces. For example, select WAN and click Edit.

   The interface's window opens:

   a. In **IP Address Override**, enter the actual network IP address to override the template Network address.

   b. Click **OK** and do this procedure again for all the interfaces.

   c. Click **Next**.

10. Select a member and click **Initialize**:

    a. Enter the trusted communication (SIC) details.

       Click **OK**.

    b. Do this again for the second member.

    c. Click **Next**.

11. Select how to create a VPN certificate:

    - For a VPN certificate from the Internal Check Point CA, select **I wish to create a VPN Certificate from the Internal CA**.
    - For a VPN certificate from a third party CA (for example, if your organization already has certificates from an external CA for other devices), clear this checkbox and request the certificate from the appropriate CA server.

12. Select **Edit SmartLSM cluster properties after creation** to work with the newly created object

13. Click **Finish**.

After the wizard finishes, the SIC initialization takes a few minutes to complete. When it completes, you can see the cluster object and its two members. Double-click the cluster object to see that the topology is configured with the actual addresses.

On each Small Office Appliance, open the WebUI **Home** > **Security Management** page and click **Fetch Policy** to manually pull the policy immediately. Alternatively, the appliance connects to the Security Management Server at predefined periodic intervals to pull the policy.

Pushing a Policy in SmartProvisioning

In the general SmartLSM system, you can manually push a policy to a SmartLSM gateway. For a SmartLSM cluster, push the policy to the cluster object. All the cluster members will receive the policy.

To push a policy to a SmartLSM cluster:

1. Right-click the SmartLSM cluster object in the **Device** pane of the SmartLSM GUI client.
2. Select **Actions** > **Push Policy**.

   You can also push a policy with the command line interface.

Activating a SmartLSM Cluster with QoS

To activate a SmartLSM cluster with QoS:

1. In SmartConsole, create a SmartLSM Cluster profile (see *"Creating a SmartLSM Security Cluster Profile" on page 125*).
2. On the SmartLSM **Cluster Profile** > **General Properties** page, select **QoS**.
3. On the **Topology** page, click **Edit**.
4. Double-click the QoS cluster interface.

   The **Interface Properties** window opens.
5. On the **QoS** tab, configure:
   - Inbound and Outbound bandwidth allocation
   - DiffServ and Low Latency classes
6. Go to **Security Policies > Access Control > QoS**, open SmartDashboard, and on the **QoS** tab define QoS policy.
7. Install the QoS policy on the SmartLSM profile.

For more information on how to configure QoS, see the *R81.10 QoS Administration Guide*.

To activate a SmartLSM cluster in SmartProvisioning

1. Right-click the SmartLSM Cluster object.
2. Select **Actions** > **Push Policy**.

   Note - These steps are not mandatory. Gateways periodically fetch their policies from the Security Management Server.

Dynamic Objects

Dynamic Objects are logical objects whose values, IP addresses or ranges, are resolved differently per gateway. This enables you to create rules, Security Policies, and SmartProvisioning SmartLSM Security Profiles that are can be re-used for numerous gateways.

Dynamic Objects are defined in SmartConsole and referenced in Security Policies, NAT tables, and profiles. Some Dynamic Objects are provided by default.

Dynamic Objects let you:

- Create a VPN tunnel between CO gateways and SmartLSM Security Gateways.
- Represent generic servers that exist in remote sites and easily manage numerous remote servers from a central control.
- Install Security Policy rules with Dynamic Objects on SmartLSM Security Profiles, which automatically localize a generic rule for each gateway.

Dynamic Object Types

There are different types of Dynamic Objects, differentiated by how they are resolved.

- **Automatically Resolved**: Created by default when you create a new SmartLSM Security Gateway object. Auto-Resolved Dynamic Objects are replaced with their values when the gateway loads an updated profile from the Security Management Server or Domain Management Server. You cannot edit these Dynamic Objects.

  See table

Default Dynamic Object	Resolves to:
AuxiliaryNet	IP address range, based on the IP address and net mask of the interface configured as the **Auxiliary** network for the SmartLSM Security Gateway
DMZNet	IP address range, based on the IP address and net mask of the interface configured as the **DMZ** network for the SmartLSM Security Gateway
InternalNet	IP address range, based on the IP address and net mask of the LAN behind the SmartLSM Security Gateway configured as the **Internal** network
LocalMachine	External IP address of the SmartLSM Security Gateway, based on the IP address of the interface marked **External**

Default Dynamic Object	Resolves to:
LocalMachine_ All_Interfaces	DAIP machine interfaces, both static and dynamic

- **Centrally Resolved:** A Dynamic Object is created in SmartConsole. For each SmartLSM Security Gateway, you define the IP address or range to which the Dynamic Object is resolved.

Dynamic Object Values

Dynamic Objects resolve to actual IP address or IP address ranges. They are automatically resolved when a gateway fetches a SmartLSM Security Policy from the Security Management Server or Domain Management Server.

You can also actively push the values of Dynamic Objects, and make sure that new values take effect immediately. To push Dynamic Object values, select **Actions** > **Push Dynamic Objects**.

When a SmartLSM Security Gateway fetches its SmartLSM Security Profile, automatically or by push, the SmartLSM Security Policy is localized for each gateway. Localization is performed in this order:

1. Anti-Spoofing and Encryption-Domain information are automatically calculated.
2. Dynamic Objects are resolved, in the *Automatic-Central-Local* order.
3. Relevant gateways are updated with Provisioning Profiles.
4. The relevant Check Point Security Policy is installed or updated on SmartLSM Security Gateways.

Dynamic Objects Using

1. In SmartConsole, create the Dynamic Objects, the Security Policy that uses the Dynamic Objects, and the LSM Profile.
2. Install the Security Policy on the Security Profile.
3. In SmartProvisioning, add an SmartLSM Security Gateway. Assign the SmartLSM Security Profile to the Security Gateway.
4. Configure the gateway's Dynamic Object list to include and resolve the Dynamic Objects of the Security Policy.

Dynamic Object Examples

These examples show how to create a Security Policy in SmartConsole that uses Dynamic Objects. After you create the Rule Base, install the Security Policy on the SmartLSM Security Profile.

The Dynamic Objects are localized and resolved to the real IP addresses of each gateway assigned to the SmartLSM Security Profile. Therefore, for each gateway of a profile on which the Security Policy with the Dynamic Objects is installed, make sure that the gateway has these Dynamic Objects configured with real IP addresses and net masks.

Note - The value of the **LocalMachine** Dynamic Object is resolved to the external IP address of the SmartLSM Security Gateway.

Hiding an Internal Network

This example uses the **InternalNet** and **LocalMachine** default Dynamic Objects to create a rule in a Security Policy that can be applied to any SmartLSM Security Profile object, and therefore, to any number of gateways. This rule hides the internal network behind the external IP address of the SmartLSM Security Gateway.

Example - NAT Hide

Source	Destination	Service	Source	Destination	Service
InternalNet	Any	Any	LocalMachine (H)	Any	Any

Defining Static NAT for Multiple Networks

This example uses Dynamic Objects that you can define for yourself, based on the needs of your organization and the requirements for the SmartLSM Security Gateways. This rule configures static NAT on all incoming HTTP traffic going to a published IP address (the IP address is represented by a Dynamic Object called **PublishedIP**), as if it were going to a Web server (represented by a Dynamic Object called **WebServer**).

