SmartLSM Guide

NG with Application Intelligence

For additional technical information about Check Point products, consult Check Point’s SecureKnowledge at

http://support.checkpoint.com/kb/

Part No.: 700556
June 2003
The following statements refer to those portions of the software copyrighted by the OpenSSL Project. This software is provided "as is" to anyone in the world, with no express or implied warranty. Copyright © 2000-2007 The OpenSSL Project. All rights reserved. This product and related documentation are protected by copyright law andavailble for use, copying, distribution, and reproduction under the terms of the GNU General Public License. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files ("the Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

1. The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

2. The Software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and freedom from infringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising in any way out of the use of this Software, even if advised of the possibility of such damage.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Table Of Contents

SmartLSM User Guide Supplement
  Introduction  1
  Overview  1
    SmartLSM Overview  1
    Gateway Profiles & ROBO Gateway Objects  2
    Policy Management  3
    Policy Localization — Dynamic Objects  3
    VPN  4
    CO Gateway  5
    Convert  6
    Upgrade  6
    Safe@ Integration  7
    Supported Features  7
    Unsupported Features and Known Limitations  8

Getting Started
  Check Point VPN-1/FireWall-1  9
  Supported Platforms  9
  Installing SmartLSM  10
    Installing SVN Foundation  10
    Installing the SmartCenter Server  10
    Installing a ROBO Gateway  10
    Installing the CO Gateway  10
    Installing the SmartLSM  11

Smart LSM Command Line Utility
  Introduction  14
  Help  14
  LSMcli Actions  14
    AddCP  15
    AddSW  16
    ModifyCP  17
    ModifySW  18
    ResetSic  19
    ResetIke  20
    UpdateCO  20
    Remove  21
    Show  21
    SmartUpdate Actions for a ROBO Gateway  22
    Install  23
    Uninstall  23
    VerifyInstall  24
    Upgrade  25
Profiles and Policies
Defining Check Point Gateway Profiles 35
Defining Policies for the Gateway Profile Objects 36
Defining a Policy to allow VPN from the ROBO Gateway to the CO Gateway 37
Working with a Default Profile 38
Defining a Policy to the Gateway that Protects the SmartCenter Server 38

SmartLSM
SmartLSM — Overview 41
Logging into SmartLSM 42
Gateways List Pane 45
Status View — Action Status Tab 46
Status View — Critical Notifications Tab 47
Menus and Toolbars 47
Menus 47
Toolbar 49
Adding a New ROBO Gateway 49
Adding a Safe@ ROBO Gateway 51
Editing a ROBO Gateway 53
Editing a Safe@ ROBO Gateway 57
Updating a CO Gateway 59
Modifying Policies 60
Deleting a ROBO Gateway Object 60
Push Actions for a Gateway 60
Status Information 61

Troubleshooting
Status Information 63
Logging 63
VPN Troubleshooting Tools 63
SmartLSM User Guide Supplement

Introduction

Check Point SmartLSM is an integral part of Check Point VPN-1/FireWall-1 New Generation with Application Intelligence (VPN-1/FireWall-1 R54). This document describes the SmartLSM features added to VPN-1/FireWall-1 R54. Please review this information before installing SmartLSM. Please read the SmartCenter Guide for information about VPN-1/FireWall-1.

Overview

In This Section

<table>
<thead>
<tr>
<th>SmartLSM Overview</th>
<th>page 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Profiles &amp; ROBO Gateway Objects</td>
<td>page 2</td>
</tr>
<tr>
<td>Policy Management</td>
<td>page 3</td>
</tr>
<tr>
<td>Policy Localization — Dynamic Objects</td>
<td>page 3</td>
</tr>
<tr>
<td>VPN</td>
<td>page 4</td>
</tr>
<tr>
<td>Supported Features</td>
<td>page 7</td>
</tr>
<tr>
<td>Unsupported Features and Known Limitations</td>
<td>page 8</td>
</tr>
</tbody>
</table>

SmartLSM Overview

SmartLSM allows system administrators to manage thousands of simple, similar Check Point Remote Office/Branch Office (ROBO) Gateways from a single SmartCenter Server, in a cost effective way.
The SmartLSM management concept is based on “Gateway Profiles”, which are defined in the standard Check Point SmartDashboard. Instead of representing a single physical Gateway, each Gateway Profile object represents multiple ROBO Gateways.

A separate, scalable and simple utility, the SmartLSM application, is used to define all the ROBO Gateways and their specific properties (e.g. their IKE Certificates). Within this utility each ROBO Gateway is mapped to a Profile object.

The same SmartCenter Server that manages ROBO Gateways can also manage standard Check Point CO (Corporate Office) Gateways.

SmartLSM reduces the administrative overhead per Gateway, by defining most of the Gateway properties, as well as the Policy, per Profile Object instead of per physical ROBO Gateway.

SmartLSM reduces the run-time load on the SmartCenter Server by using the Periodic Policy Fetch technology instead of the Push Policy technology (e.g. Policy Installation), and by utilizing various Check Point products, such as, Customer Log Module (CLM) and Multi customer Log Module (MLM) etc.

**Gateway Profiles & ROBO Gateway Objects**

A Profile is used to define a ROBO Gateway type. Each individual ROBO Gateway inherits the majority of its properties, as well as its Policy, from a Profile. Profiles are defined and managed through Check Point SmartDashboard.

Once a Gateway Profile object is defined in SmartDashboard, you can define the respective ROBO Gateways in SmartLSM. The task of defining each individual ROBO Gateway is simple. You simply specify the name of the ROBO Gateway. The following three properties are also mandatory, but they are selected by default when you create a new ROBO Gateway:

- The ROBO Gateway type, whether a Check Point ROBO Gateway or Safe@ROBO Gateway (the default is Check Point ROBO Gateway)
- The ROBO Gateway version (the default is the latest version depending on the type selected above)
- The Profile from which the ROBO Gateway will obtain all of its other properties (the default is the profile that was selected in SmartDashboard in the **Global Properties — Profile Based Management** page). Varied profiles allow you to differentiate between the various ROBO Gateways (e.g. allow a VPN Encryption Tunnel to CO Gateways from ROBO Gateways mapped to one Profile, but not to ROBO Gateways mapped to another Profile).
Policy Management

Policies are managed per-Profile, and not per-ROBO Gateway, for better scalability.

A Policy is defined and installed via SmartDashboard per Profile. This operation only prepares the Policy files on the SmartCenter Server (it does not push the Policy to any specific Gateway).

Policy Fetching

The Policy is fetched periodically by the ROBO Gateways. The Periodic Policy Fetch Interval is configurable per-Profile in the Masters page of the Check Point Gateway Profile Object. Each ROBO Gateway randomly chooses a time slot in the periodic fetch interval to fetch its Policy.

Policy fetching can also be initiated manually, from the ROBO Gateway, or centrally, from the SmartLSM (using the Push Policy command — see “Push Actions for a Gateway” on page 60).

Once a Policy is fetched by the ROBO Gateway, it is localized as follows:
- the specific properties of the ROBO Gateway are used.
- Anti-Spoofing and Encryption-Domain information are automatically calculated.
- automatically Calculated Dynamic Objects are assigned their values.
- centrally resolved Dynamic Objects are assigned their values.
- the Policy is installed.

Note - This process is skipped if there were no changes in the Policy or in any of the centrally resolved Dynamic Objects.

Policy Localization — Dynamic Objects

SmartLSM utilizes Dynamic Objects to localize the Policy of the Profile Object for potentially hundreds and thousands of ROBO Gateways.

SmartLSM uses several methods to resolve Dynamic Objects’ values:

1. Automatically Resolved Dynamic Objects — these objects automatically get their values when the ROBO Gateway loads a Policy. These objects can be seen in the Dynamic Objects tab of the Edit ROBO Gateway window. They appear by default when a new ROBO Gateway is created:
   - LocalMachine — the Dynamic Object’s value is resolved to the external IP address of the ROBO Gateway itself (based on the IP address of the interface marked as External).
• **InternalNet** — the Dynamic Object’s value is resolved to the IP address range of the internal network, based on the IP address and netmask of the interface marked as *Internal*.

• **DMZNet** — the Dynamic Object’s value is resolved to the IP address range of the DMZ network, based on the IP address and netmask of the interface marked as *DMZ*.

• **AuxiliaryNet** — the Dynamic Object’s value is resolved to the IP address range of the Auxiliary network, based on the IP address and netmask of the interface marked as *Auxiliary*.

2 Centrally Resolved Dynamic Objects from the SmartLSM (see “Editing a ROBO Gateway” on page 53).

3 Locally Resolved Dynamic Objects, which are resolved manually on the ROBO Gateway itself via the `dynamic_objects` command line.

**Note** - Notice that you must resolve all Dynamic Objects that are used in the policy. An unresolved Dynamic Object referenced in a rule will result in dropping all the packets that match the other characteristics of that rule.

**VPN**

**VPN Tunnels**

SmartLSM supports the inclusion of ROBO Profiles as members in star VPN Communities (as satellites), and in Remote Access communities (as centers). A VPN tunnel can be established from a ROBO Gateway to a regular static IP address CO Gateway (similar to the way that DAIP Gateways establish VPN tunnels to static IP Gateways). A Corporate Office Gateway (CO Gateway) recognizes (and authenticates) an incoming VPN tunnel as a tunnel from a ROBO Gateway, using the IKE Certificate of the ROBO Gateway. The CO Gateway treats the peer ROBO Gateway as if it were a regular DAIP Gateway, whose properties are defined by the Profile to which the ROBO Gateway is mapped.

A CO Gateway can also initiate a VPN tunnel to a ROBO Gateway, supported for CO Gateways in version R54. (In previous versions traffic was encrypted from the CO Gateway to the ROBO Gateway through “Back Connections” – which entailed initiating a tunnel from the ROBO Gateway to the CO Gateway.) SmartLSM also supports **VPN routing for satellites**. Community properties are used to set parameters for this routing. Using the option **To Center, or through the center to other satellites, to internet and other VPN targets**, you can establish ROBO-to-ROBO VPN tunnelling through the CO Gateway; or ROBO-to-other Gateway, via the CO Gateway.
Determining the Profile of a ROBO Gateway

Upon establishing IKE authentication, a CO Gateway determines which ROBO Profile is applied to the initiating ROBO Gateway. This is done by a lookup of the ROBO Gateway’s IKE DN in a dedicated ROBO mapping database. This database maps the IKE DN to the respective Profile of the initiating ROBO Gateway.

