Important Information

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

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=22923
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07 February 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Smart Provisioning R76 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td><strong>Introduction to SmartProvisioning</strong></td>
<td>9</td>
</tr>
<tr>
<td>Check Point SmartProvisioning SmartConsole</td>
<td>9</td>
</tr>
<tr>
<td>Supported Features</td>
<td>9</td>
</tr>
<tr>
<td>SmartProvisioning Objects</td>
<td>10</td>
</tr>
<tr>
<td>Gatesways</td>
<td>10</td>
</tr>
<tr>
<td>Profiles</td>
<td>10</td>
</tr>
<tr>
<td>Profile Fetching</td>
<td>10</td>
</tr>
<tr>
<td>VPNs and SmartLSM Security Gateways</td>
<td>11</td>
</tr>
<tr>
<td><strong>Enabling SmartProvisioning</strong></td>
<td>12</td>
</tr>
<tr>
<td>Managing SmartProvisioning Components</td>
<td>12</td>
</tr>
<tr>
<td>Activating SmartProvisioning</td>
<td>12</td>
</tr>
<tr>
<td>Preparing SecurePlatform Gateways</td>
<td>13</td>
</tr>
<tr>
<td>Preparing SecurePlatform SmartLSM Security Gateways</td>
<td>13</td>
</tr>
<tr>
<td>Preparing CO Gateways</td>
<td>13</td>
</tr>
<tr>
<td>Preparing SecurePlatform Gateways</td>
<td>14</td>
</tr>
<tr>
<td>Preparing UTM-1 Edge Gateways</td>
<td>14</td>
</tr>
<tr>
<td>Installing SmartProvisioning SmartConsole</td>
<td>14</td>
</tr>
<tr>
<td><strong>Logging in to SmartProvisioning</strong></td>
<td>15</td>
</tr>
<tr>
<td>Defining SmartProvisioning as a SmartConsole</td>
<td>15</td>
</tr>
<tr>
<td>Defining SmartProvisioning Administrators</td>
<td>15</td>
</tr>
<tr>
<td>Logging In</td>
<td>16</td>
</tr>
<tr>
<td><strong>SmartProvisioning User Interface</strong></td>
<td>17</td>
</tr>
<tr>
<td>Main Window Panes</td>
<td>17</td>
</tr>
<tr>
<td>Tree Pane</td>
<td>17</td>
</tr>
<tr>
<td>Work Space Pane</td>
<td>17</td>
</tr>
<tr>
<td>Status View</td>
<td>19</td>
</tr>
<tr>
<td>SmartProvisioning Menus and Toolbar</td>
<td>20</td>
</tr>
<tr>
<td>Actions &gt; Packages</td>
<td>22</td>
</tr>
<tr>
<td>Working with the SmartProvisioning GUI</td>
<td>23</td>
</tr>
<tr>
<td>Find</td>
<td>23</td>
</tr>
<tr>
<td>Show/Hide Columns</td>
<td>23</td>
</tr>
<tr>
<td>Filter</td>
<td>24</td>
</tr>
<tr>
<td>Export to File</td>
<td>24</td>
</tr>
<tr>
<td>SSH Applications</td>
<td>25</td>
</tr>
<tr>
<td>Web Management</td>
<td>25</td>
</tr>
<tr>
<td><strong>SmartLSM Security Policies</strong></td>
<td>26</td>
</tr>
<tr>
<td>Understanding Security Policies</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Default SmartLSM Security Profile</td>
<td>26</td>
</tr>
<tr>
<td>Guidelines for Basic SmartLSM Security Policies</td>
<td>26</td>
</tr>
<tr>
<td>Creating Security Policies for Management</td>
<td>27</td>
</tr>
<tr>
<td>Creating Security Policies for VPNs</td>
<td>28</td>
</tr>
<tr>
<td>Downloading to UTM-1 Edge Devices</td>
<td>28</td>
</tr>
<tr>
<td><strong>SmartLSM Security Gateways</strong></td>
<td>29</td>
</tr>
<tr>
<td>Creating Security Gateway SmartLSM Security Profiles</td>
<td>29</td>
</tr>
<tr>
<td>Adding SmartLSM Security Gateways</td>
<td>29</td>
</tr>
<tr>
<td>Handling SmartLSM Security Gateway Messages</td>
<td>30</td>
</tr>
<tr>
<td>Opening Check Point Configuration Tool</td>
<td>30</td>
</tr>
<tr>
<td>Activation Key is Missing</td>
<td>31</td>
</tr>
<tr>
<td>Operation Timed Out</td>
<td>31</td>
</tr>
<tr>
<td>Complete the Initialization Process</td>
<td>31</td>
</tr>
<tr>
<td><strong>UTM-1 Edge SmartLSM Security Gateways</strong></td>
<td>32</td>
</tr>
</tbody>
</table>
Check Point SmartProvisioning enables you to manage many gateways from a single Security Management Server or Multi-Domain Security Management Domain Management Server, with features to define, manage, and provision (remotely configure) large-scale deployments of Check Point gateways.

The SmartProvisioning management concept is based on profiles — a definitive set of gateway properties and when relevant, a Check Point Security Policy. Each profile may be assigned to multiple gateways and defines most of the gateway properties per Profile object instead of per physical gateway, reducing the administrative overhead.

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

**Supported Features**

SmartProvisioning provides the following 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
- Tracking logs 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 for Security Gateway 80 devices.
SmartProvisioning Objects

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

Gateways

SmartProvisioning manages and provisions different types of gateways.

- **SmartLSM Security Gateways**: Remote gateways provide firewall security to local networks, while the security policies are managed from a central Security Management Server or Domain Management Server. By defining remote gateways through SmartLSM Security Profiles, a single system administrator or smaller team can manage the security of all your networks.

- **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, where the satellites are SmartLSM Security Gateways. The CO gateway has a static IP address, ensuring continued communications with SmartLSM Security Gateways that have dynamic IP addresses.

- **Provisioned Gateways**: SmartProvisioning can provision the Operating System and network settings of gateways, such as DNS, interface routing, providing more efficient management of large deployment sites.

Profiles

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

- **SmartLSM Security Profiles**: A SmartLSM Security Profile defines a Check Point Security Policy and other security-based settings for a type of SmartLSM Security Gateway. Each SmartLSM Security Profile can hold the configuration of any number of actual SmartLSM Security Gateways. SmartLSM Security Gateways must have a SmartLSM Security Profile; however, these profiles are not relevant for CO gateways or Provisioned gateways. SmartLSM Security Profiles are defined and managed through Check Point SmartDashboard.

- **Provisioning Profiles**: A Provisioning Profile defines specific settings for networking, device management, and the operating system. CO gateways, SmartLSM Security Gateways, and regular gateways may have Provisioning Profiles, if they are UTM-1, Power-1, SecurePlatform, IPSO 6.2-Based IP appliances, or UTM-1 Edge devices. Provisioning Profiles are defined and managed in SmartProvisioning. Defining options and features for Provisioning Profiles differ according to device platform.

Profile Fetching

All gateways managed by SmartProvisioning fetch their assigned profiles from the Security Management Server or Domain Management Server. You define the SmartLSM Security Profiles on SmartDashboard, preparing the security policies on the Security Management Server or Domain Management Server. You define Provisioning Profiles on SmartProvisioning, preparing the gateway settings on the SmartProvisioning database. Neither definition procedure pushes the profile to any specific gateway.

Managed gateways fetch their profiles periodically. Each gateway randomly chooses 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/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 specific properties of the gateway are used to localize the profile changes for each gateway. Thus, one profile is able to update potentially hundreds and thousands of gateways, each acquiring the new common properties, while maintaining its own local settings.
VPNs and SmartLSM Security Gateways

This section explains how your SmartLSM Security Gateways in a virtual private network (VPN) secure communications within your organization.

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

A VPN tunnel can be established from a SmartLSM Security Gateway to a regular, 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, using the IKE Certificate of the SmartLSM Security Gateway. The CO gateway treats the peer SmartLSM Security Gateway as if it were a regular DAIP gateway, whose properties are defined by the SmartLSM Security Profile to which the SmartLSM Security Gateway is mapped. A CO gateway can also initiate a VPN tunnel to a SmartLSM Security Gateway.

You can establish VPN tunneling for SmartLSM-to-SmartLSM, or SmartLSM-to-other gateway configurations, through the CO gateway.
Chapter 2

Enabling SmartProvisioning

In This Chapter

Managing SmartProvisioning Components 12
Activating SmartProvisioning 12
Preparing SecurePlatform Gateways 13
Preparing UTM-1 Edge Gateways 14
Installing SmartProvisioning SmartConsole 14

Managing SmartProvisioning Components

SmartProvisioning is an integral part of the Security Management or the Domain Management Server.

To use SmartProvisioning on the Security Management Server or the Domain Management Server, you must obtain and add a SmartProvisioning license to the Security Management Server or Domain Management Server.

Enabling of SmartProvisioning includes configuration of:
- SmartLSM Security Gateways
- Corporate Office Gateways
- Provisioned Gateways
- SmartProvisioning GUI

Activating SmartProvisioning

SmartProvisioning is an integral part of the Security Management Server or Domain Management Server.

To enable SmartProvisioning on the Security Management Server:
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.
3. For Domain Management Server, enable SmartProvisioning and run the command LSMenabler on. This message is displayed: Check Point services should be restarted. Restart now (y/n) [y]?
4. Enter y to restart the Check Point services.

To verify that SmartProvisioning is enabled:
1. Connect to the Security Management Server or to the Domain Management Server using SmartDashboard.
2. Edit the Security Management object.
3. In the General Properties page of the Security Management object, in the Software Blades section, Management tab, ensure Provisioning is selected. It is selected if the license for SmartProvisioning is installed.
Preparing SecurePlatform Gateways

Preparing SecurePlatform SmartLSM Security Gateways

SmartLSM Security Gateway is a Check Point gateway that has an assigned SmartLSM Security Profile. SmartLSM Security Gateways may, or may not, be enabled for provisioning.

To prepare a SmartLSM Security Gateway:
1. Make sure that Check Point Security Gateway R60 or higher is installed.
2. Execute these CLI commands:
   
   LSMenabler -r on
   cpstop
   cpstart

3. Open the Check Point Configuration Tool (cpconfig) on the gateway to the ROBO Interfaces page and define an External interface.
4. Decide whether you want this gateway to be provisioned or not. If this gateway should support provisioning, install SmartProvisioning with the SmartProvisioning Wizard (see SmartProvisioning Wizard - Getting Started (see "SmartProvisioning Wizard" on page 34)).

After completing installation of SmartProvisioning on gateways and the Security Management Server or Domain Management Server, open SmartDashboard and create a Security Policy and SmartLSM Security Profile required by SmartLSM Security Gateways.

To prepare the SmartLSM Security Gateway required objects:
1. In SmartDashboard select File > New, create a Security Policy and save it.
2. In the Network Objects tree, right-click Check Point and select SmartLSM Profile > UTM-1/Open Server/UTM-1/Power-1/Open Server/IP Series Gateway or 80 series Gateway.
3. In the SmartLSM Security Profile window, configure the SmartLSM Security Profile, and then click OK.
5. Click OK.
   Repeat for each SmartLSM Security Profile that you want. If you want to manage gateways of different types (UTM-1 Edge or Security Gateway), you will need a SmartLSM Security Profile for each type.
6. Close SmartDashboard.
7. Open SmartProvisioning and add the SmartLSM SecurePlatform gateways. See SmartLSM Security Gateways - Getting Started (see "SmartLSM Security Gateways" on page 29).

Preparing CO Gateways

A Corporate Office (CO) gateway represents the center of a Star VPN, in which the satellites are SmartLSM Security Gateways. The CO gateway may, or may not, be enabled for provisioning.

To prepare a CO gateway:
1. On the Check Point Security Gateway, execute the command:
   LSMenabler on
2. Open SmartDashboard and do the following:
   a) In the VPN tab, right-click and select New Community > Star.
   b) In the Star Community Properties window, select Center Gateways and add the CO gateway.
   c) In Satellite Gateways, add SmartLSM Security Profiles as required.
3. Close SmartDashboard.
4. In SmartProvisioning, right-click the CO gateway and select Update selected CO Gateway.
**Preparing SecurePlatform Gateways**

To prepare a SecurePlatform gateway for provisioning:

1. Ensure that R65 HFA 40 or later is installed.
   - If the R65 gateways are not ready to be provisioned, you must manually add the HFA 40 (or later) package for SecurePlatform to the SmartUpdate repository on the Security Management Server or Domain Management Server.
2. Install SmartProvisioning using the SmartProvisioning Wizard (on page 34).

**Preparing UTM-1 Edge Gateways**

A UTM-1 Edge gateway is a Check Point device. It may be a SmartLSM Security Gateway, with an assigned SmartLSM Security Profile, or it may be enabled for Provisioning, or both. Each UTM-1 Edge device is configured with Safe @ or Edge Firmware. Consult with Technical Support for the firmware version needed to support SmartProvisioning.

Configure SmartProvisioning to recognize the firmware of a UTM-1 Edge gateway.

**To configure firmware:**

1. In a Devices work space, right-click a UTM-1 Edge gateway and select **Edit Gateway**.
2. In the **UTM-1 Edge [SmartLSM] Gateway** window, select the **Firmware** tab.
3. Select the option that describes this UTM-1 Edge SmartLSM Security Gateway.
   - **Use default**: Firmware defined as Default in SmartUpdate.
   - **Use SmartLSM Security Gateway's installed firmware**: Firmware currently installed on a UTM-1 Edge SmartLSM Security Gateway.
   - **Use the following firmware**: Firmware to be uploaded (with SmartUpdate) to the UTM-1 Edge gateway.

**Installing SmartProvisioning SmartConsole**

After you enable the SmartProvisioning on the Security Management Server or Multi-Domain Server, the SmartProvisioning SmartConsole is provided automatically.

1. From the **Start** menu, select **Programs > Check Point SmartConsole > SmartProvisioning**.
2. When logging in, provide the IP address of the SmartProvisioning Security Management Server or the Domain Management Server.
Chapter 3

Logging in to SmartProvisioning

In This Chapter
- Defining SmartProvisioning as a SmartConsole
- Defining SmartProvisioning Administrators
- Logging In

Defining SmartProvisioning as a SmartConsole

This section describes how to define the workstation on which the SmartProvisioning SmartConsole is installed, as a Check Point SmartConsole client.

To define the SmartProvisioning SmartConsole:
1. On the Security Management Server, open the Check Point Configuration Tool (cpconfig); in a Multi-Domain Security Management environment, open the mdsconfig tool or the SmartDomain Manager.
2. Select the GUI Clients tab.
3. Identify the SmartProvisioning workstation by any one of the following:
   - IP address
   - Machine name
   - IP/Net mask: Range of IP addresses
   - IP address with wildcards: For example: 192.22.36.*
   - Any: Enable any machine to connect to the Domain Management Server as a client
   - Domain (Multi-Domain Security Management only): Enable any host in the domain to be a recognized GUI client

Defining SmartProvisioning Administrators

Login permissions to the SmartProvisioning Console are given to administrators, which are defined in SmartDashboard or in the Check Point Configuration Tool. In SmartDashboard, you can further define specific permissions of administrators. In particular, you can define an administrator’s permissions for provisioning devices with SmartProvisioning.

To edit the Permissions Profile of an administrator of SmartProvisioning:
1. Open SmartDashboard.
2. Open the Administrator Properties window of a new or existing administrator.
3. Click the New button that is next to the Permissions Profile field.
4. Select Customized and click Edit.
5. In the General tab, make sure that SmartLSM Security Gateways Database has Read/Write permissions.
6. In the **Provisioning** tab, define SmartProvisioning permissions for this administrator.

<table>
<thead>
<tr>
<th>Option</th>
<th>Read/Write</th>
<th>Read Only</th>
<th>Deselected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Provisioning Profiles</td>
<td>Add, edit, delete, assign provisioning profiles to gateways</td>
<td>Assign existing provisioning profiles to gateways</td>
<td>Provisioning features are unavailable</td>
</tr>
<tr>
<td>Manage Device Settings</td>
<td>Edit all gateway network settings</td>
<td>View gateway network settings</td>
<td>Gateway network settings are unavailable</td>
</tr>
<tr>
<td>Run Scripts</td>
<td>Add, edit, delete, and run scripts on gateways</td>
<td></td>
<td>Run script commands are unavailable</td>
</tr>
</tbody>
</table>

7. Click **OK**.
   The changes in permissions are applied the next time the administrator logs in.

**Logging In**

**To log into SmartProvisioning SmartConsole:**

1. Start SmartProvisioning:
   - From the Windows **Start** menu, select **Programs > Check Point SmartConsole > SmartProvisioning**.
   - From SmartDashboard, select **Window > SmartProvisioning**.

2. Provide an Administrator user name and password, and click **OK**.
Chapter 4

SmartProvisioning User Interface

In This Chapter

Main Window Panes 17
SmartProvisioning Menus and Toolbar 20
Working with the SmartProvisioning GUI 23

Main Window Panes

The main SmartProvisioning window has separate panes, each with its own purpose and each with a different connection to the other panes.

Tree Pane

The tree pane provides easy access to the list of objects that you can view and manage in the work space.

Work Space Pane

The view of the work space pane changes according to the object selected in the tree.

- **Devices** work space - Use this work space to manage gateways and other device objects, such as clusters.
- To show the Devices work space, click Devices in the tree.
- To see a Device work space by type of configuration, select Device Configuration > Networking, and then the tree item that describes the configuration you want (DNS, Routing, Interfaces, Hosts, Domain Name, Host Name).

- Profiles work space - Use this work space to manage Provisioning Profiles. Click Profiles in the tree.

- Status - Shows dynamic status of devices. Click Status in the tree.
Status View

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

- **Action Status**: For each device upon which you initiate an action, you can view the status and details of the action performance:
  - **Name**: The name of the action.
  - **Action type**: The type of action. See SmartProvisioning Menus and Toolbar (on page 20)
  - **Start Time**: The time when the action actually 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 status of the gateway, 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

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

### Policy Status Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Gateway is up and performing correctly</td>
</tr>
<tr>
<td>Waiting</td>
<td>SmartProvisioning is waiting for status from Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>Unknown</td>
<td>Status of gateway is unknown</td>
</tr>
<tr>
<td>Not installed</td>
<td>Security policy is not installed on this gateway</td>
</tr>
<tr>
<td>Not updated</td>
<td>Installed security policy has been changed; gateway should fetch new policy from Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>May be out of date</td>
<td>Security Policy was not retrieved within the fetch interval</td>
</tr>
</tbody>
</table>

### Provisioning Profile Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>SmartProvisioning Agent is installed and operating</td>
</tr>
</tbody>
</table>
### SmartProvisioning Menus and Toolbar

This section is a reference for the menus and toolbar buttons in SmartProvisioning. The menu commands that are available at any time 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.

#### SmartProvisioning Menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Description</th>
<th>For further information</th>
</tr>
</thead>
</table>
| File | New     | Define new SmartLSM Security Gateway or Provisioning Profile | See Creating Security Gateway SmartLSM Security Profiles (on page 29)  
See Adding UTM-1 Edge SmartLSM Security Gateways (on page 32)  
See Creating Provisioning Profiles |
<p>|      | Export to file... | Export objects list to file | See Export to File (on page 24) |
|      | Exit    | Close SmartProvisioning |
| Edit | Edit gateway | Edit selected gateway | See All Gateway Management Overview |
|      | Delete SmartLSM Security Gateway | Delete selected gateway; only for devices with SmartLSM Security Profiles | See Deleting Gateway Objects (on page 47) |
|      | Edit Provisioning profile | Edit Provisioning Profile of selected gateway | See Provisioning (on page 36) |
| Find |         | Find specific object in visible list | See Find (on page 23) |
| View | Toolbar | Show/Hide Status Bar |</p>
<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Description</th>
<th>For further information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status bar</td>
<td>Show/Hide Status View pane</td>
<td>See Main Window Panes</td>
<td></td>
</tr>
<tr>
<td>Status View</td>
<td>Show/Hide Status View pane</td>
<td>See Status View (on page 19)</td>
<td></td>
</tr>
<tr>
<td>Clear All Filters</td>
<td>Clears all the configured</td>
<td>See Filtering Columns (on page 24)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Show/Hide columns</td>
<td>Open the Show/Hide Columns</td>
<td>See Show/Hide Columns (on page 23)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>window and select the data</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to be displayed in the work</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>space</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage</td>
<td>Open Selected Policy</td>
<td>Open SmartDashboard to edit Security Policy installed on selected</td>
<td>SmartLSM Security Policies (on page 26)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SmartLSM Security Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open Selected Policy</td>
<td>Open SmartDashboard to view Security Policy of selected SmartLSM Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Read Only)</td>
<td>Security Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom Commands</td>
<td>Add/Edit user-defined executables to run on remote gateways</td>
<td>See Executing Commands (on page 48)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select SSH Application</td>
<td>Provide pathname to SSH application for remote management of devices</td>
<td>See SSH Applications (on page 25)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Push Dynamic objects</td>
<td>Push values resolved in Smart Provisioning to SmartLSM Security Gateway</td>
<td>See Dynamic Objects (&quot;Provisioning&quot; on page 36)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Push Policy</td>
<td>Push values resolved in Smart Provisioning to SmartLSM Security Gateway</td>
<td>See Immediate Gateway Actions (on page 46)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance &gt; Stop Gateway</td>
<td>Stop Check Point services on selected gateway</td>
<td>See Remotely Controlling Gateways (on page 46)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance &gt; Start Gateway</td>
<td>Start Check Point services on selected gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance &gt; Restart Gateway</td>
<td>Restart Check Point services on selected gateway</td>
<td></td>
</tr>
<tr>
<td>Menu</td>
<td>Command</td>
<td>Description</td>
<td>For further information</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Maintenance &gt; Reboot Gateway</td>
<td>Reboot the device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Get Status Details</td>
<td>Open Gateway Status Details</td>
<td>See Viewing Status of Remote Gateways (on page 75)</td>
</tr>
<tr>
<td></td>
<td>Get actual settings</td>
<td>Fetch configuration settings from device to management server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Packages</td>
<td>Software management</td>
<td>See Actions &gt; Packages (on page 22)</td>
</tr>
<tr>
<td></td>
<td>Update Corporate office gateway</td>
<td>Update a CO Gateway to reflect changes in managed gateways</td>
<td>See Remotely Controlling Gateways (on page 46)</td>
</tr>
<tr>
<td></td>
<td>Updated Selected Corporate Office Gateway</td>
<td>Update selected CO (available when CO gateway is selected)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advanced Permissions</td>
<td>Create a custom script</td>
<td>See Running Scripts (on page 75)</td>
</tr>
<tr>
<td></td>
<td>Backup</td>
<td>Create a backup image</td>
<td>See Immediate Backup of Security Gateways (on page 76)</td>
</tr>
<tr>
<td></td>
<td>Push Settings and Action</td>
<td>Immediate execute of Backup and fetch of profile settings</td>
<td>See Applying Changes (on page 77)</td>
</tr>
<tr>
<td></td>
<td>Define UTM-1 Edge cluster</td>
<td>Configure two UTM-1 Edge SmartLSM Security Gateways for high availability</td>
<td>See UTM-1 Edge clusters (“SmartLSM Clusters” on page 89)</td>
</tr>
<tr>
<td></td>
<td>Remove UTM-1 Edge clusters</td>
<td>Disassociate the two members of a UTM-1 Edge Cluster</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run SmartProvisioning Wizard</td>
<td>Opens SmartProvisioning wizard from Overview page</td>
<td>See SmartProvisioning Wizard (on page 34)</td>
</tr>
<tr>
<td>Window</td>
<td>Access other SmartConsole clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td>View version information and open online help</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Actions > Packages**

The Actions menu also includes the Packages menu. Package commands enable you to manage software on Security Gateways and SmartLSM Security Gateways.

