Alcatel·Lucent

Alcatel-Lucent Security Management Server (SMS)

Release 9.4

Installation Guide

060274-00 REV B
CC109735423
260-100-018R9.4 Issue 2, July 2009

Notice

Every effort was made to ensure that this information product was complete and accurate at the time of printing. However, information is subject to change.

Security statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of remote access features. In such an event, applicable tariffs require the customer to pay all network charges for traffic. Alcatel-Lucent cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

Limited warranty

For terms and conditions of sale, contact your Alcatel-Lucent Account Team.

Ordering Information

The ordering number for this information product is 260-100-018R9.4.

Technical Support

In the contintental United States, when you need additional technical assistance, the Alcatel-Lucent Global TSS Contact Center is your first point of contact. Technical assistance is available 24 hours a day, 7 days a week. Contact the Global TSS Contact Center at 1-866-582-3688.

Outside the United States, contact your Local Customer Support (LCS) or the support organization designated by your Alcatel-Lucent customer team representative. If you are unsure of who to call, contact the Global TSS Contact Center at +1 630-224-4672.

Information product support

Use the following email address if you have any errors to report or questions to ask about this information product: comments@alcatel-lucent.com .

Contents

About this information product ix

Purpose ix

How to use this information product ix

Supported Brick devices xi

Related information xi

How to order xii

Safety information xii

How to comment xii

1 Safety Information 1

Structure of hazard statements 1

2 SMS on a *Microsoft*® *Windows*® Server Platform 3

Overview 3

Introduction 4

Hardware Requirements 6

Software Requirements 7

Pre-Installation Requirements (Clean Installations) 8

To Install the SMS Application (Clean Installation) 10

To Manually Un-Install SMS 16

To Upgrade the SMS Software 17

What To Do Next 23

3 SMS on a *Microsoft*® *Vista*® Server Platform 25

Overview 25

Introduction 26

Hardware Requirements 29

Software Requirements 30

Pre-Installation Requirements (Clean Installations) 31

To Install the SMS Application (Clean Installations With Server Running *Microsoft*® *Vista*®) 33
To Manually Un-Install SMS 39
To Upgrade the SMS Software 40
What To Do Next 44

4 **SMS on a *Sun*® *Solaris*® Server Platform** **45**
Overview 45
Introduction 46
Hardware Requirements 48
Software Requirements 49
Pre-Installation Requirements (Clean Installations) 50
To Install the SMS Application (Clean Installation) 53
To Manually Un-Install SMS 58
To Upgrade the SMS Software 59
What To Do Next 64

5 **SMS on a Linux Server Platform** **65**
Overview 65
Introduction 66
Minimum Hardware/Software Requirements 68
Pre-Installation Requirements (Clean Installations) 69
To Install the SMS Application (Clean Installation) 72
Post-Installation Steps 78
To Manually Un-Install SMS 79
To Upgrade the SMS Software 80
What To Do Next 84

A **Registering SMS Software License Keys and Obtaining Installation Keys** **A-1**
Overview 85
To Register a Software License Key and Obtain an Installation Key 86

B **SMS Hardening Guidelines** **B-1**
Overview 111
SMS and Operating System Hardening Guidelines 112

C **License Terms for Third Party Software** **C-1**

Overview 117
License terms for third party software 118

Index 125

List of figures

VPN Firewall Product Registration and Support Login Page 87

Registration Web Page for New Users (Step 1: Verify Registration Keys) 88

Verify Registration Keys Information (Example) 89

Registration Web Page for New Users (Step 2: Enter Customer & Contact Info) 90

Customer Information and Key Contact Information (Example) 92

Registration Web Page for New Users (Step 3: Enter Product Info) 94

Brick Hardware and Vendor Information (Example) 96

Registration Web Page for New Users (Step 4: Enter Username & Password) 97

Username and Password Information (Example) 98

Registration Web Page for New Users (Step 5: Verify & Submit) 99

Registration Completed Page Showing Registered Software License Key and Installation Key Obtained (Example) 100