If the IKE DN of the initiating ROBO Gateway is *not* found in the mapping database, then a “Default Profile” may be selected instead as the ROBO Gateway’s profile. To do so, select the Default Profile in the Global Properties — Profile Based Management window. You can determine the default mapping by setting a flag in the Global Properties — Profile Based Management window.

It is important that the mapping database be updated whenever ROBO Gateways are added, deleted or modified. The update can be performed either from the SmartLSM GUI, by selecting Update Corporate Office Gateways in the ROBO Gateway’s Actions menu — or from SmartDashboard, by reinstalling the policy.

ROBO Gateway Encryption Domain

A ROBO Gateway’s encryption domain is automatically calculated based on the IP address and netmask of the ROBO Gateway’s internal interfaces. Complicated networks behind a ROBO Gateway are not supported.

From the CO Gateway’s perspective, the ROBO Gateway’s encryption domain is defined by the ROBO Gateway’s external IP address. It is assumed that everything is NAT-hidden behind the external IP address.

New in version R54, Dynamic Objects can be used to enhance the encryption domain of the ROBO Gateway. Define a Dynamic Object in the SmartDashBoard to represent the desired encryption domain, and designate its IP range per ROBO Gateway. Ensure that you check the Add to VPN Domain option. All other internal networks behind a ROBO Gateway should be hidden using NAT Hide.

CO Gateway

The SmartCenter Server has the ability to manage both standard Check Point Gateways and ROBO Gateways. Standard Gateways which are assigned static IPs can serve as targets for VPN Tunnels initiated from ROBO Gateways. These target Gateways are referred to as Corporate Office Gateways, or in short, CO Gateways.
**Convert**

SmartLSM supports fast conversion of regular Check Point Gateway to ROBO Gateway and vice versa. There is no need to delete existing objects and create new objects, since the conversion operation will do this automatically, while preserving the relevant SIC certificates.

When will use the conversion capabilities? If you have just started to use SmartLSM you may want to convert regular Gateways to ROBO Gateways, or to import the Gateways you have in order to manage them through SmartLSM. For example, you may currently have only a small number of Branch offices and you may want to add many more – and decide to manage all of them through SmartLSM.

You may also need to convert a ROBO Gateway to a regular Gateway if a specific ROBO Gateway has increased its management requirements and you decide to manage it separately as a regular Gateway. In this case, after converting ROBO Gateway to a Check Point Gateway, the sophisticated conversion process is finished through SmartDashboard (which is used to define interfaces, update VPN communities, and install policies). Check Point services should be restarted afterwards.

After any conversion operation, remember to run the Install Policy action on the new gateway (including ROBO Gateways) to update it with new information created by the Check Point conversion process.

**Upgrade**

SmartLSM supports upgrades of Check Point products for ROBO Gateways via the SmartLSM GUI, using SmartUpdate.

In order to upgrade your system follow these steps –

1. Upgrade your SmartCenter server.

2. If you have new Check Point Module Upgrade packages, add to the Smart Update Repository. Similarly, if you have new Safe@ firmware packages, add these SmartUpdate repository. If you have both, add both to the Repository.

3. Upgrade your CO Gateways.

4. Use the SmartLSM GUI to upgrade your ROBO Gateways. The upgrade commands and icons are similar to the SmartUpdate commands. Alternatively, you may use the SmartLSM Command Line Utility.
Safe@ Integration

SmartLSM supports Safe@ Gateways as ROBO Gateways. This requires the installation of SSC component on the SmartCenter Server – the same as for the regular SmartCenter support of Safe@ Gateways. You must define Safe@ Gateway Profiles through the SmartDashboard, and other Safe@ Gateway properties through the SmartLSM GUI. Although some Safe@ ROBO Gateways properties may differ from those of Check Point ROBO Gateways such as licenses and products, other aspects of working with Safe@ ROBO Gateways are the same as for Check Point ROBO Gateways, for example in terms of setting up VPN communities, policy installation, or defining troubleshooting statuses.

Supported Features

SmartLSM supports the following R54 features:

- DAIP (Dynamically Assigned IP) and static IP address ROBO Gateways.
- All FireWall features that are supported by NG DAIP Gateways.
- Centrally resolved Dynamic Objects.
- VPN tunnels from ROBO Gateways to CO Gateways, based on IKE with Internal Certificate Authority (ICA) Certificates, and from CO Gateways to ROBO Gateways.
- Automatic calculation of Anti-Spoofing information for ROBO Gateways.
- Periodic, randomized Policy Fetch by the ROBO Gateways.
- A unique ID (in the form of an IP address) per-ROBO Gateway, used to track logs generated from a ROBO Gateway, even if its external IP address changes.
- Local logging, CLMs and MLMs, used to reduce the logging load.
- High level & In-Depth status monitoring of ROBO Gateways.
- SmartUpdate capabilities — ROBO Gateway License Management through SmartLSM, central upgrades of ROBO Gateways.
- Provider-1 — CMAs support SmartLSM.
- Security Servers are supported on ROBO Gateways.
- Client Authentication, Session Authentication and User Authentication are supported by ROBO Gateways.
- Safe@ Gateways are supported as ROBO Gateways
- Conversion between ROBO Gateway and a regular Gateway.
- Command Line Utility to manage ROBO Gateways.
Unsupported Features and Known Limitations

- Only VPN-1/FireWall-1 can be installed on a ROBO Gateway.
- VPN is only supported using IKE Authentication with the Check Point Internal CA Certificates.
- Only simple internal networks (as defined by the IP address and Netmask of the internal interfaces) are supported.
- The SmartLSM GUI cannot update a ROBO Gateway Object when SmartDashboard is open in Read/Write mode.
- Limited support for Remote Access to a ROBO Gateway.
Getting Started

In This Section

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point VPN-1/FireWall-1</td>
<td>9</td>
</tr>
<tr>
<td>Supported Platforms</td>
<td>9</td>
</tr>
<tr>
<td>Installing SmartLSM</td>
<td>10</td>
</tr>
</tbody>
</table>

Check Point VPN-1/FireWall-1

Check Point SmartLSM is an integral part of Check Point VPN-1/FireWall-1 with Application Intelligence. Familiarize yourself with Check Point VPN-1/FireWall-1 by reading the Check Point SmartCenter Guide provided with this package. Then read this document, which describes the SmartLSM-specific features.

This document assumes the reader has a working knowledge of Check Point VPN-1/FireWall-1 with Application Intelligence.

Supported Platforms

The supported platforms for Check Point SmartLSM are identical to the supported platforms for VPN-1/FireWall-1.

Note - The ROBO Gateway is supported on the following platforms: Windows, Linux and NOKIA.
Installing SVN Foundation

SVN Foundation is needed for SmartCenter Server, ROBO Gateway and CO Gateway. To install the SVN Foundation, use the standard SVN Installation procedure.

Installing the SmartCenter Server

To install the SmartCenter Server:
- use the standard SmartCenter Server installation procedure.
- Execute LSMenabler on to enable support for ROBO Gateways on the server

Note - You will need a SmartCenter Pro license to activate SmartLSM functionality.

Installing a ROBO Gateway

To install a ROBO Gateway, proceed as follows:

1. Install the ROBO Gateway as if you were installing a regular Check Point Gateway.
2. Execute LSMenabler -r on to turn the Gateway into a ROBO Gateway
3. In the cpconfig utility, in the Interfaces page, make sure that you define an External Interface. The other three options can be completed at a later stage.

No special license is needed for the ROBO Gateway.

Installing the CO Gateway

To install a CO Gateway, proceed as follows:
Installing SmartLSM

• Install the CO Gateway as if you were installing a regular Check Point Gateway. A CO Gateway is identical to a standard NG Gateway and is installed and configured according to the standard installation procedure. No special license is needed for the CO Gateway.

• Execute LSMenabler on to enable support for ROBO Gateway on the CO Gateway.

Installing the SmartLSM

For installation details see the most current online documentation:

Smart LSM Command Line Utility

In This Section

<table>
<thead>
<tr>
<th>Action</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>14</td>
</tr>
<tr>
<td>Help</td>
<td>14</td>
</tr>
<tr>
<td>LSMcli Actions</td>
<td>14</td>
</tr>
<tr>
<td>AddCP</td>
<td>15</td>
</tr>
<tr>
<td>AddSW</td>
<td>16</td>
</tr>
<tr>
<td>ModifyCP</td>
<td>17</td>
</tr>
<tr>
<td>ModifySW</td>
<td>18</td>
</tr>
<tr>
<td>ResetSic</td>
<td>19</td>
</tr>
<tr>
<td>ResetIke</td>
<td>20</td>
</tr>
<tr>
<td>UpdateCO</td>
<td>20</td>
</tr>
<tr>
<td>Remove</td>
<td>21</td>
</tr>
<tr>
<td>Show</td>
<td>21</td>
</tr>
<tr>
<td>Install</td>
<td>23</td>
</tr>
<tr>
<td>Uninstall</td>
<td>23</td>
</tr>
<tr>
<td>VerifyInstall</td>
<td>24</td>
</tr>
<tr>
<td>Upgrade</td>
<td>25</td>
</tr>
<tr>
<td>VerifyUpgrade</td>
<td>25</td>
</tr>
<tr>
<td>ShowRepository</td>
<td>27</td>
</tr>
<tr>
<td>Stop</td>
<td>27</td>
</tr>
<tr>
<td>Start</td>
<td>28</td>
</tr>
</tbody>
</table>
**Introduction**

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

**Note** - Since LSMcli can run from different locations other than from the SmartConsole clients, be sure to define the location that LSMcli is running from as one of the SmartConsole (use cpconfig on the SmartCenter Server)

**Help**

Displays command line usage and provides examples for different actions.

**Usage**

LSMcli [-h | --help]

**LSMcli Actions**

Use this command format to perform a ROBO Gateway command.