These commands are not relevant or available for UTM-1 Edge gateways. To manage the software of UTM-1 Edge devices, use the UTM-1 Edge portal (right-click > Launch UTM-1 Edge Portal).
The table below describes the commands of the Packages menu. See Managing Software (on page 73) to learn more about managing Check Point software packages with SmartProvisioning.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Package command</th>
<th>Action</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Upgrade all packages</td>
<td>Download Security Gateway software upgrade from Package Repository and install all contained packages on selected gateway</td>
<td>See Upgrading Packages with SmartProvisioning (on page 74)</td>
</tr>
<tr>
<td></td>
<td>Distribute package</td>
<td>Download Hotfix or HFA from Package Repository and install on selected gateway</td>
<td>See Distributing Packages with SmartProvisioning (on page 74)</td>
</tr>
<tr>
<td></td>
<td>Pre-install verifier</td>
<td>Verify that an installation is needed and possible</td>
<td>See Verifying Pre-Install (on page 74)</td>
</tr>
<tr>
<td></td>
<td>Get Gateway data</td>
<td>View installed Check Point packages on selected Security Gateway.</td>
<td>See Viewing Installed Software (on page 74)</td>
</tr>
</tbody>
</table>

**Working with the SmartProvisioning GUI**

This section describes SmartConsole customizations and general functions.

**Find**

You can search for strings in the SmartProvisioning console.

To open the Find window:

1. 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
   - Security Profile
   - Provisioning Profile
   - Policy Name
   - Last Applied Settings
   - Gateway Status: Use a valid status string (see "Status View" on page 19)
   - Policy Status: Use a valid status string ("Status View" on page 19)
   - Provisioning Status: Use a valid status string ("Status View" on page 19)
   - Maintenance Mode: Yes or No ("Maintenance Mode" on page 77)

**Show/Hide Columns**

You can customize the information displayed in Device lists.

To customize Device list columns:

1. Select View > Show/Hide Columns.
2. In the Show/Hide Columns window, select the check boxes of the columns that you would like to be displayed.
3. Clear the check boxes of the columns that you would like to hide.
It is also possible to hide a column by right-clicking the column header selecting **Hide Column** from the popup menu.

**Filter**

You can filter a **Devices** work space for more convenient displays.

**To filter the list:**
1. Select the **Devices** work space.
2. In **Look for**, enter the filter number or text.
3. From the **In** drop-down list, select the filter category that you want. You can select one of these filter categories:
   - **All**: The filter number or text is applied to all the filter categories. (Default)
   - **Name**: name of the gateway and icon indicating its type (Security Management server, Domain Management Server, SmartLSM Security Gateway, UTM-1 Edge 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 Profile.
   - **Provisioning Status**: Security Gateway provisioning status.
   - **DNS Overrides Profile**: The **Devices** work space is filtered to display only the objects (gateways, servers, clusters and so on) that match the filter number or text for that category.

**Filtering Columns**

You can filter columns in **Devices** and **Devices Configuration** displays according to the content of that column.

**To filter a column:**
1. In the tree, select **Devices** or the **Device Configuration** display.
2. Right-click the column heading and select **Add/Edit Filter**.
   - The Advanced Filter window is displayed.
3. Configure the filter settings for that column.
4. Click **OK**.
5. To clear the filter settings, right-click the column heading and select **Clear Filter**.

**Export to File**

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

**To export SmartProvisioning data to a file:**
1. 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.
**SmartProvisioning User Interface**

- **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 provide management features for remote devices. This feature is supported by SecurePlatform devices.

### Selecting a Default SSH Application

If you have not yet opened an SSH application, you can provide the path from within SmartProvisioning. The first time you select an SSH application, choose a default application from Manage > Select SSH Application. Each subsequent time that you want to open an SSH terminal, you can right-click on any object whose operating system is SecurePlatform and select Launch SSH Terminal.

**To 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, choose a predefined application template, such as Putty or SecureCRT, or create your own by selecting Custom. Verify 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 Network Objects

After you have selected a default SSH application for the first time, you can launch it from any object whose operating system is SecurePlatform.

**To launch the default SSH application from a Network object:**
1. Right-click on a Network object
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 SecurePlatform gateways. This is especially useful with remote gateways that need individual changes, or system administration management.

**To manage a SecurePlatform gateway through its Web portal:**
   A web browser opens to https://<IP_address>.
2. Log in with the administrator user name and password.
   The features available from the Web portal enable you to manage networking, routing, servers, and many other local device configurations.
Chapter 5

SmartLSM Security Policies

In This Chapter

- Understanding Security Policies .............................................. 26
- Configuring Default SmartLSM Security Profile ......................... 26
- Guidelines for Basic SmartLSM Security Policies ....................... 26
- Creating Security Policies for Management .............................. 27
- Creating Security Policies for VPNs ...................................... 27
- Downloading to UTM-1 Edge Devices .................................... 28

Understanding Security Policies

A SmartLSM Security Gateway has a SmartLSM Security Profile (created in SmartDashboard), 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, the Security Policies must exist in SmartDashboard, and you must have at least one SmartLSM Security Profile that calls a Security Policy for SmartLSM Security Gateways.

This section describes how to create a Security Policy for a SmartLSM Security Gateway to be managed by SmartProvisioning. We recommend that you define a separate Security Policy for every SmartLSM Security Profile. In the Installable Target field of the Security Policy, add only the SmartLSM Security Profile object.


Configuring Default SmartLSM Security Profile

You can select a default profile to serve as the SmartLSM Security Gateway's profile. This SmartLSM Security Profile will be assigned to all new SmartLSM Security Gateways of the appropriate type (UTM-1 Edge or Security Gateway).

To configure a SmartLSM Security Gateway to reference a default SmartLSM Security Profiles:

1. In SmartDashboard, open Policy > Global Properties, and select the SmartLSM Profile Based Management tab.
2. Select the Use default SmartLSM profile's check box.
3. From the Default SmartLSM Security Profile drop-down list, select an existing SmartLSM Security Profile to be the default profile for Security Gateway or UTM-1 Edge SmartLSM Security Gateways.
4. From the Default UTM-1 Edge drop-down list, select an existing SmartLSM Security Profile to be the default profile for UTM-1 Edge SmartLSM Security Gateways.
5. Click OK and then install the policy.

Guidelines for Basic SmartLSM Security Policies

The following procedure can be used as a guideline for creating a Security Policy for a SmartLSM Security Profile. The specific rules of the Security Policy depend on the needs of your environment and the requirements of the SmartLSM Security Gateways that will reference the SmartLSM Security Profile.
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 according to the needs of your organization and the requirements for the SmartLSM Security Gateways, using 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 Management

You must specify 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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Type of Allowed Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Server</td>
<td>FW1</td>
<td>Firewall control</td>
</tr>
<tr>
<td>Server</td>
<td>Any</td>
<td>FW1</td>
<td>Firewall control</td>
</tr>
<tr>
<td>Any</td>
<td>Server</td>
<td>CPD</td>
<td>CPD control</td>
</tr>
<tr>
<td>Server</td>
<td>Any</td>
<td>CPD</td>
<td>CPD control</td>
</tr>
<tr>
<td>Any</td>
<td>Server</td>
<td>FW1_ica_pull</td>
<td>Pulling certificates</td>
</tr>
<tr>
<td>Server</td>
<td>Any</td>
<td>FW1_ica_push</td>
<td>Pushing certificates</td>
</tr>
<tr>
<td>Server</td>
<td>Any</td>
<td>FW1_CPRID</td>
<td>Check Point Remote Installation Protocol, for Push actions</td>
</tr>
<tr>
<td>Any</td>
<td>Server</td>
<td>FW1_log</td>
<td>Logs</td>
</tr>
<tr>
<td>Server</td>
<td>Any</td>
<td>CPD_amon</td>
<td>Status monitoring</td>
</tr>
</tbody>
</table>
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 26), 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 R76 VPN Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).

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: The following rule allows encrypted telnet traffic that matches the community criteria.

   Example — Telnet Through VPN Traffic Rule

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>VPN</th>
<th>Action</th>
<th>Install On</th>
<th>Any</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Telnet</td>
<td>Community</td>
<td>Accept</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>


7. Update the CO gateway with the new or changed SmartLSM Security Profiles. In Smart Provisioning, click Update Corporate Office Gateway.

Downloading to UTM-1 Edge Devices

SmartLSM Security Gateways on UTM-1 Edge devices can get security policies from the Security Management Server or Domain Management Server through the UTM-1 Edge Portal. You can use this option if, for some reason, Smart Provisioning is unable to fetch the SmartLSM Security Profile or unable to push the Security Policy.

To download a Security Policy to a SmartLSM Security Gateway from the UTM-1 Edge Portal:

1. Log in from the UTM-1 Edge portal to my.firewall.
2. Select Services > Accounts > Refresh, or select Services > Software Updates > Update Now.
3. The UTM-1 Edge SmartLSM Security Gateway polls for updates, and downloads the latest Security Policy.

To verify a successful download:

1. Log in from the UTM-1 Edge portal to my.firewall.
2. Select Reports > Event Log.
3. Find the following message: Installed updated Security Policy (downloaded).
5. Verify that the SmartLSM Security Profile in the Policy field is the UTM-1 Edge Profile that references the correct Security Policy.
Chapter 6

SmartLSM Security Gateways

In This Chapter

Creating Security Gateway SmartLSM Security Profiles 29
Adding SmartLSM Security Gateways 29
Handling SmartLSM Security Gateway Messages 30

Creating Security Gateway 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 Smart Provisioning, the SmartLSM Security Profiles and the Security Policies that they reference must exist in SmartDashboard.

This procedure describes how to create a SmartLSM Security Profile for Security Gateways or UTM-1 Edge Gateways. After you complete this, you can add the gateway objects to Smart Provisioning.

To create a Security Gateway SmartLSM Security Profile:

1. Open SmartDashboard and log in.
2. Open the Security Policy that you want to be enforced on the SmartLSM Security Gateways.
3. Right-click the Network Objects tab and select New > SmartLSM Profile > Security Gateway. The SmartLSM Security Profile window opens.
4. Define the SmartLSM Security Profile using the views of this window.
   To open the online help for each view of this window, click Help.
5. Click OK and then install the policy.

   Note - To activate Smart Provisioning functionality, a security policy must be installed on the gateway. Until the policy is installed, the new Smart Provisioning profile is not available.

Adding SmartLSM Security Gateways

This procedure describes how to add a SmartLSM Security Gateway to Smart Provisioning management.

Before you begin, you must have at least one Smart Provisioning SmartLSM Security Profile for Security Gateway gateways. See Creating Security Gateway SmartLSM Security Profiles (on page 29) for details.

To add a SmartLSM Security Gateway to Smart Provisioning management:

1. In the tree, click Devices.
2. Select File > New > SmartLSM Security Gateway. A wizard opens, taking you through the steps to define the SmartLSM Security Gateway.
3. Provide a name for the SmartLSM Security Gateway and optional comments, and click Next. This name is for Smart Provisioning management purposes. It does not have to be the name of the gateway device; the name should be selected to ease management and recognition for users.
4. In the More Information page, define the SmartLSM Security Gateway by its properties as follows:
   • SmartLSM Security Gateway: Select the version that is installed on the gateway.
   • Security Profile: Select a SmartLSM Security Profile object created in SmartDashboard.
   • OS: Select the Operating System of the gateway.
• **Enable Provisioning**: Select to enable the assignment of Provisioning Profiles to this gateway. Clear this option if you are sure that this gateway should be managed in a unique way; if you are sure that Provisioning Profiles would not be useful in the management, or might be harmful to the operations, of this gateway.

• **No Provisioning Profile**: Select to enable provisioning for this gateway, while leaving the actual assignment of Provisioning Profile for later.

• **Provisioning Profile**: Select a Provisioning Profile to assign to this gateway. This option is available only if **Enable Provisioning** is selected.

  **Note** - If the Provisioning options are not available, check that you have created Provisioning Profiles in SmartProvisioning. You can add the gateway and create the profiles later. The Provisioning options are enabled when you have a Provisioning Profile of the appropriate operating system.

5. Click **Next**.

6. In the **SmartLSM Security Gateway Communication Properties** page, define an **Activation Key**.

   An activation key sets up a Secure Internal Communication (SIC) Trust between the SmartLSM 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 SmartLSM Security Gateway.

   Provide an activation key by doing one of the following:

   • Select **Generate Activation Key automatically** and click **Generate**. The Generated Activation Key window opens, displaying the key in clear text. Make note of the key (to enter it on the SmartLSM Security Gateway for SIC initialization) and then click **Accept**.

   • Select **Activation Key** and provide an eight-character string to be the key. Enter it again in the **Confirm Activation Key** field.

7. If you know the IP address of this SmartLSM Security Gateway, select **This machine currently uses this IP address** and then provide the IP address in the field. If you can complete this step, the SIC certificate is pushed to the SmartLSM Security Gateway.

   If you do not know the IP address, you can select **I do not know the current IP address**. SmartProvisioning will pull the SIC certificate from the Security Management Server or Domain Management Server after you finish this wizard. See Complete the Initialization Process.

8. Click **Next**.

   The **VPN Properties** page opens.

9. If you want a CA certificate from the Internal Check Point CA, select the **I wish to create a VPN Certificate from the Internal CA** check box.

   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 have completed this wizard.

10. Click **Next**.

11. If you want to continue configuring the gateway, select the **Edit SmartLSM Security Gateway properties after creation** check box.

12. 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 Security Gateway or UTM SmartLSM Security Gateway, during the SmartProvisioning processing of the gateway object.

**Opening Check Point Configuration Tool**

The following sections may suggest that you open the Check Point Configuration tool to handle an issue.

**To open the Check Point Configuration tool:**

- On a SecurePlatform, Linux, or Solaris gateway, run **sysconfig** to access a complete list of **cpconfig** options.
- On a Windows-based gateway, click **Start > Programs > Check Point > Check Point Configuration Tool**.

**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. Select the gateway in the work space and then select **Edit > Edit Gateway**.
2. In the **General** tab, click **Communication**.
   - The **Communication** window opens, providing 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 and then **OK** to close the **Edit** window.
5. Open the Check Point Configuration tool on the SmartLSM Security Gateway and click **Reset SIC**.

**Operation Timed Out**

During the process of adding a new SmartLSM Security Gateway, SmartProvisioning connects between the Security Management Server/Domain Management Server and the SmartLSM Security Gateway, to match and initialize SIC and VPN certificates.

If a message appears indicating **Operation Timed Out**, the most common cause is that SmartProvisioning could not reach the Security Management Server/Domain Management Server or the SmartLSM Security Gateway. The gateway is still added to SmartProvisioning, but you should 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, click **Communication**.
3. Check the value of **Trust status**. 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, a message appears:

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** - If you are using 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**).
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.
Chapter 7

UTM-1 Edge SmartLSM Security Gateways

Creating UTM-1 Edge SmartLSM Security Profiles

When a SmartLSM Security Gateway is installed on a UTM-1 Edge device, the Check Point software is embedded. Features and maintenance for SmartLSM Security Gateways on UTM-1 Edge are somewhat different from similar procedures for SmartLSM Security Gateways on other hardware platforms.

Every 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 any SmartLSM Security Gateway to SmartProvisioning, have the SmartProvisioning SmartLSM Security Profiles prepared in SmartDashboard.

This procedure describes how to create a SmartLSM Security Profile for UTM-1 Edge SmartLSM Security Gateways. After you have completed this, you can add the gateway objects to SmartProvisioning.

To create a UTM-1 Edge SmartLSM Security Profile:

1. In SmartDashboard, open the Security Policy for your SmartLSM Security Gateways. If necessary, edit the policy. See the SmartDashboard online help or the R76 Security Management Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).
2. Right-click the Network Objects tab and select New > SmartLSM Profile > UTM-1 Edge Gateway. The SmartLSM UTM-1 Edge/Embedded Profile window opens.
3. Define the SmartLSM Security Profile in this window. Refer to the online help for more information.
4. Install the policy.
   The new profile is not available until the policy is installed.

Adding UTM-1 Edge SmartLSM Security Gateways

This procedure describes how to add a UTM-1 Edge SmartLSM Security Gateway to the SmartProvisioning management.

Before you begin, you must have at least one SmartLSM Security Profile for UTM-1 Edge gateways. See Creating UTM-1 Edge SmartLSM Security Profiles (on page 32) for details.

To add a UTM-1 Edge SmartLSM Security Gateway to SmartProvisioning management:

1. In the SmartProvisioning tree, click Devices.
   From the SmartProvisioning menu, select File > New > UTM-1 Edge SmartLSM Security Gateway. A wizard opens, taking you through the definition steps.
2. In the New UTM-1 Edge SmartLSM Gateway window, enter a name and optional comments. This name is used by Multi-Domain Security Management. It need not be the name of the gateway device, but should be easily recognizable by users.
3. In the More Information window, define the SmartLSM Security Gateway as follows:
- **SmartLSM Security Gateway** - Select the gateway hardware.
- **Security Profile** - Select a SmartLSM Security Profile created in SmartDashboard.
- **OS** - Select the operating system of the gateway.
- **Enable Provisioning** - Select to enable provisioning for this gateway. Clear this option if you are sure that this gateway should be managed in a unique way; if you are sure that Provisioning Profiles would not be useful in the management, or might be harmful to the operations, of this gateway.
- **No Provisioning Profile** - Select to leave the actual assignment of Provisioning Profile for later.
- **Provisioning Profile** - Select a Provisioning Profile to assign to this gateway.

  **Note** - This option is disabled for platforms that do not support SmartProvisioning.

4. In the **SmartLSM Security Gateway Communication Properties** window, establish SIC Trust between the gateway and the management server using one of the below methods:
   - Select **Generate Registration Key automatically** and click **Generate**. The **Generated Registration Key** window opens, displaying the key in clear text. Make note of the key (to enter it on the SmartLSM Security Gateway for SIC initialization) and then click **Accept**.
   - Select **Registration Key** and provide an eight-character string to be the key. Enter it again in the **Confirm Registration Key** field.

In **SmartLSM Gateway VPN Properties** window, enable the **I wish to create a VPN Certificate from the Internal CA** option if the gateway is part of a VPN. If the gateway is not part of a VPN community in SmartDashboard, clear this option.

5. In the **Finished** window, select the **Edit SmartLSM Security Gateway properties after creation** check box if you wish to edit or configure additional properties.

### Handling New UTM-1 Edge SmartLSM Messages

This section explains how to handle a message that may appear after you finish the wizard to add a UTM-1 Edge SmartLSM Security Gateway, during the SmartProvisioning processing of the gateway object.

**Registration Key is Missing**

If you did not generate or select a Registration Key for SIC setup, a message opens:

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

Click **Yes** to let SmartProvisioning add the gateway now and handle the SIC setup later, or click **No** and then **Back** to the **Communication Properties** page.

**To handle the SIC setup after the gateway is added:**

1. Select the gateway in the work space and then select **Edit > Edit Gateway**.
2. In the **General** tab, click **New Key**.
3. In the **Registration Key** window, click **Generate Key**. After the key is provided, click **Set**.
4. Click **OK** to close the **Edit** window.

### Customized UTM-1 Edge Configurations

In SmartDashboard, you can view and edit the configuration script to ensure that a specific gateway will perform those commands when it rises. Any changes that you make to the script will be performed when the gateway fetches its SmartProvisioning settings.

For more detailed information about configuration scripts, see the R76 **Command Line Interface Reference Guide**.

**To open the Configuration Scripts:**

In the **UTM-1 Edge SmartLSM Security Gateway** window, click **Configuration Script**.
Chapter 8

SmartProvisioning Wizard

In This Chapter

SmartProvisioning Wizard 34
Before Using the SmartProvisioning Wizard 34
Using the SmartProvisioning Wizard 35

SmartProvisioning Wizard

When you open SmartProvisioning, the System Overview work space contains the Getting Started area, which includes the SmartProvisioning Wizard button. Before using the wizard, you must have defined devices enabled for provisioning without any Provisioning Profiles assigned.

It offers the following operations (one or more of which you can choose to perform on the selected 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.

Before Using the SmartProvisioning Wizard

Before you open the SmartProvisioning wizard, prepare all gateways to be provisioned:

- Check Point Gateways are of one of these versions:
  - Check Point NGX R65 with HFA 40 or higher
  - Check Point R70 or higher
- IP Appliances have:
  - IPSO 6.2 operating system
  - Check Point R70.40
- All gateways have a Security Policy installed

Note - If the NGX R65 gateways are not ready, you must manually add the HFA 40 (or higher) package for SecurePlatform to the SmartUpdate repository on the Security Management server or Domain Management Server, before you can use the SmartProvisioning Wizard.

To upload packages to the repository:

1. Open SmartUpdate (Window > SmartUpdate).
2. Select Packages > Add and select a source:
   - File or DVD: Prepare the files (*.tgz format) and browse to the files to add to the repository. When you click OK, the package is added to the Package Repository.
   - Download Center: Have your username and password for the Check Point User Center. When your credentials are authenticated, the Get Packages from Download Center window opens, displaying the packages that are available to you. Select the packages to download and click Download.
3. Reboot the gateways after installing the HFA.
Using the SmartProvisioning Wizard

To use the SmartProvisioning wizard:
1. Make sure the Devices list displays the relevant gateways.
2. In the System Overview view, click SmartProvisioning Wizard.
3. Click Next.
4. Select the device type. You can provision only one type of device at a time.
5. In the list of devices that Smart Provisioning recognizes in your environment, select each device on which you want the operations to be performed.
   If you will be assigning a Provisioning Profile to the devices, select the devices to which you want to assign the same profile.
6. Click Next.
7. Select the operations that you want to perform on the selected gateways.
   If you select Associate devices with a Provisioning Profile, select the Provisioning Profile from the drop-down list (contains only profiles of the selected type of device); or click New Profile and create a Provisioning Profile for the selected devices.
   
   Note - This is the only operation that is available for UTM-1 Edge devices.
8. Click Next.
   The Summary step appears. This window lists the operations you selected.
9. Click Finish.

Installing the SmartProvisioning Agent

If you selected Verify Smart Provisioning agent is running on the device, install it if required (in the Choose Operations step), after you click Finish, the Distribute Packages window opens.
1. Select the package shown: the Check Point Smart Provisioning Agent.
   The options of this window become available.
2. Select Distribute and install packages and Backup image for automatic revert.
3. If this device can safely be rebooted, select Allow reboot if required.
4. Click Start.

   Note - If the device has operational communications with Smart Provisioning, but this operation fails on Error: Run 'Get Gateway Data', and try to run this procedure again, check that an administrator is logged in.
Chapter 9

Provisioning

In This Chapter

Provisioning Overview 36
Creating Provisioning Profiles 36
Configuring Settings for Provisioning 37
UTM-1 Edge Provisioning 38
Security Gateway Provisioning 40
Assigning Provisioning Profiles to Gateways 44

Provisioning Overview

SmartProvisioning allows for large scale gateway management. SmartProvisioning enables you to configure similar devices in a similar way and to manage multiple gateways with single commands by using Provisioning Profiles. You create a Provisioning Profile. The profile holds configurations for a gateway's receiving services, networking, and maintenance.