Example - Static NAT

Source	Destination	Service
Any	PublishedIP	HTTP
Any	WebServer	HTTP

Securing LAN-DMZ Traffic

This example uses the **InternalNet** and **DMZNet** default Dynamic Objects to secure traffic between a gateway's internal LAN and its DMZ. This example shows that when you create rules with Dynamic Objects, you must make sure to install them on the relevant SmartLSM Security Profile, the profile for which all its gateways have these Dynamic Objects configured.

LAN Rules

Source	Destination	VPN	Service	Action	Log	Install On
InternalNet	DMZNet	*Any Traffic	Any	Accept	None	Profile1

Allowing Gateway Ping

This example shows a rule that allows external hosts to ping the external IP address of a SmartLSM Security Gateway.

It is installed on multiple profiles, which lets this rule be a part of numerous gateways.

External Hosts Rules

Source	Destination	VPN	Service	Action	Log	Install On
Any	LocalMachine	*Any Traffic	echo-request echo-reply	Accept	None	Profile1 LSMProfile1

Tunneling Part of a LAN

This example uses a centrally resolved Dynamic Object to hold an IP address range that represents part of an internal LAN behind a SmartLSM Security Gateway.

The complete range is 192.0.2.1 - 192.0.2.255.

You want only 192.0.2.1 - 192.0.2.128 of this LAN to be in a VPN tunnel with the CO Security Gateway.

In SmartConsole:

1. Create a Dynamic Object called **Safe_Internal**.
2. Add this object to the VPN community (called **MyComm** in this example) that includes the IP addresses of the CO Security Gateway (**MyCO**) and its VPN domain (**CO_VPN**).
3. Create a SmartLSM Security Profile object called **MyProfile**.
4. Create a Security Policy with these rules.

VPN with Range

Source	Destination	VPN	Service	Action	Install On
Any	LocalMachine	MyComm	ftp telnet	Accept	MyCO
Safe_ Internal	CO_VPN	MyComm	ftp telnet	Accept	MyProfile
CO_VPN	Safe_Internal	MyComm	ftp telnet	Accept	MyProfile

In SmartProvisioning:

1. Make sure the SmartLSM Security Gateway with the internal LAN is assigned to **MyProfile**.
2. Add **Safe_Internal** to the Dynamic Objects list of this gateway.
3. Configure the IP address range of **Safe_Internal** to the safe range of the LAN: 192.0.2.1 - 192.0.2.128.
4. Push the Dynamic Objects and then the policy to the SmartLSM Security Gateway.

User-Defined Dynamic Objects

Creating User-Defined Dynamic Objects

1. In SmartConsole, go to **Objects** > **Network Objects** > **Dynamic Objects** > **New Dynamic Object**.
2. Provide the relevant information.

   Click **OK**.

Configuring User-Defined Dynamic Object Values

If a fetched SmartLSM Security Policy includes Dynamic Objects for which you did not configure values, the firewall drops all packets that match any rules with these Unresolved Dynamic Objects. Therefore, you must define all Centrally Resolved Dynamic Objects, and verify that local administrators in remote and branch offices define the values for Locally Resolved Dynamic Objects.

After you create a Dynamic Object in SmartConsole, you can add it to a SmartLSM Security Gateway. Provide the exact IP address or range to which SmartProvisioning will resolve the Dynamic Object.

Note - The **Dynamic Objects** tab on the gateway has an **Add** button. With the Add button, you cannot create new Dynamic Objects. The Add button lets you add a new resolve-to value to an already defined Dynamic Object for the selected SmartLSM Security Gateway. If you click **Add** and already resolved all defined Dynamic Objects, this message shows: **All defined Dynamic Objects are already resolved. Use the Check Point SmartConsole in order to add more Dynamic Objects**.

Specifying the resolution value of a user-defined Dynamic Object

1. Double-click a SmartLSM Security Gateway.
2. In the Gateway window, select the **Dynamic Objects** tab.
3. Click **Add**.
4. From the **Name** drop-down list, select the Dynamic Object, as defined in SmartConsole.

   The **Comments** field displays the comments provided by the Dynamic Object creator.
5. Select the relevant type of value:
   - **IP Address**: If there is one IP address for the Dynamic Object value, select this option and provide the address.
   - **IP Address Range**: If there is a range for the Dynamic Object value, select this option and provide the first and last IP addresses of this range.
6. Click **OK**.

   The Dynamic Object name is added to the **Resolved Dynamic Objects** table. If the value is a single IP address, this address is listed in the **First IP** column.

Use Case

This chapter describes an example scenario of a multiple gateway environment run by SmartProvisioning. This use case leads you through all the steps you must take to configure a SmartProvisioning environment. Note that this is an example scenario only which fits a particular environment. You can use SmartProvisioning to create any type of deployment which best fits your environment.

Use Case Scenario

A Bank has 1,000 ATMs and 300 branches deployed in a certain country.

- Each ATM is protected by a 1100 appliance gateway.
- Each branch is protected by a 3200 appliance gateway.

The Bank administrator can define security profiles and provisioning profiles to manage the gateways efficiently.

Deployment Considerations

Number of Security Profiles

The Bank's ATMs transfer information to a main processing server. The route that needs to be secured is the route of each ATM to the ATM processing server. The needs of a branch are different. Each branch needs to transfer information to certain departments in the Bank's headquarters, like the Human Resources department, the Finance department and so on. Each branch also needs an external internet connection.

The ATM gateways and the Branch gateways therefore, must have different Security Policies. The Bank administrator must create 2 separate Security Profiles, one for the ATM gateways and one for the branch gateways.

VPN

All gateways, both the 1100 and the 3200, connect the information to the main Security Gateway at the Bank's headquarters. To make sure that the connection between the gateways and the main Security Gateway is secure, create a VPN community for the Bank's gateways. The VPN Community must be a star community. A Star VPN Community is a "hub and spoke" community, in which there is a central Security Gateway (a hub) creates tunnels only with the satellites (spokes). In our example, define the Bank Headquarters gateway as the CO Security Gateway, and define the ATM Security Profile and the Branch Security Profile as the satellites.

Number of Provisioning Profiles

The decision of how many Provisioning Profiles to create can be the result of many factors. For example:

- Type of device - A Provisioning Profile can support one type of device.
- Geography - You can create a different Provisioning Profile for each geographic area. This way, the gateways can receive a faster response from the servers defined in the Provisioning Profile, such as the DNS or RADIUS servers.
- Load on servers - To balance the load on the servers defined in the Provisioning Profile, such as the Host, DNS server, RADIUS server, or backup server, you can create multiple Provisioning Profiles. In each Provisioning Profile, define a different server for DNS, RADIUS and so on.

Therefore, we must create a separate Provisioning Profile for each set of gateways. In our example, we can create 2 provisioning profiles for each type of device.

Workflow for Creating the SmartProvisioning Environment

Manage the gateways with SmartProvisioning. Take the following steps

1. Enable SmartProvisioning support on the Security Management Server.
2. Enable SmartProvisioning support on all Gaia Security Gateways, which you wish to manage with SmartProvisioning.
3. Enable SmartProvisioning on the CO gateway.
4. Create a Security Profile for the gateways that protect the ATMs.
5. Create a Security Profile for the gateways that manage the branches.
6. Create a Star VPN Community.
7. Create Provisioning Profiles for the gateways that manage the ATMs.
8. Create Provisioning Profiles for the gateways that manage the branches.

Use Case Configuration

Procedure

Enable SmartProvisioning support on the Security Management Server

Obtain a license for SmartProvisioning, and add the license to the Security Management Server or Domain Management Server, with `cpconfig` or SmartUpdate.