**Usage**

LSMcli [-d] <Server> <User> <Pswd> <Action>
Parameters

TABLE 3-1  LSMLi parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>the name/IP address of the Smart Center Server</td>
</tr>
<tr>
<td>User</td>
<td>the username used in the standard Check Point authentication method</td>
</tr>
<tr>
<td>Pswd</td>
<td>the password used in the standard Check Point authentication method</td>
</tr>
</tbody>
</table>

AddCP

Add a new Check Point ROBO Gateway to SmartLSM. Applicable for Check Point ROBO Gateways only.

Use to add a new Check Point ROBO Gateway to the SmartLSM system and assign it a specified security profile. If a one-time password is supplied, an SIC certificate will be created. If an IP address is supplied also, the SIC certificate will be pushed to the ROBO Gateway (in such cases, the ROBO Gateway SIC one-time password should be initialized first). If no IP address is supplied, the SCI certificate will be pulled from the ROBO Gateway afterwards. It is also possible to assign an IP range to Dynamic Objects, specifying whether to add them to the VPN domain.

Usage

AddCP <ROBO> <Profile> [-O=OTP [-I=Ip]] [-D[E]::D.O. name>=IP1[-IP2] [-D[E]::..]
Parameters

TABLE 3-2  AddCP parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of Check Point ROBO Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>the name of the Profile</td>
</tr>
<tr>
<td>OTP</td>
<td>SIC one-time password. (For this action, a certificate will be generated)</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of ROBO (For this action, certificate will be pushed to ROBO)</td>
</tr>
<tr>
<td>DO Name</td>
<td>name of the Dynamic Object</td>
</tr>
<tr>
<td>E</td>
<td>Dynamic Object is to be added to VPN domain</td>
</tr>
<tr>
<td>Ip1-Ip2</td>
<td>IP range for the Dynamic Object</td>
</tr>
</tbody>
</table>

Example

AddCP  MyRobo AnyProfile
AddCP  MyRobo AnyProfile -O=AnyOTP -I=1.2.3.4 -DE:FirstDO=1.1.1.1

This action will add a new Check Point ROBO Gateway MyRobo and assign it the specified security profile AnyProfile. A one-time password is supplied, an IP address is supplied and the Dynamic Object is added to the VPN domain.

AddSW

Add a new Safe@ ROBO Gateway. Applicable for Safe@ ROBO Gateways only.

Use to add a new Safe@ ROBO Gateway to the SmartLSM system and assign it a specified security profile. Specify the product type of the Safe@ ROBO Gateway and the firmware installed, which can be set as local, default or user-defined. It is also possible to assign an IP range to Dynamic Objects, specifying whether to add them to the VPN domain.

To load new firmware on the Safe@ ROBO Gateway, use SmartUpdate.

Usage

Modify a Check Point ROBO Gateway. Applicable for Check Point ROBO Gateways only. This action will modify the SmartLSM details for an existing ROBO Gateway and can be used to update properties previously supplied by the user.

**Usage**

ModifyCP <ROBO> [and at least one of: [-P=Profile] [-D[E]:<D.O. name>=IP1[-IP2] [-D[E]:...]] ]
**Parameters**

TABLE 3-4  ModifyCP parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>the name of the Profile</td>
</tr>
<tr>
<td>DO Name</td>
<td>name of the Dynamic Object</td>
</tr>
<tr>
<td>E</td>
<td>Dynamic Object is to be added to VPN domain</td>
</tr>
<tr>
<td>Ip1-Ip2</td>
<td>IP range for the Dynamic Object</td>
</tr>
</tbody>
</table>

**Example**

ModifyCP       MyRobo -P=AnyProfile
ModifyCP       MyRobo -D:FirstDO=1.1.1.1 -DE:SecondDO=2.2.2.2-2.2.2.8
ModifyCP       MyRobo -P=AnyProfile -D:FirstDO=1.1.1.1

**ModifySW**

Modify a Safe@ ROBO Gateway. Applicable for Safe@ ROBO Gateways only. This action will modify the SmartLSM details for an existing Safe@ ROBO Gateway and can be used to update properties previously supplied by the user.

**Usage**


**Parameters**

TABLE 3-5  ModifySW parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Safe@ ROBO Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>the name of the Profile</td>
</tr>
<tr>
<td>ProductType</td>
<td>the product type</td>
</tr>
<tr>
<td>RegistrationKey</td>
<td>the Registration Key</td>
</tr>
<tr>
<td>Firmware</td>
<td>the firmware name, or LOCAL or DEFAULT</td>
</tr>
</tbody>
</table>
ResetSic

Reset the SIC Certificate of a ROBO Gateway. Applicable for Check Point ROBO Gateways only. This action will revoke the existing Gateway SIC certificate and create a new one using the one-time password provided by the user. If an IP address is supplied for the ROBO Gateway, the SIC certificate will be pushed to the ROBO Gateway, in which case the ROBO 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 ROBO Gateway.

Usage
ResetSic <ROBO> <OTP [-I=IP]>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
<tr>
<td>OTP</td>
<td>SIC one-time password. (For this action, a certificate will be generated)</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of ROBO. (For this action, certificate will be pushed to ROBO)</td>
</tr>
</tbody>
</table>

Example
ResetSic MyRobo AnyOTP -I=1.2.3.4
**ResetIke**

Reset the IKE Certificate of a ROBO Gateway. Applicable for Check Point and Safe@ROBO Gateways. This action will revoke the existing IKE certificate and create a new one.

**Usage**

`ResetIke <ROBO>`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point or Safe@ROBO Gateway</td>
</tr>
<tr>
<td>OTP</td>
<td>SIC one-time password. (For this action, a certificate will be generated)</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of ROBO (For this action, certificate will be pushed to ROBO)</td>
</tr>
</tbody>
</table>

**Example**

`ResetSic MyRobo AnyOTP -I=1.2.3.4`

**UpdateCO**

Update a Corporate Office Gateway. This action will update the Corporate Office Gateway with up-to-date available information about the ROBO Gateways VPN domains. Perform after adding a new ROBO Gateway to enable the Corporate Office Gateway to initiate a VPN tunnel to the new ROBO Gateway. (Alternatively it is possible to run the Install Policy action on the Corporate Office Gateway to obtain updated VPN Domain information.) Applicable for Corporate Office Gateways only.

**Usage**

`UpdateCO <COgwName|COgwCluster>`
**Remove**

Delete a ROBO Gateway. This action will revoke all the certificates used by the ROBO Gateway, release all the licenses and, finally, will remove the ROBO Gateway. Applicable for Check Point and Safe@ ROBO Gateways.

**Usage**

Remove <ROBO> <ID>

**Parameters**

**TABLE 3-9  Remove parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>name of Check Point / Safe@ ROBO Gateway</td>
</tr>
<tr>
<td>ID</td>
<td>The ID of the ROBO Gateway (use Show to check the ID of the specific ROBO Gateway)</td>
</tr>
</tbody>
</table>

**Example**

Remove MyRobo 0.0.0.251

**Show**

Display a list of existing Gateways. Applicable for Check Point and Safe@ ROBO Gateways.

**Usage**

Show [-N=Name] [-F= nbitvpglskd]
Parameters

**TABLE 3-10** Show parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name of the Gateway to display. If the -N flag is not included, this action will print the list of all existing Gateways, including ROBO Gateways, to the stdout (standard output).</td>
</tr>
<tr>
<td>-N</td>
<td>One can filter the information printed out using the following flags:</td>
</tr>
<tr>
<td>n</td>
<td>name</td>
</tr>
<tr>
<td>b</td>
<td>ID</td>
</tr>
<tr>
<td>i</td>
<td>IP Address</td>
</tr>
<tr>
<td>t</td>
<td>type</td>
</tr>
<tr>
<td>v</td>
<td>version</td>
</tr>
<tr>
<td>p</td>
<td>profile</td>
</tr>
<tr>
<td>g</td>
<td>gateway status</td>
</tr>
<tr>
<td>l</td>
<td>policy status</td>
</tr>
<tr>
<td>s</td>
<td>SIC DN</td>
</tr>
<tr>
<td>k</td>
<td>IKE DN</td>
</tr>
<tr>
<td>d</td>
<td>list of Dynamic Objects assigned to this ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

Show MyRobo
Show -F=nibtp

SmartUpdate Actions for a ROBO Gateway

In order to install software on gateways, note that the software must be loaded to the SmartCenter Server previously. Installations are then conducted using SmartUpdate. Before installing software, it is recommended that you check that software is compatible by running the VerifyInstall command first, see “VerifyInstall” on page 24. Install software using the Install command, see “Install” on page 23. Uninstall using the Uninstall command, see “Uninstall” on page 23.
Install

Install a product to a ROBO Gateway. This action will install the specified software on the ROBO Gateway. Note that the software must be loaded to the SmartCenter Server before attempting to install it to the ROBO Gateway. It is recommended that you run the `VerifyInstall` command first, before installing software on the ROBO Gateway. Applicable to Check Point ROBO Gateways only.

Usage

Install `<ROBO> <Product> <Vendor> <Version> <SP> [-P=Profile] [-boot]`

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>the name of the package</td>
</tr>
<tr>
<td>Vendor</td>
<td>the 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 security profile to the ROBO Gateway after installation</td>
</tr>
<tr>
<td>boot</td>
<td>reboot the ROBO Gateway after the installation is finished</td>
</tr>
</tbody>
</table>

Example

Install `MyRobo firewall checkpoint NG_AI fcs -P=AnyProfile -boot`

Uninstall

Uninstall a product on a ROBO Gateway. This action will uninstall the specified package from the ROBO Gateway. One can use `ShowInfo` command to see what products are installed on the ROBO Gateway. Applicable to Check Point ROBO Gateways only.

Usage

Uninstall `<ROBO> <Product> <Vendor> <Version> <SP> [-P=Profile] [-boot]`
Parameters

TABLE 3-12 Uninstall parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>the name of the package</td>
</tr>
<tr>
<td>Vendor</td>
<td>the 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 security profile to the ROBO Gateway after installation</td>
</tr>
<tr>
<td>boot</td>
<td>reboot the ROBO Gateway after the installation is finished</td>
</tr>
</tbody>
</table>

Example

Uninstall MyRobo firewall checkpoint NG_AI fcs -boot

VerifyInstall

This action will verify whether selected software can be installed on the ROBO Gateway, i.e. that 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 ROBO Gateway. Applicable to Check Point ROBO Gateways only.