VPN Firewall Product Registration and Support Login Page 101

VPN Firewall Registration Web Page 103

Registered Keys Web Page 104

SMS Help > About Window 105

Register New Keys Web Page 106

Register New Keys Upgrade License Key Entry (Example) 107

Register New Keys Confirmation Window 108

Register New Key Confirmation Window, Selecting Associated License Key From Previous Release (Example) 109

Registration Completed Page, Successful Registration of Upgrade License Key and Installation Key Obtained (Example) 110

About this information product

Purpose

This preface provides an overview of this information product, which is the *Alcatel-Lucent Security Management Server (SMS) Installation Guide.*

The purpose of the *Alcatel-Lucent Security Management Server (SMS) Installation Guide* is to explain how to install the Alcatel-Lucent Security Management Server (SMS) application.

How to use this information product

This document is divided into chapters that describe how to install the SMS on a *Microsoft*® *Windows*®, *Microsoft*® *Vista*®, *Sun*® *Solaris*®, and Linux server platform, respectively.

This *Installation Guide* is organized as follows:

Chapter Title	Description
Chapter 2, "SMS on a *Microsoft*® *Windows*® Server Platform"	Describes how to install the SMS application on a host running *Microsoft*® *Windows*® XP Professional or *Windows*® Server 2003. Includes hardware and software requirements, pre-installation requirements, and detailed installation procedures for a new and upgrade installation for both a Primary SMS and redundant SMS configurations. Also provides post-installation configuration requirements and how to access the SMS application on your PC desktop. Also provides a procedure for manually un-installing the SMS from a de-commissioned server as needed.

Chapter Title	Description
Chapter 3, “SMS on a *Microsoft*® *Vista*® Server Platform”	Describes how to install the SMS application on a host running *Microsoft*® *Vista*®. Includes hardware and software requirements, pre-installation requirements, and detailed installation procedures for a new and upgrade installation for both a Primary SMS and redundant SMS configurations. Also provides post-installation configuration requirements and how to access the SMS application on your PC desktop. Also provides a procedure for manually un-installing the SMS from a de-commissioned server as needed.
Chapter 4, “SMS on a *Sun*® *Solaris*® Server Platform”	Describes how to install the SMS application on a host running the *Sun*® *Solaris*® Release 9 or 10 operating system. Describes hardware and software requirements for installing SMS on a *Solaris*® server platform, pre-installation requirements, and and detailed installation procedures for a new and upgrade installation for both a Primary SMS and redundant SMS configurations. Also provides post-installation configuration requirements and how to access the SMS application on your PC desktop. Also provides a procedure for manually un-installing the SMS from a de-commissioned server as needed.
Chapter 5, “SMS on a Linux Server Platform”	Describes how to install the SMS application on a host running Red Hat Enterprise Linux 4 (RHEL4) or Red Hat Enterprise Linux 5 (RHEL5). Includes hardware and software requirements, pre-installation requirements, and detailed instructions for a new and upgrade installations on a Linux platform server. Also provides post-installation configuration requirements and how to access the SMS application on your PC desktop. Also provides a procedure for manually un-installing the SMS from a de-commissioned server as needed.
Appendix A, “Registering SMS Software License Keys and Obtaining Installation Keys”	This appendix provides instructions on how to register the SMS product and software license key, and obtain an installation key, which is needed to install a new or upgraded SMS release or feature option.
Appendix B, “SMS Hardening Guidelines”	This appendix provides general security hardening recommendations for the SMS and server operating system.

Chapter Title	Description
Appendix C, "License Terms for Third Party Software"	This appendix contains information about licensing terms and agreements for third party software.

Supported Brick devices

The following available Brick models are supported by the current SMS release:

- Alcatel-Lucent *VPN Firewall Brick*™ Model 20 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*™ Model 50 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*™ Model 150 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*™ Model 350 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*™ Model 1100/1100A Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*™ Model 700 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*™ Model 1200 Standard and HS VPN Security Appliances

  Important! *Note: only later Model 20 Brick devices are supported with this release. Model 20 Bricks that have 6-8 MB of RAM and 8 MB of flash are not supported with this release.*

Some of the above Brick device models require a specific patch of the current SMS release in order to be fully supported. For details about the SMS patch release required for a specific Brick device model, refer to the *User's Guide* for the Brick device model or contact your Alcatel-Lucent customer support team representative for more information.