You can also use the `cplic` command to add the license.

Enable SmartProvisioning support on a Security Gateway

1. From the CLI, run these commands in the Expert mode:

   ```
   LSMenabler -r on
   cpstop
   cpstart
   ```

2. Run:

   ```
   cpconfig
   ```

3. Go to **ROBO Interfaces** and define an `External` interface.

Note - This procedure is not required for Small Office Appliances.

Enable SmartProvisioning on the CO Security Gateway

On the Check Point Security Gateway, execute this command in the Expert mode:

```
LSMenabler on
```

Create a Security Profile

1. In SmartConsole, go to **Menu > Manage policies and layers > Policies > New**, create a Security Policy and save it.
2. Go to **Menu > New Object > LSM Profile**>:
   - For the ATM gateways, select **New Small Office Appliance Gateway**.
   - For the branches gateways, select **New Check Point Appliance/Open Server Gateway**.
3. In the **SmartLSM Security Profile** window, configure the settings for the SmartLSM Security Profile.

Type of Profile	Configuration
For the ATM Gateways	Configure these settings: a. In the **General Properties** tab, enable **IPSec VPN**. b. In the **Platform** section > **Hardware**, select **1100 Appliances**. c. In the **IPSec VPN** tab, click **Add** to enter the VPN community in which the LSM Security Profile is a member. d. Optional: In the **Fetch Policy** tab: i. This page specifies the default Security Management Server from which to fetch the policy. Click **Add** to enter a different Security Management Server. ii. In the **Fetch policy from the Security Management Server** section, there is a predefined schedule for fetching the policy. Click **New** to define a new schedule.
For the branch Gateways	Configure these settings: a. In the **General Properties** tab, enable **IPsec VPN** and **IPS**. b. In the **IPSec VPN** tab, click **Add** to enter the VPN community in which the LSM Security Profile is a member. c. Optional: In the **Fetch Policy** tab: i. This page specifies the default Security Management Server from which to fetch the policy. Click **Add** to enter a different Security Management Server. In a High Availability environment, click **Add** to add one or more Security Management Servers. ii. In the **Fetch policy from the Security Management Server** section, there is a predefined schedule for fetching the policy. Click **New** to define a new schedule

4. Click **OK**.
5. Install the Security Policy on the SmartLSM Security Profile.
   a. Click **Install Policy**.
   b. Select the SmartLSM Security Profile object.
   c. Click **Install**.
6. Frin the Menu, open SmartProvisioning and add the SmartLSM Security Gateways (see *"Security Profiles for Check Point Appliance Security Gateways" on page 33*).

In the **Finish** page, make sure you select **I wish to create a VPN Certificate from the Internal CA**.

Create a star VPN community

1. In SmartConsole, go to **Security Policies > Access Control > Access Tools > VPN Communities**.
2. Click **New** > **Star Community**.
3. In the **Gateways** tab:
   a. **Center Gateways**, click the **+** sign and add the Headquarters from the drop-down list.
   b. **Satellite Gateways**:
      i. Click the **+** sign to add the ATM gateways Security Profile.
      ii. Click the **+** sign again to add the branch gateways Security Profile.
4. In **Security Policies > Access Control > Policy**, create a Rule Base for the VPN Community.
5. Install the Access Control Policy on the CO Gateway.
6. Open SmartProvisioning, and in the toolbar click the **Update Corporate Office Gateway** button.

Configure VPN Properties on the gateways

1. In SmartProvisioning, double-click the Security Gateway.
2. In the **Topology** tab, select **All IP addresses behind the gateway based on interfaces information**.
3. In the **Interfaces** tab, select **Manage Settings on the Device**.

Create a Provisioning Profile

1. Open SmartProvisioning.
2. From the Launch Menu, select **File** > **New** > **Provisioning Profile**.

   The **New Provisioning Profile Wizard** opens.
3. Enter a name for the profile.
4. From the **Select Type** drop-down list, select the platform or operating system to be supported by this profile:

- For the ATM gateway profile, select **Small Office Appliance**
- For the branch gateway profile, select **Gaia**

Each Provisioning Profile can support only one operating system.

5. Click **Next**.
6. If you want to configure the settings of the Provisioning Profile now, select **Edit Provisioning Profile properties after creation**.
7. Click **Finish**.

Configure the settings of a provisioning profile

For each set of configurations managed with a Provisioning Profile, you can decide which settings have preference: *local* (not provisioned) or *central* (from SmartProvisioning individual management or from Provisioning Profile).

1. In the Profile window, click any category tab (other than **General**).
2. Select **Manage settings centrally from this application**: Each gateway assigned to this profile gets its configuration for this setting from the Provisioning Profile or from the SmartProvisioning gateway object.
3. Click **Advanced**.

   The **Profile Settings** window opens.
4. Select **Allowed**. This means that you can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
5. Click **OK**.
6. Configure the Settings for each tab.

For a more detailed explanation of the configuration options. See *Configuring Provisioning Profile Settings* for more information.

Managing Security through API

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

API

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

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

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

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

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.

    Note - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), the API Documentation web portal (`https://<Server IP Address>/api_docs`) stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

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

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

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

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

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

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

Configuring the API Server

To configure the API Server:

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

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

   Configuring Startup Settings

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

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

Configuring Access Settings

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

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

6. Click **OK**.
7. In the upper left section, click **Permissions & Administrators**.
8. In the object of each applicable Administrator, make sure the assigned Permission Profile allows access to Management API.

   Instructions

   a. Edit the Administrator object.

   b. In the left panel, click **General**.

   c. In the **Permissions** section, on the right side of the selected Permission Profile, click the eye icon.

      The Permission Profile object opens in the read-only view.

   d. In the left panel, click **Management**.

   e. The permission **Management API Login** has to be selected.

      If it is not selected, then close this window and edit this Permission Profile object.

      For more information, see *Assigning Permission Profiles to Administrators*.

   f. Click **Close**.

9. Publish the SmartConsole session.
10. Restart the API Server on the Management Server with this command:

```
api restart
```

Notes:

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

```
mdsenv <IP Address or Name of Domain Management Server>
```

- The output of this command must show:

```
API started successfully
```

11. Examine the status of the API server on the Management Server with this command:

```
api status
```

Notes:

- The output of this command must show:

```
------------------------------------------
Overall API Status: Started
------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- The output this command may show the state of the "**API**" process as "**Stopped**" when the API access is set to "**All IP addresses that can be used for GUI clients**", and more than 200 Trusted Clients are configured:

```
Processes:

Name      State     PID       More Information
-----------------------------------------------
API       Stopped   ...
```

Command Line Reference

See the *R81.10 CLI Reference Guide*.

Below is a limited list of applicable commands.

Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.

Character	Description
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

Check Point LSMcli Overview

Check Point SmartLSM Command Line Utility (LSMcli) is a simple command line utility, an alternative to SmartProvisioning SmartConsole GUI.

LSMcli lets you perform SmartProvisioning GUI operations from a command line or through a script.

Notes:

- LSMcli can run from hosts other than SmartConsole clients. Make sure to define the hosts, from which you run the LSMcli as GUI clients.
- The first time you run the LSMcli from a client, it shows the Management Server's fingerprint. Confirm the fingerprint.
- In the LSMcli, commands can use the abbreviation *ROBO* (Remote Office/Branch Office) Security Gateways.
  In SmartProvisioning GUI, these Security Gateways are called SmartLSM Security Gateways.

Syntax