Usage

VerifyInstall <ROBO> <Product> <Vendor> <Version> <SP>

Parameters

TABLE 3-13 VerifyInstall parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
<tr>
<td>Product</td>
<td>the name of the package</td>
</tr>
</tbody>
</table>
Upgrade

This action will upgrade all the (appropriate) available software packages on the ROBO Gateway. Applicable to Check Point ROBO Gateways only.

Usage
Upgrade <ROBO> [-P=Profile] [-boot]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>assign a security profile to the ROBO Gateway after installation</td>
</tr>
<tr>
<td>boot</td>
<td>reboot the ROBO Gateway after the installation is finished</td>
</tr>
</tbody>
</table>

Example
Upgrade MyRobo -boot

VerifyUpgrade

This action will verify whether selected software can be upgraded on the ROBO Gateway, i.e. that the software is compatible. Note that this action does not perform an installation. Run this command before using the upgrade command. Applicable to Check Point ROBO Gateways only.

Usage
VerifyUpgrade <ROBO>
**Parameters**

**TABLE 3-15** VerifyUpgrade parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

VerifyUpgrade MyRobo

**GetInfo**

This action will collect product information from the ROBO Gateway. You must run this command before running the ShowInfo command if you change the product configuration on a ROBO Gateway manually, that is, if you manually upgrade any package rather than use SmartUpdate. Applicable to Check Point ROBO Gateways only.

**Usage**

GetInfo <ROBO>

**Parameters**

**TABLE 3-16** GetInfo parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

GetInfo MyRobo

**ShowInfo**

This action will display product information for the list of the products installed on the ROBO Gateway. For a Check Point ROBO Gateway, run the GetInfo command before using this action to be sure the information displayed is up-to-date. Applicable to Check Point and Safe@ ROBO Gateways.

**Usage**

GetInfo <ROBO>
**Parameters**

**TABLE 3-17 ShowInfo parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point or Safe@ ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

GetInfo MyRobo

**ShowRepository**

This action will show the list of the available products on SmartCenter Server. Use SmartUpdate to manage the products, load new products, remove products, and so on.

**Usage**

ShowRepository

**Parameters**

**TABLE 3-18 ShowRepository parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBO</td>
<td>the name of the Check Point or Safe@ ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

ShowRepository

**Stop**

This action will stop a Gateway. This action will stop Check Point services on the chosen Gateway. Note that this action utilizes CPRID, so CPRID services must be running on the Gateway. Applicable to Check Point Gateways and Check Point ROBO Gateways.

**Usage**

Stop <GW>
Parameters

TABLE 3-19 Stop parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW</td>
<td>the name of the Check Point ROBO Gateway or Check Point Gateway</td>
</tr>
</tbody>
</table>

Example

Stop MyRobo

Start

This action will start Check Point services on the chosen Gateway. Note that this action utilizes CPRID, so CPRID services must be running on the Gateway. Applicable to Check Point Gateways and Check Point ROBO Gateways.

Usage

Start <GW>

Parameters

TABLE 3-20 Start parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW</td>
<td>the name of the Check Point ROBO Gateway or Check Point Gateway</td>
</tr>
</tbody>
</table>

Example

Start MyRobo

Restart

This action will re-start Check Point services on the chosen Gateway. Note that this action utilizes CPRID, so CPRID services must be running on the Gateway. Applicable to Check Point ROBO Gateways, Safe@ ROBO Gateways, Safe@ Gateways and Check Point Gateways.

Usage

Restart <GW>
Parameters

TABLE 3-21 Restart parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW</td>
<td>the name of the Check Point ROBO Gateway, Safe@ ROBO Gateway, Safe@ Gateway or Check Point Gateway</td>
</tr>
</tbody>
</table>

Example

Restart MyRobo

Reboot

This action will reboot the chosen Gateway. Note that this action utilizes CPRID, so CPRID services must be running on the Gateway. Applicable to Check Point ROBO Gateways, Safe@ ROBO Gateways, Safe@ Gateways and Check Point Gateways.

Usage

Reboot <GW>

Parameters

TABLE 3-22 Reboot parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW</td>
<td>the name of the Check Point ROBO Gateway, Safe@ ROBO Gateway, Safe@ Gateway or Check Point Gateway</td>
</tr>
</tbody>
</table>

Example

Reboot MyRobo

Push Actions

The following commands are used to push a gateway Policy, or a Dynamic Object policy respectively. After creating a gateway or dynamic object in the SmartLSM system, it must be assigned a security policy. Use the push action in order to commit the security policy: see “PushPolicy” on page 30, and “PushDOs” on page 30.
**PushPolicy**

This action will push a Policy to the chosen Gateway. Note that this action utilizes CPRID, so CPRID services must be running on the Gateway. Applicable to Check Point ROBO Gateways and Safe@ ROBO Gateways.

**Usage**

```
PushPolicy <Robo>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robo</td>
<td>the name of the Check Point / Safe@ ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
PushPolicy MyRobo
```

**PushDOs**

This action will update a Dynamic Object’s information on the ROBO Gateway. Note that this action will not remove/release the IP range for the deleted Dynamic Object, but only add new ones. To overcome this difficulty, run the PushPolicy command. Applicable to Check Point ROBO Gateways and Safe@ ROBO Gateways.

**Usage**

```
PushDOs <Robo>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robo</td>
<td>the name of the Check Point / Safe@ ROBO Gateway</td>
</tr>
</tbody>
</table>

**Example**