Related information

The *Alcatel-Lucent Security Management Server (SMS) Installation Guide* is part of a set of documents that support the SMS.

An online version of this document set, in PDF format, is available through the Help feature of the SMS application software.

Documentation

The document set that supports the SMS application consists of the following documents:

- *Alcatel-Lucent Security Management Server (SMS) Policy Guide*, which instructs users how to create security policies and set up VPN tunnels on Alcatel-Lucent *VPN Firewall Brick*™ Security Appliances.
- *Alcatel-Lucent Security Management Server (SMS) Administration Guide*, which instructs users how to administer the SMS application.
- *Alcatel-Lucent Security Management Server (SMS) Installation Guide*, which instructs users how to install the SMS application.

- *Alcatel-Lucent Security Management Server (SMS) Reports, Alarms, and Logs Guide*, which instructs users how to use log files, configure triggers and actions to generate alarms, and how to compile and view reports.
- *Alcatel-Lucent Security Management Server (SMS) Tools and Troubleshooting Guide*, which instructs users how to use the Command Line Interface (CLI) commands.
- *Alcatel-Lucent Security Management Server (SMS) Technical Overview*, which provides a general technical description of the Alcatel-Lucent VPN Firewall solution.

How to order

To order SMS information products, contact your Alcatel-Lucent Technologies customer team representative or contact Alcatel-Lucent at one of the following telephone numbers:

- From the United States, call 888-582-3688, prompt 1.
- From Canada, call 317-322-6616.
- From Europe, the Middle East, Asia, Africa, the Pacific, China, the Caribbean, and Latin America, call 317-322-6416.

Safety information

This information product contains hazard statements for your safety. Hazard statements are given at points where safety consequences to personnel, equipment, and operation may exist. Failure to follow these statements may result in serious consequences.

How to comment

To comment on this information product, go to the Online Comment Form (http://www.lucent-info.com/comments/enus/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 Safety Information

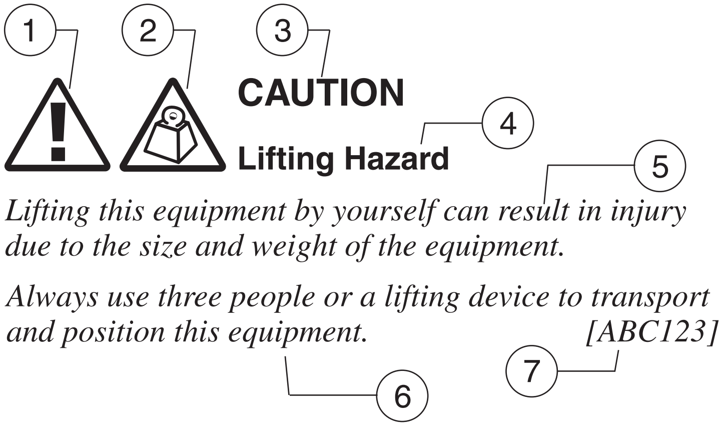
Structure of hazard statements

Overview

Hazard statements describe the safety risks relevant while performing tasks on Alcatel-Lucent products during deployment and/or use. Failure to avoid the hazards may have serious consequences.

General structure

Hazard statements include the following structural elements:


1
2
3
CAUTION
4
Lifting Hazard
5
Lifting this equipment by yourself can result in injury due to the size and weight of the equipment.
Always use three people or a lifting device to transport and position this equipment.
[ABC123]
7
6

Item	Structure element	Purpose
1	Personal-injury symbol	Indicates the potential for personal injury (optional)
2	Hazard-type symbol	Indicates hazard type (optional)
3	Signal word	Indicates the severity of the hazard

Item	Structure element	Purpose
4	Hazard type	Describes the source of the risk of damage or injury
5	Damage statement	Consequences if protective measures fail
6	Avoidance message	Protective measures to take to avoid the hazard
7	Identifier	The reference ID of the hazard statement (optional)

Signal words

The signal words identify the hazard severity levels as follows:

Signal word	Meaning
DANGER	Indicates an imminently hazardous situation (high risk) which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation (medium risk) which, if not avoided, could result in death or serious injury.
CAUTION	*When used with the personal injury symbol:* Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in personal injury. *When used without the personal injury symbol:* Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in property damage, such as service interruption or damage to equipment or other materials.