```
LSMcli {-h | --help}
```

```
LSMcli [-d] <Mgmt Server> <Username> <Password> <Action>
```

Parameters

Parameter	Description
`[-d]`	Runs the command in the debug mode.
<Mgmt Server>	Specifies the Security Management Server or Domain Management Server by its Name or IPv4 address.
<Username>	Specifies the username used in the standard Check Point authentication method.
<Password>	Specifies the password used in the standard Check Point authentication method.
<Action>	Specifies the function performed (see the next sub-sections for a complete list of actions).

Syntax Notation

Square brackets (**[ ]**) are used in the LSMcli utility syntax. These brackets are correct and syntactically necessary.

This is an example of how they are used:

- **A [b [c]]** - means that for parameter **A**, you can provide **b**. If you provide **b**, you can provide **c**.
- **A [b] [c]** - means that for parameter **A**, you can provide **b**, **c**, or **b** and **c**.
- **A [b c]** - means that for parameter **A**, you can provide **b** and **c**.

SmartLSM Security Gateway Management Actions

This section describes commands that perform management actions on SmartLSM Security Gateways.

LSMcli AddROBO VPN1

Description

This command adds a new Check Point SmartLSM Security Gateway to SmartProvisioning and assigns it a SmartLSM Security Profile.

If a one-time password is supplied, a SIC certificate is created.

If an IP address is also supplied, the SIC certificate is pushed to the SmartLSM Security Gateway (in such cases, the SmartLSM Security Gateway SIC one-time password must be initialized first).

If no IP address is supplied, the SIC certificate is pulled from the SmartLSM Security Gateway afterwards.

You can also assign an IP address range to Dynamic Objects, and specify whether or not to add them to the VPN domain.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO VPN1
<ROBOName> <Profile> [-RoboCluster=<OtherROBOName>] [-
O=<ActivationKey> [-I=<IP>]] [[-CA=<CaName> [-
R=<CertificateIdentifier#>] [-KEY=<AuthorizationKey>]]] [-
D]:<DynamicObjectName>=<IP1>[-<IP2] [-D]:...
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.

Parameter	Description
<RoboName>	Name of a SmartLSM Security Gateway.
<Profile>	Name of a SmartLSM Security Profile that was defined in SmartConsole.
<OtherROBOName>	Name for an already defined SmartLSM Security Gateway that participates in the SmartLSM Cluster with the newly created Security Gateway (if the "-RoboCluster" argument is provided).
<ActivationKey>	SIC one-time password (for this action, a certificate is generated).
<IP>	IP address of the Security Gateway (for this action, a certificate is pushed to the Security Gateway).
<CaName>	Name of the Trusted CA object (created from SmartConsole). The IKE certificate request is sent to this CA. Default is Check Point Internal CA.
<CertificateIdentifier#>	Key identifier for third-party CA.
<AuthorizationKey>	Authorization Key for third-party CA.
<DynamicObjectName>	Name of the Dynamic Object.
<IP1>	Single IP address for the Dynamic Object.
<IP1-IP2>	Range of IP addresses for the Dynamic Object.

Example 1

This command adds a new SmartLSM Security Gateway `MyRobo` and assigns it the specified SmartLSM Security Profile `AnyProfile`.

A SIC password and an IP address are supplied, so the SIC Activation Key can be sent to the new SmartLSM Security Gateway.

A Dynamic Object called `FirstDO` is resolved to an IP address for this Security Gateway.

```
LSMcli mySrvr name pass AddROBO VPN1 MyRobo AnyProfile -O=MyPass -
I=192.0.2.4 -DE:FirstDO=192.0.2.100
```

Example 2

```
LSMcli mySrvr name pass AddROBO VPN1 MyRobo AnyProfile -O=MyPass -
I=10.10.10.1 -DE:FirstDO=10.10.10.5 -CA=OPSEC_CA -R=cert123 -
KEY=abc456
```

LSMcli ModifyROBO VPN1

Description

This command modifies a Check Point SmartLSM Security Gateway.

This action modifies the SmartProvisioning details for an existing SmartLSM Security Gateway and can be used to update properties previously supplied by the user.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBO VPN1
<RoboName> ...
```

and at least one of these:

```
... [-P=Profile] [-RoboCluster={<OtherROBOName> | -NoRoboCluster}]
[-D:<DO Name>=<IP1>[-<IP2>] [-KeepDOs]...]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Profile>	Name of a SmartLSM Security Profile that was defined in SmartConsole.
<OtherROBOName>	Name of the already defined SmartLSM Security Gateway that is to participate in the Cluster with the newly created Security Gateway (if the "`-RoboCluster`" argument is provided).
`-NoRoboCluster`	This parameter is equivalent to the **Remove Cluster** operation in the SmartProvisioning GUI. When you issue a `ModifyROBO VPN1` command with this argument on a Security Gateway that participates in a cluster, the cluster is removed.
<DO Name>	Name of the Dynamic Object.

Parameter	Description
`<IP1>`	Single IP address for the Dynamic Object.
`<IP1-IP2>`	Range of IP addresses for the Dynamic Object.
`-KeepDOs`	Keeps all existing dynamic objects in the dynamic objects list when you add new dynamic objects. If a dynamic object already exists in the list, its IP resolution is updated. If this flag is not specified, the dynamic objects list is deleted when you use the `LSMcli` command to add new dynamic objects.

Example

This example resolves Dynamic Objects for the given Security Gateway.

```
LSMcli mySrvr name pass ModifyROBO VPN1 MyRobo -
D:MyEmailServer=123.45.67.8 -D:MySpecialNet=10.10.10.1-10.10.10.6
```

LSMcli ModifyROBOManualVPNDomain

Description

This command modifies the SmartLSM VPN Domain, to take effect when the VPN Domain becomes defined as Manual.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyROBOManualVPNDomain <RoboName> {-Add=<FirstIP>-<LastIP> | -
Delete=<Index>} [-IfOverlappingIPRangesDetected={exit | ignore |
warn}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster.
<FirstIP>-<LastIP>	IP address range.
<Index>	Value displayed by the *"LSMcli ShowInfo" on page 182* command or the *"LSMcli ShowROBOTopology" on page 172* command.
-IfOverlappingIPRangesDetected	Optional. Determines the course of action, if overlapping IP address ranges are detected: exit, ignore, or show a warning.

Example 1

```
LSMcli mySrvr name pass ModifyROBOManualVPNDomain MyRobo -
Add=192.0.2.1-192.0.2.20
```

Example 2

```
LSMcli mySrvr name pass ModifyROBOManualVPNDomain MyRobo -Delete=1
```

LSMcli ModifyROBOTopology VPN1

Description

This command modifies the SmartLSM VPN Domain configuration for a selected Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBOTopology
VPN1 <RoboName> -VPNDomain={not_defined | external_ip_only |
topology | manual}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
`VPNDomain`	Specifies the VPN Domain topology: ■ `not_defined` - Equivalent to the **Not Defined** option on the **Topology** tab of a SmartLSM Security Gateway in the SmartProvisioning GUI (or in the output of the *"LSMcli ShowROBOTopology" on page 172* command). ■ `external_ip_only` - Equivalent to the **Only the external interface** configuration in the SmartProvisioning GUI. ■ `topology` - Equivalent to the **All IP Addresses behind the Gateway based on Topology information** configuration in the SmartProvisioning GUI. ■ `manual` - Equivalent to **Manually defined**. VPN domain is defined according to the configuration made with the *"LSMcli ModifyROBOManualVPNDomain" on page 159* command.

Example