```
PushDOs MyRobo
```

**GetStatus**

This action will fetch various statistics from the chosen Gateway. Applicable to Check Point ROBO and Check Point Gateways.
Converting Gateways

Usage
GetStatus <Robo>

Parameters
TABLE 3-25 GetStatus parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW</td>
<td>the name of the Check Point ROBO or Check Point Gateway</td>
</tr>
</tbody>
</table>

Example
GetStatus MyRobo

Converting Gateways

Following are commands which allow you to convert a Gateway from a ROBO Gateway to a regular Gateway and vise versa.

Convert CPROBO

This action will convert a Check Point ROBO Gateway to a Check Point Gateway. The user can specify whether the Gateway should have a Dynamic IP Address or be a CO Gateway, or neither. Applicable to Check Point ROBO Gateways only.

Usage
Convert CPROBO <Name> [-Daip | -CO] [-Force]

Parameters
TABLE 3-26 Convert CPROBO parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>the name of the Check Point or Safe@ ROBO Gateway</td>
</tr>
<tr>
<td>Daip</td>
<td>the resulting Gateway will be defined with Dynamic IP Address</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>
</tbody>
</table>
The `Force` flag should be used with caution, because a forced conversion will “succeed” even if no connection with the ROBO Gateway exists. If this happens, the user should finish off the remote operations manually on the ROBO Gateway computer, using the following commands:

- Execute the command `LSMenabler -r off` to turn off ROBO Gateway support.
- Execute the command `LSMenabler on` to make the Gateway a CO Gateway.

The user must then define Gateway parameters, such as interfaces, communities, policies and so on, using SmartDashboard. The policy should be installed using SmartDashboard.

**Note** - Using the `Daip` flag on a computer with no DHCP configured may result in a malfunction of the Gateway.

**Example**

Convert CPROBO MyRobo -CO
Convert CPROBO MyRobo -Daip -Force

**Convert CPGW**

Convert a Check Point Gateway to a Check Point ROBO Gateway. The user can specify whether the Gateway should have a Dynamic IP Address or be a CO Gateway, or neither. Applicable to Check Point Gateways only.

**Usage**


**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>the name of the Check Point or Safe@ ROBO Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>assign a security profile to the ROBO Gateway after installation</td>
</tr>
<tr>
<td>EXT</td>
<td>the name of external interface</td>
</tr>
<tr>
<td>INT</td>
<td>the name of internal interface</td>
</tr>
<tr>
<td>DMZ</td>
<td>the name of auxiliary interface</td>
</tr>
</tbody>
</table>
Convert SWROBO

The Force flag should be used with caution, because a forced conversion will “succeed” even if no connection with the ROBO Gateway exists. If this happens, the user should finish off the remote operations manually on the ROBO Gateway computer, using the following commands:

- Execute the command `LSMenabler -r off` to turn off ROBO Gateway support.
- Execute the command `LSMenabler on` to make the Gateway a CO Gateway.

The user must then define Gateway parameters, such as interfaces, communities, policies and so on, using SmartDashboard. The policy should be installed using SmartDashboard.

**Example**

Convert CPGW MyGW MyProfile -NoRestart
Convert CPGW MyGW MyProfile -E=hme0 -I=hme1 -D=hme2 -Force

**Convert SWROBO**

Convert a Safe@ ROBO Gateway to a Safe@ Gateway. The gateway will be assigned the specified security Profile. The user must completely define the Gateway using SmartDashboard, as well as adjusting the security policy and reinstalling it. Applicable to Safe@ Gateways only.

**Usage**

Convert SWROBO <Name> <Profile>

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>the name of the Safe@ ROBO Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>assign a security profile to the Gateway after installation</td>
</tr>
</tbody>
</table>
**Example**
Convert SWROBO MyRobo MySWProfile

**Convert SWGW**
Convert a Safe@ Gateway to a Safe@ ROBO Gateway. The gateway will be assigned the specified security Profile. The user must completely define the Gateway using SmartDashboard, as well as adjusting the security policy and reinstalling it. Applicable to Safe@ Gateways only.

**Usage**
Convert SWGW <Name> <Profile>

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>the name of the Safe@ Gateway</td>
</tr>
<tr>
<td>Profile</td>
<td>assign a security profile to the Gateway after installation</td>
</tr>
</tbody>
</table>

**Example**
Convert SWGW MyRobo MySWProfile
Profiles and Policies

In This Section

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining Check Point Gateway Profiles</td>
<td>35</td>
</tr>
<tr>
<td>Defining Policies for the Gateway Profile Objects</td>
<td>36</td>
</tr>
<tr>
<td>Defining a Policy to allow VPN from the ROBO Gateway to the CO Gateway</td>
<td>37</td>
</tr>
<tr>
<td>Working with a Default Profile</td>
<td>38</td>
</tr>
</tbody>
</table>

Defining Check Point Gateway Profiles

Profile objects are defined in SmartDashboard as ROBO Gateway Profiles. Proceed as follows:

1. Add a new ROBO Gateway Profile object as follows

   From the Manage menu, select Network Objects<Check Point<ROBO Gateway Profile, then select whether you would like to create a VPN-1/FireWall-1 ROBO Gateway Profile or a Safe@ ROBO Gateway Profile.

   The selected Gateway Profile window is displayed, showing its General page.

2. In the General page, define the new object as a Gateway Profile by entering the following settings:

   - To create a new Gateway Profile, the only compulsory field to be entered is the Name of the Profile
   - Add an optional Comment

   Note: By default, the Check Point Products section is set to NG Feature Pack 3, and to the Products VPN-1 and FireWall-1.
3 Configure all the additional Gateway Profile pages, these pages and the fields therein are common to regular Gateway objects. For more information see the SmartCenter Guide.

4 Once all pages are configured, click OK to exit the Gateway Profile window. The new Profile will be added to the Network Objects tab of the Objects Tree.

### Defining Policies for the Gateway Profile Objects

**Note** - It is recommended to define a separate Policy for every Profile, by configuring only the Profile object as the “Installable Target” of the Policy.

To define Policies for the Gateway Profiles object, proceed as follows:

1 Use the LocalMachine dynamic object to represent the ROBO Gateway.

2 Use the InternalNet, DMZnet, and AuxiliaryNet dynamic objects to represent the respective networks behind the ROBO Gateway.

**Note** - You can define and use additional dynamic objects. The values for these dynamic objects will be set centrally using SmartLSM (see Chapter 5 “SmartLSM”).

3 You can use dynamic objects in NAT rules as well.

   Example 1: to hide the InternalNetwork behind the external IP address of the ROBO Gateway you can define the following rule:

   TABLE 4-1 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>

Example 2: to have static NAT on all the incoming http traffic arriving to a published IP address (where the IP address is represented in the policy by a dynamic object called PublishedIP) to a web server (represented by a dynamic object called WebServer) define the following rule:
TABLE 4-2  Static NAT

<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>Any</td>
<td>PublishedIP</td>
<td>HTTP</td>
<td>Any</td>
<td>WebServer</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

4. To allow push actions from the SmartLSM, you must add a rule allowing an incoming **FW1_CPRID** service from the SmartCenter Server to **LocalMachine**.

5. Install the Policy on the Profile object. This action will only prepare the Policy on the SmartCenter Server to be fetched by the ROBO Gateways that reference this Profile.

**Defining a Policy to allow VPN from the ROBO Gateway to the CO Gateway**

1. Define a **Star VPN Community**. Configure all the relevant authentication and encryption properties for it.

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

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

4. Add a security rule that allows VPN traffic:

   **TABLE 4-3  Security rule that allows VPN traffic**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>If Via</th>
<th>Action</th>
<th>Install On</th>
<th>Time</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>

   For example, this rule will allow encrypted telnet traffic that matches the community criteria defined previously.

5. Define a NAT Hide rule that will hide all the internal networks of a VPN behind the external IP address of the ROBO Gateway. For example:

   **TABLE 4-4  Example — NAT Hide Rule**

<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</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(H)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   this rule hides the **InternalNet** interface. Define similar rules for **DMZNet** and **AuxiliaryNet** if necessary.
6 To update the CO Gateway with the mapping of ROBO Gateways to Profiles, select the **Update Corporate Office Gateway** command from the **Actions** menu in the SmartLSM Application.

**Working with a Default Profile**

Default Profiles can be defined and used for VPN Purposes. The default profile concept enables the CO Gateway to accept all VPN tunnels from unknown ROBO Gateways as if they're mapped to the default profile. This is especially useful in scenarios where only one profile is used. To work with default profiles, proceed as follows; in SmartDashboard:

1 Define a profile.
2 Check **Default Profiles** in the **Profile Based Management** tab of the **General Properties** window.
3 Choose a profile to be used as the default profile.
4 Install the policy on all CO Gateways.

**Defining a Policy to the Gateway that Protects the SmartCenter Server**

You must specify explicit rules to allow Management traffic between ROBO Gateways and the SmartCenter Server. Since the ROBO Gateways can have Dynamic IPs, you must use "ANY" to represent all possible ROBO Gateways addresses. Add the following rules:

1 **ANY| SmartCenterServer| FW1| Accept** — to allow FW Control traffic
2 **ANY| SmartCenterServer| CPD| Accept** — to allow CPD Control traffic
3 **ANY| SmartCenterServer| FW1_log| Accept** — to allow log traffic
4 **SmartCenterServer| ANY| CPD_amon| Accept** — to allow status monitoring traffic
5 **ANY| SmartCenterServer| FW1_ica_pull| Accept** — to allow pulling certificates from the ROBO Gateway
6 **SmartCenterServer| ANY| FW1_CPRID| Accept** — to allow Push actions from SmartLSM (see Chapter 5 “SmartLSM”).
7 **SmartCenterServer| ANY| FW1| Accept** — to allow FireWall-1 Control traffic
8 **SmartCenterServer| ANY| CPD| Accept** — to allow CPD Control traffic
Defining a Policy to the Gateway that Protects the SmartCenter Server

9 SmartCenterServer | ANY | FW1_ica_push | Accept — to allow pushing certificates to the ROBO Gateway
SmartLSM

In This Section

SmartLSM — Overview  page 41
Logging into SmartLSM  page 42
Menus and Toolbars  page 47
Adding a New ROBO Gateway  page 49
Editing a ROBO Gateway  page 53
Deleting a ROBO Gateway Object  page 60
Push Actions for a Gateway  page 60
Status Information  page 61

SmartLSM — Overview

SmartLSM is used to define new ROBO Gateway Objects, manage existing ROBO Gateway Objects and troubleshoot problems with ROBO Gateways.

The main view of SmartLSM features a spreadsheet look-and-feel interface. Each separate row represents a ROBO Gateway, with all the relevant information shown as column entries in that row. You can use the Sort, Find and Filter commands to display the required data, thereby facilitating the management of multiple ROBO Gateways through this GUI.
Logging into SmartLSM

SmartLSM is a standard Check Point SmartConsole. As such, you should define the workstation on which it is running as a SmartConsole in the **GUI Clients** tab of the Check Point Configuration Tool (cpconfig) installed on the SmartCenter Server (FIGURE 5-1). In a Provider-1/SiteManager-1 environment, define your workstation in the **SMART Clients** view of the Multi-Domain GUI application.

**FIGURE 5-1** SMART Clients tab of the Check Point Configuration Tool

In the **SmartLSM** window, you must supply the credentials of an administrator who is allowed to work with SmartDashboard.