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

Provisioning Profiles function in a manner similar to SmartLSM Security Profiles. The main differences between Provisioning Profiles and SmartLSM Security Profiles are described in the following table:

<table>
<thead>
<tr>
<th><strong>Provisioning Profiles and SmartLSM Security Profiles</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provisioning Profile</strong></td>
</tr>
<tr>
<td>Provides</td>
</tr>
<tr>
<td>Requires</td>
</tr>
<tr>
<td>Required by</td>
</tr>
<tr>
<td>Managed by</td>
</tr>
</tbody>
</table>

In addition, gateways that are provisioning-enabled have more management features, such as multiple automatic backups. See Security Gateway Actions (on page 75) to learn more.

Creating Provisioning Profiles

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 Read/Write permissions for Provisioning Profiles (see Defining SmartProvisioning Administrators) (see "Defining SmartProvisioning Administrators" on page 15).

**To create 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/operating system to be supported by this profile.
   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.

Configuring Settings for Provisioning

Each Provisioning Profile holds settings that are provisioned onto the gateways that reference this profile. This section describes the general properties of a Provisioning Profile and the configurations that are common to all devices.

Viewing General Properties of Provisioning Profiles

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

Either the UTM-1 Edge Profile window or the Security Gateway Profile window opens, depending on the operating system for which the profile was created.

Note - The window for Security Gateway 80 does not have the Backup tab.

For both profile windows, the General view opens.

This 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 can reference this profile.

Configuring Profile Settings

For each set of configurations that can be managed with a Provisioning Profile, you can decide which settings will have preference: local (not provisioned) or central (from SmartProvisioning individual management or from Provisioning Profile).

To determine profile settings:
1. In the Profiles List, right-click a profile and select Edit Provisioning Profile.
2. In the Profile window, click any category tab (other than General).
3. Decide whether this Provisioning Profile will provide central management of the setting to gateways that reference the profile:
   - **Manage settings locally on the device**: Select this option if each gateway that references this profile should have its own settings, configured locally (not on SmartProvisioning), which cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioning gateway object. If you choose this option, the Gateway window will show: settings are defined to be managed locally on the device.
   - **Manage settings centrally from this application**: Select this option if each gateway that references this profile should get its configuration for this setting from the Provisioning Profile or from the SmartProvisioning gateway object.
4. If you select to manage settings centrally, click Advanced. The Profile Settings window opens.
5. 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; or you can leave the profile settings as they are.
6. Click **OK**.

The choice you make here determines the functionality of the Gateway window, for the type of device configuration for which you made this profile setting.

For example, if you set Hosts configuration to **Central** and **Allowed**: the Hosts tab on the gateway will enable you to manage the Host List of a gateway by:

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

The table below maps the selections in the **Profile Settings** to the displayed options in the Gateway windows.

### Local or Central Management of Provisioned Gateways

<table>
<thead>
<tr>
<th>Profile managed</th>
<th>Profile Override</th>
<th>Gateway Window Display and options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally</td>
<td>Not relevant</td>
<td>Settings are defined to be managed locally on the device. To change this, refer to Provisioning Profile <code>profile_name</code>. (controls are unavailable)</td>
</tr>
<tr>
<td>Centrally</td>
<td>Override denied</td>
<td>Data must be taken from profile (controls are Read-Only, configured by profile)</td>
</tr>
</tbody>
</table>
| 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.** (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. |

**Warning** - If the **Use the following settings** option is selected and no values are entered for a specific topic, the current settings on the device will be deleted.

### UTM-1 Edge Provisioning

Some provisioning options are available only to UTM-1 Edge devices. Because UTM-1 Edge devices are embedded with Check Point products and configurations, some management options are handled differently than for non-Edge devices.

A Provisioning Profile can provision any or all of the network configurations. You can determine that one group of settings is provisioned and another set up locally; see Configuring Profile Settings (on page 37).

### Configuring Date and Time for Provisioning

You can synchronize all your UTM-1 Edge devices.
To configure the date and time in a Provisioning Profile:
1. Open the UTM-1 Edge Profile window, and select the Date and Time tab.
2. If you select central management, click Advanced to set central management options. See Configuring Settings for Provisioning (on page 37) for more information.
3. If you select an option that uses the profile settings, decide how the gateway clock is synchronized:
   - If you want gateways of this profile to synchronize their date and time using a specific NTP server, select the Use Network Time Protocol (NTP) to synchronize the clock check box.
   - If you want gateways of this profile to synchronize their date and time using the Security Management Server/Domain Management Server, clear this check box and click OK. Gateways of this profile will be synchronized when they fetch their Provisioning Profile.
4. If you select the Use Network Time Protocol (NTP) to synchronize the clock check box, provide the IP address or host name of the NTP server. If available, provide the IP address and name of a secondary NTP server.
5. From the Time Zone drop-down list, select the time zone of the NTP server.

Configuring Routing for Provisioning
You can configure the Routing table of a UTM-1 Edge gateway through the Provisioning Profile. The first option is whether the gateways that reference this profile will have their routing configured by the profile, or locally.

To configure routing by provisioning:
1. Open the UTM-1 Edge Profile window, and select the Routing tab.
2. If you select central management, click Advanced to set central management options.
3. If you selected an option that uses the profile settings, click Add.
4. Provide the Source Settings, or leave Any Source selected:
   - Source IP: Source IP address (for example, this gateway's IP address; or the IP address of a source behind the gateway).
   - Source Mask: Net mask of the source network.
5. Provide the Destination Settings, or leave Any Destination selected:
   - Destination IP Address: Destination IP address for this route (for example, the IP address of the CO gateway or the Security Management Server/Domain Management Server).
   - Destination Mask: Net mask of the destination network.
6. Select the defining options:
   - Service: Select ANY or a specific service to be allowed along with route.
   - Next Hop IP or network: Select a pre-defined network or provide the IP address of the closest router or default gateway.
   - Metric: Specify the distance in hops to the destination.
7. Click OK.
8. Configure all the routes that you want in this table.

Configuring HotSpot for Provisioning
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, configuring 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 RADIUS in the Provisioning Profile; see Configuring RADIUS for Provisioning (on page 40).

To configure a HotSpot for Provisioning:
1. Open the UTM-1 Edge Profile window, and select the HotSpot tab.
2. If you select central management, click Advanced to set the central management options. See Configuring Settings for Provisioning (on page 37) for more information.
3. Provide a **HotSpot Title**.

4. In the **HotSpot Terms** field, specify the terms for valid access or End-User License.
   This may include: time limits, number of users, warnings that only known clients will be allowed, and any other term that is relevant for your users and according to your organization's policy.

5. Select the appropriate options:
   - **HotSpot is password-protected**: Select this option if users should provide the HotSpot password.
   - **Allow a user to login from more than one computer at the same time**: This option is available only if a password is required. If not, the gateway does not need to recognize multiple logins of the same user account.
   - **Use HTTPS**: Select this option to allow access only with secured HTTP.
   - **After login, redirect to URL**: Provide the URL of the Web page that users should see after successful login through the HotSpot.

6. Click **OK**.

### Configuring RADIUS for Provisioning

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

**To configure RADIUS in a Provisioning Profile:**

1. Open the **UTM-1 Edge Profile** window, and select the **RADIUS** tab.

2. If you select central management, click **Advanced** to set the central management options. See Configuring Settings for Provisioning (on page 37) for more information.
   - The **RADIUS Servers** lists show all the servers that are define in SmartDashboard to be RADIUS servers.

3. In the **Primary RADIUS Server** list, select the RADIUS server that you want to be the primary RADIUS server of the gateways that reference this Provisioning Profile.

4. In the **Secondary RADIUS Server** list, select the RADIUS server that you want to be the secondary RADIUS server of the gateways.

5. If you want to configure the RADIUS server permissions, click **Advanced**.

6. From the **Administrator Level** drop-down list, select the permissions that an administrator on gateways that reference this Provisioning Profile will have on the RADIUS server:
   - **Read Write**
   - **Read Only**
   - **Users Manager**
   - **No Access**

7. Select permissions that you want to allow to users on the network of gateways that reference this Provisioning Profile, with authentication from the RADIUS server:
   - **VPN Remote Access**: Allows access to the VPN from a remote station, authenticating through the RADIUS server.
   - **Web Filtering Override**: Allows authenticated users to see Web sites that would otherwise be blocked by the RADIUS server configurations.
   - **HotSpot access**: Allows users access to the RADIUS server, and thus to the protected environment, from wireless HotSpot connections.
   - **Remote Desktop Access**: Allows users to access desktops inside the protected environment from a remote station.
Security Gateway Provisioning

This section explains the provisioning configurations that are available to Security Gateway gateways.

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.

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 DNS for Provisioning

You can configure DNS servers on a Provisioning Profile, providing the configuration for all gateways that reference this profile.

To configure DNS servers on a Provisioning Profile:
1. Open the Security Gateway Profile window, and select the DNS tab.
2. If you select central management, click Advanced to set the central management options.
3. Provide the IP address of the First, Second, and Third DNS servers of the network.

Configuring DNS for Provisioning - Security Gateway 80

This section explains how to configure the DNS server provisioning profile for Security Gateway 80. You can configure DNS servers on a Provisioning Profile, providing the configuration for all Security Gateway 80s that reference this profile.

To configure DNS servers on a Provisioning Profile:
1. Open the Security Gateway Profile window, and select the DNS tab.
2. 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 Configuring Profile Settings (on page 37).
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 Security Gateway 80 appliance as your default DNS proxy, select Enable DNS Proxy - resolves local DNS requests.

Configuring Firmware for Provisioning - Security Gateway 80

This section explains how to configure firmware installation settings for the provisioning profile for Security Gateway 80. When you configure firmware settings on a Provisioning Profile, you give the configuration for all Security Gateway 80s that reference this profile.

The Security Gateway version must match its SmartLSM profile's version as defined in SmartDashboard for correct policy behavior. In some instances, it may be necessary to define exceptions for the default SmartLSM security profile that will replace 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.

Let's say you have a scenario with these details:
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.

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 that references this profile.

- **According to time ranges** - You can define download and installation time ranges for the firmware image. The download and installation time can be limited to a specified list of time ranges in the week. They will start at the nearest time range after firmware settings were applied. For example, if the firmware installation settings were 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 06:00
  
  The firmware will be installed between Wednesday 23:00 and Thursday 06:00.

  In the event that the Security Gateway did not succeed to download and/or install the firmware during the nearest time range, it will try again in the next time range.

---

**To configure firmware installation settings on a Provisioning Profile:**

1. Open the **Security Gateway Profile** window, and select the **Firmware** tab.
2. 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 Configuring Profile Settings (on page 37).
5. In **Firmware image**, click **Select** to select a firmware image that has been uploaded through SmartUpdate.
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 SmartDashboard 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 current version you have now.
7. If necessary, click **Exceptions** to choose 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/change an exception for a SmartLSM profile replacement. SmartLSM profiles will not be shown unless they are from a version higher than R71.
     - **Current SmartLSM Profile** - Select a SmartLSM profile from the list. A SmartLSM profile is shown only if the version is not R71 and not the selected firmware version. Make sure you have installed policy for the SmartLSM profile in SmartDashboard.
     - **SmartLSM Profile after installation** - Select a SmartLSM profile that will 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 have installed policy for the SmartLSM profile in SmartDashboard.
   - **Remove** - Click to remove a SmartLSM profile exception setting.
8. Select one of the options to install the firmware:
   - **Immediately**
   - **According the these time ranges** - Select to use the Security Gateway time or local time.
Provisioning

- **Add/Edit** - Click Add or Edit to open the Time Range window to define/change the weekdays and times for downloading and installing the firmware image. Select the days and times and 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 Hosts for Provisioning**

You can configure hosts on a Provisioning Profile, providing the configuration for all gateways that reference this profile. This is especially useful for gateways on the same LAN or network, such as Security Gateways with HA.

**To configure hosts on a Provisioning Profile:**
1. Open the **Security Gateway Profile** window, and select the **Hosts** tab.
2. If you select central management, click **Advanced** to set the central management options.
3. Click **New**.
4. Provide the host name and the IP address, and click **OK** to return to the **Hosts** tab.
5. Repeat for all relevant hosts.
   - Every gateway that references this Provisioning Profile receives this Host list.

**Configuring Domain Name for Provisioning**

You can configure the domain on a Provisioning Profile, providing the configuration for all gateways that reference this profile. This is useful for gateways that share a domain; you only have to configure it once for all the gateways.

**To configure the domain on a Provisioning Profile:**
1. Open the **Security Gateway Profile** window, and select the **Domain Name** tab.
2. If you select central management, click **Advanced** to set the central management options.
3. Provide the domain name.

**Configuring Backup Schedule**

You can set all gateways that reference this Provisioning Profile to be backed up on a schedule. When each gateway in turn fetches the Provisioning Profile, its backup is created.

For example, if you want to ensure that all gateways are backed up without causing 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.

**To configure backup settings of a Provisioning Profile:**
1. Open the **Security Gateway Profile** window, and select the **Backup** tab.
2. If you select central management, click **Advanced** to set the central management options. See Configuring Settings for Provisioning (on page 37) for more information.
3. Select **Enable Backup**.
4. In the **Start at** field, select the hour (on European 24-hour units) and minute for the backup to start.
5. Select the frequency at which the backup is to recur:
   - Select the **Day of the month** radio button and then select a date.
   - Select the weekdays radio button and then select each relevant day.
6. If you want the log files to be included in the backup, select the **Include Check point products log files in the backup** checkbox.
Such backups are generally much larger than without the logs, so be sure to 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 the backups to be stored on a machine other than the SmartProvisioning console. This option is relevant only if all gateways that will reference this Provisioning Profile are on the same network, with access to the server that will get and store the backups.

7. If you want the backups to be saved on another server, click **Backup Target**.
   The **Backup Target** window opens.

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

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

10. For SCP servers, provide the **Username** and **Password**.

11. Click **OK**.

**Assigning Provisioning Profiles to Gateways**

After you create a Provisioning Profile, you can assign gateways to be automatically managed by this profile. Make sure that the actual gateway fits the operating system and software version of the Provisioning Profile.

**To assign a Provisioning Profile to a gateway:**

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 the **Enable Provisioning** check box is selected.

4. Select **Provisioning Profile**.

5. From the drop-down menu, select the Provisioning Profile whose settings you want to use to configure this gateway; or click **New** and create a new Provisioning Profile.
Overview of Managing Gateways

SmartProvisioning can manage SmartLSM Security Gateways, Provisioned Gateways, and CO gateways on UTM-1 Edge devices or Security Gateway devices; on any supported platform and operating system. Configurations for these different types of gateways sometimes differ. 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 Read/Write permissions for Managing Device Settings.

Adding Gateways to SmartProvisioning

Gateways are added to SmartProvisioning through the device configuration. The following is true of all Power-1, UTM-1, and UTM-1 Edge gateways.

- You add SmartLSM Security Gateways to SmartProvisioning management when you configure the Check Point Security Gateway to enable SmartLSM configuration. After installing the gateway software, execute the command: `LSMenabler -r`
  Gateways are recognized as CO gateways, and managed by SmartProvisioning, after you create a Star VPN in SmartDashboard and define this gateway as the central gateway.
  If a SmartLSM or CO gateway has the SmartProvisioning enabled, it can also be provisioned.

- Gateways are managed by SmartProvisioning when the Provisioning blade is enabled on the Security Management Server. You can attach a Provisioning Profile to this gateway, and thereby have access to provisioning features — automated installations and configurations — for this gateway and simultaneously with the other gateways that reference this profile.

Opening the Gateway Window

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

To open the Gateway window:
1. In the tree, click Devices.
2. Do one of the following:
   - 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.
Immediate Gateway Actions

At any point while configuring or managing a gateway you can perform a number of immediate actions on the gateway. Some actions are for Provisioned gateways only, some are relevant 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.

Remotely Controlling Gateways

You can manage remote gateways using SmartProvisioning. You can start, stop, and restart the Check Point Security Gateway services, and you can reboot devices. This is relevant for all types of SmartProvisioning gateways, except that the software of UTM-1 Edge devices (for SmartLSM and Provisioned gateways) cannot be stopped or started, only restarted in one command.

Remote Actions on Check Point Services and Gateways

<table>
<thead>
<tr>
<th>To:</th>
<th>On Gateway of Type</th>
<th>Select Actions &gt; Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Check Point services</td>
<td>Security Gateway</td>
<td>Stop Gateway</td>
</tr>
<tr>
<td>Start Check Point services</td>
<td>Security Gateway</td>
<td>Start Gateway</td>
</tr>
<tr>
<td>Restart Check Point services</td>
<td>Security Gateway, UTM-1 Edge</td>
<td>Restart Gateway</td>
</tr>
<tr>
<td>Reboot device</td>
<td>Security Gateway, UTM-1 Edge</td>
<td>Reboot Gateway</td>
</tr>
</tbody>
</table>

Updating Corporate Office Gateways

It is important that the CO gateway be updated whenever 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). The CO gateway is the center of the Star VPN, in which SmartLSM Security Gateways are the satellites.

To update a CO gateway:
1. Click the Update CO Gateway toolbar button:
2. From the Corporate Office Gateway drop-down list, select the CO gateway that is the center of the SmartLSM Security Gateway's Star VPN.
3. Click OK.

**Deleting Gateway Objects**

You can remove a SmartLSM Security Gateway as a SmartProvisioning object. This revokes all certificates of the gateway.

**To delete a SmartLSM Security Gateway:**
1. In the work space, select the gateway.
2. Select Edit > Delete SmartLSM Security Gateway.

Provisioned gateways can be deleted in SmartDashboard.

**Editing Gateway Properties**

**Gateway Comments**

You can view the properties that define a gateway in the **General** tab of the Gateway window. Some of the properties can also be edited.

- The **Name** of this gateway cannot be changed after you add it to SmartProvisioning.
- The **Comments** field displays comments that were added when the gateway object was created in SmartDashboard. If the gateway is a SmartLSM Security Gateway (either UTM-1 Edge or Security Gateway), you can edit the comments here. If the gateway is a Provisioned gateway or CO gateway, this field is Read-Only.

**Changing Assigned Provisioning Profile**

SmartProvisioning gateways may be managed 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** check box 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. Of course, this is not available for Provisioning Profiles. It must be different for each device.

**Note** - SmartLSM Security Gateways: If **All IP addresses behind the gateway based on Topology information** is selected in the gateway **Topology** page, 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.

**To add an interface to the gateway’s configuration:**
1. Do Actions > Get Actual Settings.

**Note** - For IP Appliances:
The interface configuration for these appliances is complex. To prevent mistakes, you must first do 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 Smart Provisioning, open the Gateway window and select the Interfaces tab.
   - To manage the interfaces locally on the device, preventing changes in Smart Provisioning from affecting the device, select **Manage settings locally on the device**.
   - To configure interfaces through Smart Provisioning, overriding the local settings, select **Use the following settings**.

   The controls are different according to machine type: SecurePlatform gateway, IP Appliance, or UTM-1 Edge device.

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

3. Click **Add**.

   A menu of interface types opens. Select an interface type. This menu is different for SecurePlatform gateways, IP Appliances, and UTM-1 Edge devices. The window that opens is different for each selected interface.

4. Enter the required data and click **OK**.

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

### Executing Commands

You can run executables or shell commands on a managed gateway with **Custom Commands**.

For example, if you want to check the connection between the Smart Provisioning 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.

**To prepare 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 be used.

**To execute a prepared custom command:**

1. Right-click a gateway in a **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.

### Converting Gateways to SmartLSM Security Gateways

You can convert a Security Gateway or UTM-1 Edge gateway managed with SmartDashboard to a SmartLSM Security Gateway managed with Smart Provisioning. There is no need to delete existing objects, or to create new ones, because the Check Point Suite handles object management automatically during the conversion. It also preserves relevant SIC certificates.

For example, when you acquire the Smart Provisioning license, you can convert relevant Check Point gateways to SmartLSM Security Gateways, without having to re-configure the gateway objects.
To convert to a SmartLSM Security Gateway:
1. In SmartDashboard, create the SmartProvisioning SmartLSM Security Profile to be associated with the new SmartLSM Security Gateway.
3. In the SmartProvisioning CLI, execute one of the following commands (see Converting Gateways (see "Gateway Conversion Actions" on page 129) for details and more options).
   - Security Gateway: LSMcli <server> <user> <pswd> Convert Gateway VPN1 <Name> <Profile>
   - UTM-1 Edge: LSMcli <server> <user> <pswd> Convert Gateway VPN1Edge <Name> <Profile>
5. Update the CO gateway.
Chapter 11

Managing SmartLSM Security Gateways

In This Chapter

Immediate SmartLSM Security Gateway Actions 50
Common SmartLSM Security Gateway Configurations 51
Changing Assigned SmartLSM Security Profile 51
Managing SIC Trust 51
Tracking Details 53
Configuring Log Servers 53
SmartLSM Security Gateway Licenses 53
Configuring SmartLSM Security Gateway Topology 55
Converting SmartLSM Security Gateways to Gateways 56

Immediate SmartLSM Security Gateway Actions

At any point while configuring or managing a SmartLSM Security Gateway you can perform immediate actions on the gateway.

Applying Dynamic Object Values

SmartLSM Security Profiles can bring a Security Policy, with rules for source/destination IP addresses, and localize these rules for each SmartLSM Security Gateway that references the profile. See Dynamic Objects (on page 98) to learn more about dynamic objects. Dynamic objects are managed in SmartProvisioning only for SmartLSM Security Gateways.

For example:
The Security Policy that is fetched by a SmartLSM Security Profile has a rule to drop traffic from IP addresses on a StormCenter. This one profile is referenced by ten SmartLSM Security Gateways: some of the SmartLSM Security Gateways that reference this profile should use one StormCenter site; others should use a different one. You do not have to create a new rule for each gateway. You 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 that references 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 have resolved 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:

Select Actions > Push Dynamic Objects.
Getting Updated Security Policy

If you change the Security Policy in SmartDashboard that is used by a SmartLSM Security Profile, including installing it on gateways, it is not applied to SmartLSM Security Gateways. Each SmartLSM Security Gateway fetches its SmartLSM Security Profile on interval, and thus gets its updated Security Policy.

You can apply the changes immediately by pushing the policy onto the SmartLSM Security Gateway by selecting Actions > Push Policy.

For any gateway with Provisioning enabled, you can initiate an immediate fetch of the Provisioning Profile with the same command by selecting Actions > Push Policy.

Common SmartLSM Security Gateway Configurations

SmartLSM Security Gateways may be on UTM-1 Edge devices; or non-Edge devices, with Check Point Security Gateway or Check Point UTM-1 Edge software.

Configurations for these different types of SmartLSM Security Gateways sometimes differ, but this chapter explains management concepts and procedures that are common to all SmartLSM Security Gateways.

The administrator must have Read/Write permissions for managing device settings (see "Defining SmartProvisioning Administrators" on page 15).

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

To open the SmartLSM Security Gateway window:
1. In the tree, click Devices.
2. Do one of the following:
   • 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. (This section is applicable only to SmartLSM Security Gateways, of both UTM-1 Edge and Security Gateway types.)