```
LSMcli mySrvr name pass ModifyROBOTopology VPN1 MyRobo -
VPNDomain=manual
```

LSMcli ModifyROBOInterface VPN1

Description

This command modifies the Internal Interface list.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyROBOInterface VPN1 <RoboName> <InterfaceName> -i=<IPAddress>
[-Netmask=<NetMask>] [-IfOverlappingIPRangesDetected={exit |
ignore | warn}]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<InterfaceName>	Name of the existing interface.
<IPAddress>	IP address of the interface.
<NetMask>	Net mask of the interface.
-IfOverlappingIPRangesDetected	Optional. Determines the course of action, if overlapping IP address ranges are detected: exit, ignore, or show a warning.

Example

```
LSMcli mySrvr name pass ModifyROBOInterface VPN1 MyRobo eth0 -
i=192.0.2.1 -Netmask=255.255.255.0
```

LSMcli AddROBOInterface VPN1

Description

This command adds a new interface to the selected SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBOInterface
VPN1 <RoboName> <InterfaceName> -i=<IPAddress> -NetMask=<NetMask>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<InterfaceName>	Name of an existing interface.
<IPAddress>	IP address of the interface.
<NetMask>	Net mask of the interface.

Example

```
LSMcli mySrvr name pass AddROBOInterface VPN1 MyRobo eth0 -
i=192.0.2.1 -Netmask=255.255.255.0
```

LSMcli DeleteROBOInterface VPN1

Description

This command deletes an interface from the selected Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
DeleteROBOInterface VPN1 <RoboName> <InterfaceName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<InterfaceName>	Name of an existing interface.

Example

```
LSMcli mySrvr name pass DeleteROBOInterface VPN1 MyRobo eth0
```

LSMcli ExportIke

Description

This command exports the IKE Certificate into a P12 file(encrypted with a provided password) from SmartLSM Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member.

The default location of the exported file is the `$FWDIR/conf/` directory.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ExportIke
<RoboName> <Password> <FileName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member, whose certificate is exported.
<Password>	Password used to protect the p12 file.
<FileName>	Destination file name (is created).

Example

```
LSMcli mySrvr name pass ExportIke MyROBO ajg42k93N MyROBOCert.p12
```

LSMcli ResetIke

Description

This command resets the IKE Certificate of a SmartLSM Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member.

This action revokes the existing IKE certificate and creates a new one.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ResetIke
<RoboName> [-CA=<CaName> [-R=<CertificateIdentifier#>] [-
KEY=<AuthorizationKey>]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member.
<CaName>	Name of the Trusted CA object (created from SmartConsole) the IKE certificate request is sent to this CA.
<CertificateIdentifier>	Key identifier of the specific certificate.
<AuthorizationKey>	Authorization Key to be sent to the CA for the certificate retrieval.

Example

```
LSMcli mySrvr name pass ResetIke MyROBO -CA=OPSEC_CA -R=cer3452s -
KEY=ad23fgh
```

LSMcli Remove

Description

This command deletes a SmartLSM Security Gateway.

This action revokes all the certificates used by the SmartLSM Security Gateway, releases all the licenses and, finally, removes the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Remove <RoboName>
<ID>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the Security Gateway.
<ID>	ID of the SmartLSM Security Gateway. Use the *"LSMcli Show" on page 170* command to check the ID of the specific SmartLSM Security Gateway.

Example

```
LSMcli mySrvr name pass Remove MyRobo 0.0.0.251
```

LSMcli ResetSic

Description

This command resets the SIC Certificate of a SmartLSM Security Gateway or SmartLSM Cluster Member.

This action revokes the Security Gateway's SIC certificate and creates a new one with the one-time password provided by the user.

If an IP address is supplied for the SmartLSM Security Gateway, the SIC certificate is pushed to the SmartLSM Security Gateway, in which case the SmartLSM Security Gateway SIC one-time password must be initialized first.

Otherwise, if no IP address is given, the SIC certificate is later pulled from the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ResetSic
<RoboName> <ActivationKey> [-I=<IPAddress>]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster Member.
<ActivationKey>	One-time password for the Secure Internal Communications with the SmartLSM Security Gateway.
<IPAddress>	IP address of Security Gateway (for this action, the certificate is pushed to the Security Gateway).

Example 1

```
LSMcli mySrvr name pass ResetSic MyROBO aw47q1
```

Example 2

```
LSMcli mySrvr name pass ResetSic MyFixedIPROBO sp36rt1 -
I=10.20.30.1
```

LSMcli Show

Description

This command displays a list of existing Security Gateways.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Show [-N=<Gateway Name>] [-F=<FilterFlags>]
```

Parameters

Parameter	Description
`<Mgmt Server>`	Name or IP address of the Security Management Server or Domain Management Server.
`<Username>`	User name of standard Check Point authentication method.
`<Password>`	Password of standard Check Point authentication method.
`<Gateway Name>`	Name of the Security Gateway to display. If the "`-N`" flag is not included, the command prints the existing **Devices** work space, including SmartLSM Security Gateways.
`-F=<` *`FilterFlags`*`>`	You can use these flags to filter the printed information: ■ `b` - ID ■ `c` - Cluster ID ■ `d` - List of Dynamic Objects assigned to this SmartLSM Security Gateways ■ `g` - Gateway status ■ `i` - IP address ■ `k` - IKE DN ■ `l` - Policy status ■ `n` - Name ■ `p` - SmartLSM Security Profile ■ `s` - SIC DN ■ `t` - Type ■ `v` - Version **Note** - To specify more than one filter flag, write them together. Example: `-F=bn`

Example 1

```
LSMcli mySrvr name pass Show -N=MyRobo
```

Example 2

```
LSMcli mySrvr name pass Show -F=binpt
```

LSMcli ShowROBOTopology

Description

This command displays the Topology information of the SmartLSM Security Gateway.

It lists the defined Interfaces and their respective IP Addresses and Network Masks, and the VPN Domain configuration.

You can use the indexes of the manually defined VPN domain IP address ranges, on the displayed list, when you request to delete a range, with the *"LSMcli ModifyROBOManualVPNDomain" on page 159* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ShowROBOTopology
<RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of Security Gateway.

Example

```
LSMcli mySrvr name pass ShowROBOTopology MyRobo
```

LSMcli UpdateCO

Description

This command updates a Corporate Office (CO) Security Gateway.

This action updates the CO Security Gateway with up-to-date available information about the VPN Domains of the SmartLSM Security Gateways.

Perform this action after you add a new SmartLSM Security Gateway to enable the CO gateway to initiate a VPN tunnel to the new SmartLSM Security Gateway.

Alternatively, you can Install Policy on the CO gateway to obtain updated VPN Domain information.

Note - This command supports CO Security Gateways only.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> UpdateCO {<COgw>
| COgwCluster}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<CoGw>	Name of a CO gateway.
<CoGwCluster>	Name of a cluster of CO gateways.

Example

```
LSMcli mySrvr name pass UpdateCO MyCO
```

SmartUpdate Actions

This section describes commands that perform SmartUpdateactions on SmartLSM Gateways.

Before you can install software on gateways, you must first load it to the Security Management Server.

Best Practice - Run the *"LSMcli VerifyInstall" on page 178* command to make sure that the software is compatible.

Use the *"LSMcli Install" below* command to install the software.