□

2 SMS on a *Microsoft*® *Windows*® Server Platform

Overview

Purpose

This chapter explains how to install or upgrade the SMS application on a *Microsoft*®*Windows*® server platform. It also includes a procedure for manually un-installing the SMS as needed.

Contents

Introduction	4
Hardware Requirements	6
Software Requirements	7
Pre-Installation Requirements (Clean Installations)	8
To Install the SMS Application (Clean Installation)	10
To Manually Un-Install SMS	16
To Upgrade the SMS Software	17
What To Do Next	23

□

Introduction

Overview

The SMS application can be installed on a host running *Microsoft*® *Windows*® XP Professional or Server 2003.

Release 9.4 can be installed as a first time (clean) installation or as an upgrade.

This chapter provides step-by-step instructions for installing the SMS application as:

- a Primary SMS. Use this procedure to install a single SMS or the first SMS in a multi-site SMS redundancy configuration
- a Secondary SMS associated with a Primary SMS in a redundant pair or as part of a multi-site SMS redundancy configuration
- a Compute Server associated with a Primary or Secondary SMS

Upgrades

CAUTION

Service-disruption hazard

Security Precaution

It is highly recommended that the SMS server be protected with a Brick device and that as little as possible be put on the same trusted subnet as the SMS.

SMS configurations

The SMS can be deployed in one of the following configurations:

- A Primary SMS (stand-alone configuration)
- A Primary SMS and Secondary SMS (in a redundant configuration)
- A Primary SMS and up to three Secondary SMSs (Multi-Site configuration)
- A Primary SMS and up to three Secondary SMSs, each with up to five Compute Servers (Compute Server configuration)

Multi-Site SMS configuration

A multi-site SMS configuration consists of a Primary SMS and up to three Secondary SMSs. The Primary SMS and Secondary SMS (s) share the same database, which is updated periodically across the network. The Primary SMS and Secondary SMS(s) are simultaneously active, synchronizing status and configuration at the same time.

Compute servers

To maximize scalability of the SMS/Brick security solution, the SMS provides the option of adding a separate set of servers called Compute Servers (CSs), which are associated with a Primary or Secondary SMS and act as collection points for Brick log traffic. Using a CS to collect Brick log data frees up computing resources on the SMS itself and extends the number of Brick devices and total log traffic that can be handled. Each Brick device managed by the SMS can be homed to one of the associated CSs or the managing SMS for logging purposes.

Up to five CSs can be configured for a Primary or Secondary SMS.

Implementing Primary SMS/Secondary SMS configurations

During the installation of the Secondary SMS, there is a point at which the Secondary SMS attempts to contact the Primary SMS to replicate the Primary SMS database on the Secondary SMS. If the Secondary SMS cannot contact the Primary SMS, correct the problem and retry the operation on the Secondary SMS.

For reasons of security, we strongly recommend that you deploy a Brick device ″in front″ of the Primary and Secondary SMS(s) to protect all servers.

To ensure that the Primary SMS and Secondary SMS(s) can contact each other through both Brick devices, follow the course of action outlined below when you order the installation:

1. Install the Primary SMS first. The two installation procedures in this chapter provide step-by-step instructions for a new installation and an upgrade installation.
2. Once the Primary SMS is operational, use it to configure two Bricks and assign the pre-configured ruleset *administrativezone* to the ports that will be connected to the SMS. Refer to the *Configuring Brick Ports* section in the *SMS Administration Guide* for instructions on how to do this.
3. Connect the Primary SMS to the port on one Brick, and the host that will be the Secondary SMS to the port on the other. Then, deploy the two Bricks: the primary SMS and the host that will be the Secondary SMS in the network.
4. To ensure that the Primary SMS and remote host can communicate, add a ping rule (*dir=both, source=**, *dest=**, *service=ping_request,action=pass*) to the *administrativezone* ruleset, and then ping the host from the SMS. Once the ping is successful, remove the rule for security reasons. (Refer to the *Brick Zone Rulesets* section in the *SMS Policy Guide* for instructions on how to create a rule.)
5. When you have established that the two SMS servers can communicate, install the Secondary SMS.