You can use either a User/Password combination or a certificate-based authentication, as with standard Check Point SmartConsole clients. Please consult the *SmartCenter* Guide for the standard login information.

**Note** - You can open multiple SmartLSM windows with Read/Write permissions at the same time, and simultaneously work in SmartDashboard with Read/Write permissions.

The SmartLSM is displayed (FIGURE 5-2).
Logging into SmartLSM

FIGURE 5-2 SmartLSM ROBO Gateway Setup Utility

SmartLSM consists of two panes:
- The top pane, the ROBO Gateways List pane, lists the various ROBO Gateways defined in the system along with Gateways defined in the SmartDashboard.
- The bottom pane is called the Status View, it is divided into two tabs:
  - the Status View — Critical Notifications tab, highlights objects require the attention of the system administrator.
  - the Status View — Action Status tab, describes the status of the actions currently performed on the above Gateways.

Working with the SmartLSM GUI

In This Section

Find  
Show/Hide Columns  page 44  
page 44
Find

In this window you can enter a string consisting of any text. The Find operation searches for the specified string in whatever location you choose to determine in the Look in field.

To open the Find window, select Find from the Edit menu.

Find Parameters:

- **Find what** — enter the string that you would like to find
- **Look in** — determine whether your search is across all the fields, or a specific field only.
- **Match Whole Word** — the string for which you are searching should be the exact replica of the string entered in the Find what field. If this option is not checked, sub-strings will also be searched.
- **Match Case** — the string for which you are searching should match the case of the text entered in the Find what field.
- **Direction** — select the direction in which you would like to search.

Show/Hide Columns

You can choose to show or hide columns by selecting Show/Hide Columns from the View menu.

In the Show/Hide Columns window, uncheck all the columns that you would like to hide and check all columns that you would like to display. It is also possible to hide a column, by right-clicking on the desired column header and by choosing Hide Column from the displayed menu.

You can also hide columns by dragging the right edge of the column header to the left until it disappears.

Filter

You can filter the Gateways list to show only specific Gateways. Filtering is done by specifying conditions on the columns. You can specify multiple column filters, to achieve progressive filtering. For example, if you would like to see only the gateway whose Policy status is not updated, you can do this quickly and efficiently by selecting to Filter the Policy Status column.
To filter a column right-click the desired column header and select **Column Filter...**

Define the desired filter in the **Filter** window that is displayed.

Specify the nature of the filter, in other words decide what must or must not be filtered. Generally you will need to enter a value to be filtered, whether it is the name of a status, an IP Address, etc. The values that you are required to select or enter depend on the column that you have chosen to filter.

Once a filter exists for a specified column, the funnel icon in the column heading takes on a light green color. This color will disappear when the filter is cleared. You can make multiple filter operations on a specified Column.

To clear all filters in the SmartLSM, select **Clear All Filters** from the **View** menu, alternately, to clear a specific filter, right-click on the desired column and select **Clear Column Filter** from the displayed menu.

To view existing filters, select **Filter Details** from the **View** menu.

**Sort Column Content**

To toggle the content of a specified column between ascending and descending order, click on the desired column heading and the order of the column content will reverse itself.

**Export to File**

Click on **Export To** to export the whole objects list to a specific file.

Check **Show Headers** to include the column headers in the export file

Stipulate your delimiters in the **Use the following delimiters** field. You can use a **Tab** as a delimiter or you can specify another delimiter in the **Other** field.

You can choose to export all columns, or, you can choose not to export columns which are hidden, by checking **Export only shown columns**.

**Gateways List Pane**

The top pane provides the information on each Gateway listed, following are some of the displayed fields:

- **Gateway Name** — the name of the Gateway.

*Note* - Certain of the fields are relevant to ROBO Gateways only.
Status View — Action Status Tab

The Status View — Action Status tab provides the following information on each action that was initiated from this SmartLSM to one of the Gateways, following are some of the displayed fields:

- **Name** — the name of the Gateway.
- **Action** — the action that was performed on the Gateway (e.g. Reboot).
- **Start Time** — the full date and time on which the above action started.
- **Status** — the status of the action, which can be one of the following: **In Progress**, **Completed** or **Failed**.
- **Details** — additional information on the action (e.g. the reason for the failure of the action).

You can sort the entries in this view by clicking on any one of the column headers. You can also clear one or more action at a time from this list. To clear one Action Status, right-click on the desired column heading and select **Clear Selected**. To clear all the Action Statuses right-click on any column heading and select **Clear All**.
To see further details regarding the Action Status, right-click on the desired column heading and select **Action History**. The **Action History** window provides information regarding an action that was initiated from the Check Point SmartLSM to the selected Gateway. It displays a running log of events as they happen at the Gateway, including status information regarding action progress, completion or failure.

**Status View — Critical Notifications Tab**

The Status View — Critical Notifications tab provides the following information:

- **Name** — the name of the Gateway.
- **Updated** — the time of the status update
- **Gateway Status** — the status of the Gateway, see “Status Information” on page 61
- **Policy Status** — the status of the Policy installed on this Gateway, see “Status Information” on page 61

You can sort the entries in this view by clicking on any of the column headers.

**Menus and Toolbars**

**Menus**

The SmartLSM menus are described in **TABLE 5-1**.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Export to File...</td>
<td>Export the content of the Gateways list to a CSV (Comma Separated Values) format, Excel or HTML file</td>
</tr>
<tr>
<td></td>
<td>Exit</td>
<td>Close SmartLSM</td>
</tr>
<tr>
<td>New</td>
<td>Check Point ROBO Gateway...</td>
<td>Define a new ROBO Gateway</td>
</tr>
<tr>
<td></td>
<td>Safe@ Gateway...</td>
<td>Define a new Safe@ Gateway</td>
</tr>
<tr>
<td>View</td>
<td>Toolbar</td>
<td>Toggle the display of the toolbar</td>
</tr>
<tr>
<td></td>
<td>Status Bar</td>
<td>Toggle the display of the status bar</td>
</tr>
<tr>
<td></td>
<td>Status View</td>
<td>Toggle the display of the Status View</td>
</tr>
<tr>
<td></td>
<td>Default Column Width</td>
<td>Restore the default width of the columns</td>
</tr>
<tr>
<td></td>
<td>Clear All Filters</td>
<td>Remove all filters</td>
</tr>
</tbody>
</table>
### TABLE 5-1 SmartLSM Menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Details</td>
<td>Display all existing filters</td>
<td></td>
</tr>
<tr>
<td>Show/Hide Columns</td>
<td>Show or Hide columns</td>
<td></td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Push Dynamic Objects</td>
<td>Push and install values of Dynamic Objects to the selected Gateway</td>
<td></td>
</tr>
<tr>
<td>Push Policy</td>
<td>Initiate a Fetch Policy from the selected Gateway</td>
<td></td>
</tr>
<tr>
<td>Stop Gateway</td>
<td>Stop the Check Point Gateway services on the selected Gateway</td>
<td></td>
</tr>
<tr>
<td>Start Gateway</td>
<td>Start the Check Point Gateway services on the selected Gateway</td>
<td></td>
</tr>
<tr>
<td>Restart Gateway</td>
<td>Restart the Check Point Gateway services on the selected Gateway</td>
<td></td>
</tr>
<tr>
<td>Reboot Gateway</td>
<td>Reboot the selected Gateway</td>
<td></td>
</tr>
<tr>
<td>Get Status Details...</td>
<td>Get in-depth status information about the selected ROBO Gateway</td>
<td></td>
</tr>
<tr>
<td>Products&gt;Upgrade All Products</td>
<td>Upgrade the Check Point products on selected ROBO Gateway to the last available</td>
<td></td>
</tr>
<tr>
<td>Products&gt;Install Product</td>
<td>Install one or more available Check Point products on the selected ROBO Gateway.</td>
<td></td>
</tr>
<tr>
<td>Products&gt;Uninstall Product</td>
<td>Uninstall one of the existing Check Point products from the selected ROBO Gateway</td>
<td></td>
</tr>
<tr>
<td>Products&gt;Verify Installation</td>
<td>Verify if the installation of the specified Check Point product will succeed</td>
<td></td>
</tr>
<tr>
<td>Products&gt;Get Gateway Data</td>
<td>Retrieves the information about Check Point products installed on selected ROBO Gateway</td>
<td></td>
</tr>
<tr>
<td>Update Corporate Office Gateway...</td>
<td>Update a CO Gateway to reflect all the configuration changes in the ROBO Gateways’ encryption domain</td>
<td></td>
</tr>
</tbody>
</table>
**Toolbar**

The toolbar provides shortcuts to the most commonly used menu commands.

**Adding a New ROBO Gateway**

SmartLSM supports two types of ROBO Gateways: Check Point ROBO Gateways and Safe@ ROBO Gateways. To add a new Check Point ROBO Gateway, use the Add Check Point ROBO Gateway Wizard. Proceed as follows:

1. choose one of the following:
   - Select New>Check Point ROBO Gateway... from the Edit menu, or
• Click in the toolbar.

Use the drop down menu from the arrow to the left of the icon of a new Gateway to define whether to create a new Check Point or Safe@ ROBO Gateway. The **New Check Point ROBO Gateway** window is displayed, showing its **General** page.

2 In the **General** page, enter the following information:

- **Name** — define the name of the ROBO Gateway.
- **Comments** — free form text used to identify the ROBO Gateway (e.g. “The Restaurant at the End of the Universe”).

3 In the **More Information** page

- **Version** — the Version of the Gateway type, chosen above
- **Gateway Profile** — select the Profile the ROBO Gateway is mapped to from the drop-down list. The default value is the profile that was selected in SmartDashboard in the **Global Properties — Profile Based Management** page

4 In the **Communication** page

Define an Activation Key that will be used to set up Secure Internal Communication (SIC) Trust between the ROBO Gateway and the SmartCenter Server. This is the same Activation Key that you should enter in the **SIC** tab of the Check Point Configuration Tool (CPConfig) on the ROBO Gateway. You can either enter your own key, or have SmartLSM generate an 8 character long random key for you.

For automatic generation proceed as follows:

- Select the **Generate Activation Key Automatically** option.
- Click **Generate**.

The **Generated Activation Key** window is displayed. The key is displayed in clear text, so you can view it, and enter it later on the ROBO Gateway for the SIC initialization.

Choose one of the following:

- **Accept** — click to accept the automatically generated key and return to the **Communication** window. The two Activation Key fields will now display the new key in hidden text.

**Note** - Once the generated key is accepted, there is no way to view it in clear text.
Cancel — click to exit the Generated Activation Key window without accepting the automatically generated key.

For manual key definition, proceed as follows:

- Select the “Activation Key” option.
- Enter your own key, and enter it again in the confirmation box.

To clear the key, click Clear.