Use the *"LSMcli Uninstall" on page 176* command to uninstall the software.

LSMcli Install

Description

This command installs the specified software on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - Before you can install software on SmartLSM Security Gateways, you must first load it to the Security Management Server.

Best Practice - Run the *"LSMcli VerifyInstall" on page 178* command to make sure that the software is compatible.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Install <RoboName>
<Product> <Vendor> <Version> <SP> [-P=<Profile>] [-boot] [-
DoNotDistribute]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.

Parameter	Description
<Vendor>	Name of the vendor of the package.
<Version>	Major Version of the package.
<SP>	Minor Version of the package.
<Profile>	Assign a different SmartLSM Security Profile (already defined in SmartConsole) after installation.
`boot`	Reboot the SmartLSM Security Gateway after installation.
`-DoNotDistribute`	Optional. Install previously distributed packages.

Example

```
LSMcli mySrvr name pass Install MyRobo firewall checkpoint NG_AI
fcs -P=AnyProfile -boot
```

LSMcli Uninstall

Description

This command uninstalls the specified package from the SmartLSM Security Gateway or SmartLSM Cluster Member.

You can use the *"LSMcli ShowInfo" on page 182* command to see what products are installed on the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Uninstall
<RoboName> <Product> <Vendor> <Version> <SP> [-P=<Profile>] [-
boot]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major Version of the package.
<SP>	Minor Version of the package.
<Profile>	Assign a different SmartLSM Security Profile (already defined in SmartConsole) after uninstall.
`boot`	Reboot the SmartLSM Security Gateway after installation.

Example

```
LSMcli mySrvr name pass Uninstall MyRobo firewall checkpoint NG_AI
fcs -boot
```

LSMcli Distribute

Description

This command distributes a package from the Repository to the SmartLSM Security Gateway or SmartLSM Cluster Member, but does not install it.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Distribute
<RoboName> <Product> <Vendor> <Version> <SP>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major version of the package.
<SP>	Minor version of the package.

Example

```
LSMcli mySrvr name pass Distribute MyRobo fw1 checkpoint NG_AI R54
```

LSMcli VerifyInstall

Description

This command makes sure that the software is compatible to install on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - Note that this action does not perform an installation.

Best Practice - Run this command before you install the software on the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> VerifyInstall
<RoboName> <Product> <Vendor> <Version> <SP>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major version of the package.
<SP>	Minor version of the package.

Example

```
LSMcli mySrvr name pass VerifyInstall MyRobo firewall checkpoint
NG_AI fcs
```

LSMcli VerifyUpgrade

Description

This command verifies if you can upgrade a selected software on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - This command does not perform an installation.

Best Practice - Run this command before you run the *"LSMcli Upgrade" on page 180* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> VerifyUpgrade
<RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.

Example

```
LSMcli mySrvr name pass VerifyUpgrade MyRobo
```

LSMcli Upgrade

Description

This command upgrades all the (appropriate) available software packages on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Best Practice - Run the *"LSMcli VerifyUpgrade" on page 179* command before you run this command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Upgrade <RoboName>
[-P=<Profile>] [-boot]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Profile>	Assign a different SmartLSM Security Profile (already defined in SmartConsole) after installation.
boot	Reboot the SmartLSM Security Gateway after the installation is finished.

Example

```
LSMcli mySrvr name pass Upgrade MyRobo -P=myprofile -boot
```

LSMcli GetInfo

Description

This command collects product information from the SmartLSM Security Gateway or SmartLSM Cluster Member.

Important - If you upgrade any package manually instead of using SmartUpdate, you must run this command before you run the *"LSMcli ShowInfo" on page 182* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> GetInfo <RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.

Example

```
LSMcli mySrvr name pass GetInfo MyRobo
```

LSMcli ShowInfo

Description

This command displays product information for the list of the products installed on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Important - Before you run this command, run the *"LSMcli GetInfo" on page 181* command to make sure the information is up-to-date.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ShowInfo
<RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the Security Gateway.

Example

```
LSMcli mySrvr name pass ShowInfo MyRobo
```

LSMcli ShowRepository

Description

This command shows the list of the available products on the Management Server.

Use SmartUpdate to manage the products, load new products, remove products, and so on.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ShowRepository
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.

Example

```
LSMcli mySrvr name pass ShowRepository
```

LSMcli Stop

Description

This command stops Security Gateway services on the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Stop {<RoboName>
| <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Stop MyRobo
```

LSMcli Start

Description

This command starts Security Gateway services on the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Start {<RoboName>
| <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Start MyRobo
```

LSMcli Restart

Description

This command restarts Security Gateway services on the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Restart
{<RoboName> | <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Restart MyRobo
```

LSMcli Reboot

Description

This command reboots the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Reboot {<RoboName>
| <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Reboot MyRobo
```

LSMcli Push Actions

These commands are used to push updated values, settings, and security rules to gateways.

After you create a gateway or a dynamic object in the SmartProvisioning system, you must assign (push) a security policy to it.

LSMcli PushPolicy

Description

This command pushes a policy to the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Clusters.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> PushPolicy
{<RoboName> | <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway, or SmartLSM Cluster.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass PushPolicy MyRobo
```

LSMcli PushDOs

Description

This command updates a Dynamic Object's information on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - This command does not remove/release the IP address range for the deleted Dynamic Object, but only adds new ones. To overcome this difficulty, run the *"LSMcli PushPolicy" on page 189* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> PushDOs <RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster Member.

Example

```
LSMcli mySrvr name pass PushDOs MyRobo
```

LSMcli GetStatus

Description

This command fetches various statistics from the selected gateway.

Note - This command supports Security Gateways, SmartLSM Security Gateways, and Gateway or SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> GetStatus
{<RoboName> | <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster Member.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass GetStatus MyRobo
```

Managing SmartLSM Clusters with LSMcli

With the `LSMcli` command, you can define SmartLSM clusters, and configure most of the options available in SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard and in the **Edit** windows).

This section lists unique commands for SmartLSM Clusters.

Other commands that also apply to SmartLSM Clusters:

- *"LSMcli Distribute" on page 177*
- *"LSMcli GetInfo" on page 181*
- *"LSMcli GetStatus" on page 191*
- *"LSMcli Install" on page 174*
- *"LSMcli ModifyROBOManualVPNDomain" on page 159*
- *"LSMcli PushDOs" on page 190*
- *"LSMcli PushPolicy" on page 189*
- *"LSMcli Reboot" on page 187*
- *"LSMcli Reboot" on page 187*
- *"LSMcli ResetIke" on page 166*
- *"LSMcli ResetSic" on page 168*
- *"LSMcli Restart" on page 186*
- *"LSMcli ShowInfo" on page 182*
- *"LSMcli Start" on page 185*
- *"LSMcli Stop" on page 184*
- *"LSMcli Uninstall" on page 176*
- *"LSMcli Upgrade" on page 180*
- *"LSMcli VerifyInstall" on page 178*
- *"LSMcli VerifyUpgrade" on page 179*

Note - There is no convert action for or to SmartLSM clusters.

LSMcli AddROBO VPN1Cluster

Description

This command defines a new SmartLSM cluster.

You can configure all of the options available in the **New SmartLSM Cluster** wizard of the SmartProvisioning GUI.

The only exception is the configuration of Topology overrides (see *"LSMcli ModifyROBONetaccess VPN1Cluster" on page 197*).