□

Hardware Requirements

Minimum hardware requirements

Regardless of which operating system you are running, the host on which you install the SMS application must meet the following minimum hardware requirements:

- 400 MHz Pentium processor
- 512 MB of RAM
- Swap space at least as large as the amount of RAM
- 1 GB free space on an NTFS partition
- CD-ROM drive
- 3.5 inch floppy drive, USB port, or serial port. For information on the hardware required to boot specific Lucent Brick device models, consult the *User's Guide* for the specific Brick or contact your Alcatel-Lucent customer support team representative.
- Ethernet interface card
- Video card capable of 1024 x 768 resolution (65,535 colors)

  Important! Because of the memory requirements of SMS R9.4, older Brick 20 models with only 8 MB of RAM may not be able to be configured with all features.

  To verify the amount of RAM on the Brick device, log into the Brick device via the remote console and run the `display mem` command.

If you are managing many Brick devices, supporting many IPSec clients, or generating large amounts of audit data, you may require additional memory. Refer to the *Sizing Guidelines* appendix in the *SMS Administration Guide* to help you determine how much additional memory you may need.

One optional piece of equipment you may want to consider is a modem. Having a modem in the host allows you to set up alarms that page an administrator when a problem is encountered. If you decide to add a modem, it must be Hayes-compatible and configured so that it cannot accept incoming calls and cannot be shared by other services, such as a Remote Access Server.

□

Software Requirements

Required software components

The following software is required to run the SMS application on a Microsoft *Windows*®
platform:

- *Windows*® XP Professional and Service Pack 1 2, or 3, or *Windows*® Server 2003 and Service Pack 4 or higher.
- A hard drive with at least one NTFS partition. The drive can have the FAT file system installed, but it must have at least one NTFS partition to hold the SMS software.

In addition, the following software is not required, but is highly recommended:

- A browser such as *Microsoft*® *Internet Explorer*® or Firefox to view SMS reports and display the on-line help.
- Adobe Acrobat Reader. This application is required to display the on-line manuals.

Installations on a *Windows*® Server 2003 platform

If you are installing the SMS application on a*Windows*® Server 2003 platform, do not install Terminal Server in *Windows*®. An error message is generated when attempting to install SMS and it does not work.

Security patches

It is strongly recommended that you install security patches on a regular basis to keep security on your machine up-to-date. Use caution when installing service packs. It is not guaranteed that the current SMS software can be installed or run with new service packs.

□

Pre-Installation Requirements (Clean Installations)

Overview

Before you proceed with the actual installation of the SMS application for the first time on a host, some pre-installation steps are required:

1. Install the service pack.
2. Resolve potential web server port conflicts.
3. Install Adobe Acrobat Reader.
4. Obtain the SMS installation keys.

Install the service pack

Check the host that you are using to see if the correct service pack is installed. If it is not, you must install the appropriate service pack before beginning the installation. Service packs can be downloaded from the *Microsoft*® website.

Resolve potential web server port conflicts

The SMS application contains a web server which will conflict with any existing web server currently active on the host machine. If there is another web server running on the SMS host (such as *Microsoft*® Internet Information Server or Apache), you must either:

- Shut the web server down
- Check system services and set the Startup Type to Manual or Disabled rather than Automatic so that the web server will not start up when the OS is rebooted.

Port 80 is the default SMS web server port. In the event that another web server is already using port 80 (such as Apache), you must either change the port on that web server or select a different port when configuring the SMS web server.

Install Adobe Acrobat Reader

Adobe Acrobat Reader is required to view the on-line documentation that is provided with the application. A copy of this application can be downloaded from the Adobe website, http://www.adobe.com.