This procedure should also be performed if the assigned SmartLSM Security Profile was changed in SmartDashboard, to ensure immediate application of the changes.

To apply a change in SmartLSM Security Profile:
1. In SmartDashboard, 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. Select Actions > Push Policy.

Managing SIC Trust

Getting New Registration Key for UTM-1 Edge Device

You can force a UTM-1 Edge SmartLSM Security Gateway to get a new SIC key, by generating a new Registration Key for the gateway.

To generate a new key:
1. Double-click a UTM-1 Edge device.
2. In the UTM-1 Edge SmartLSM Security Gateway window > General tab, find the Secure Internal Communication > Registration Key field.
3. Click **New Key**.
4. Click **Generate Key**, and then click **Set** to set the new key.

**Verifying SIC Trust on SmartLSM Security Gateways**

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

**To check a SmartLSM Security Gateway’s SIC Trust:**

1. In the **SmartLSM Security Gateway** window > **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, you should change the SIC Trust State.
2. Click **Communication**.
3. Check the value of the **Trust State** field, which indicates the status of this SmartLSM Security Gateway's SIC Trust with the Security Management Server or Domain Management Server.
   - **Initialized**: Indicates that the SmartLSM Security Gateway has a valid SIC certificate.
   - **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 **Trust State** is **Uninitialized**, and the **IP address** field has the IP address of the SmartLSM Security Gateway, 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 an Activation Key, or select **Activation Key** to provide one that you have from the Security Management Server or Domain Management Server.
2. Click **Initialize**. A new SIC certificate is created for this SmartLSM Security Gateway, and its trust state becomes **Initialized**.

**Pulling SIC from Security Management Server**

If the **IP address** field is empty, you must pull the SIC certificate from the Security Management Server or Domain Management Server using 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 **Activation Key** 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 have replaced the gateway host machine, or if you have lost the **Activation Key**.

From the time that you reset SIC, up to the second that trust is re-established, internal communications between Check Point applications, the management server, and managed devices is down. This procedure actually revokes the current certificate and provides a new one. Thus, it is recommended that you continue only if you are sure that SIC should be reset, and after this procedure, you should 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 might 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
The Details tab of the Gateway window for SmartLSM Security Gateways and UTM-1 Edge SmartLSM Security Gateways provides identification information for log tracking and cluster usage.

You can edit the ID by which the actual device of the gateway is known 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 send logs to a Log Server, the logs are stored by 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 (Security Gateway) or MAC Address (UTM-1 Edge):** 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 whatever format is best for the environment and the SmartLSM Security Gateway.
- **Customer Details:** Often used to hold environment details of the SmartLSM site, which can be especially useful if the SmartProvisioning administrators are not personally familiar with the remote office.
- **Participates in UTM-1 Edge cluster** *(available for UTM-1 Edge only ("UTM-1 Edge Clusters" on page 87)).*

Configuring Log Servers
When you create a SmartLSM Security Profile for Security Gateway gateways in SmartDashboard, 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 SmartDashboard.

To change log servers of SmartLSM Security Gateways:
1. Open the Security Gateway window, and select the Advanced tab.
2. Clear the As defined in SmartLSM Profile check box.
3. Select the servers which should hold the logs 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.

Note - UTM-1 Edge gateways are configured for log servers through the UTM-1 Edge Portal > Setup > Logging. For more information about log servers, see the UTM-1 Edge User Guide.
SmartLSM Security Gateway Licenses

You have a License Repository with the licenses that you acquired for your environment. You can manage the licenses of 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: Window > SmartUpdate > Licenses and Contracts
2. Click Licenses & Contracts > Add License and then select a source location.
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.
   - The displayed licenses are those that are in your License Repository but currently are unattached to any gateway. If an original license is in use on another SmartLSM Security Gateway, you will not see the corresponding upgraded license displayed in the License Repository.
3. Select the licenses that you want 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, either attaching or detaching are performed immediately. The License Operation message appears:
     Attaching/Detaching Licenses. Please wait...

Attaching License to UTM-1 Edge SmartLSM Security Gateways

UTM-1 Edge devices have embedded licenses. To release features, you need the Product Key.

To attach a license to a UTM-1 Edge SmartLSM Security Gateway:
1. Open the UTM-1 Edge SmartLSM Security Gateway window, and select the Licenses tab.
2. Provide the Product Key.
3. Click Show Product Description to see the features that are enabled by this license.

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 have finished running 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, you will receive a notification stating that you may either remove the upgrade license alone, or both licenses.
- If both the original and the upgrade license are in the **License Repository**, and you attempt to add the upgrade license to the gateway, you will receive a notification stating that if you proceed, both licenses will be added to the gateway.

**Configuring SmartLSM Security Gateway Topology**

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

**To configure the topology of a SmartLSM Security Gateway:**

1. Open the Gateway window, and select the **Topology** tab.
2. Select the option that best describes the topology of this SmartLSM Security Gateway:
   - **Not defined**: No VPN is defined for this gateway. To enable this Gateway to participate in a VPN, another option must be selected. Select this option if this device is not a gateway for a network.
   - **Only the external interface**: 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.
   - **Automatically determined by the topology configured on the Edge device**: The VPN domain of the gateway consists of all the IP addresses configured locally on the UTM-1 Edge device, regardless of the interface configuration of the Edge object in SmartDashboard. Selecting this option requires the OSPF feature of the CO gateway to dynamically learn the VPN domain of the UTM-1 Edge device.

   **Note** - This option is only available for UTM-1 Edge devices ("Configuring the Automatic VPN Domain Option for UTM-1 Edge" on page 56), and requires:

   Manual definition of VTIs on the device and CO gateway for the CO gateway to learn the VPN domain. The domain topology is stored on the Edge device, and not acquired through an install policy action or automatic update from the CO.

   OSPF feature of the CO gateway to dynamically learn the VPN domain of the UTM-1 Edge device.

   - **Manually defined**: The previous options do not describe the VPN domain you want to support, and you want to define it yourself. The range table is enabled.
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.

3. If you select Manually defined, click Add.
   Provide the topology information in the IP Address Range Configuration window.

4. Provide the IP addresses that define a network behind this gateway.

5. Provide comments to help manage this network.

6. Click OK.

7. Repeat to add as many ranges as needed to define the VPN of this gateway to the CO gateway.

8. Select Actions > Push Policy.
   You are prompted to save the data and then SmartProvisioning validates the topology you have defined. If successfully validated, the topology is immediately pushed to the gateway.

9. Update the CO gateway (see Updating Corporate Office Gateways (on page 46)).
   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. (see "Configuring VPNs on SmartLSM Security Gateways" on page 82)

Configuring the Automatic VPN Domain Option for UTM-1 Edge

The topology of the VPN domain can be determined automatically on the UTM-1 Edge device.

- When the automatic option is configured, the VPN domain of the gateway consists of all the IP addresses configured locally on the UTM-1 Edge device, regardless of the interface configuration of the Edge object in SmartDashboard.

- Selecting this option requires the OSPF feature of the CO gateway to dynamically learn the VPN domain of the UTM-1 Edge device.

Converting SmartLSM Security Gateways to Gateways

You can convert a SmartLSM Security Gateway managed with Smart Provisioning to a Security Gateway or UTM-1 Edge gateway managed with SmartDashboard. There is no need to delete existing objects, nor to create new ones, because the Check Point Suite handles object management automatically during the conversion. It also preserves relevant SIC certificates.

For example, if a remote gateway has so many customized requirements that Profiles are ineffective, you can manage it as a separate gateway through SmartDashboard.

To convert to a SmartDashboard gateway:

1. In the SmartProvisioning CLI, execute one of the following commands (see Converting Gateways (see "Gateway Conversion Actions" on page 129) for details and more options).
   - Security Gateway: LSMcli <server> <user> <pswd> Convert ROBO VPN1 <Name>
   - UTM-1 Edge: LSMcli <server> <user> <pswd> Convert ROBO VPN1Edge <Name>

2. Define the gateway interfaces.

3. Update relevant VPN communities.


5. Restart Check Point services.

6. Update the CO gateway to which the SmartLSM Security Gateway was a satellite.
Chapter 12

Managing Security Gateways

In This Chapter

Security Gateway Settings 57
Security Gateway 80 Settings 59
Managing Software 73
Security Gateway Actions 75
Maintenance Mode 77

Security Gateway Settings

Some management configurations are common to all Security Gateways and UTM-1 Edge gateways that reference a Provisioning Profile, whether they are SmartLSM Security Gateways, CO gateways, or Provisioning-only gateways.

You can manage the provisioned settings if the Profile Settings are set for central management and the Use the following settings option is selected. See Configuring Settings for Provisioning (on page 37) to learn more about local and central management of gateways with Provisioning Profiles.

Before you begin, make sure that your administrator user name has Read/Write permissions for Managing Device Settings (see Defining Smart Provisioning Administrators (on page 15)).

Scheduling Backups of Security Gateways

You can set up a schedule for backups of the individual Security Gateway, or view how it is managed centrally with a Provisioning Profile.

To set up a backup schedule on a Security Gateway:

1. Open the Security Gateway window, and select the Backup tab.
   If Use the following settings is selected, the Backup controls are available.
2. Select the Enable Backup check box.
3. Select the Show profile settings check box to see how the backup schedule is configured by the Provisioning Profile and to verify that an individual schedule for this gateway is necessary.
4. Define the schedule settings:
   - Start at: Set the hour and minute when the backup should start.
   - Recur every: Select either Day of the month and provide a date, or select the day(s) of the week, to set how many times a week or month, and on which days, the backup should occur.
5. If you want the backup to include product log files, select the Include Check point products log files in the backup check box.
   If disk space is an issue for the target machine, clear this check box.
6. If you want the backup file to be stored on a server other than the selected gateway, click Backup Target.
7. Select the server on which you want the backup file to be stored and provide the relevant information for Smart Provisioning to reach this server.
8. Click OK to close the Backup Target window.
9. Click OK to close the Gateway window.
   The new backup schedule is applied to the gateway the next time it fetches its profile and settings.
Managing Security Gateways

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

To configure DNS servers on a Security Gateway:
1. Open the [SmartLSM] Security Gateway window, and select the DNS tab.
   If Use the following settings is selected, the DNS controls are available.
2. Provide the IP addresses of the First, Second, and Third DNS servers, as relevant for the environment.

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

To configure hosts on a Security Gateway:
1. Open the [SmartLSM] Security Gateway window, and select the Hosts tab.
   If Use the following settings is selected, the Hosts controls are available.
2. Click New.
3. Provide the Host name and IP address, and click OK.

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

To configure the domain on a Security Gateway:
1. Open the [SmartLSM] Security Gateway window, and select the Domain Name tab.
   If Use the following settings is selected, the control is available.
2. Provide the Domain name, and click OK.

Configuring Host Name
You can see or change the host name of the individual Security Gateway in SmartProvisioning. This is especially useful with SmartLSM Security Gateways, to manage such basic configurations from a remote central console. Of course, this is not available for Provisioning Profiles. It must be different for each device.

To configure the host name on a Security Gateway:
1. Open the [SmartLSM] Security Gateway window, and select the Host Name tab.
   If Use the following settings is selected, the control is available.
2. Enter the host name of the gateway, and click OK.

Configuring Routing for Security Gateways
You can manage the routing settings of individual Security Gateways through SmartProvisioning. You must configure the interfaces before the routes, because there are different types of routing configurations for different interfaces, depending on device. Of course, this is not available for Provisioning Profiles. It must be different for each device.

To configure routing for Security Gateway devices:
1. Open the Gateway window, and select the Routing tab.
   • To manage the settings on the device, preventing changes in SmartProvisioning from affecting the device, select Manage settings locally on the device.
   • To configure settings through SmartProvisioning, overriding the local settings, select Use the following settings.
     If Use the following settings is selected, the Routing controls are available.
2. Click Add.
   A menu opens, displaying these options:
3. **Select a route type.**
   A different **Routing** window opens for each type.

4. Enter the data and click **OK**.

There are different windows and options for different route types for SecurePlatform Security Gateways. If the gateway is an IP appliance, the windows offer other options.

The IP Appliance alternative to **Metric**, is **Next Hop Type**:
- **Normal**: Allow traffic to the gateway.
- **Reject**: Block traffic where the gateway is the destination, and acknowledge.
- **Black Hole**: Block traffic without acknowledging.

**Configuring Net Route**
- **Destination IP Address**: Destination IP address for this route (for example, the IP address of the CO gateway or the Security Management Server/Domain Management Server).
- **Destination Mask**: Net mask of the destination network.
- **Interface**: Select a pre-configured interface for this route.
- **Gateway**: IP address of the gateway providing access to this route.
- **Metric**: Distance in hops to the destination. (This value should be as accurate as possible: too low a value may cause lost communications with looping; too high a value may cause security issues.)

**Configuring Host Route**
- **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 should be a very low number; if the host is not behind routers, the metric should be zero.

**Configuring Default Route**
- **Gateway**: IP address of the gateway providing access to the default external route.
- **Metric**: Distance in hops to the gateway. (This value should be as accurate as possible: too low a value may cause lost communications with looping; too high a value may cause security issues.)

**Security Gateway 80 Settings**

For more about the Security Gateway 80 settings, see the *Security Gateway 80 Administration Guide* (http://supportcontent.checkpoint.com/solutions?id=sk91140).
Configuring DNS

Configure the DNS server in the **DNS** tab.

**To configure DNS:**

1. From the **Devices** window, double-click the Security Gateway 80. 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 that is being 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 Security Gateway 80 appliance as your default DNS proxy, select **Enable DNS Proxy - resolves local DNS requests**.
7. Click **OK**.

Configuring Interfaces

Configure the Security Gateway 80 interfaces in the **Interfaces** tab in the Security Gateway window.

**To configure the interfaces:**

1. From the **Devices** window, double-click the Security Gateway 80. 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. In **Security Zone**, select **Wireless, DMS, External**, or **Internal**. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.

7. To configure the DHCP settings for the interface:
   a) In the DHCP section, select **Enabled**.
   b) In **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 override MAC address value.
   c) From **Link speed/Duplex**, select the bandwidth for the interface.

9. Click **OK**.
   The Edit window closes.

10. 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.

11. To enable the configured connection, select the interface and click **Enable**.

### Adding a VLAN

**You can add a new VLAN to a configured interface.**

**To create a VLAN (according to the IEEE 802.1q Standard) on one of the interfaces:**

1. From the **Devices** window, double-click the Security Gateway 80.
   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:
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 Security Gateway 80 as a LAN switch in the Interfaces tab in the Security Gateway window.

**To configure LAN switch parameters:**

1. From the Devices window, double-click the Security Gateway 80.
   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 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 Security Gateway 80 starts using the secondary Internet connection.

These are the Internet connections:

- **Static IP** - A fixed (non-dynamic) IP address.
- **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network.
- **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.
- **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing 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.

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

**To configure High Availability:**

1. Select **Revert to Primary connection when possible**.
2. Click **OK**.

### Configuring a Static Internet Connection

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

**To configure a static IP Internet connection:**

1. From the **Devices** window, double-click the Security Gateway 80 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. **Click OK.**

### Configuring a DHCP Internet Connection

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

**To configure a DHCP Internet connection:**

1. From the **Devices** window, double-click the Security Gateway 80 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. Click OK.

**Configuring a PPPoE Internet Connection**

You can configure an Internet connection that uses PPPoE protocol.

**To configure a PPPoE Internet connection:**

1. From the Devices window, double-click the Security Gateway 80 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

**To configure PPPoE advanced settings:**

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 Security Gateway 80 uses the PPPoE Internet connection:
   - **Auto Connect** - The Security Gateway 80 automatically establishes a PPPoE connection to the Internet.
   - **Connect on Demand** - The Security Gateway 80 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.

5. Click **OK**.
Configuring a PPTP or L2TP Internet Connection

You can configure an Internet connection that uses PPTP or L2TP protocol.

**To configure a PPTP Internet connection:**

1. From the **Devices** window, double-click the Security Gateway 80 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 User Name**
   - **ISP 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

**To configure PPTP or L2TP advanced settings:**

1. From the Primary Internet Configuration window for PPTP or L2TP, select **Advanced**.
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 Security Gateway 80 uses the PPTP or L2TP Internet connection:
   - **Auto Connect** - Security Gateway 80 automatically establishes a PPTP or L2TP connection to the Internet.
   - **Connect on Demand** - Security Gateway 80 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.
6. Click **OK**.
Configuring a Bridge Connection

You can configure an Internet connection that is a bridge.

**To configure a bridge connection:**

1. From the Devices window, double-click the Security Gateway 80 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 **Bridge**.
5. Click **Configure**. The Primary Internet Configuration window for the bridge opens.

6. From **Assign Interface**, select the interface that is being configured as a bridge.
7. In the **IP Settings** section, enter these IP address parameters:
   - **IP Address**
   - **Subnet Mask**
   - **Default Gateway**
8. In the **DNS** section, enter the IP addresses for the DNS servers.
9. 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**.
10. Click **OK**.
Configuring ICMP

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 have enabled High Availability, then the Security Gateway 80 can activate the other Internet connection when necessary.

To configure the ICMP settings:
1. From the Devices window, double-click the Security Gateway 80.
   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, 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 steps A and B for all the servers that are being 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.
Managing Security Gateways

**Configuring Routing Settings**

You must configure Security Gateway 80 interfaces before configuring 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 ("Configuring Internet Connection Types" on page 63). 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 Security Gateway 80 to automatically select the interface or gateway that is used for a route. But you cannot select the **Automatic** option for both the interface and the gateway.

You can use SmartProvisioning to configure network routes for Security Gateway 80. You should use a network route to configure routing for an internal network.

**To configure a network route:**

1. In the **Devices** window, double-click the Security Gateway 80. 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 number of hops to the destination. **Note**: This value should 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 Security Gateway 80. A host route configures access to a specific host.

**To configure a host route:**

1. In the **Devices** window, double-click the Security Gateway 80. The Security Gateway window opens.
2. Select the **Routing** tab.
3. Select **Use the following settings**.
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 should be a low number. If the host is not behind routers, the metric should be zero.

9. Click OK.

**Configuring Firmware Installation Settings**

You can use SmartProvisioning to manage the firmware installation settings for Security Gateway 80.

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 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 that references this profile.
- According to time ranges - You can define download and installation time ranges for the firmware image. The download and installation time can be limited to a specified list of time ranges in the week. They will start at the nearest time range after firmware settings were applied. For example, if the firmware installation settings were 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 06:00

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

    In the event that the Security Gateway did not succeed to download and/or install the firmware during the nearest time range, it will try again in the next time range.

To configure firmware installation settings:

1. In the Devices window, double-click the Security Gateway 80.
   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 has been 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 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/change the weekdays and times for downloading and installing the firmware image. Select the days and times and 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 RADIUS

You can configure the RADIUS server (Remote Authentication Dial In User Service) that provides authentication, authorization, and accounting for Security Gateway 80 gateways. By configuring RADIUS in the Provisioning Profile, you can configure it once for all gateways that reference this profile. The RADIUS server must be already defined as a SmartDashboard 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.

To configure RADIUS:
1. In the Devices window, double-click the Security Gateway 80. The Security Gateway window opens.
2. Select the RADIUS tab.
3. Select Use the following settings.
4. Click Add to add RADIUS servers that have been defined in SmartDashboard, select a RADIUS server from the list and click OK.
5. To remove a server, select a server in the list and click Remove.
6. Use Up/Down to set the priority used for contacting RADIUS servers.
7. Click Allow administrators from specific RADIUS groups only (comma separated) to allow authentication from specified groups as defined on the RADIUS server. Only administrators belonging to those groups can get access.
8. Click OK.

Managing Software

You can manage the software installed on SmartLSM Security Gateways and standard Security Gateways. Package commands (from the Actions menu) and the Package toolbar buttons are available only when a non-Edge gateway is selected in a Devices workspace.

These commands are not relevant or available for UTM-1 Edge gateways. To manage the software of UTM-1 Edge devices, use the UTM-1 Edge portal (right-click > Launch UTM-1 Edge Portal).

Uploading Packages to the Repository

Security Gateway software is available for SmartProvisioning management if it is in the Package Repository on the Security Management Server or Domain Management Server.

To upload packages to the repository:
1. Open SmartUpdate (Window > SmartUpdate).
2. Select Packages > Add and select a source:
   - File or DVD: Have the files (*.tgz format) ready and browse to the ones you want to add to the repository. When you click OK, the package is added to the Package Repository.
Download Center: Have your user name and password for the Check Point Download/User Center ready. When your credentials are authenticated, the Get Packages from Download Center window opens, displaying the packages that are available to you. Select the ones you want and click Download.

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.

To view the packages list on a gateway:
1. Open the [SmartLSM] Security Gateway window
2. Select the Packages tab.
   The operating system of the gateway, and all installed Check Point packages are listed.

Verifying Pre-Install

Before installing a Check Point software package on a gateway, you can test whether the package is compatible with the selected gateway.

To verify package pre-installation:
1. In the Devices work space, select a Security Gateway.
2. Click the Pre-Install Verifier toolbar button.
   A message appears: Getting targets for install. Please wait...
   If there are packages in the Package Repository (see Uploading Packages to the Repository (on page 73)), the Verify Installation window opens.
3. Select a listed package and click Verify.
   In Status View > Action Status, see the verification phases in the Details column:
   - Checks connection between gateway and Security Management Server or Domain Management Server.
   - Checks for sufficient disk space on the 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 gateway, the Status column shows Completed, and the Details column shows:
     `<package>' is compatible with installed packages

Upgrading Packages with SmartProvisioning

Use the Upgrade All Packages features to upgrade devices for a new version of the Security Gateway software.

To upgrade Check Point software on a gateway:
1. In the work space, select the gateway.
2. Click Upgrade All Packages on the toolbar.
   If there are packages in the Package Repository (see Uploading Packages to the Repository (on page 73)), 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 then rerun Upgrade All Packages.

Distributing Packages with SmartProvisioning

Use the Distribute Packages feature to distribute Check Point Hotfixes and HFAs to the specific gateways which can be enhanced by installing the package.

To install a Check Point package on a gateway:
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 gateway (see Verifying Pre-Install (on page 74)).

3. Click Distribute Packages on the toolbar. A warning opens, explaining 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 installation, 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 73)), 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 gateway, but do not install them yet.
   - Install previously distributed packages: Install packages that were previously distributed to the selected gateway.

7. If you want the gateway to automatically reboot after the installation, if the installation requires this, select the Allow reboot if required check box.

8. Select the Backup image for automatic revert check box (available only for SecurePlatform gateways). Clear this check box only if disk space is a real issue.

Creating the image may take some time.

9. If Change to a new profile after install is enabled, you must select an appropriate SmartLSM Security Profile for the gateway from the drop-down list.

This field is enabled, and required, only if the change is necessary.

10. Click Start.

Security Gateway Actions

You can execute immediate actions on SmartLSM Security Gateways and Security Gateway Provisioned gateways. You can run these actions on individual gateways, or on a SecurePlatform Provisioning Profile, effectively running the action on all gateways that reference this profile.

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

Viewing Status of Remote 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 gateway:
1. Make sure an administrator is logged into the gateway.
2. Select Actions > Get Status Details.

Running Scripts

You can execute complex gateway management with your own scripts on any provisioned gateway. The Run Script feature is not available for UTM-1 Edge devices or UTM-1 Edge Provisioning Profiles.