**Note** - The SIC certificate and the IKE certificate for this gateway will be created only after you click Finish in the Finish page.

You may push the SIC certificate to the ROBO Gateway if you know its IP address, but if you do not, you may leave the IP address field empty. In this case, the certificate will later be pulled automatically from the ROBO Gateway.

5 In the Finish page:

Check Edit Robo after creation in order to start working with the newly created object as soon as you have completed it.

Click Finish to complete the Robo Gateway creation.

**Adding a Safe@ ROBO Gateway**

To add new Safe@ ROBO Gateway, use the Add Safe@ ROBO Gateway Wizard. Proceed as follows:

1 You can either:
   - Select New>Safe@ ROBO Gateway... from the Edit menu, or
   - Click in the toolbar

2 Use the drop down menu on the icon of a new ROBO Gateway to define which type of ROBO Gateway you want to define. The New Safe@ ROBO Gateway window is displayed, showing its General page.

3 In the General page, enter the following information:
   - Name — define the name of the Gateway
   - Comments — free form text used to identify the ROBO Gateway (e.g. Roanoke Call Center.)

4 In the More Information page, enter the following:
   - Gateway Type — the type of your Safe@ Gateway
Adding a Safe@ ROBO Gateway

Chapter 5  SmartLSM  52

- **Gateway Profile** — select a security Profile for the ROBO Gateway from the drop-down list. (The default profile will be the one set as a default through the SmartDashboard in the Global Properties — Profile Based Management page.)

5 In the Communication page:
- Define a Registration Key that will be used to set up Secure Internal Communication (SIC) Trust between the ROBO Gateway and the SmartCenter Server. You can either enter your own key, or have SmartLSM generate an 8 character long random key for you. It is important to enter the same Registration Key on the Safe@ ROBO Gateway.

To automatically generate a Registration Key:
- Select the Generate Registration Key Automatically option.
- Click Generate.

The Generated Activation Key window is displayed. The key is displayed in clear text, so you can view it, and enter it later on the ROBO Gateway for the SIC initialization. Choose one of the following:
- **Accept** — click to accept the automatically generated key and return to the Communication window. The two Activation Key fields will now display the new key in hidden text.
- **Cancel** — click to exit the Generated Activation Key window without accepting the automatically generated key.

Note - Once the generated key is accepted, there is no way to view it in clear text.

For manual key definition, proceed as follows:
- Select the “Registration Key” option.
- Enter your own key, and re-enter it in the confirmation box.

To clear the key, click Clear.

Note - The IKE certificate for this gateway will be created only after you click Finish in the Finish page.

6 In the Finish page:
- Check Edit Robo after creation in order to start working with the newly created object as soon as you have completed it.
- Click Finish to complete the ROBO Gateway creation.
Editing a ROBO Gateway

To edit an existing ROBO Gateway, first click to select the ROBO Gateway in the Gateways list.

1 Choose one of the following:
   - Select **Edit ROBO Gateway...** from the Edit menu, or
   - Click in the toolbar, or
   - Double-click the record of this ROBO Gateway in the SmartLSM list pane.

The **Edit ROBO Gateway** window is displayed. Edit properties by selecting the appropriate tab.

2 Edit the **General** tab:
   - The **Name** of the gateway cannot be edited.
   - **Comments** — enter an optional comment
   - **Version** — edit the version number of the gateway
   - **Profile** — change the Profile to which the ROBO Gateway is mapped. The next time the ROBO Gateway fetches its Policy it will get the Policy and properties of the new Profile object.

   **Note** - If you want the Profile change to take effect immediately, you must perform the following actions:

   1. Actively push a Policy to this ROBO Gateway
   2. Update the CO Gateway(s).

   **Secure Internal Communication (SIC)** —

   If a certificate was already issued for this gateway the ROBO Gateway’s DN (Distinguished Name) will be displayed. This DN will be in the form of: “CN=ROBO-name,O=Management-domain-name”. For example: “CN=R_172,O=mgtHost.acme.com.abcdef”. The DN is sometimes referred to as the “SIC name” of the Gateway.

   **Viewing or Changing the SIC Trust**

   Click **Communication** to view or change the SIC Trust between the ROBO Gateway and the SmartCenter Server. The **Communication** window is displayed. In the **Communication** window, the **Trust State** shows the current trust state with the ROBO gateway:

   - **Uninitialized** indicates that the ROBO Gateway does not have a valid SIC certificate (either because it was never initialized, or because its certificate was revoked).
• **Initialized** indicates that the ROBO gateway has a valid SIC certificate.

### Initializing and Uninitialized Gateway

To initialize an Uninitialized gateway, proceed as follows:

• Specify the Activation Key. You can either enter it manually, or have SmartLSM generate it for you (this is done similar to specifying the Activation Key when adding a new ROBO gateway).

• Select one of the following:
  - **This machine currently uses this IP address** — enter the IP address. This requires that SIC was initialized on the ROBO Gateway (in other words, the Activation Key was entered) via the `cpconfig` utility.
  - **I do not know the current IP address**

• Click **Initialize**. A new SIC certificate will be created for this ROBO gateway, and its trust state will change to **Initialized**.

If an SIC certificate was not pushed to the ROBO Gateway—in other words if the current IP address of the ROBO Gateway was not entered in the SmartLSM GUI—in order to complete the SIC Trust process you must select to **Reset & Pull SIC** (pull the SIC certificate) on the ROBO Gateway (via the `cpconfig` utility). Enter the new Activation Key, the Name (or IP Address) of the SmartCenter Server, and the Name given to the ROBO Gateway. This will pull the new certificate from the SmartCenter Server, and will install it on the ROBO Gateway. After `cpconfig` configuration is complete, restart Check Point Services on this Gateway by rebooting the computer.

### Resetting

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

To Reset an Initialized gateway click the **Reset** button. You will be prompted to confirm that you would like to reset SIC. Answer **Yes**. To complete this procedure, you must **Reset SIC** on the ROBO Gateway, and restart the Check Point services, by rebooting the machine after the completion of the configuration in `cpconfig`.

The Gateway’s SIC certificate will be revoked, and its Trust State will change to **Uninitialized**. Now you will be able to specify a new Activation Key, and to re-initialize.

**3** Edit the **Details** tab as necessary

The following information is reported per ROBO Gateway:
- The **ROBO ID** is a unique ID, in the form of an IP address, per-ROBO Gateway. When the ROBO Gateway send logs to a Log Server, it specifies this **ROBO ID** as the log origin. This allows consistent tracking of the ROBO Gateway’s logs, even if its external IP address has changed. This ID cannot be edited.

- **IKE DN** — the ROBO gateway’s Distinguished Name (DN) for IKE negotiations. The IKE DN cannot be edited. However, you may re-initialize the IKE certificate by clicking the **Reset** button. If you reset the IKE DN, ensure that you update the CO Gateway(s) afterwards.

- **Device ID** — a free field used to specify a unique device identification (such as the gateway’s MAC Address).

- **Customer Details** — a free text field for Customer details.

4 Edit the **Dynamic Objects** tab

Dynamic Objects are placeholders for IP Address ranges. They are defined in SmartDashboard, and can be referenced in the Security Policy and Network Address Translation (NAT) rule bases. In this tab you can customize the Profile’s policy to the specific IP addresses of the edited ROBO gateway.

**Resolved Dynamic Objects**: the following properties are displayed for each Dynamic Object:

- **Name** — the name of the Dynamic Object as defined in SmartDashboard.

- **First IP** — this is the first or the only IP address in the IP address range that is assigned to the Dynamic Object.

- **Last IP** — this is the last IP address in the IP address range that is assigned to the Dynamic Object.

- **Comment** — the comment defined for the Dynamic Object in SmartDashboard.

The objects are managed using the following buttons:

Click **Add** to add a resolved Dynamic Object through the **Dynamic Object Configuration** window. Enter the following information:

- **Name** — select the Dynamic Object from the drop-down list.

- **Comments** — display the comment entered for that Dynamic Object

- **Resolved IP Address** — choose one of the following IP address resolution methods:
  - **IP Address** — enter the Dynamic Object’s IP address.
  - **IP Address in Range** — enter the Dynamic Object’s IP address range.
  - **Add to VPN Domain** — check to add the Dynamic Object IP address to the VPN Domain table for the ROBO Gateway. (This will be used by the CO Gateway for identification.)

---

55 June 2003
To add the resolved value, click OK. The newly added Object will be displayed in the Resolved Dynamic Objects list.

Click Edit to edit the Object selected in the Resolved Dynamic Objects list through the Dynamic Object Configuration window.

Click Remove to remove the assigned IP address values of the selected Dynamic Object. You will be asked to confirm the delete operation.

If you set a value for a Dynamic Object, it will be installed on the ROBO Gateway during the next Policy fetch (e.g. during the periodic fetch). If you want the new values to take effect immediately, you can actively push and install the new values from the SmartLSM (see “Push Actions for a Gateway” on page 60).

Note: If you do not set a value for a dynamic object that is used in the Policy, the rule that uses the dynamic object will never be matched and the packet will be dropped.

5 Edit the Licenses tab

This window shows the licenses that are currently installed on this ROBO Gateway:

- **Name** — the name of the license
- **SKU/Features** — the features guaranteed by the license
- **IP Address** — the IP Address of the gateway
- **Expiration Date** — the date on which the license expires

Click on Add to add a license from the License Repository. All available licenses are displayed in the License Repository window. You can select more than one license at a time in the License Repository window and add it to the Licenses tab.

Click Remove, to remove an existing license from the Licenses tab.

6 Edit the Advanced tab

- **Log Servers** — define up to two Log Servers. The former is where all logs should be sent (send logs to), and the latter should be used only when the former cannot be reached (when unreachable, send to). Select As defined in ROBO profile to maintain the settings that were configured for Log Servers when the profile was created or uncheck As defined in ROBO profile to create your own Log Servers definitions.

7 At any point while editing of the ROBO gateway you can:

...
Menus and Toolbars

- click **Action**, to perform one a variety or product related actions on the edited ROBO gateway. You will be asked to save your changes before any action operation can be performed.
- click **OK** to complete the editing of the ROBO gateway object
- click **Cancel** to cancel editing of the ROBO gateway object

**Editing a Safe@ ROBO Gateway**

To edit an existing ROBO Gateway, first click to select the ROBO Gateway in the Gateways list.

1 Choose one of the following:
   - Select **Edit Safe@ ROBO Gateway...** from the **Edit** menu, or
   - Click **Edit** in the toolbar, or
   - Double-click the record of a Safe@ ROBO Gateway in the SmartLSM list pane.

The **Edit ROBO Gateway** window is displayed. Edit properties by selecting the appropriate tab.

You can edit the following Safe@ ROBO Gateway properties:

1 Edit the **General** tab:
   - The **Name** of the gateway cannot be edited.
   - **Comments** — enter an optional comment