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO
VPN1Cluster <Profile> <MainIPAddress> <SuffixName> [-
S=<SubstitutedNamePart>] [-CA=<CaName> [-R=<KeyIdentifier#>] [-
KEY=<AuthorizationCode>]]
```

Parameters

Parameter	Description	SmartLSM GUI Location
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.	
<Username>	User name of standard Check Point authentication method.	
<Password>	Password of standard Check Point authentication method.	
<Profile>	Name of cluster Profile to which to map the new cluster.	**New SmartLSM Cluster** wizard.
<MainIPAddress>	Main IP address of cluster.	**New SmartLSM Cluster** wizard.
<SuffixName>	A suffix to be added to cluster and member Profile names.	**New SmartLSM Cluster** wizard.
<SubstitutedName Part>	A part of the Profile name to be replaced by the suffix in the previous field.	SmartProvisioning GUI supports adding Prefix and/or Suffix, not substitution.

Parameter	Description	SmartLSM GUI Location
<CaName>	The name of the Trusted CA object, defined in SmartConsole, to which a VPN certificate request is sent.	Double-click the SmartLSM cluster object > **Edit** window > **VPN** tab
<KeyIdentifier#>	Number to identify the specific certificate, once generated.	Double-click the SmartLSM cluster object > **Edit** window > **VPN** tab
<AuthorizationCode>	Authorization Key to be sent to CA to enable certificate retrieval.	Double-click the SmartLSM cluster object > **Edit** window > **VPN** tab

LSMcli ModifyROBO VPN1Cluster

Description

You can change a SmartLSM cluster main IP address.

You can resolve a dynamic object for a SmartLSM cluster.

Syntax for changing the Main IP Address

You can change a SmartLSM cluster main IP address in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Cluster** tab), or with this command:

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBO
VPN1Cluster <ROBOClusterName> -I=<MainIPAddress>
```

Syntax for resolving a Dynamic Object

You can resolve a dynamic object for a SmartLSM cluster in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Dynamic Objects** tab), or with this command:

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBO
VPN1Cluster <ROBOClusterName> -D:<DO Name>={<IP> | <IP1-IP2>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<Profile>	Name of cluster Profile to which to map the new cluster.
<MainIPAddress>	Main IP address of cluster.
<DO Name>	Name of the Dynamic Object.
<IP>	Single IP address.
<IP1-IP2>	Range of IP addresses.

LSMcli ModifyROBOTopology VPN1Cluster

Description

You can set the VPN domain of a SmartLSM cluster in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Note - When the VPN domain is set to Manual, the IP address ranges are those set in the SmartProvisioning GUI, or with the *"LSMcli ModifyROBOManualVPNDomain" on page 159* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBOTopology
VPN1Cluster <RoboClusterName> -VPNDomain={not_defined | external_
ip_only | topology | manual}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboClusterName>	Name of the SmartLSM Cluster.
`VPNDomain`	Specifies the VPN Domain topology: ▪ `not_defined` - Equivalent to the **Not Defined** option on the **Topology** tab of a SmartLSM Security Gateway in the SmartProvisioning GUI (or in the output of the *"LSMcli ShowROBOTopology" on page 172* command). ▪ `external_ip_only` - Equivalent to the **Only the external interface** configuration in the SmartProvisioning GUI. ▪ `topology` - Equivalent to the **All IP Addresses behind the Gateway based on Topology information** configuration in the SmartProvisioning GUI. ▪ `manual` - Equivalent to **Manually defined**. VPN domain is defined according to the configuration made with the *"LSMcli ModifyROBOManualVPNDomain" on page 159* command.

LSMcli ModifyROBONetaccess VPN1Cluster

Description

For the actual SmartLSM cluster, you can override the profile topology definitions of a cluster (virtual) interface in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyROBONetaccess VPN1Cluster <ClusterName> <InterfaceName> -
Mode={by_profile|override} [-TopologyType={external|internal}] [-
DMZAccess={true|false}] [-InternalIP={not_defined|this|specific}
[-AllowedGroup=<GroupName>]] [-AntiSpoof={true|false} [-
AllowedGroup=<GroupName>][-SpoofTrack={none|log|alert}]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ClusterName>	Name of SmartLSM cluster.
<InterfaceName>	Name of the cluster (virtual) interface. If the interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case, use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-Mode`	Specifies the configuration mode: ▪ `by_profile` - Configure as defined in the cluster **Profile**. ▪ `override` - Configure the settings here. In this case, specify the "`-TopologyType`".

Parameter	Description
`-TopologyType`	Specifies the interface topology: ■ `external` - Leads out to the Internet. ■ `internal` - Leads to the local network.
`-DMZAccess`	Specifies whether this interfaces leads to DMZ (`true`), or not (`false`).
`-InternalIP`	Specifies the network behind an internal interface: ■ `not_defined` - Network is not defined. ■ `this` - Network is defined by the IP address and net mask of this interface. ■ `specific` - Network is defined by the value of the "`-AllowedGroup`".
`-AntiSpoof`	Specifies whether to perform Anti-Spoofing: ■ `true` - Perform Anti-Spoofing based on interface topology. In this case, optionally use the "`-AllowedGroup`" and "`-SpoofTrack`". ■ `false`- Do not perform Anti-Spoofing. If the interface is internal, and the IP addresses behind the interface are not defined, Anti-Spoofing is not possible.
`-AllowedGroup`	If Anti-Spoofing is performed, specifies the Network Group object, from which packets are not checked. ■ If "`-TopologyType=external`", this parameter defines a group, from which packets are not checked if Anti-Spoofing is performed ■ If "`-TopologyType=internal`", this parameter explicitly defines the networks behind the internal interface.
`-SpoofTrack`	If Anti-Spoofing is performed, specifies the tracking action when spoofing is detected: ■ `none` - No action ■ `log` - Generate a log ■ `alert` - Show an alert popup

LSMcli AddClusterSubnetOverride VPN1Cluster

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member interfaces
- IP addresses of cluster member interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 201* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only this "`AddClusterSubnetOverride`" command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 203* command.
- To define overrides for a private (monitored or non-monitored) interface, use one of these commands:
  - *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 205*
  - *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 207*
  - *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 209*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
AddClusterSubnetOverride VPN1Cluster <ROBOClusterName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -
CNetMask=<ClusterNetMask>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"
- "`-CIP`" *and* "`-CNetMask`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM cluster.
<InterfaceName>	Name of cluster (virtual) interface, as defined in the **Profile** topology. Use the name of the cluster interface even if you set values for cluster members' interfaces. If the cluster interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.
`-CIP`	New IP address for the cluster (virtual) interface.
`-CNetMask`	Net mask for the cluster (virtual) interface.

LSMcli ModifyClusterSubnetOverride VPN1Cluster

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member interfaces
- IP addresses of cluster member interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only this "`ModifyClusterSubnetOverride`" command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 199* command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 203* command.
- To define overrides for a private (monitored or non-monitored) interface, use one of these commands:
  - *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 205*
  - *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 207*
  - *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 209*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyClusterSubnetOverride VPN1Cluster <ROBOClusterName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -
CNetMask=<ClusterNetMask>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"
- "`-CIP`" *and* "`-CNetMask`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM cluster.
<InterfaceName>	Name of cluster (virtual) interface, as defined in the **Profile** topology. Use the name of the cluster interface even if you set values for cluster members' interfaces. If the cluster interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.
`-CIP`	New IP address for the cluster (virtual) interface.
`-CNetMask`	Net mask for the cluster (virtual) interface.