Before you begin, make sure that your administrator has permissions for running scripts.
Running Scripts on Individual Gateways

To run a script on a single gateway:
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

With the same Run Script feature you can simultaneously manage multiple gateways by running scripts on a Security Gateway Provisioning Profile.

To run a script on all gateways of a Provisioning Profile:
1. In the tree in the main window, select Profiles.
2. Select an existing Provisioning Profile for UTM-1/Power-1/SecurePlatform 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 the all gateways that reference 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 an Action command on a specific gateway, or on a Security Gateway Provisioning Profile to create a backup image of all gateways that reference this profile.

You can choose to store backups on the selected gateway, or on another backup server. If you choose 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.

Note - Smart Provisioning does not provide backup management for UTM-1 Edge devices or UTM-1 Edge Provisioning Profiles. UTM-1 Edge backups are managed through the UTM-1 Edge Portal (right-click > Launch UTM-1 Edge Portal), using the Export Tool. For more information, see the R75.40VS UTM-1 Edge Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).

To execute an immediate backup of a Security Gateway:
1. Right-click a [SmartLSM] Security Gateway window or UTM-1/Power-1/SecurePlatform Provisioning Profile and select Actions > Backup.
2. If you want the backup to include Check Point logs, select the Include Check Point products log files in the backup check box.
3. Provide details of the device on which the backup will be stored, or select Locally on device, if each device will hold its own backup file.
4. Click OK.
5. Select Actions > Push Settings and Actions.
The backup is created and pushed to the 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 gateways.

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

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

To apply profile changes and actions immediately, select Actions > Push Settings and Actions.

**Maintenance Mode**

Security Gateways that reference a Provisioning Profile have a maintenance feature. Enable Maintenance Mode on a Security Gateway while testing 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.

**For example:**

You have a SmartLSM Security Gateway on your SmartProvisioning management which has operational issues. The remote office where this SmartLSM Security Gateway sits is too far away for you to manage it 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 have already made to it from your central SmartProvisioning console. You 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* - Disabling Maintenance Mode overrides any local changes with the central SmartProvisioning configurations. If the local administrator discovers that changes need to be made on this gateway, make sure you have the data before switching back.

**To enable Maintenance Mode:**

1. Open the [SmartLSM] Security Gateway window.
2. In the General tab, select the Maintenance Mode check box.

Remember:

- Changes to the Provisioning Profile do not affect the gateway as long as Maintenance Mode is selected.
- If you clear the Maintenance Mode check box, all local changes are overridden by central configurations.
Chapter 13

Managing UTM-1 Edge Gateways

In This Chapter

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTM-1 Edge Portal</td>
<td>78</td>
</tr>
<tr>
<td>UTM-1 Edge Ports</td>
<td>78</td>
</tr>
<tr>
<td>UTM-1 Edge Gateway Provisioned Settings</td>
<td>79</td>
</tr>
</tbody>
</table>

UTM-1 Edge Portal

UTM-1 Edge gateways, SmartLSM and Provisioning, have some configurations that are managed through the UTM-1 Edge Portal. SmartProvisioning provides you with access to these configurations through the Gateway window, and for some sets of configurations, with UTM-1 Edge Provisioning Profiles.

**To access the UTM-1 Edge Portal:**

1. In a Devices work space, right-click a UTM-1 Edge device
2. Select Launch UTM-1 Edge Portal. Your default browser opens to the Web User Interface of UTM-1 Edge management.

For more information on UTM-1 Edge configuration, see the R75.40VS UTM-1 Edge Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).

UTM-1 Edge Ports

The UTM-1 Edge Portal Web UI has a Ports tab. In this tab you configure the physical ports of the selected UTM-1 Edge device, configuring valid use for different ports. For example, you can assign a LAN port to be used for a LAN network or a VLAN network. You can assign a RS232 port for a dial-up modem or for a serial console.

You can edit port usage through SmartProvisioning. This is available to UTM-1 Edge SmartLSM Security Gateways and to UTM-1 Edge Provisioning gateways. SmartProvisioning settings affect the devices only if the device topology is set to All IP addresses behind the gateway based on Interfaces information.

**To manage UTM-1 Edge device ports:**

1. Open the UTM-1 Edge [SmartLSM] Gateway window and select the Ports tab.
2. Decide if you want to manage the ports of the selected UTM-1 Edge device from SmartProvisioning, or if you want to make sure that local configurations are used.
   - **Manage settings locally on the device:** Disable SmartProvisioning management of the physical ports of the UTM-1 Edge device; enforce local management.
   - **Use the following settings:** Configure port settings of the UTM-1 Edge device here. When local administrators access the Ports tab of the UTM-1 Edge Portal, they can edit these settings and add more ports for configuration.
3. Select a port from the list and click Edit. You cannot add port assignments from SmartProvisioning. This should be done locally, to prevent configurations of ports that are not actually on the device.
   - The window that opens depends on the type of port you selected, and on the options that were set on the UTM-1 Edge Portal.
   - For example, if a local administrator set a LAN port to have no settings for port security, when you click Edit on the LAN port, the security setting will be disabled.
If the local administrator had enabled Port Security to enforce 802.1x authentication, you could disable this temporarily (until the local administrator changes it back) and set a quarantine network for clients that failed authentication.

**UTM-1 Edge Gateway Provisioned Settings**

Some management configurations are common to all UTM-1 Edge gateways that reference a Provisioning Profile, whether they are SmartLSM, CO, or Provisioning-only.

You can manage the provisioned settings if the Profile Settings are set for central management and you want to use the Use the following settings option. See Configuring Settings for Provisioning (on page 37) to learn more about local and central management of gateways from Provisioning Profiles.

Before you begin, make sure that your administrator has Read/Write permissions for Managing Device Settings (see Defining SmartProvisioning Administrators (on page 15)).

**Synchronizing Date and Time on UTM-1 Edge Devices**

You can configure the date and time of the individual UTM-1 Edge gateway, synchronizing it with a specified Network Time Protocol, or view how it is managed centrally with a Provisioning Profile.

To configure date and time on a UTM-1 Edge gateway:

1. Open the UTM-1 Edge [SmartLSM] Gateway window and select the Date and Time tab. If Use the following settings is selected, the controls are available.
2. Select the Show profile settings to see how the synchronization is configured by the Provisioning Profile and to be sure that an individual schedule for this gateway is necessary.
3. Select the Use Network Time Protocol (NTP) to synchronize the clock check box, or clear this check box to synchronize this gateway to the clock of the Security Management Server or Domain Management Server.
4. If you select the Use Network Time Protocol (NTP) to synchronize the clock check box, provide the IP address of the Primary NTP Server and, if available, of the Secondary NTP Server; then select the Time Zone.
5. Click OK. The changes you made here will affect the selected gateway, overriding the settings configured for the gateway by the referenced Provisioning Profile. To apply these settings to the gateway, select Actions > Push Policy.

**Configuring Routing for UTM-1 Edge Gateways**

You can manage the valid routes of the individual gateway, or view how they are managed centrally with a Provisioning Profile. This option is common to UTM-1 Edge gateways (SmartLSM and Provisioned) that reference a Provisioning Profile.

To add a route to the gateway’s routing table:

1. Open the UTM-1 Edge [SmartLSM] Gateway window > Routing.
   - If the gateway has an assigned Provisioning Profile, select Use profile settings to leave the profile configuration as-is. (If the gateway does not have a Provisioning Profile, this option is not available.)
   - If you want to manage the settings on the device, preventing changes in SmartProvisioning from affecting the device, select Manage settings locally on the device.
   - If you want to configure settings through SmartProvisioning, overriding the profile and the local settings, select Use the following settings.
   If Use the following settings is selected, the Routing table and controls are available.
2. Click Add.
3. Provide the required data to configure the new route on the selected gateway:
   - Source IP: Source IP address (for example, this gateway's IP address; or the IP address of a source behind the gateway).
   - Source Mask: Net mask of the source network.
   - Destination IP Address: Destination IP address for this route (for example, the IP address of the CO gateway or the Security Management Server or Domain Management Server).
- **Destination Netmask:** Net mask of the destination network.
- **Service:** From the drop-down list, select ANY or a specific service that is to be allowed along with route.
- **Next Hop IP or network:** IP address of the closest router or default gateway.
- **Metric:** Distance in hops to the destination. Make sure this is as accurate as possible, to avoid looped or dropped traffic.

4. Click **OK.**
   The changes made here will affect the selected gateway, overriding the settings configured for the gateway by the referenced Provisioning Profile.
   To apply these settings to the gateway, select **Actions > Push Policy.**

### Configuring RADIUS Server for SmartProvisioning Gateways

You can view and change the RADIUS server configuration for any connected gateway.

**To configure a RADIUS server on a gateway:**

1. Open the **UTM-1 Edge [SmartLSM] Gateway** window and select the RADIUS tab.
   If **Use the following settings** is selected, the RADIUS controls are available. The **RADIUS Servers** list shows all the servers that are configured through SmartDashboard to be RADIUS servers.
2. Select the servers that you want to be the RADIUS servers of this gateway.
3. If you want to configure the RADIUS server permissions, click **Advanced.**
4. From the **Administrator Level** drop-down list, select the permissions that an administrator on this gateway will have on the RADIUS server.
5. Select the permissions that you want to assign to users on the network of this gateway, with authentication from the RADIUS server:
   - **VPN Remote Access:** Select to allow access to the VPN from a remote station, authenticating through the RADIUS server.
   - **Web Filtering Override:** Select to allow authenticated users to see Web sites that would otherwise be blocked by the RADIUS server configurations.
   - **HotSpot access:** Select to allow users access to the RADIUS server, and thus to the protected environment, from wireless HotSpot connections.
   - **Remote Desktop Access:** Select to allow users to access desktops inside the protected environment from a remote station.
6. Click **OK.**
   The changes made here will affect the selected gateway, overriding the settings configured for the gateway by the referenced Provisioning Profile.
   To apply these settings to the gateway, select **Actions > Push Policy.**

### Configuring HotSpot for SmartProvisioning Gateways

You can configure a HotSpot for wireless access of the individual UTM-1 Edge gateway, or view how it is managed centrally with a Provisioning Profile.

**To configure a HotSpot on a UTM-1 Edge gateway:**

1. Open the **UTM-1 Edge [SmartLSM] Gateway** window, and select the HotSpot tab.
   If **Use the following settings** is selected, the HotSpot controls are available.
2. Select the **Show profile settings** to see how the HotSpot is configured by the Provisioning Profile and to be sure that an individual schedule for this gateway is necessary.
3. Provide the **HotSpot Title**, which appears as the name of the login window.
4. In the **HotSpot Terms** field, specify your organization's terms of use and policies.
5. If the user should have a valid user name and password to access the HotSpot, select the **HotSpot is password-protected** check box.
6. If the password check box is selected, you can select the **Allow a user to login from more than one computer at the same time** check box; or clear this check box to ensure that any user account is used only once for a login session.
7. If the HotSpot can be reached only over a secure Internet connection with HTTPS, select the **Use HTTPS** check box.

8. In the **After login, redirect to URL** field, provide the URL that users of this HotSpot should reach after login. For example, this could be the welcome page of your company site, or the home page of your company intranet.

9. Click **OK**.

   The changes made here will affect the selected gateway, overriding the settings configured for the gateway by the referenced Provisioning Profile. To apply these settings to the gateway, select **Actions > Push Policy**.
Chapter 14

VPNs and SmartLSM Security Gateways

In This Chapter
- Configuring VPNS on SmartLSM Security Gateways 82
- Creating VPNS for SmartLSM Security Gateways 83
- Sample VPN Rules for a SmartLSM Security Gateway 83
- VPN with One or More LSM Profiles 84
- Special Considerations for VPN Routing 86

Configuring VPNS on SmartLSM Security Gateways

Secured communication between your CO gateway and the SmartLSM Security Gateways is dependent 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 SmartDashboard. See the R76 Security Management Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).

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

To configure 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 SmartLSM Security Gateway Topology" on page 55).
3. Select the VPN tab.
   - If, when you created this SmartLSM Security Gateway in the New SmartLSM Security Gateway wizard, you cleared the I wish to create a VPN Certificate from the Internal CA check box, you can select VPN Not supported. No IKE certificate will be generated. You can change this setting at any time.
   - If you want this SmartLSM Security Gateway to participate in a VPN, continue with the next steps.
4. Select the Use Certificate Authority Certificate.
   - If you selected the I wish to create a VPN Certificate from the Internal CA check box 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 SmartDashboard.
   - If you cleared the I wish to create a VPN Certificate from the Internal CA check box in the wizard, you can select a third-party CA from this list.
   - If you selected the I wish to create a VPN Certificate from the Internal CA check box 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, provide 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.
   - If you want 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 Gateways" on page 46).

Creating VPNs for SmartLSM Security Gateways

The previous sections explained how to configure a SmartLSM Security Gateway to be part of a VPN. This section explains how to create the VPN itself in SmartDashboard. Before doing so, you must have first configured, in SmartProvisioning, the SmartLSM Security Gateways to support VPN participation.

To create a VPN tunnel between a SmartLSM Security Gateway and a CO gateway:
1. Define a VPN Star Community (VPN Communities > Site To Site > New > Star).
2. Open Star Community Properties > Central Gateways, click Add, select the CO gateway from the displayed list, and click OK.
3. Open Star Community Properties > Satellite Gateways, click Add, select the SmartLSM Security Gateway or SmartLSM Security Profile from the displayed list, and click OK.
   If you select the profile, rather than a single gateway, all SmartLSM Security Gateways that reference this SmartLSM Security Profile are added to the VPN community, if they are configured with the ability to participate in a VPN (see Configuring VPNs on SmartLSM Security Gateways (on page 82)).
4. Open Star Community Properties > Advanced Settings > Advanced VPN Properties, and specify the IKE Phase properties.
5. Open Star Community Properties > Advanced Settings > Shared Secret, and clear the Use only Shared secret for all External Members check box.
6. Open Security Policy Rule Base, and create a rule base defining the services allowed for the VPN community. See Example Rules for VPN with SmartLSM Security Gateway (see “Sample VPN Rules for a SmartLSM Security Gateway” on page 83).
7. 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.

After you have created the VPN tunnel in SmartDashboard, perform the following:
1. Update the CO gateway. See Updating Corporate Office Gateways (on page 46).
2. Establish the VPN tunnel. Send a test connection with an allowed service (according to the rules created in Security Policy Rule Base) and then use SmartView Monitor or SmartView Tracker to verify that the test was successfully encrypted, sent, and received.

Sample VPN Rules for a SmartLSM Security Gateway

Creating VPNs for SmartLSM Security Gateways (on page 83) includes a step for creating a rule in SmartDashboard’s Security Policy Rule Base that defines the services for the VPN community. This section provides examples of such a rule base.

In the rules, the following Dynamic Objects are used:
- **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 UTM-1 Edge SmartLSM Security Gateways, or the network behind the UTM-1 Edge gateway.

**Rule for Outgoing Connections**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>MyCommunity</td>
<td>ftp</td>
<td>Accept</td>
<td>MyCO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>telnet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VPN Rules for Incoming Connections

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge_Net</td>
<td>CO_VPN</td>
<td>MyCommunity</td>
<td>ftp</td>
<td>Accept</td>
<td>MyProfile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>telnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO_VPN</td>
<td>Edge_Net</td>
<td>MyCommunity</td>
<td>ftp</td>
<td>Accept</td>
<td>MyProfile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>telnet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VPN with One or More LSM Profiles

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

The procedure requires configuration in:
- SmartDashboard
- Security Management Server CLI
- SmartProvisioning Console
- Center Gateway CLI

Using SmartDashboard

In SmartDashboard 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.

To configure a VPN star community between two SmartLSM Profiles in SmartDashboard:
1. Create and configure a SmartLSM Profile Cluster.
   When you configure the topology, make sure that the interface name exactly matches the name of the physical interface.
2. Create and configure a SmartLSM Profile Gateway.
3. Create a regular Security Gateway to be the Center Gateway.
   ![Note] - Security Gateway 80 gateways cannot be the Center Gateway.
4. Create a VPN Star Community: VPN Communities tab > Right-click and select New > Site to Site > Star.
   a) Select Center Gateways from the tree.
   b) Click Add and select the Security Gateway that you created to be the Center Gateway.
   c) Select Satellite Gateways from the tree.
   d) Click Add and select the SmartLSM Profile Cluster and SmartLSM Profile Gateway (or second cluster).
   e) Select Advanced Settings > VPN Routing from the tree.
   f) Select To center and to other satellites through center.
5. Create a Network object that represents the internal network of each satellite in the VPN community.
   a) From the Network Objects tree, right-click Networks and select Network.
   b) 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.
6. Create a Node object that represents the external IP address of each satellite in the VPN community.
   a) From the Network Objects tree, right-click Nodes and select Node > Gateway.
b) 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.

7. Create a Group object that represents the networks for each satellite object:
   a) From the Network Objects tree, right-click and select New > Groups > Simple Group.
   b) Enter a Name for the group that is unique for one satellite.
   c) Select the Network object that you created for that satellite's internal network and click Add.
   d) Select the Node object that you created for that satellite's external IP address and click Add.

8. Create a Group object that represents the Center Gateway.
   a) From the Network Objects tree, right-click and select New > Groups > Simple Group.
   b) Enter a Name for the group that is unique for the Center Gateway.
   c) Select the Gateway object and click Add.

Using the CLI

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

To edit the vpn_route.conf file:

1. Open the vpn_route.conf file.
   - In a Multi-Domain Security Management environment, on a Domain Management Server:
     - If satellites are 80 series Gateways or Clusters:
       /var/opt/CPmds-<version>/customers/<Domain Management Server_name>/CPSG80CMP-<version>/conf/vpn_route.conf
     - If satellites are on a different SecurePlatform appliance or open server:
       /opt/CPmds-<version>/customers/<Domain Management Server_name>/CPsuite-<version>/fw1/conf/vpn_route.conf
   - In a Security Management Server environment:
     - If satellites are 80 series Gateways or Clusters:
       /opt/CPSG80CMP-<version>/conf/vpn_route.conf
     - If satellites are on a different SecurePlatform appliance or open server:
       /opt/CPsuite-<version>/fw1/conf/vpn_route.conf

2. If two SmartLSM Gateways on different LSM Gateway profiles will communicate with each other through the Center gateway, edit the file:
   ```
   # destination router [install on]
   <Simple Group Name of internal network of SmartLSM Gateway> <Center Gateway> <Name of second LSM Profile>
   <Simple Group Name of internal network of second SmartLSM Gateway> <Center Gateway> <Name of LSM Profile>
   ```

3. If more than one SmartLSM Gateway in the same LSM Profile will communicate with each other through the Center gateway, edit the file:
   ```
   # destination router [install on]
   <Simple Group Name of internal network of SmartLSM Gateway> <Center Gateway> <Name of LSM Profile>
   ```

4. Install policy on the SmartLSM Profiles and on the Center Gateway.
Completing the Configuration

Complete the configuration in the SmartProvisioning Console and the CLI of the Center Gateway.

**To complete the VPN configuration:**

1. Open the SmartProvisioning GUI Console.
2. Create a new SmartLSM Cluster or Gateway based on the type of device you have. Select **File > New** > select an option.
3. Generate a VPN certificate for each Gateway or Cluster member:
   a) Open the cluster or gateway object > VPN tab.
   b) Select **Use Certificate Authority Certificate**.
   c) Click **Generate**.
   d) Do these steps again for each cluster member.

   **Note** - If 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).

4. In the CLI of the Center Gateway, run: `LSMenabler on`
5. In the SmartProvisioning GUI Console, right-click the Center Gateway and select **Actions > Update Gateway**.
6. In the **Topology** tab of each object, make sure that the topology of 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 configure correctly as "External" and "Internal".
   - If the interfaces show without IP addresses, click: **Get Actual Settings**.
7. In the **Topology** tab, configure the VPN domain:
   - For SmartLSM Profile Gateways choose an option.
   - For SmartLSM Profile Clusters, select **Manually defined** and manually add the encryption domains that you want to include.
8. **Push Policy.**

All traffic between the satellites and Center Gateway is encrypted.

Special Considerations for VPN Routing

**VPN Routing for SmartLSM Security Gateways**

The VPN routing option **To center and to other satellites through center** is not supported by SmartLSM Security Gateways. This procedure explains how to overcome this limitation.

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

For 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:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Router</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartLSM_domain</td>
<td>Center_gws</td>
<td>SmartLSM_profile</td>
</tr>
</tbody>
</table>

You can have a Star VPN topology for multiple routing gateways, if one of these conditions is met.
The gateways are listed under `install on` in `vpn_route.conf`

The satellite gateways selected in SmartDashboard are also NGX R65 or higher level gateways.

For more information, see `Route Based VPN` in the R76 VPN Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140).

**UTM-1 Edge Clusters**

A UTM-1 Edge Cluster (formerly known as a SmartLSM cluster) is a logical entity that provides high-availability VPN connectivity by using two UTM-1 Edge devices, each serving as an entry point to the same network. In a UTM-1 Edge cluster:

- There are only two UTM-1 Edge devices
- The devices belong to the same VPN domain. A device can only participate in one cluster at a time.
- There is no state synchronization between the devices: if the active UTM-1 Edge cluster member becomes unavailable, users are not automatically connected to the other member. The party that initiated the communication must actively intervene to reconnect the users.

To create a topology in which two UTM-1 Edge SmartLSM Security Gateways serve as entry points to the same network, a mechanism such as VRRP clustering must be configured for that network. This configuration handles the routing in situations where only one of the gateways is available, as well as in situations where both of the gateways are available.

**VRRP Configuration Prerequisites for UTM-1 Edge clusters**

- The *internal* (LAN) interfaces of both devices are configured with different IP addresses.
- Both the interfaces need to have a third, shared IP address, to be utilized by the member, designated as the VRRP master. (The VRRP master designates which UTM-1 Edge cluster member is active.)
- The *external* interfaces of both devices need to have different IP addresses.
- The VPN domains of both gateways have to be the same.

The Corporate Office (CO) gateway recognizes that the two UTM-1 Edge SmartLSM Security Gateways in any UTM-1 Edge cluster represent entry points to the same network. When the CO gateway initiates communication with that network, it communicates with the UTM-1 Edge cluster member that last communicated with the CO gateway. (The CO gateway may recognize several UTM-1 Edge clusters, on different networks.)

**Creating UTM-1 Edge clusters**

To create a UTM-1 Edge cluster:

1. In Smart Provisioning, right-click a UTM-1 Edge SmartLSM Security Gateway that you want to designate as a member of the UTM-1 Edge cluster.
2. Select **Actions > Define UTM-1 Edge cluster**.
3. Check that the gateway name displayed in the **First Member** field is the gateway that you want to be the primary gateway of the UTM-1 Edge cluster. If it is not, click **Find** to select another gateway.
4. In the **Search to** field, begin to type the name of the gateway that you want to add to the cluster and then click **Find**.
   
   The Search SmartLSM Security Gateway window displays UTM-1 Edge SmartLSM Security Gateways that may be selected to join the cluster.
5. Select the gateway that you want and then click **OK**.
6. In the **Define UTM-1 Edge cluster** window, in the **Second Member** field, click **Find** and select the second member of the UTM-1 Edge cluster.
7. Click **OK**.
Viewing UTM-1 Edge Cluster Pairs

To view the name of the gateway that participates in a UTM-1 Edge cluster:
1. From SmartProvisioning, open the UTM-1 Edge SmartLSM Security Gateway window.
2. Click the Details tab.