   - The **Gateway Type** of the gateway cannot be edited
   - **Profile** — change the security Profile assigned to the ROBO Gateway. This will be put into effect the next time the ROBO Gateway fetches its Policy. It will get the Policy and the properties of the new Profile.

   **Note** - If you want the Profile change to take effect immediately, you must perform the following actions:

1. Push the Policy to the Safe@ ROBO Gateway to ensure that the Policy is applied
2. Update the CO Gateways

   - **Secure Internal Communication (SIC)** — If a Registration Key is already entered, it will appear as hidden text ***** in the **Registration Key** field. You may change the Registration Key by clicking **New Key** button.

2 Edit the **Details** tab as necessary. The following information is reported per Safe@ ROBO Gateway:
• The **ROBO ID** is a unique ID, in the form of an IP address, assigned to each ROBO Gateway. Note that the **ROBO ID** cannot be edited. When the ROBO Gateway sends logs to a Log Server, it uses this ID to specify the log origin. This permits consistent tracking of ROBO Gateway logs, even if the external IP address is changed.

• **IKE DN** — The ROBO Gateway’s Distinguished Name (DN) for IKE negotiations. This DN cannot be edited. You may re-initialize the IKE certificate by clicking the Reset button. Ensure that you update the CO Gateway(s) afterwards.

• **MAC Address** — A free field used to specify the Gateway’s MAC Address.

• **Customer Details** — A free text field for Customer details.

3 Edit the **Firmware** tab as necessary. Use it to identify Firmware to be installed on the Safe@ ROBO Gateway. Choose one of the following:

  • **Use default** — Use the firmware defined as **Default** in the SmartUpdate application.

  • **Use ROBO Gateway’s installed firmware** — Use the firmware currently installed on the ROBO Gateway.

  • **Use the following firmware** — Select firmware to be uploaded to the Safe@ ROBO Gateway (which will be done via the SmartUpdate application).

4 The **Dynamic Objects** tab provides access to Dynamic Objects, which are placeholders for IP Address ranges. They are initially defined in the SmartDashboard, and are managed through Security Policies and Network Address Translation (NAT) rule bases. You may customize a Dynamic Object’s Profile policy to the specific IP addresses of the ROBO gateway.

The following properties are displayed for **Resolved Dynamic Objects**:

  • **Name** — the name of the Dynamic Object as defined in the SmartDashboard.

  • **First IP** — this is the first or the only IP address in the IP address range that is assigned to the Dynamic Object.

  • **Last IP** — this is the last IP address in the IP address range that is assigned to the Dynamic Object.

  • **Comment** — the comment defined for the Dynamic Object in the SmartDashboard.

Click **Add** to add a resolved Dynamic Object through the **Dynamic Object Configuration** window. Enter the following information:

  • **Name** — select the Dynamic Object from the drop-down list.

  • **Comments** — display the comment entered for that Dynamic Object.
Menus and Toolbars

- **Resolved IP Address** — choose one of the following IP address resolution methods:
  - **IP Address** — enter the Dynamic Object’s IP address.
  - **IP Address Range** — enter the Dynamic Object’s IP address range.
  - **Add to VPN Domain** — check it if you want this Dynamic Object IP address to be added to VPN Domain of the ROBO Gateway (as seen by CO Gateway).

To add the resolved value, click **OK**. The newly added Object will be displayed in the **Resolved Dynamic Objects** list.

Click **Edit** to edit the Object selected in the **Resolved Dynamic Objects** list through the **Dynamic Object Configuration** window.

Click **Remove** to remove the assigned IP address values of the selected Dynamic Object. You will be asked to confirm the delete operation.

If you set a value for a Dynamic Object, it will be installed on the ROBO Gateway during the next Policy fetch (e.g. during the periodic fetch). If you want the new values to take effect immediately, you can actively push and install the new values from the SmartLSM.

**Note** - If you do not set a value for a dynamic object that is used in the Policy, the rule that uses the dynamic object will never be matched and the packet will be dropped.

5 The **Licenses** tab displays the **Product Key** currently installed on the Safe@ ROBO Gateway. If you wish to install an update, you can correct the **Product Key** by filling in the **Product Key** field. Use **Show Product Description** to display detailed information about the Product Key entered.

6 At any point while editing the Safe@ ROBO gateway you can:
  - click on **Action**, to perform a variety of product related actions on the edited Safe@ ROBO gateway. You will be asked to save your changes before any action operation can be performed.
  - click **OK** to complete the editing of the ROBO gateway object
  - click **Cancel** to cancel editing of the ROBO gateway object

**Updating a CO Gateway**

To update a CO Gateway, proceed as follows:

1 Choose one of the following:
  - from the **Actions** menu, choose **Update Corporate Office Gateway...**, or
• in the toolbar, click 

The **Update Corporate Office** window is displayed.

2 Select the CO Gateway to be updated from the **Corporate Office Gateway** drop-down list, and click **OK**. The updated CO Gateway now has the latest copy of the ROBO DB, including any Profile changes.

Alternatively, select the Gateway you want to update and choose **Update Selected Corporate Office Gateway**... from the **Actions** menu.

### Modifying Policies

You can change the Policy of a Profile, and then install it. The next time a ROBO Gateway mapped to this Profile fetches a Policy, it will get the updated Policy.

You can change the general properties of the Profile using SmartDashboard. The next time the ROBO Gateways mapped to the Profile fetch their Policy, the changes will take effect.

You can actively push a Policy to a specific ROBO Gateway (see “Push Actions for a Gateway” on page 60).

### Deleting a ROBO Gateway Object

To remove a ROBO Gateway, select this ROBO Gateway in the Gateways list and select **Delete ROBO Gateway from** the **Edit** menu.

This action revokes all the certificates of the ROBO Gateway.

### Push Actions for a Gateway

You can manipulate a selected Gateway that has a known IP Address using any of the following tools:

- The SmartLSM menus (see “Menus” on page 47)
- The SmartLSM toolbar (see “Toolbar” on page 49)
- Right-click on a Gateway in the List pane and select a menu option

You can perform any of the following operations:

- **Launch SmartDashboard** — launch SmartDashboard. SmartDashboard will open with the last installed Policy of the respective Profile object.
- **Actions** — initiate any of the operations available for the selected ROBO Gateway:
  - **Push Dynamic Objects** — push and install values of Dynamic Objects to the Gateway.
  - **Push Policy** — initiate a manual Fetch Policy from the ROBO Gateway.
Status Information

- **Stop Gateway** — stop the Check Point Gateway services on the Gateway.
- **Start Gateway** — start the Check Point Gateway services on the Gateway.
- **Restart Gateway** — restart the Check Point services on the Gateway
- **Reboot Gateway** — reboot the Gateway.
- **Get Status Details** — Display in-depth status information for the selected Gateway

**Status Information**

Every Gateway row in the Gateways List pane has two Status fields which relay status information about the Gateway and the Policy respectively.

Following are the various status indications. They are relevant for both Gateways and Policies unless otherwise stipulated:

- **OK** — the Gateway or Policy is up and running
- **Waiting** — the SmartLSM has not yet received the status from the Server
- **Unknown** — the status of the Gateway or policy is unknown
- **Not Responding** — (gateway status only) the Gateway that has not communicated with the SmartCenter Server
- **Needs Attention** — (gateway status only) the Gateway has some issue and needs to be examined
- **Untrusted** — (gateway status only) SIC Trust was not established between the Gateway and the SmartCenter Server
- **Not Installed** — (policy only) the policy has not been installed on the Gateway
- **Not Updated** — (policy only) the policy has not been updated, the version of the policy installed on the Gateway is not the latest version reported as fetched by the SmartCenter Server
- **May be out of date** — (policy only) the ROBO gateway has not fetched its policy within the periodic fetch interval

To get detailed status information for a specific Gateway, select the gateway’s row and select **Get Status Details** from the Actions menu. All the information pertinent to the status will be displayed.
CHAPTER 6

Troubleshooting

Status Information
SmartLSM supports the Sign of Life status notification for every ROBO Gateway. You can get an In-Depth status monitoring information (similar to the information displayed in Check Point SmartView Status) per ROBO Gateway. To do so right-click on a ROBO Gateway row, and choose Actions > Get Status Details...

Logging
You can use the ID field of a ROBO Gateway to track logs in the Check Point SmartView Tracker. This ID will be the Origin IP address of all logs generated by a ROBO Gateway (this is necessary since a ROBO Gateway can have a dynamic IP address, so using that IP address as the identifier of logs is futile).

VPN Troubleshooting Tools
You can use the information in the IKE DN field of SmartLSM to track IKE Negotiations between a ROBO Gateway and a peer CO Gateway.
Index

A
Action Stats Pane 46, 47
AddCP 15
AddSW 16
Anti-Spoofing 7
AuxiliaryNet 4

C
Certificate 7
CO Gateway 2
Comma Separated Value
see CSV 47
conversion
Check Point Gateway to
ROBO Gateway 6
ROBO Gateway to Check
Point Gateway 6
Convert
Check Point Gateway to Check
Point ROBO Gateway 32
Check Point ROBO Gateway
to Check Point Gateway 31
Safe@ Gateway to Safe@
ROBO Gateway 34
Safe@ ROBO Gateway to
Safe@ Gateway 33
Convert CPGW 32
Convert CPROBO 31
Convert SWGW 34
Convert SWROBO 33
Corporate Office Gateway
see CO Gateway 2
CPрид service 37
CSV 47

D
DAIP 4
Delete a ROBO Gateway 21
Display a list of existing Gateways 21
DMZNet 4
Dynamic Object 3
resolution methods
automatic
central 4
local 4
value resolution methods
DMZNet 4
InternalNet 4
LocalMachine 3

F
Fetch 2
Policy 7
Fetch Interval
see Periodic Policy Fetch
Interval 3

G
Gateways List Pane 45
GetInfo 26
GetStatus 30
Getting Product Information 26
Getting Status Information 30

I
ICA 7
ID 63
IKE 7, 63
IKE certificate 4
IKE DN 63
Install 23
Install a product to a ROBO
Gateway 23
Internal Certificate Authority
see ICA 7
InternalNet 4

L
Large Scale Manager
purpose 1
LocalMachine 3
Logging 63
logging 7

M
map Gateway to Profile 2
Modify a Corporate Gateway 17
ModifyCP 17
ModifySW 18

P
periodic fetch interval 3
Periodic Policy Fetch 2
platforms
supported 9
Policy
Fetch 2, 3, 7
management 3
Periodic Fetch 2
Push 2
Profile 2, 35
definition 2
Profile Gateway
define 35
Push Actions for a ROBO
Gateway 27, 28, 29, 30
Push Policy 2
PushDynamicObject 30
Pushing Dynamic Objects 30
Pushing Policy 30
PushPolicy 30

R
Reboot Gateway 29
Rebooting a Gateway 29
Remote Office/Branch Office
see ROBO 1
Remove 21
Reset the IKE Certificate 20
Reset the SIC Certificate 19
ResetIke 20
ResetSic 19
Restart Gateway 28
Restarting a Gateway 28
ROBO 1
ROBO Gateway
IKE DN 63
ROBO Gateway ID 63

S

Secure Internal Communication
see SIC 53
Show 21
ShowInfo 26
Showing Product Information 26
Showing Product Repository 27
ShowRepository 27
SIC 53
Sign of Life status notification 63
SmartCenter Server 2
installation 10
SmartLSM 2, 10
Start Gateway 28
status
Sign of Life notification 63
Stop 27
Stop Gateway 27
supported 9

T

Trust 50, 52
see SIC 53
Tunnel
see VPN Encryption Tunnel 2

U

Uninstall 23, 24
Uninstall a product on a ROBO
Gateway 23
Update a Corporate Office
Gateway 20
UpdateCO 20

Upgrade 25
Upgrading All Products 25

V

Verify Installation 24, 25
Verifying Installation of a Product 24
Verifying Upgrade of All Products 25
VerifyUpgrade 25
VPN
Encryption Tunnel 2
VPN Tunnel 4, 7

65 June 2003