Obtain the SMS installation keys

To install the SMS application, two keys are required:

- *Software license key*
  The software license key is provided with the SMS application. You will need this key to register the product and to obtain the installation key, which is required to perform the installation.
- *Installation key*
  The installation key is required to install the product.

For complete instructions on how to register a software license key and obtain an installation key, refer to Appendix A, “Registering SMS Software License Keys and Obtaining Installation Keys”.

There are six categories of installation keys available, depending on the type of installation you are performing. The six categories are:

- Primary SMS (Clean Install)
- Upgrade for Primary SMS
- Secondary SMS associated with a Primary SMS (Clean Install)
- Upgrade for Secondary SMS associated with a Primary SMS
- Compute Server SMS (Clean Install)
- Upgrade for Compute Server SMS

The installation key that you enter, which sets parameters affecting the operation of the SMS, cannot be changed.

You will be prompted to enter the software installation key during the installation process. If you have purchased any optional feature licenses, refer to the procedure “To register a software license key and obtain an installation key for upgrade or feature option” (p. 101) in Appendix A, “Registering SMS Software License Keys and Obtaining Installation Keys” for instructions on how to register these license keys and obtain installation keys that you will use to enable these features on your SMS. Optional features are enabled after the software installation/upgrade is complete, using the New Feature Setup utility.

To enable optional features, run the New Feature Setup utility on the Primary SMS after you finish the software installation process and enter your optional feature installation keys. Optional features enabled on the Primary SMS are also automatically enabled on all associated Secondary and Compute Server SMS machines. It may be necessary to restart services to enable some features.

For more information on New Feature Setup, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

Software patches and documentation updates

It is a good idea to check the VPN Firewall Product Registration and Support website (https://vpn-firewall-brick.alcatel-lucent.com) periodically for patches and documentation updates issued since you purchased the product.

If you are installing the SMS application for the first time, the installation keys that you will receive are only for an initial installation of the current software release. If you are upgrading from an earlier release of the SMS software, these installation keys are only for an upgrade to the current software release. When installing a patch version of the SMS application, you do not need an installation key.

□

To Install the SMS Application (Clean Installation)

When to use

Use this procedure to install the SMS application for the first time on a host.

Before you begin

Before you begin this task, if you are installing a Secondary or Compute Server SMS, you must first:

1. Install the Primary SMS, using this procedure.
2. Log into the Primary SMS and add the Secondary or Compute Server SMS to the **LSMSs and LSCSs** folder using the exact SMS Name, IP Address, and installation key that will be used to install it. For instructions on how to add a Secondary or Compute Server SMS, refer to the *SMS Administration Guide*.

Procedure

Use the following procedure to install the SMS application for the first time on a host.

1 With the CD-ROM in the drive, open the Windows Explorer and locate this directory on the CD-ROM:

Windows

2 Double-click the file *LSMS-9.4.xxx.exe* where xxx is the build number of the software.

This is the installation program. Windows that indicate the progress of the unpacking and setup during these processes are displayed first.

Result: Upon completion of these processes a Welcome window is displayed.

3 Read the text in the Welcome window, and when you are finished, click **Next** to continue with the installation.

4 Scroll through the Software License Agreement, and if it is acceptable, click **Yes** to proceed.

Result: The Installation Key window is displayed.

5 Enter the installation key applicable to this SMS that you obtained from the VPN Firewall Product Registration and Support website (https://vpn-firewall-brick.alcatel-lucent.com) and click **Next**. Refer to the "Obtain the SMS installation keys" (p. 8) section for the types of installation keys available.

> **Result:** The program verifies the key, and then displays the Choose Destination Location window.

6 The Root Directory for the Alcatel-Lucent Security Management Server window allows you to specify where the SMS software will be installed. The default is: *c:\isms*

Click **Next** to do this, or click the **Browse** button and enter a new destination location before clicking **Next**.

> **Result:** Once you have indicated the directory, the **Where do you want the logs to go?** window is displayed.
>
> The destination directory for the SMS application must reside on an NTFS partition. If not, you will have to select another directory that is on an NTFS partition, or terminate the installation and run the *Windows*® convert utility on the partition on which you want to install the SMS software.