Deleting or Changing UTM-1 Edge Clusters

To change one member of a UTM-1 Edge cluster, you must first remove the existing UTM-1 Edge cluster and then create the new one.

To delete a UTM-1 Edge cluster:

From SmartProvisioning, right-click a gateway in the pair and select Actions > Remove UTM-1 Edge cluster.
Chapter 15

SmartLSM Clusters

In This Chapter

Overview ........................................ 89
Managing SmartLSM Clusters .......... 90

A SmartLSM Cluster is a logical entity that provides high-availability VPN connectivity by using two devices, each serving 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 the other member. The party that initiated the communication must actively intervene to reconnect the users.

To create a SmartLSM Cluster, you need two UTM-1 Edge SmartLSM Security Gateways. A gateway can participate in only one SmartLSM Cluster at a time.

To create a topology in which two UTM-1 Edge SmartLSM Security Gateways serve as entry points to the same network, a mechanism such as VRRP clustering must be configured for that network. This configuration handles the routing in situations where only one of the gateways is available, as well as in situations where both of the gateways are available.

Overview

The basic procedure for creating and configuring SmartLSM clusters includes these steps:

1. Create a SmartLSM security profile ("Creating a SmartLSM Profile" on page 90) in SmartDashboard. Profiles set common parameters and policies for SmartLSM clusters created using that profile.
2. Create SmartLSM cluster objects in SmartProvisioning based on a SmartLSM security profile.
3. Configure parameters for individual networks using SmartProvisioning, or using LSMcli commands.

You define these common parameters in SmartLSM a cluster security profile:

- Cluster members.
- Cluster member physical interfaces.
- Interface network objective (Cluster, Sync etc.).
- 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 - It is convenient to have a component of cluster and cluster member names describe the specific cluster, and another component, common to all clusters that are mapped to a given Profile, reflect the relative function in the cluster. The common component is defined at the Profile level. The cluster-specific component is defined in SmartProvisioning for the specific cluster, as a prefix or a suffix to the common component. For example, you could have two two-member clusters, named First_cluster and Second_cluster. You could then name the respective members First_member1, First_member2, Second_member1 and Second_member2. In this example, you would define the names _cluster, _member1 and _member2 at the Profile level. Then, when you define individual clusters, you will need to define only the names First and Second as name prefixes.

SmartProvisioning Clusters can be managed either by a Security Management Server or by a Domain Management Server.
Managing SmartLSM Clusters

In This Section

- Creating a SmartLSM Profile
- Configuring SmartLSM Clusters
- Additional Configuration
- Pushing a Policy
- Command Line Reference

Creating a SmartLSM Profile

A SmartProvisioning Security Cluster profile is a template for policies that apply to SmartLSM clusters. When you define a new SmartLSM cluster, you select the SmartLSM profile to automatically assign the configuration settings and security policies. Use SmartDashboard to create SmartLSM Security Cluster Profiles.

When you make a new SmartLSM cluster using a 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.

To create a SmartLSM Security Cluster Profile:

1. In SmartDashboard, right-click Check Point in the Network Objects tree.
2. Select SmartLSM Profile and then select the cluster you want:
   - Check Point Appliance/Open Server Cluster
   - 80 Series 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 using this profile.
   b) If your clusters use a third-party clustering platform (such as IPSO or Crossbeam), clear ClusterXL.
      Note - When using third party cluster platforms, create a different SmartLSM Profile for each platform type.
   c) Make sure that IPSec VPN is selected, if clusters using 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 using this Profile.
5. Configure the applicable parameters on the ClusterXL or 3rd Party Configuration page.
7. Configure each interface in the cluster column. Set the options in the Topology tab. The information in the other two tabs is according to the information in the Topology spreadsheet.

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 will retain 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 whole cluster IP addresses are here only place holders. You will later define them in SmartLSM for each SmartLSM cluster.
• Make sure that the host ID for the external interface of the SmartLSM cluster profile is the same as the actual 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. Optionally 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 Smart Provisioning.
10. Click OK to confirm the settings, and save the Policy Package.
11. In SmartDashboard, install policies to the cluster Profile.

Configuring SmartLSM Clusters

Before you define a SmartLSM cluster, there must be an applicable SmartLSM Security Cluster Profile definition ("Creating a SmartLSM Profile" on page 90) in SmartDashboard. Use Smart Provisioning to create and configure a SmartLSM cluster. SmartDashboard must be closed or in Read Only mode.

Note - Alternatively, you can use LSMcli commands (possibly, in a script) to define SmartLSM clusters, for example AddROBO VPN1Cluster. Using LSMcli commands enables replacing a part of Profile names, which is not possible when using the Smart Provisioning interface.

To define a SmartLSM Cluster

1. From the File menu, select New > SmartLSM Cluster.
2. Enter a Cluster Name Prefix and/or Suffix to be added onto the Profile cluster and member names.
3. Enter the main IP address of the SmartLSM cluster, and click Next.
5. Verify the resulting names, and click Next.
   The network overrides window opens. This window shows the interface topology defined on the Cluster Profile object in SmartDashboard. The profile topology includes generic (template) IPs for any SmartLSM Cluster mapped to this profile. The IP addresses in the list can be overridden with new values for a specific SmartLSM Cluster.
6. Select each interface and Edit it.
   The settings here will override Profile settings.
7. 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.
   For fields left empty, the values will be taken from the Profile. You can define the overrides later on by editing the cluster object. You can also override interface topology by editing the cluster object.
8. Click Next.
9. Select each member, and, for each member, Initialize SIC communication (alternatively, you can do this later - edit the member object and, in the General tab, click Communication). The Communication window opens. SIC will be actually initialized only upon completing the wizard.
10. Click Next.
11. Specify whether to create a VPN certificate for the cluster.
   The certificate will be actually created only upon completing the wizard. You can, later on, create VPN certificates for the individual cluster members - edit the member object and, in the VPN tab, click Generate.
12. Click Next.
13. Specify whether you will want to configure additional cluster options (such as VPN settings or Dynamic Objects) once the SmartLSM cluster object is created, and click Finish.
   Smart Provisioning creates the SmartLSM Cluster object and its members.
Note - Once 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.

14. To retrieve the policy for the first time, from the command line of each SmartLSM Cluster member, run:
   \[ \text{fw fetch_robo -n -f} \]

**Additional Configuration**

You can configure the above and additional properties (VPN, Dynamic Objects, SIC etc.) by double-clicking cluster and/or member objects in SmartLSM. Member properties are also accessible from the Cluster tab of the cluster properties.

Various SmartLSM and ClusterXL options and commands are available for SmartLSM Clusters ("Managing SmartLSM Clusters with LSMcli" on page 92).

**Pushing a Policy**

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 SmartLSM.
2. From the Action menu, select Push Policy.
   You can also push a policy using the command line interface.

**Command Line Reference**

This section covers:
- LSmenabler
- LMScli

**LSMenabler**

This general LSM command applies to SmartLSM Clusters.

To view parameters and the current LSM definition (Security Management Server, SmartLSM gateway etc.), run LSmenabler with no parameters.

**Managing SmartLSM Clusters with LSMcli**

Using the LSMcli command, you can define SmartLSM clusters, and configure most of the options available in SmartLSM (in the New SmartLSM Cluster wizard and in Edit windows).

The LSMcli command syntax is:
\[ \text{LSMcli [-d] <server> <user> <pswd> <action>} \]

This section lists available actions for SmartLSM Clusters. Substitute the command syntaxes in this section for the <actions> field in the above syntax.

**What You Can Do with LSMcli**

The main SmartLSM Cluster actions are:
- Define a new SmartLSM cluster
- Change a SmartLSM cluster main IP address
- Resolve a dynamic object for a SmartLSM cluster
- Set the VPN domain of a SmartLSM cluster
- Define the topology of a cluster (virtual) interface (external/internal, anti-spoofing etc.)
- Manage overrides for cluster members’ interface names and network addresses, and for cluster interface IP addresses and net masks
- Delete a SmartLSM cluster

**AddROBO VPN1Cluster**

You can define a new SmartLSM cluster with the AddROBO VPN1Cluster action. You can configure all of the options available in the New SmartLSM Cluster wizard, with the AddROBO VPN1Cluster command parameters. The only exception is the Topology overrides ("ModifyROBO Netaccess VPN1Cluster" on page 94).

To define a new SmartLSM cluster, substitute the following for `<action>` in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```
AddROBO VPN1Cluster <Profile> <MainIPAddress> <NameSuffix> [-S=<SubstitutedNamePart>] [-CA=<CaName>] [-R=<KeyIdentifier#>] [KEY=<AuthorizationCode>]
```

where the parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>SmartLSM GUI Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Name of cluster Profile to which to map the new cluster.</td>
<td>New SmartLSM Cluster wizard.</td>
</tr>
<tr>
<td>MainIPAddress</td>
<td>Main IP address of cluster.</td>
<td>New SmartLSM Cluster wizard.</td>
</tr>
<tr>
<td>NameSuffix</td>
<td>A suffix to be added to cluster and member Profile names.</td>
<td>New SmartLSM Cluster wizard.</td>
</tr>
<tr>
<td>SubstitutedNamePart</td>
<td>A part of the Profile name to be replaced by the suffix in the previous field.</td>
<td>SmartLSM GUI supports adding Prefix and/or Suffix, not substitution.</td>
</tr>
<tr>
<td>CAName</td>
<td>The name of the Trusted CA object, defined in SmartDashboard, to which a VPN certificate request will be sent.</td>
<td>VPN tab of Edit window (double-click SmartLSM object).</td>
</tr>
<tr>
<td>KeyIdentifier#</td>
<td>Number to identify the specific certificate, once generated.</td>
<td>VPN tab of Edit window (double-click SmartLSM object).</td>
</tr>
<tr>
<td>AuthorizationCode</td>
<td>Authorization Key to be sent to CA to enable certificate retrieval.</td>
<td>VPN tab of Edit window (double-click SmartLSM object).</td>
</tr>
</tbody>
</table>

**ModifyROBO VPN1Cluster**

- **I - Changing the Main IP Address**

You can change a SmartLSM cluster main IP address either in the Cluster tab of the cluster Edit window (double-click the cluster object), or with the ModifyROBO VPN1Cluster action.

To change a SmartLSM cluster main IP address with the ModifyROBO VPN1Cluster action, substitute the following for `<action>` in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```
ModifyROBO VPN1Cluster <ROBOClusterName> -I=<MainIPAddress>
```

where `<ROBOClusterName>` is the cluster name, and `<MainIPAddress>` is the new IP address.
**-D - Resolving a Dynamic Object**

You can resolve a dynamic object for a SmartLSM cluster either in the Dynamic Objects tab of the cluster Edit window (double-click the cluster object), or with the ModifyROBO VPN1Cluster action.

To resolve a dynamic object for a ROBO cluster, substitute the following for `<action>` in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```bash
ModifyROBO VPN1Cluster <ROBOClusterName> -D:<DO Name>=<IP|IP1-IP2>
```

where

- `<ROBOClusterName>` is the cluster name,
- `<DO Name>` is the Dynamic Object name, and
- `<IP|IP1-IP2>` is an IP address or a range of IP addresses.

**ModifyROBOTopology VPN1Cluster**

You can set the VPN domain of a SmartLSM cluster either in the VPN Domain area in the Topology tab of the cluster Edit window (double-click the cluster object), or with the ModifyROBO VPN1Cluster action.

To set the VPN domain of a SmartLSM cluster, substitute the following for `<action>` in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```bash
ModifyROBOTopology VPN1Cluster <RoboClusterName> -VPNDomain=<not_defined|external_ip_only|topology|manual>
```

The parameters are the same as in the regular (non-cluster) ModifyROBOTopology VPN1, at the cluster level.

**Note** - When the VPN domain is set to Manual, the IP address ranges are those set in the SmartLSM GUI or with the ModifyROBOManualVPNDomain action.

**ModifyROBOManualVPNDomain**

This general LSM command applies to SmartLSM Clusters, with the same syntax, using the cluster name for `<ROBOName>`.

**ModifyROBONetaccess VPN1Cluster**

You can, for the actual SmartLSM cluster, override the profile topology definitions of a cluster (virtual) interface either by Editing the interface in the upper half of the cluster Topology tab of the cluster Edit window, and then going to the interface Topology tab, or with the ModifyROBONetaccess VPN1Cluster action.

To define the topology of an interface, substitute the following for `<action>` in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```bash
ModifyROBONetaccess VPN1Cluster <ClusterName> <InterfaceName> -Mode=<by_profile|override> [-TopologyType=<external|internal>] [-InternalIP=<not_defined|this|specific> [-AllowedGroup=<GroupName>]] [-DMZAccess=<true|false>] [-AntiSpoof=<false|true] [-AllowedGroup=<GroupName>] [-SpoofTrack=<none|log|alert>]
```

Explanations of the above parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterName</td>
<td>Name of SmartLSM cluster.</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Name of cluster (virtual) interface. If the interface’s network objective (as defined in the Profile topology) is Sync only (not cluster+sync), there is no cluster interface, only member interface. In this case use the network objective (e.g., 1st Sync) for this parameter.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mode</td>
<td>by_profile to set as defined in cluster Profile, or override to here define the settings, in which case specify -TopologyType.</td>
</tr>
<tr>
<td>TopologyType</td>
<td>external (leads out to the internet) or internal (leads to the local network).</td>
</tr>
<tr>
<td>AntiSpoof</td>
<td>true, to perform Anti-Spoofing based on interface topology, in which case optionally define an AllowedGroup, and set SpoofTrack; or false, to not perform Anti-Spoofing. If the interface is internal and the addresses behind the interface are not defined, Anti-Spoofing is not possible.</td>
</tr>
<tr>
<td>AllowedGroup</td>
<td>If TopologyType=external, AllowedGroup defines a group from which packets are not checked, if Anti-Spoofing is performed. If TopologyType=internal, AllowedGroup specifically (explicitly) defines the hosts behind the internal interface.</td>
</tr>
<tr>
<td>SpoofTrack</td>
<td>Desired tracking action when detecting spoofing: none, log or alert.</td>
</tr>
<tr>
<td>InternalIP</td>
<td>Defines hosts behind an internal interface: not_defined; network defined by IP and net mask of this interface; or: specific, by AllowedGroup.</td>
</tr>
<tr>
<td>DMZAccess</td>
<td>true, if internal interface leads to DMZ. Otherwise, false.</td>
</tr>
</tbody>
</table>

**ClusterSubnetOverride Actions (Add, Modify and Delete)**

Cluster members' interface names and network addresses, and cluster interface IP addresses and net masks, have default values from the Profiles they are associated with. These values can (and in the case of addresses, usually should) be overridden for the individual SmartLSM cluster.

In SmartLSM, this is done by Editing the interface, either in the New ROBO Cluster wizard, or in the Topology tab of the general Edit window for the cluster (double-click the cluster object).

In LSMcli, substitute the following for <action> in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```
<Add|Modify|Delete>ClusterSubnetOverride VPN1Cluster <ROBOClusterName> <InterfaceName> [-IName=<MembersInterfaceName>] [-MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -CNetMask=<ClusterNetMask>]
```

If there is a set override value, and you want to change it, use only ModifyClusterSubnetOverride. If the override value you want to set is not defined (except at the Profile level), because it has never been defined or because it was deleted, use only AddClusterSubnetOverride. To cancel a value and return to the Profile value, use DeleteClusterSubnetOverride.

The action must define at least one parameter: -IName, -MNet, or both -CIP and -CNetMask.

*Note* - To define overrides for a private (monitored or non-monitored) interface, use the PrivateSubnetOverride action.

Explanations of the parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Modify</td>
</tr>
<tr>
<td>ROBOClusterName</td>
<td>The SmartLSM cluster to override values for.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Name of cluster (virtual) interface, as defined in the Profile topology. Use the cluster interface name even though you may be setting values for members’ interfaces. If the interface’s network objective (as defined in the Profile topology) is Sync only (not cluster-sync), there is no cluster interface, only member interface. In this case use the network objective (e.g., 1st Sync) for this parameter.</td>
</tr>
<tr>
<td>MembersInterfaceName</td>
<td>New interface name for cluster members. The name must match the name defined in the operating system.</td>
</tr>
<tr>
<td>MembersNetAddress</td>
<td>New network address for cluster members. This address will be combined with the host parts defined in the Profile to produce complete IP addresses.</td>
</tr>
<tr>
<td>ClusterIPAddress</td>
<td>New IP address for the cluster (virtual) interface.</td>
</tr>
<tr>
<td>ClusterNetMask</td>
<td>Net mask for ClusterIPAddress.</td>
</tr>
</tbody>
</table>

**PrivateSubnetOverride Actions (Add, Modify and Delete)**

This action is similar to the ClusterSubnetOverride ("ClusterSubnetOverride Actions (Add, Modify and Delete)" on page 95) action, for a private (monitored or non-monitored) interface. For a private interface, you can only override cluster members’ interface names and network addresses, not cluster interface IP addresses or net masks.

In LSMcli, substitute the following for <action> in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

<Add|Modify|Delete>PrivateSubnetOverride VPN1ClusterMember <ROBOMemberName> <InterfaceName> [-IName=<MembersInterfaceName>] [-MNet=<MembersNetAddress>]

If there is a set override value, and you want to change it, use only ModifyPrivateSubnetOverride. If the override value you want to set is not defined (except at the Profile level), because it has never been defined or because it was deleted, use only AddPrivateSubnetOverride. To cancel a value and return to the Profile value, use DeletePrivateSubnetOverride.

The action must define at least one parameter: -IName or -MNet.

Explanations of the parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Modify</td>
</tr>
<tr>
<td>ROBOMemberName</td>
<td>The SmartLSM cluster member to override values for.</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Current name of member interface, as defined in the Profile topology.</td>
</tr>
<tr>
<td>MembersInterfaceName</td>
<td>New interface name. The name must match the name defined in the operating system.</td>
</tr>
<tr>
<td>MembersNetAddress</td>
<td>New network address for this interface. This address will be combined with the host parts defined in the Profile to produce complete IP addresses.</td>
</tr>
</tbody>
</table>
**RemoveCluster**

This action will revoke all the certificates used by the SmartLSM cluster and its members, release all the licenses and, finally, will delete the SmartLSM cluster and member objects.

In LSMcli, substitute the following for `<action>` in the LSMcli syntax ("Managing SmartLSM Clusters with LSMcli" on page 92):

```
RemoveCluster <ROBOClusterName>
```

**ResetSic**

This general LSM command applies to SmartLSM Clusters, with the same syntax as for regular SmartLSM gateways, using a cluster `member` name for `<ROBOName>`

**ResetIke**

This general LSM command applies to SmartLSM Clusters, with the same syntax as for regular SmartLSM gateways. For `<ROBOName>` use either a cluster name, to reset IKE for the cluster, or a cluster member name, to reset IKE for that member.

**ExportIke**

This general LSM command applies to SmartLSM Clusters, with the same syntax as for regular SmartLSM gateways. For `<ROBOName>` use either a cluster name, to export IKE for the cluster, or a cluster member name, to export IKE for that member.

**Convert Actions**

There is no convert action for or to SmartLSM clusters.

**SmartUpdate Actions**

The SmartUpdate actions listed in this guide apply to SmartLSM cluster `members`, with the same syntax as for regular SmartLSM gateways.

**Push Policy**

This general LSM command applies to SmartLSM Clusters, with the same syntax as for regular SmartLSM gateways. In the command syntax, use the cluster name (not a cluster member name). The policy is pushed to all cluster members.

**Other Push Actions**

PushDOs and GetStatus are general LSM commands that apply to SmartLSM cluster `members`, with the same syntax as for regular SmartLSM gateways.
Chapter 16
Dynamic Objects

In This Chapter
Understanding Dynamic Objects 98
User-Defined Dynamic Objects 99
Dynamic Object Examples 100

Understanding Dynamic Objects
Profiles enable you to update large numbers of gateways using Dynamic Objects — logical objects whose values, IP addresses or ranges, are resolved differently per gateway. In other words, Dynamic Objects localize a general profile. You can create one SmartLSM Security Profile or Provisioning Profile that can be applied to any number of actual gateways.

Dynamic Objects are defined in SmartDashboard and referenced in Security Policies, NAT tables, and profiles.

Some Dynamic Objects are provided by default; however, if you want to create your own, to more efficiently manage your unique environment, you need to create these objects in SmartDashboard.

Benefits of Dynamic Objects
In SmartDashboard, create Dynamic Objects to hold values for SmartProvisioning gateways. This enables you to create rules, Security Policies, and SmartProvisioning SmartLSM Security Profiles that are can be reused for numerous gateways.

Dynamic Objects enable you to:
- 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, automatically localizing 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 whenever you create a new SmartLSM Security Gateway object, Auto-Resolved Dynamic Objects are replaced with their values as soon as the gateway loads an updated profile from the Security Management Server or Domain Management Server. These Dynamic Objects cannot be edited. See table below.

- Centrally Resolved: A Dynamic Object is created in SmartDashboard and for each SmartLSM Security Gateway, you define the IP address or range to which the Dynamic Object will be resolved.

Auto Resolved Dynamic Objects

<table>
<thead>
<tr>
<th>Default Dynamic Object</th>
<th>Resolves to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuxiliaryNet</td>
<td>IP address range, based on the IP address and net mask of the interface configured as the Auxiliary network for the SmartLSM Security Gateway</td>
</tr>
</tbody>
</table>
Default Dynamic Object | Resolves to:
--- | ---
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
LocalMachine_All_Interfaces | DAIP machine interfaces, both static and dynamic

**Dynamic Object Values**

Dynamic Objects, created in SmartDashboard and used in Security Policy rules, are resolved to actual IP address or IP address ranges. When the Security Policy is fetched by a SmartLSM Security Profile for a SmartLSM Security Gateway, SmartProvisioning resolves the Dynamic Objects.

Dynamic Objects are automatically resolved whenever a gateway fetches a SmartLSM Security Profile from the Security Management Server or Domain Management Server.

You can also actively push the values of Dynamic Objects, ensuring 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, either on internal or by push, the SmartLSM Security Profile is localized for each gateway. Localization is performed in the following 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.

**Using Dynamic Objects**

To use Dynamic Objects:

1. In SmartDashboard, create the Dynamic Objects, the Security Policy that uses the Dynamic Objects, and the SmartProvisioning Profile that calls the Security Policy.
2. In SmartProvisioning, add a SmartLSM Security Gateway based on the SmartLSM Security Profile, and then configure the gateway's Dynamic Object list to include and resolve the Dynamic Objects of the Security Policy.

**User-Defined Dynamic Objects**

**Creating User-Defined Dynamic Objects**

To create centrally and locally resolved Dynamic Objects:

1. In SmartDashboard, select **Manage > Network Objects > New > Dynamic Object**.
2. Provide the relevant information and click **OK**.

**Configuring User-Defined Dynamic Object Values**

If a fetched SmartLSM Security Profile 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 be sure to 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 have created a Dynamic Object in SmartDashboard, you can add it as a Dynamic Object to a SmartLSM Security Gateway, providing the exact IP address or range to which SmartProvisioning will resolve the Dynamic Object.