LSMcli DeleteClusterSubnetOverride VPN1Cluster

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member interfaces
- IP addresses of cluster member interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only this *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 201* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 205* command.
- To cancel a value and return to the value set by the **Profile**, use this "`DeleteClusterSubnetOverride`" command.
- To define overrides for a private (monitored or non-monitored) interface, use one of these commands:
  - *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 205*
  - *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 207*
  - *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 209*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
DeleteClusterSubnetOverride VPN1Cluster <ROBOClusterName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -
CNetMask=<ClusterNetMask>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"
- "`-CIP`" *and* "`-CNetMask`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM cluster.
<InterfaceName>	Name of cluster (virtual) interface, as defined in the **Profile** topology. Use the name of the cluster interface even if you set values for cluster members' interfaces. If the cluster interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.
`-CIP`	New IP address for the cluster (virtual) interface.
`-CNetMask`	Net mask for the cluster (virtual) interface.

LSMcli AddPrivateSubnetOverride VPN1ClusterMember

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member monitored interfaces or non-monitored interfaces
- IP addresses of cluster member monitored interfaces or non-monitored interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 207* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only this "`AddPrivateSubnetOverride`" command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 209* command.
- To define overrides for a cluster interface, use one of these commands:
  - *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 199*
  - *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 201*
  - *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 203*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
AddPrivateSubnetOverride VPN1ClusterMember <ROBOMemberName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOMemberName>	Name of the SmartLSM cluster member.
<InterfaceName>	Name of cluster member private interface, as defined in the **Profile** topology.
-IName	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
-MNet	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.

LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member monitored interfaces or non-monitored interfaces
- IP addresses of cluster member monitored interfaces or non-monitored interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the "`ModifyPrivateSubnetOverride`" command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 205* command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 209* command.
- To define overrides for a cluster interface, use one of these commands:
  - *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 199*
  - *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 201*
  - *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 203*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyPrivateSubnetOverride VPN1ClusterMember <ROBOMemberName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOMemberName>	Name of the SmartLSM cluster member.
<InterfaceName>	Name of cluster member private interface, as defined in the **Profile** topology.
-IName	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
-MNet	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.

LSMcli DeletePrivateSubnetOverride VPN1ClusterMember

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member monitored interfaces or non-monitored interfaces
- IP addresses of cluster member monitored interfaces or non-monitored interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 207* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 205* command.
- To cancel a value and return to the value set by the **Profile**, use the "`DeletePrivateSubnetOverride`" command.
- To define overrides for a cluster interface, use one of these commands:
  - *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 199*
  - *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 201*
  - *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 203*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
DeletePrivateSubnetOverride VPN1ClusterMember <ROBOMemberName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOMemberName>	Name of the SmartLSM cluster member.
<InterfaceName>	Name of cluster member private interface, as defined in the **Profile** topology.
-IName	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
-MNet	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.

LSMcli RemoveCluster

Description

This command:

1. Revokes all the certificates used by the SmartLSM cluster and its members.
2. Releases all the licenses.
3. Deletes the SmartLSM cluster and member objects.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> RemoveCluster
<ROBOClusterName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM Cluster.

Using LSMcli Commands for Small Office Appliances

This section describes `LSMcli` commands for managing Small Office Appliances and Small Office Appliance Clusters.

LSMcli AddROBO <Appliance_Model>

Description

This command adds a Small Office Appliance Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO
<Appliance_Model> <ROBOName> <Profile> [-O=<ActivationKey> [-
I=<IP>]] [[-CA=<CaName> [-R=<CertificateIdentifier#>] [-
KEY=<AuthorizationKey>]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<Appliance_Model>	Model of appliance: ■ For 1100 appliances, enter: `CPSG80` ■ For 1200R appliances, enter: `1200R` ■ For 1430 or 1450 appliances, enter: `1430/1450` ■ For 1470 or 1490 appliances, enter: `1470/1490` ■ For 1530 or 1550 appliances, enter: `1530/1550` ■ For 1570 or 1590 appliances, enter: `1570/1590`
<RoboName>	Name of a SmartLSM Security Gateway.

Parameter	Description
<Profile>	Name of a SmartLSM Security Profile that was defined in SmartConsole.
<ActivationKey>	SIC one-time password (for this action, a certificate is generated).
IP	IP address of the gateway (for this action, a certificate is pushed to the gateway).
<CaName>	Name of the Trusted CA object (created from SmartConsole). The IKE certificate request is sent to this CA. Default is Check Point Internal CA.
<CertificateIdentifier#>	Key identifier for third-party CA.
<AuthorizationKey>	Authorization Key for third-party CA.

Examples

- To add a 1100 appliance Security Gateway:

```
LSMcli 192.168.3.26 aa aaaa AddROBO CPSG80 Paris_GW small_
office_profile
```

- To add a 1470/1490 appliance Security Gateway:

```
LSMcli 192.168.3.26 aa aaaa AddROBO 1470/1490 Paris_GW small_
office_profile
```

LSMcli AddROBO <Appliance_Model> Cluster

Description

This command adds a Small Office Appliance Cluster.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO
<Appliance_Model>Cluster <Profile> <MainIPAddress> <SuffixName> [-
S=<SubstitutedNamePart>] [-CA=<CaName> [-R=<KeyIdentifier#>] [-
KEY=<AuthorizationCode>]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
*<Appliance_ Model>*Cluster	Model of appliance: ■ For 1100 appliances, enter: `CPSG80Cluster` ■ For 1200R appliances, enter: `1200RCluster` ■ For 1430 or 1450 appliance, enter: `1430/1450Cluster` ■ For 1470 or 1490 appliance, enter: `1470/1490Cluster` ■ For 1530 or 1550 appliance, enter: `1530/1550Cluster` ■ For 1570 or 1590 appliance, enter: `1570/1590Cluster`
<Profile>	Name of cluster Profile to which to map the new cluster.
<MainIPAddress>	Main IP address of cluster.
<SuffixName>	A suffix to be added to cluster and member Profile names.
<SubstitutedName Part>	A part of the Profile name to be replaced by the suffix in the previous field.
<CaName>	The name of the Trusted CA object, defined in SmartConsole, to which a VPN certificate request is sent.
<KeyIdentifier#>	Number to identify the specific certificate, once generated.

Parameter	Description
<*AuthorizationCode*>	Authorization Key to be sent to CA to enable certificate retrieval.

Example

To add a 1450 cluster:

```
LSMcli 192.168.3.26 aa aaaa AddRobo 1430/1450Cluster cluster_
profile 1.1.1.1 Paris
```

Other LSMcli Commands for Small Office Appliances

- For all other commands on Small Office Appliance Gateways, replace the "`VPN1`" with the "`CPSG80`", for all appliance types.

  For example, change the profile (see *"LSMcli ModifyROBO VPN1" on page 157*):

  - For a 1100 Security Gateway:

    ```
    LSMcli 192.168.3.26 aa aaaa ModifyROBO CPSG80 Paris_GW -
    P=second_small_office_profile
    ```

  - For a 1200R Security Gateway:

    ```
    LSMcli 192.168.3.26 aa aaaa ModifyROBO CPSG80 Paris_GW -
    P=second_small_office_profile
    ```

- For all other commands on Small Office Appliance clusters, replace the "`VPN1Cluster`" with the "`CPSG80Cluster`", for all appliance types (for example, in *"LSMcli ModifyROBO VPN1Cluster" on page 195*).

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

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

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

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

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

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.