7 The **Where do you want the logs to go?** window allows you to specify the folder where the SMS logs will be stored. If you chose the default in the previous step, this selection defaults to: *c:\isms\lmf*

You may either accept this selection, or click the **Browse** button and enter a new destination location before clicking **Next**.

After completing the installation, you may elect to redefine the location of the *log* directory or even`ftp` the logs to another machine. Either of these changes can be done through the SMS Configuration Assistant. Refer to the *Using the Configuration Assistant* chapter in the *SMS Administration Guide* for more details.

8 The Select Program Folder window allows you to select the folder in which the SMS application will appear on the Windows Start menu. The default is: **Alcatel-Lucent Security Management Server**

It is recommended that you accept the default. Click **Next** to do this, or select another directory from the Existing Folders and then click **Next**.

> **Result:** The What You Should Know about this Release window is displayed.

9 Read the Release Notes, which gives important information regarding this release. When finished, click **Next**.

Result: Installation of the files will now begin. While the files are being installed, a progress screen will indicate the status of the installation.

10 When the installation is complete, click **OK**.

Result: The SMS Web Server Configuration window is displayed.

11 The SMS Web Server Configuration window allows you to select the type of web server to be installed and the port to be used:

- **Type**. Enter the type of web server. The choices are **HTTP** (the default) and **HTTPS**, which relies on a digital certificate and is substantially more secure. If administrators will be logging into the SMS remotely, it is a good idea to use **HTTPS**. (To obtain and install a digital certificate, refer to the *Digital Certificates* section in the *SMS Policy Guide*.)
- **Port**. Enter the web server port. The default value is *80*, the standard port for HTTP; *443* is the standard port for HTTPS. If you are using HTTPS, or if port 80 is already in use, you can change the port.

12 After you have made your choices, click **Next** to continue with the installation.

Result: The SNMP Agent Configuration window is displayed.

13 The SMS SNMP Agent Configuration window allows you to choose the port that the SMS SNMP agent will use. The SMS SNMP agent is used for remote monitoring of the SMS and Brick devices.

The default value is *161*, which is the standard port for SNMP. You can change this if port 161 is already in use by another SNMP application.

14 When you have made your choice, click **Next** to continue with the installation.

For more information on how the SMS interacts with SNMP, refer to the *SNMP* appendix in the *SMS Reports, Logs and Alarms Guide*.

15 The Select SMS Type window shows the following information:

- **SMS IP Address**. The application is able to detect all of the available IP addresses configured on the machine. Choose the desired address from the drop down box.
- **SMS Name**. This field defaults to the SMS Machine name, but you may override it and type your own selection.
- **SMS Type**. Based on the installation key entered, either **Primary SMS**, **Secondary SMS**, or **Compute Server SMS** is selected and the others are grayed out.

16 If the installation is a Primary SMS, the installation will proceed immediately to Step 17.

If the installation is either a Secondary SMS or a Compute Server installation, you will be asked to enter the IP address for either the Primary SMS or the SMS to which the Compute Server will home. The program will perform the additional steps required and proceed to Step 20.

If the Secondary SMS cannot contact the Primary SMS, or the Compute Server cannot contact its associated SMS, the installation program prompts you to retry with a different IP address. If you cannot enter a valid IP address, you must terminate the installation program using the Task Manager. The inability to contact the specified IP address may indicate a network problem that must be corrected before proceeding with the installation.

For security reasons, the Secondary SMS must be installed/upgraded within 7 days of installing/upgrading a Primary SMS. After more than 7 days, the installation or upgrade of a secondary will fail because the Primary SMS does not allow the Secondary SMS to copy/replicate the database. To allow database replication, you must open a command line window on the primary, cd to the installation directory, and enter the following command:

```
local\bin\allowSecondarySetup
```

Result For Secondary SMS or Compute Server installations, the SMS services are initialized. Go to Step 20.

17 For Primary SMS installations, the installation program begins to initialize the database.

This process will take several minutes.