**Note** - The **Dynamic Objects** tab has an **Add** button, but this does not add new Dynamic Objects; it adds a new resolve-to value for the selected SmartLSM Security Gateway to an already defined Dynamic Object. If you click **Add** and have already resolved all defined Dynamic Objects, the following message will appear: **All defined Dynamic Objects are already resolved. Use the Check Point SmartDashboard in order to add more Dynamic Objects.**

To specify the resolution value of a user-defined Dynamic Object:
1. Double-click a SmartLSM Security Gateway (either Security Gateway or UTM-1 Edge).
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 SmartDashboard.
   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.

**Dynamic Object Examples**

The examples in this section show how to create rules in SmartDashboard, to create a Security Policy that uses Dynamic Objects. After you create the rule base, install it as a Security Policy on the SmartLSM Security Profile.

For each gateway assigned to the SmartLSM Security Profile, the Dynamic Objects are localized and resolved to the real IP addresses of each gateway. 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** - Remember that the **LocalMachine** Dynamic Object in the following examples will be resolved to the external IP address of the SmartLSM Security Gateway; it is not the IP address of the SmartConsole or the Security Management Server or Domain Management Server.

**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 thus, to any number of gateways. This rule hides the internal network behind the external IP address of the SmartLSM Security Gateway.

**Example — NAT Hide**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>InternalNet</td>
<td>Any</td>
<td>Any</td>
<td>LocalMachine(H)</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>
Defining Static NAT for Multiple Networks

This example uses Dynamic Objects that you can define for yourself, according to 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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>PublishedIP</td>
<td>HTTP</td>
</tr>
<tr>
<td>Any</td>
<td>WebServer</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

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 creating rules with Dynamic Objects, you should be careful that it is installed on the relevant SmartLSM Security Profile, the profile for which all its gateways have these Dynamic Objects configured.

LAN Rules

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Log</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>InternalNet</td>
<td>DMZNet</td>
<td>*Any Traffic</td>
<td>Any</td>
<td>Accept</td>
<td>None</td>
<td>Profile1</td>
</tr>
</tbody>
</table>

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, allowing this rule to be part of numerous gateways.

External Hosts Rules

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Log</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>LocalMachine</td>
<td>*Any Traffic</td>
<td>ICMP echo-request</td>
<td>Accept</td>
<td>None</td>
<td>Profile1 LSMProfile1</td>
</tr>
</tbody>
</table>
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 gateway.

In SmartDashboard, do the following:

1. Create a Dynamic Objects called Safe_Internal.
2. Add this object to the VPN community (called MyComm in this example) that includes the IP addresses of the CO gateway (MyCO) and its VPN domain (CO_VPN).
3. Create a SmartLSM Security Profile object called MyProfile.
4. Create a Security Policy with the following rules.

**VPN with Range**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>LocalMachine</td>
<td>MyComm</td>
<td>ftp</td>
<td>Accept</td>
<td>MyCO</td>
</tr>
<tr>
<td>Safe_Internal</td>
<td>CO_VPN</td>
<td>MyComm</td>
<td>ftp</td>
<td>Accept</td>
<td>MyProfile</td>
</tr>
<tr>
<td>CO_VPN</td>
<td>Safe_Internal</td>
<td>MyComm</td>
<td>ftp</td>
<td>Accept</td>
<td>MyProfile</td>
</tr>
</tbody>
</table>

In SmartProvisioning, do the following:

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.
Chapter 17

Command Line Reference

In This Chapter
- Check Point LSMcli Overview
- SmartLSM Security Gateway Management Actions
- SmartUpdate Actions
- Push Actions
- Gateway Conversion Actions
- Multi-Domain Security Management Commands

Check Point LSMcli Overview

Check Point SmartLSM Command Line Utility (LSMcli) is a simple command line utility, an alternative to SmartProvisioning SmartConsole GUI. LSMcli provides the ability to perform SmartProvisioning GUI operations from a command line or through a script.

Note - LSMcli can run from locations other than SmartConsole clients, so be sure to define the location that LSMcli is running from as a GUI client. See Logging into SmartProvisioning (see "Logging in to SmartProvisioning" on page 15).

Terms

In the LSMcli, commands may use the abbreviation ROBO (Remote Office/Branch Office) gateways. ROBO gateways in SmartProvisioning are known as SmartLSM Security Gateways.

Notation

Throughout this chapter square brackets ([ ]) are used with the LSMcli utility. These brackets are correct and syntactically necessary. The following 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.

Help

Displays command line usage and provides examples for different actions.

Usage

LSMcli [-h | --help]

Syntax

LSMcli [-d] <server> <user> <pswd> <action>
**LSMcli Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>User</td>
<td>User name used in the standard Check Point authentication method</td>
</tr>
<tr>
<td>Pswd</td>
<td>Password used in the standard Check Point authentication method</td>
</tr>
<tr>
<td>Action</td>
<td>Specific function performed (See the following sub-sections for a complete list of actions.)</td>
</tr>
</tbody>
</table>

**Using Security Gateway 80 LSMcli ROBO Commands**

LSMcli commands for Security Gateway 80 are similar to the ROBO commands for regular Security Gateways. When you are using a command on Security Gateway 80, replace VPN1 with CPSG80. For example, if you want to use the AddROBO command:

- Regular Security Gateway: `AddROBO VPN1`
- Security Gateway 80: `AddROBO CPSG80`

For more information, use the LSMcli `Help` ("Help" on page 103) command.

**SmartLSM Security Gateway Management Actions**

### AddROBO VPN1

This command adds a new Check Point SmartLSM Security Gateway to Smart Provisioning and assigns it a specified SmartLSM Security Profile. If a one-time password is supplied, a SIC certificate will be created. If an IP address is also supplied, the SIC certificate will be pushed to the SmartLSM Security Gateway (in such cases, the SmartLSM Security Gateway SIC one-time password should be initialized first). If no IP address is supplied, the SIC certificate will be pulled from the SmartLSM Security Gateway afterwards. It is also possible to assign an IP address range to Dynamic Objects, specifying whether or not to add them to the VPN domain.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> AddROBO VPN1 <ed Name> <Profile> [-RoboCluster=<OtherROBOName>] [-O=<ActivationKey> [-I=<IP>]] [[-CA=<CaName> [-R=<CertificateIdentifier#> [-KEY=<AuthorizationKey>]]] [-D]:<DynamicObjectName>=<IP1>[-<IP2>] [-D]:..]
```

**Parameters**

### AddROBO VPN1 Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of a SmartLSM Security Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of a SmartLSM Security Profile that has been defined in SmartDashboard</td>
</tr>
<tr>
<td>OtherROBOName</td>
<td>Name for an already defined SmartLSM Security Gateway that is to participate in the SmartLSM Cluster with the newly created gateway (if the -RoboCluster argument is provided).</td>
</tr>
<tr>
<td>ActivationKey</td>
<td>SIC one-time password. (For this action, a certificate will be generated)</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of the gateway (For this action, certificate will be pushed to the gateway)</td>
</tr>
<tr>
<td>CaName</td>
<td>Name of the Trusted CA object (created from SmartDashboard). The IKE certificate request will be sent to this CA. Default is Check Point Internal CA.</td>
</tr>
<tr>
<td>CertificateIdentifier#</td>
<td>Key identifier for third-party CA.</td>
</tr>
<tr>
<td>AuthorizationKey</td>
<td>Authorization Key for third-party CA.</td>
</tr>
<tr>
<td>DynamicObjectName</td>
<td>Name of the Dynamic Object</td>
</tr>
<tr>
<td>IP1-IP2</td>
<td>IP address range for the Dynamic Object</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrvr name pass AddROBO VPN1 MyRobo AnyProfile -O=MyPass -l=192.0.2.4 -DE:FirstDO=192.0.2.100

This action 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 gateway.

AddROBO VPN1 MyRobo AnyProfile -O=MyPass -l=10.10.10.1 -DE:FirstDO=10.10.10.5 -CA=OPSEC_CA -R=cert1233 -KEY=ab345

**AddROBO VPN1Edge**

This command adds a new UTM-1 Edge SmartLSM Security Gateway. Applicable for UTM-1 Edge gateways only.

Use this command to add a new UTM-1 Edge gateway to the SmartProvisioning system and assign it a specified SmartLSM Security Profile. Specify the product type of the UTM-1 Edge gateway and the firmware installed, which can be set as local, default or user-defined. It is also possible to assign an IP address range to Dynamic Objects, specifying whether to add them to the VPN domain.

To load new firmware on the UTM-1 Edge gateway, use SmartUpdate.

**Usage**

### Parameters

**AddROBO UTM-1 Edge Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the UTM-1 Edge gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of a SmartLSM Security Profile that has been defined in SmartDashboard</td>
</tr>
<tr>
<td>ProductType</td>
<td>Product type</td>
</tr>
<tr>
<td>OtherROBOName</td>
<td>Name of the already defined SmartLSM Security Gateway that is to participate in the SmartLSM Cluster with the newly created gateway (if the <strong>-RoboCluster</strong> argument is provided)</td>
</tr>
<tr>
<td>RegistrationKey</td>
<td>Registration Key</td>
</tr>
<tr>
<td>CaName</td>
<td>Name of the Trusted CA object (created from SmartDashboard). The IKE certificate request will be sent to this CA.</td>
</tr>
<tr>
<td>CertificateIdentifier#</td>
<td>Key identifier of the specific certificate</td>
</tr>
<tr>
<td>AuthorizationKey</td>
<td>Authorization Key that will be sent to the CA for certificate retrieval</td>
</tr>
<tr>
<td>Firmware-name</td>
<td>Firmware name, or LOCAL or DEFAULT</td>
</tr>
<tr>
<td>MAC</td>
<td>Mac address of the UTM-1 Edge, in the format xx:xx:xx:xx:xx:xx where “x” is a hexadecimal digit</td>
</tr>
<tr>
<td>ProductKey</td>
<td>Product key (license), in the format xxxxxx-xxxxxxx-xxxxxxx, where “x” is a hexadecimal digit</td>
</tr>
<tr>
<td>DO Name</td>
<td>Name of the Dynamic Object</td>
</tr>
<tr>
<td>Ip1-Ip2</td>
<td>IP address range for the Dynamic Object</td>
</tr>
</tbody>
</table>

### Example

**LSMcli** mySrvr name pass AddROBO VPN1Edge MyRobo AnyProfile SBox-100  
This example creates an object in SmartProvisioning for a UTM-1 Edge SmartLSM Security Gateway called MyRobo, based on a SmartLSM Security Profile defined in SmartDashboard called AnyProfile. MyRobo is defined for a UTM-1 Edge on an SBox-100 device.

**LSMcli** mySrvr name pass AddROBO VPN1Edge MyRobo AnyProfile IP30 -O=AnyRegKey -F=DEFAULT – M=00:08:AA:BB:CC:DD -K=123456-ABCDEF-ABC123

**LSMcli** mySrvr name pass AddROBO VPN1Edge MyRobo AnyProfile SBox-100 -F=Safe@_Safe@_3.0.23_Generic_Safe@_fcs
**ModifyROBO VPN1**

This command modifies a Check Point SmartLSM Security Gateway. This action modifies the Smart Provisioning details for an existing SmartLSM Security Gateway and can be used to update properties previously supplied by the user.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> ModifyROBO VPN1 <RoboName> [and at least one of: [-P=Profile] [-RoboCluster=<OtherROBOName>|-NoRoboCluster] [-D:<DO name>=<IP1>[-<IP2>] [-KeepDOs]..]
```

**Parameters**

*ModifyROBO VPN1 Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of a SmartLSM Security Profile that has been defined in SmartDashboard</td>
</tr>
<tr>
<td>OtherROBOName</td>
<td>Name of the already defined SmartLSM Security Gateway that is to participate in the Cluster with the newly created gateway (if the -RoboCluster argument is provided)</td>
</tr>
<tr>
<td>-NoRoboCluster</td>
<td>The -NoRoboCluster parameter is equivalent to the &quot;Remove Cluster&quot; operation from GUI. When a ModifyROBO VPN1 command with this argument is issued on a gateway that participates in a cluster, the cluster is removed.</td>
</tr>
<tr>
<td>DO Name</td>
<td>Name of the Dynamic Object</td>
</tr>
<tr>
<td>IP1-IP2</td>
<td>IP address range for the Dynamic Object</td>
</tr>
<tr>
<td>-KeepDOs</td>
<td>Keeps all existing dynamic objects in the dynamic objects list when adding 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 using the LSMcli command to add new dynamic objects.</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass ModifyROBO VPN1 MyRobo -D:MyEmailServer=123.45.67.8 -D:MySpecialNet=10.10.10.1-10.10.10.6
```

This example resolves Dynamic Objects for the given gateway.
**Modify ROBO VPN1Edge**

This command modifies a UTM-1 Edge gateway. This action modifies the Smart Provisioning details for an existing UTM-1 Edge gateway and can be used to update properties previously supplied by the user.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> ModifyROBO VPN1Edge<RoboName> and at least one of: [-P=<Profile>] [-T=<ProductType>] [-RoboCluster=<OtherROBOName>|-NoRoboCluster]-O=RegistrationKey] [-F=LOCAL|DEFAULT|<Firmware-name>] [-M=<MAC>] [-K=<ProductKey>] [-D[E]:<D.O. name>=<IP1>[-<IP2>] [-KeepDOs].]
```

**Parameters**

*ModifyROBO UTM-1 Edge Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the UTM-1 Edge gateways</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of a SmartLSM Security Profile that has been defined in SmartDashboard</td>
</tr>
<tr>
<td>ProductType</td>
<td>Product type</td>
</tr>
<tr>
<td>OtherROBOName</td>
<td>Name of the already defined SmartLSM Security Gateway that is to participate in the SmartLSM Cluster with the newly created gateway (if the -RoboCluster argument is provided)</td>
</tr>
<tr>
<td>-NoRoboCluster</td>
<td>The -NoRoboCluster parameter is equivalent to the &quot;Remove SmartLSM Cluster&quot; operation from GUI. When a ModifyROBO VPN1 command with this argument is issued on a gateway that participates in a SmartLSM cluster, the cluster is removed).</td>
</tr>
<tr>
<td>RegistrationKey</td>
<td>Registration key</td>
</tr>
<tr>
<td>Firmware</td>
<td>Firmware name, LOCAL or DEFAULT</td>
</tr>
<tr>
<td>MAC</td>
<td>Mac address of the UTM-1 Edge, in the format xx:xx:xx:xx:xx:xx where &quot;x&quot; is a hexadecimal digit</td>
</tr>
<tr>
<td>ProductKey</td>
<td>Product key (license), in the format xxxxxxx-xxxxxxx-xxxxxxx, where &quot;x&quot; is a hexadecimal digit</td>
</tr>
<tr>
<td>DO Name</td>
<td>Name of the Dynamic Object</td>
</tr>
<tr>
<td>E</td>
<td>Obsolete, refer to the LSMcli command: ModifyROBOManualVPNDomain.</td>
</tr>
<tr>
<td>Ip1-Ip2</td>
<td>IP address range for the Dynamic Object</td>
</tr>
</tbody>
</table>
KeepDOs

Keeps all existing dynamic objects in the dynamic objects list when adding 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 using the LSMcli command to add new dynamic objects.

Example

LSMcli mySrvr name pass ModifyROBO VPN1Edge MyEdgeROBO -P=MyNewEdgeProfile-NoRoboCluster

ModifyROBOManualVPNDomain

This command modifies the ROBO VPN Domain, to take effect when the VPN Domain becomes defined as Manual.

Usage

LSMcli [-d] <server> <user> <pswd> ModifyROBOManualVPNDomain <RoboName> and one of: -Add=<FirstIP-LastIP> -Delete=<Index (as shown by the last ShowROBOTopology command)> and optionally: [-IfOverlappingIPRangesDetected=<exit|warn|ignore>]

Parameters

ModifyROBOManual VPN Domain Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>FirstIP-LastIP</td>
<td>IP address range</td>
</tr>
<tr>
<td>Index</td>
<td>Value displayed by ShowInfo command</td>
</tr>
<tr>
<td>IfOverlappingIPRangesDetected</td>
<td>Flag to determine course of action, if overlapping IP address ranges are detected. The options are: exit, warn and ignore</td>
</tr>
</tbody>
</table>

Example

LSMcli mySrvr name pass ModifyROBOManualVPNDomain MyRobo -Add=192.0.2.1-192.0.2.20
LSMcli mySrvr name pass ModifyROBOManualVPNDomain MyRobo -Delete=1
ModifyROBOTopology VPN1

This command modifies the ROBO VPN Domain configuration for a selected Gateway.

Usage

LSMcli [-d] <server> <user> <pswd> ModifyROBOTopology VPN1 <RoboName> -VPNDomain=<not_defined|external_ip_only|topology|manual>

Parameters

ModifyROBOTopology VPN1 Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>VPNDomain</td>
<td>Flag to determine the VPN Domain topology. The options are:</td>
</tr>
<tr>
<td></td>
<td>• not_defined : Equivalent to the Not Defined option in the Topology tab of a SmartLSM Security Gateway in the Smart Provisioning GUI (or in the ShowROBOTopology output).</td>
</tr>
<tr>
<td></td>
<td>• external_ip_only : Equivalent to Only the external interface</td>
</tr>
<tr>
<td></td>
<td>• topology : Equivalent to All IP Addresses behind the Gateway based on Topology information</td>
</tr>
<tr>
<td></td>
<td>• manual : Equivalent to Manually defined. VPN domain is defined according to ModifyROBOManualVPNDomain setting.</td>
</tr>
</tbody>
</table>

Example

LSMcli mySrvr name pass ModifyROBOTopology VPN1 MyRobo -VPNDomain=manual

ModifyROBOTopology VPN1Edge

This command modifies the VPN Domain configuration for a selected Gateway.

Usage

LSMcli [-d] <server> <user> <pswd> ModifyROBOTopology VPN1Edge <RoboName> and at least one of: [-VPNDomain=<not_defined|external_ip_only|topology|automatic|manual>]
Parameters

*ModifyROBOTopology UTM-1 Edge Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>VPNDomain</td>
<td>Flag to configure the VPN Domain topology. The options are: not_defined, external_ip_only, topology, and manual.</td>
</tr>
<tr>
<td></td>
<td>• not_defined: Equivalent to the Not Defined option in the Topology tab of a SmartLSM Security Gateway in the SmartProvisioning GUI (or in the ShowROBOTopology output).</td>
</tr>
<tr>
<td></td>
<td>• external_ip_only: Equivalent to Only the external interface</td>
</tr>
<tr>
<td></td>
<td>• topology: Equivalent to All IP Addresses behind the Gateway based on Topology information</td>
</tr>
<tr>
<td></td>
<td>• automatic: The VPN domain of the gateway consists of all the IP addresses configured locally on the UTM-1 Edge device, regardless of the interface configuration of the Edge object in SmartDashboard. Selecting this option requires:</td>
</tr>
<tr>
<td></td>
<td>• Manual definition of VTIs on the Edge and CO gateway so that the CO learns the VPN domain of the Edge device.</td>
</tr>
<tr>
<td></td>
<td>• OSPF feature of the CO gateway to dynamically learn the VPN domain of the UTM-1 Edge device.</td>
</tr>
<tr>
<td></td>
<td>• manual: Equivalent to Manually defined</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrvr name pass ModifyROBOTopology VPN1Edge MyRobo -VPNDomain=manual

**ModifyROBOInterface VPN1**

This command modifies the Internal Interface list.

**Usage**

LSMcli [-d] <server> <user> <pswd> ModifyROBOInterface VPN1 <RoboName> <InterfaceName> and at least one of: [-i=<IPAddress>] [-Netmask=<NetMask>] and optionally: [-IfOverlappingIPRangesDetected=<exit|warn|ignore>]

**Parameters**

*ModifyROBOInterface VPN1 Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server Domain Management Server</td>
</tr>
</tbody>
</table>

---

SmartProvisioning Administration Guide R76 | 111
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Name of the existing interface</td>
</tr>
<tr>
<td>IPAddress</td>
<td>IP address of the interface</td>
</tr>
<tr>
<td>NetMask</td>
<td>Net mask of the interface</td>
</tr>
<tr>
<td>IfOverlappingIPRangesDetected</td>
<td>Flag to determine course of action, if overlapping IP address ranges are detected. The options are: exit, warn and ignore</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrvr name pass ModifyROBOInterface VPN1 MyRobo eth0 -i=192.0.2.1 -Netmask=255.255.255.0

**ModifyROBOInterface VPN1Edge**

This command modifies the VPN1Edge Internal Interface list.

**Usage**

LSMcli [-d] <server> <user> <pswd> ModifyROBOInterface VPN1Edge <RoboName> <InterfaceName> and at least one of: [-i=<IPAddress>] [-NetMask=<NetMask>] [-Enabled=<true|false>] [-HideNAT=<true|false>] [-DHCPEnabled=<true|false>] [-DHCPIpAllocation=<automatic|<FirstIP-LastIP>|<IP address of DHCP Relay Server>] and optionally: [-IfOverlappingIPRangesDetected=<exit|warn|ignore>]

**Parameters**

**ModifyROBOInterface UTM-1 Edge Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Name of an existing interface</td>
</tr>
<tr>
<td>IPAddress</td>
<td>IP address of the interface</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetMask</td>
<td>Net mask of the interface</td>
</tr>
<tr>
<td>Enabled</td>
<td>Flag to enable/disable the selected interface</td>
</tr>
<tr>
<td>HideNAT</td>
<td>Flag to specify whether the interface is identified by the gateway IP address (hidden behind NAT)</td>
</tr>
<tr>
<td>DHCPEnabled</td>
<td>Flag to enable dynamically allocated IP addresses</td>
</tr>
<tr>
<td>DHCPIpAllocation</td>
<td>Flag to determine how IP addresses are dynamically allocated. The options are: automatic, &lt;FirstIP-LastIP&gt;, and DHCP Relay Server</td>
</tr>
<tr>
<td>IfOverlappingIPRangesDetected</td>
<td>Flag to determine course of action if overlapping IP address ranges are detected. The options are: exit, warn and ignore</td>
</tr>
</tbody>
</table>

### Example

`LSMcli mySrvr name pass ModifyROBOInterface VPN1Edge MyRobo DMZ -i=192.0.2.1 -Netmask=255.255.255.0 -Enabled=true -HideNAT=false -DHCPEnabled=true -DHCPIpAllocation=automatic`

### AddROBOInterface VPN1

This command adds a new interface to the selected SmartLSM Security Gateway.

### Usage

`LSMcli [-d] <server> <user> <pswd> AddROBOInterface VPN1 <RoboName> <InterfaceName> -i=<IPAddress> -NetMask=<NetMask>`

### Parameters

#### AddROBOInterface VPN1 Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Name of an existing interface</td>
</tr>
<tr>
<td>IPAddress</td>
<td>IP address of the interface</td>
</tr>
<tr>
<td>NetMask</td>
<td>Net mask of the interface</td>
</tr>
</tbody>
</table>

---

**Command Line Reference**

Smart Provisioning Administration Guide R76 | 113
Example
LSMcli mySrvr name pass AddROBOInterface VPN1 MyRobo eth0 -i=192.0.2.1 -Netmask=255.255.255.0

DeleteROBOInterface VPN1
This command deletes an interface from the selected Gateway.

Usage
LSMcli [-d] <server> <user> <pswd> DeleteROBOInterface VPN1 <RoboName> <InterfaceName>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>InterfaceName</td>
<td>Name of an existing interface</td>
</tr>
</tbody>
</table>

Example
LSMcli mySrvr name pass DeleteROBOInterface VPN1 MyRobo eth0

ResetSic
This command resets the SIC Certificate of a SmartLSM Security Gateway. Applicable for SmartLSM Security Gateways only. This action revokes the existing gateway SIC certificate and creates a new one using the one-time password provided by the user. If an IP address is supplied for the SmartLSM Security Gateway, the SIC certificate will be pushed to the SmartLSM Security Gateway, in which case the SmartLSM Security Gateway SIC's one-time password should be initialized first. Otherwise, if no IP address is given, the SIC certificate will later be pulled from the SmartLSM Security Gateway.

Usage
LSMcli [-d] <server> <user> <pswd> ResetSic <RoboName> <ActivationKey> [-i=<IP>]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
</tbody>
</table>

### SmartProvisioning Administration Guide R76

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>ActivationKey</td>
<td>One-time password for the Secure Internal Communications with the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of gateway (for this action, the certificate is pushed to the gateway)</td>
</tr>
</tbody>
</table>

### Example

**LSMcli** mySrvr name pass ResetSic MyROBO aw47q1

**LSMcli** mySrvr name pass ResetSic MyFixedIPROBO sp36rt1 -I=10.20.30.1

**ResetIke**

This command resets the IKE Certificate of a SmartLSM Security Gateway. Applicable for Security Gateway and UTM-1 Edge gateways. This action revokes the existing IKE certificate and creates a new one.

### Usage

**LSMcli** [-d] <server> <user> <pswd> ResetIke <RoboName>[-CA=<CaName> [-R=<CertificateIdentifier#>] [-KEY=<AuthorizationKey>]]

### Parameters

**ResetIke Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the Security Gateway or UTM-1 Edge gateway</td>
</tr>
<tr>
<td>CaName</td>
<td>Name of the Trusted CA object (created from SmartDashboard); the IKE certificate request will be sent to this CA</td>
</tr>
<tr>
<td>CertificateIdentifier</td>
<td>Key identifier of the specific certificate</td>
</tr>
<tr>
<td>AuthorizationKey</td>
<td>Authorization Key to be sent to the CA for the certificate retrieval</td>
</tr>
</tbody>
</table>

### Example

**LSMcli** mySrvr name pass ResetIke MyROBO -CA=OPSEC_CA -R=cer3452s -KEY=ad23fgh
**ExportIke**

This command exports the IKE Certificate of a SmartLSM Security Gateway into a P12 file, encrypted with a provided password. The default location of the exported file is `$FWDIR/conf`.

**Usage**

```
LMScli [-d] <server> <user> <pswd> ExportIke <RoboName> <Password> <FileName>
```

**Parameters**

*ExportIke Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway whose certificate will be exported</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to protect the p12 file</td>
</tr>
<tr>
<td>FileName</td>
<td>Destination file name (will be created)</td>
</tr>
</tbody>
</table>

**Example**

```
LMScli mySrvr name pass ExportIke MyROBO ajg42k93N MyROBOCert.p12
```

**UpdateCO**

This command updates a Corporate Office gateway. This action updates the CO gateway with up-to-date available information about the SmartLSM Security Gateways VPN domains. Perform after adding a new SmartLSM Security Gateway to enable the CO gateway to initiate a VPN tunnel to the new SmartLSM Security Gateway. (Alternatively, the Install Policy action can be run on the CO gateway to obtain updated VPN Domain information.) Applicable for CO gateways only.

**Usage**

```
LMScli [-d] <server> <user> <pswd> UpdateCO <COgw|COgwCluster>
```

**Parameters**

*UpdateCO Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
--- | ---
Cogw | Name of a CO gateway
CogwCluster | Name of a cluster of CO gateways

### Example

```
LSMcli mySrvr name pass UpdateCO MyCO
```

### Remove

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. Applicable for Security Gateway and UTM-1 Edge gateways.

### Usage

```
LSMcli [-d] <server> <user> <pswd> Remove <RoboName> <ID>
```

### Parameters

#### Remove Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of Security Gateway or UTM-1 Edge gateway</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the SmartLSM Security Gateway (use <strong>Show</strong> to check the ID of the specific SmartLSM Security Gateway)</td>
</tr>
</tbody>
</table>

### Example

```
LSMcli mySrvr name pass Remove MyRobo 0.0.0.251
```

### Show

This command displays a list of existing gateways. Applicable for Security Gateway and UTM-1 Edge gateways.

### Usage

```
LSMcli [-d] <server> <user> <pswd> Show [-N=Name] [-F= nbctvpglskd]
```
Parameters

Show Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the gateway to display</td>
</tr>
<tr>
<td></td>
<td>If –N flag is not included, this action prints the existing Devices workspace, including SmartLSM Security Gateways.</td>
</tr>
</tbody>
</table>

-F

One can filter the information printed out using the following flags:

- n Name
- b ID
- c Cluster ID
- i IP address
- t Type
- v Version
- p SmartLSM Security Profile
- g Gateway status
- l Policy status
- s SIC DN
- k IKE DN
- d List of Dynamic Objects assigned to this SmartLSM Security Gateway

Example

LSMcli mySrvr name pass Show -N=MyRobo
LSMcli mySrvr name pass Show -F=nibtp

ModifyROBOConfigScript

ModifyROBOConfigScript and ShowROBOConfigScript are equivalent to the Configuration Script tab in Smart Provisioning GUI for UTM-1 Edge SmartLSM Security Gateways. (Applicable only to UTM-1 Edge SmartLSM Security Gateways.)

ModifyROBOConfigScript sets the given UTM-1 Edge SmartLSM Security Gateway's configuration script to be a copy of the contents of the given text file <inputScriptFile>.

ModifyROBOConfigScript
Usage

LSMcli [-d] <server> <user> <pswd> ModifyROBOConfigScript VPN1Edge <RoboName> <inputScriptFile>

Parameters

ModifyROBOConfigScript Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of UTM-1 Edge gateway</td>
</tr>
<tr>
<td>inputScriptFile</td>
<td>The given UTM-1 Edge SmartLSM Security Gateway's configuration script is set to be a copy of the contents of the given text file.</td>
</tr>
</tbody>
</table>

Example

LSMcli mySrvr name pass ModifyROBOConfigScript VPN1Edge MyRobo myScriptFile

ShowROBOConfigScript

This command shows the given UTM-1 Edge SmartLSM Security Gateway’s configuration script, and its SmartLSM Security Profile’s configuration script.

Usage

LSMcli [-d] <server> <user> <pswd> ShowROBOConfigScript VPN1Edge <RoboName>

Parameters

ShowROBOConfigScript Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of UTM-1 Edge gateway</td>
</tr>
</tbody>
</table>

Example

LSMcli mySrvr name pass ShowROBOConfigScript VPN1Edge MyRobo
ShowROBOTopology

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. The indexes of the manually defined VPN domain IP address ranges, on the displayed list, can be used when requesting to delete a range, via the ModifyROBOManualVPNDomain command.

Usage

LSMcli [-d] <server> <user> <pswd> ShowROBOTopology <RoboName>

Parameters

ShowROBOTopology Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of Security Gateway or UTM-1 Edge gateway</td>
</tr>
</tbody>
</table>

Example

LSMcli mySrvr name pass ShowROBOTopology MyRobo

SmartUpdate Actions

Before software can be installed on gateways, it must first be loaded to the Security Management Server. We recommend that you make sure that software is compatible by running the VerifyInstall command ("VerifyInstall" on page 122) first. Install software using the Install command ("Install" on page 120).

Uninstall the software using the uninstall command ("Uninstall" on page 121).

Install

This command installs a product on a SmartLSM Security Gateway. This action installs the specified software on the SmartLSM Security Gateway. Note that the software must be loaded to the Security Management Server before attempting to install it on the SmartLSM Security Gateway. It is recommended that you run the VerifyInstall command first, before installing software on the SmartLSM Security Gateway. Applicable to SmartLSM Security Gateways only.

Usage

LSMcli [-d] <server> <user> <pswd> Install <RoboName> <Product> <Vendor> <Version> <SP> [-P=Profile] [-boot] [-DoNotDistribute]
Parameters

Install Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the package</td>
</tr>
<tr>
<td>Vendor</td>
<td>Name of the vendor of the package</td>
</tr>
<tr>
<td>Version</td>
<td>Major Version of the package</td>
</tr>
<tr>
<td>SP</td>
<td>Minor Version of the package</td>
</tr>
<tr>
<td>Profile</td>
<td>Assign a different SmartLSM Security Profile (already defined in SmartDashboard) after installation</td>
</tr>
<tr>
<td>boot</td>
<td>Reboot the SmartLSM Security Gateway after the installation is done</td>
</tr>
<tr>
<td>-DoNotDistribute</td>
<td>(Optional) Install previously distributed packages</td>
</tr>
</tbody>
</table>

Example

LSMcli mySrvr name pass Install MyRobo firewall checkpoint NG_AI fcs -P=AnyProfile -boot

Uninstall

This command uninstalls a product on a SmartLSM Security Gateway. This action uninstalls the specified package from the SmartLSM Security Gateway. The ShowInfo command can be used to see what products are installed on the SmartLSM Security Gateway. Applicable to SmartLSM Security Gateways only.

Usage

LSMcli [-d] <server> <user> <pswd> Uninstall <ROBO> <Product> <Vendor> <Version> <SP> [-P=Profile] [-boot]

Parameters

Uninstall Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>ROBO</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the package</td>
</tr>
<tr>
<td>Vendor</td>
<td>Name of the vendor of the package</td>
</tr>
<tr>
<td>Version</td>
<td>Major Version of the package</td>
</tr>
<tr>
<td>SP</td>
<td>Minor Version of the package</td>
</tr>
<tr>
<td>Profile</td>
<td>Assign a different SmartLSM Security Profile (already defined in SmartDashboard) after uninstall</td>
</tr>
<tr>
<td>boot</td>
<td>Reboot the SmartLSM Security Gateway after the installation is finished</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrvr name pass Uninstall MyRobo firewall checkpoint NG_AI fcs -boot

---

**VerifyInstall**

This command verifies whether selected software can be installed on the SmartLSM Security Gateway, whether the software is compatible. Note that this action does not perform an installation. Run this command before using the install command to install software on the SmartLSM Security Gateway. Applicable to SmartLSM Security Gateways only.

**Usage**

LSMcli [-d] <server> <user> <pswd> VerifyInstall <RoboName> <Product> <Vendor> <Version> <SP>

**Parameters**

**VerifyInstall Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the package</td>
</tr>
<tr>
<td>Vendor</td>
<td>Name of the vendor of the package</td>
</tr>
<tr>
<td>Version</td>
<td>Major version of the package</td>
</tr>
<tr>
<td>SP</td>
<td>Minor version of the package</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrvr name pass VerifyInstall MyRobo firewall checkpoint NG_AI fcs
**Distribute**

This command distributes a package from the Repository to the SmartLSM Security Gateway, but does not install it.

**Usage**

`LSMcli [-d] <server> <user> <pswd> Distribute <RoboName> <Product> <Vendor> <Version> <SP>`

**Parameters**

*Distribute Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the package</td>
</tr>
<tr>
<td>Vendor</td>
<td>Name of the vendor of the package</td>
</tr>
<tr>
<td>Version</td>
<td>Major version of the package</td>
</tr>
<tr>
<td>SP</td>
<td>Minor version of the package</td>
</tr>
</tbody>
</table>

**Example**

`LSMcli mySrvr name pass Distribute MyRobo fw1 checkpoint NG_AI R54`

**Upgrade**

This command upgrades all the (appropriate) available software packages on the SmartLSM Security Gateway. Applicable to SmartLSM Security Gateways only.

**Usage**

`LSMcli [-d] <server> <user> <pswd> Upgrade <RoboName> [-P=Profile] [-boot]`

**Parameters**

*Upgrade Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td>Assign a different SmartLSM Security Profile (already defined in SmartDashboard) after installation</td>
</tr>
<tr>
<td><strong>boot</strong></td>
<td>Reboot the SmartLSM Security Gateway after the installation is finished</td>
</tr>
</tbody>
</table>

### Example

```
LSMcli mySrvr name pass Upgrade MyRobo -P=myprofile -boot
```

### VerifyUpgrade

This command verifies whether selected software can be upgraded on the SmartLSM Security Gateway, whether the software is compatible. Note that this command does not perform an installation. Run this command before using the upgrade command. Applicable to SmartLSM Security Gateways only.

#### Usage

```
LSMcli [-d] <server> <user> <pswd> VerifyUpgrade <RoboName>
```

#### Parameters

#### VerifyUpgrade Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>server</strong></td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td><strong>user</strong></td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td><strong>pswd</strong></td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td><strong>RoboName</strong></td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
</tbody>
</table>

```
Example

LSMcli mySrvr name pass VerifyUpgrade MyRobo
```

### GetInfo

This command collects product information from the SmartLSM Security Gateway. You must run this command before running the **ShowInfo** command if you manually upgrade any package instead of using SmartUpdate. Applicable to SmartLSM Security Gateways only.

#### Usage

```
LSMcli [-d] <server> <user> <pswd> GetInfo <RoboName>
```

#### Parameters

#### GetInfo Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>server</strong></td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
</tbody>
</table>

```
Example

LSMcli mySrvr name pass GetInfo MyRobo
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>RoboName</td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrVR name pass GetInfo MyRobo

**ShowInfo**

This command displays product information for the list of the products installed on the SmartLSM Security Gateway. For a SmartLSM Security Gateway, run the `GetInfo` command before using this command to verify that the displayed information is up-to-date. Applicable to Security Gateway and UTM-1 Edge gateways.

**Usage**

LSMcli [-d] <server> <user> <pswd> ShowInfo <VPN1EdgeRoboName>

**Parameters**

*ShowInfo Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>VPN1EdgeRoboName</td>
<td>Name of the Security Gateway or UTM-1 Edge gateway</td>
</tr>
</tbody>
</table>

**Example**

LSMcli mySrVR name pass ShowInfo MyRobo

**ShowRepository**

This command shows the list of the available products on Security Management Server. Use SmartUpdate to manage the products, load new products, remove products, and so on.

**Usage**

LSMcli [-d] <server> <user> <pswd> ShowRepository

**Example**

LSMcli mySrVR name pass ShowRepository
**Stop**

This command stops Security Gateway services on the selected gateway. Note that this command utilizes CPRID, therefore CPRID services must be running on the gateway. Applicable to Security Gateways and SmartLSM Security Gateways.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> Stop <Robo|Gateway>
```

**Parameters**

**Stop Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Robo or Gateway</td>
<td>Name of the SmartLSM Security Gateway, or Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass Stop MyRobo
```

**Start**

This command starts Security Gateway services on the selected gateway. Note that this command utilizes CPRID, therefore CPRID services must be running on the gateway. Applicable to Security Gateways and SmartLSM Security Gateways.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> Start <Robo|Gateway>
```

**Parameters**

**Start Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Robo or Gateway</td>
<td>Name of the SmartLSM Security Gateway or Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass Start MyRobo
```
**Restart**

This command re-starts Security Gateway services on the chosen gateway. Note that this command utilizes CPRID, therefore CPRID services must be running on the gateway. Applicable to SmartLSM Security Gateways, UTM-1 Edge gateways and Security Gateways.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> Restart <Robo|Gateway>
```

**Parameters**

*Restart Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Robo or Gateway</td>
<td>Name of the SmartLSM Security Gateway, UTM-1 Edge gateway or Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass Restart MyRobo
```

**Reboot**

This command reboots the chosen gateway. Note that this command utilizes CPRID, therefore CPRID services must be running on the gateway. Applicable to SmartLSM Security Gateways, UTM-1 Edge gateways and Security Gateways.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> Reboot <Robo|Gateway>
```

**Parameters**

*Reboot Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Robo or Gateway</td>
<td>Name of the SmartLSM Security Gateway, UTM-1 Edge gateway or Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass Reboot MyRobo
```
### Push Actions

The following commands are used to push updated values, settings, and security rules to gateways. After creating a gateway or dynamic object in the SmartProvisioning system, it must be assigned a security policy. Use the push command to commit the security policy: see **PushPolicy** (on page 128), and **PushDOs** (on page 128).

#### PushPolicy

This command pushes a policy to the chosen gateway. Note that this command utilizes CPRID, therefore CPRID services must be running on the gateway. Applicable to SmartLSM Security Gateways and UTM-1 Edge gateways.

**Usage**

`LSMcli [-d] <server> <user> <pswd> PushPolicy <Robo|Gateway>`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server</code></td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td><code>user</code></td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td><code>pswd</code></td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td><code>Robo or Gateway</code></td>
<td>Name of the SmartLSM Security Gateway or standard gateway</td>
</tr>
</tbody>
</table>

**Example**

`LSMcli mySrvr name pass PushPolicy MyRobo`

#### PushDOs

This command updates a Dynamic Object's information on the SmartLSM Security Gateway. Note that 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 PushPolicy command**. Applicable to SmartLSM Security Gateways and UTM-1 Edge gateways.

**Usage**

`LSMcli [-d] <server> <user> <pswd> PushDOs <RoboName>`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server</code></td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td><code>user</code></td>
<td>User name of standard Check Point authentication method</td>
</tr>
</tbody>
</table>

---

**Table artworks:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server</code></td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td><code>user</code></td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td><code>Robo or Gateway</code></td>
<td>Name of the SmartLSM Security Gateway or standard gateway</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>pswd</code></td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td><code>RoboName</code></td>
<td>Name of the SmartLSM Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass PushDOs MyRobo
```

**GetStatus**

This command fetches various statistics from the chosen gateway. Applicable to Security Gateway ROBO and Security Gateways.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> GetStatus <Robo|Gateway>
```

**Parameters**

**GetStatus Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server</code></td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td><code>user</code></td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td><code>pswd</code></td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td><code>Robo or Gateway</code></td>
<td>Name of the Security Gateway ROBO or Security Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass GetStatus MyRobo
```

**Gateway Conversion Actions**

The following commands enable you to convert a gateway from a SmartLSM Security Gateway to a regular gateway and vice versa.

**Convert ROBO VPN1**

This command converts a SmartLSM Security Gateway to a Security Gateway. You can specify whether the gateway should be a CO gateway, or not. Applicable to SmartLSM Security Gateways only.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> Convert ROBO VPN1 <Name> [-CO] [-Force]
```
Parameters

**Convert ROBO VPN1 Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Security Gateway, or UTM-1 Edge gateway</td>
</tr>
<tr>
<td>CO</td>
<td>Define as a CO gateway</td>
</tr>
<tr>
<td>Force</td>
<td>Convert the gateway, even if no connection can be established</td>
</tr>
<tr>
<td></td>
<td>Use with caution, as a forced conversion will always succeed, even if no connection to the gateway exists. If this happens, make sure the remote operations are done manually on the gateway computer:</td>
</tr>
<tr>
<td></td>
<td>1. Execute the command <code>LSMenabler -r off</code> to turn off SmartLSM Security Gateway support.</td>
</tr>
<tr>
<td></td>
<td>2. Execute the command <code>LSMenabler on</code> to make the gateway a CO gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In SmartDashboard, define gateway parameters: interfaces, communities, etc.; then install the policy.</td>
</tr>
</tbody>
</table>

Example

```
LSMcli mySrvr name pass Convert ROBO VPN1 MyRobo \-CO
LSMcli mySrvr name pass Convert ROBO VPN1 MyRobo \-Force
```

**Convert Gateway VPN1**

This command converts a Security Gateway to a SmartLSM Security Gateway. You can specify whether the gateway should have a CO gateway. Applicable to Security Gateways only.

Usage

```
```

Parameters

**Convert VPN Gateway Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Security Gateway or UTM-1 Edge gateway</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Profile</td>
<td>Assign a different SmartLSM Security Profile (already defined in SmartDashboard) after conversion</td>
</tr>
<tr>
<td>EXT</td>
<td>Name of external interface</td>
</tr>
<tr>
<td>INT</td>
<td>Name of internal interface</td>
</tr>
<tr>
<td>DMZ</td>
<td>Name of DMZ interface</td>
</tr>
<tr>
<td>AUX</td>
<td>Name of Auxiliary Network interface</td>
</tr>
<tr>
<td>NoRestart</td>
<td>Do not restart Check Point services, on the remote machine, after convert operation has finished</td>
</tr>
<tr>
<td>Force</td>
<td>Convert the gateway, even if no connection can be established</td>
</tr>
</tbody>
</table>

Use with caution, as a forced conversion will always succeed, even if no connection to the gateway exists. If this happens, make sure the remote operations are done manually on the gateway computer:

1. Execute `LSMenable r` on to turn on SmartLSM Security Gateway support.
2. Define gateway parameters and map it to a SmartLSM Security Profile in SmartProvisioning.

### Example

`LSMcli mySrvr name pass Convert Gateway VPN1 MyGW MyProfile –E=hme0 –I=hme1 –D=hme2 -F`

### Convert ROBO VPN1Edge

This command converts a UTM-1 Edge SmartLSM Security Gateway to a UTM-1 Edge gateway. You must completely define the gateway using SmartDashboard, and adjust and reinstall the security policy. Applicable to UTM-1 Edge gateways only.

### Usage

`LSMcli [-d] <server> <user> <pswd> Convert ROBO VPN1Edge <Name>`

### Parameters

#### Convert ROBO UTM-1 Edge Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the UTM-1 Edge gateway</td>
</tr>
</tbody>
</table>

### Example

`LSMcli mySrvr name pass Convert ROBO VPN1Edge MyRobo`
**Convert Gateway VPN1Edge**

This command converts a UTM-1 Edge gateway to a UTM-1 Edge SmartLSM Security Gateway. The gateway is assigned the specified SmartLSM Security Profile. You must completely define the gateway using SmartDashboard, and adjust and reinstall the security policy. Applicable to UTM-1 Edge gateways only.

**Usage**

```
LSMcli [-d] <server> <user> <pswd> Convert Gateway VPN1Edge <Name> <Profile>
```

**Parameters**

**Convert Gateway UTM-1 Edge Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Security Management Server or Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the UTM-1 Edge gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>Assign a different SmartLSM Security Profile (already defined in SmartDashboard) after conversion</td>
</tr>
</tbody>
</table>

**Example**

```
LSMcli mySrvr name pass Convert Gateway VPN1Edge MyRobo MyProfile
```

**Multi-Domain Security Management Commands**

SmartProvisioning in a Multi-Domain Security Management environment has additional features and commands.

**hf_propagate**

Multi-Domain Security Management Domain Management Servers may contain INSPECT files (*.def). Use this command to propagate updated INSPECT files from the Multi-Domain Server to a given Domain Management Server.

**Usage**

```
LSMcli <server> <user> <pswd> hf_propagate [m | o | u] [--override_manual]
```

**Parameters**

**hf_propagate Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Name/IP address of the Domain Management Server</td>
</tr>
<tr>
<td>user</td>
<td>User name of standard Check Point authentication method</td>
</tr>
</tbody>
</table>
## Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pswd</td>
<td>Password of standard Check Point authentication method</td>
</tr>
<tr>
<td>m</td>
<td>Do not copy INSPECT files (default)</td>
</tr>
<tr>
<td>o</td>
<td>Replace INSPECT files</td>
</tr>
<tr>
<td>u</td>
<td>Uninstall INSPECT files</td>
</tr>
<tr>
<td>override_manual</td>
<td>Add to override manual changes in INSPECT files</td>
</tr>
</tbody>
</table>

### Example

```bash
LSMcli myCMAsrvr name pass hf_propagate
```