A master key is generated and displayed in the lower half of the SMS Setup screen. The purpose of the master key is to protect the root certificate used to authenticate communication between the SMS and the Brick devices that it manages. *Write the master key down and keep it in a secure place.* You will need the key to recover if you should forget the Administrator password and become locked out of the SMS.

Result: The installation program displays the Enter Admin ID window so that you may create an SMS Administrator ID and password.

18 Create an Administrator ID and password by entering information into the following fields:

- **Admin ID**. This is the initial ID used to log into the SMS. It can contain a maximum of 16 characters. Keep a record of the Admin ID in a secure place. You will need it to log into the SMS after installation is complete. Once you log in with this initial ID, other administrator IDs can be created, if desired.
- **Password**. The password is needed to complete the login. Enter the password, and then enter it again for verification purposes. The password can contain up to 42 characters. It is case-sensitive, so you must enter the password exactly the same each time.

19 Click **OK** to accept your choice.

Result: When the initial installation is complete, the `Initial Installation Complete` notification is displayed. You must click **Continue** at the bottom of the dialog box for the installation to proceed.

Result: The SMS services are initialized. While the services are starting, a progress bar indicates the status of the effort.

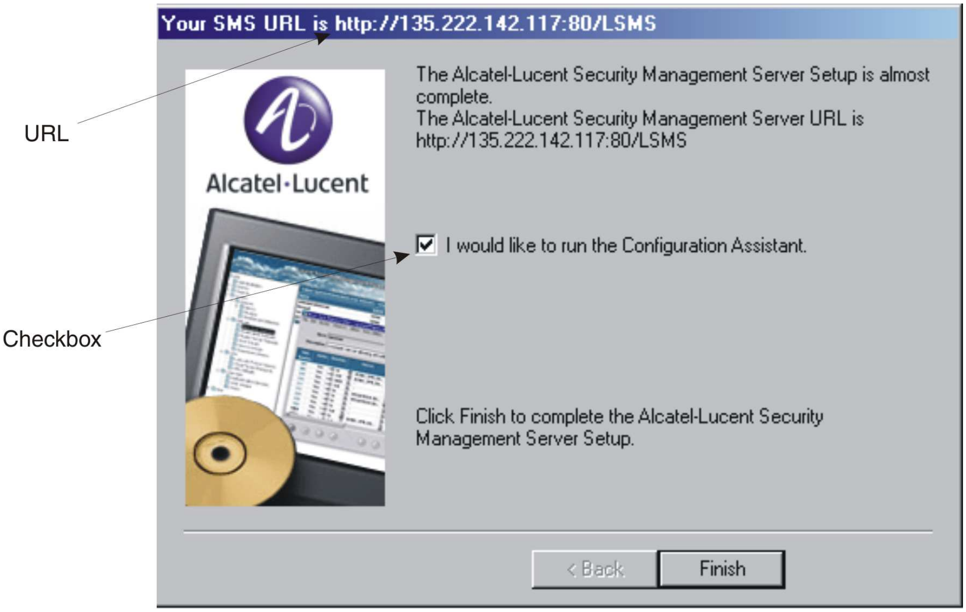
20 **Important!** In some cases, even if the installation is successfully completed, you may receive the following message:

```
This program might not have installed correctly
```

followed by a series of options. If this occurs, choose `This program installed correctly` to proceed with the installation.

When all SMS services have been successfully started, click **OK** to continue.

Result: If the installation is successful, a window similar to the following is displayed.



Your SMS URL is http://135.222.142.117:80/LSMS

The Alcatel-Lucent Security Management Server Setup is almost complete.
The Alcatel-Lucent Security Management Server URL is http://135.222.142.117:80/LSMS

☑ I would like to run the Configuration Assistant.

Click Finish to complete the Alcatel-Lucent Security Management Server Setup.

< Back | Finish

The URL of the SMS is shown at the top of the window. It consists of the IP address and port entered, and the directory that contains the SMS software. You will need this URL in order for your administrators to download the SMS Remote Navigator from a browser to their remote machines (see the *Remote Administration* chapter in the *SMS Administration Guide*).

By default, the box labeled **I would like to run the Configuration Assistant** is checked. If you leave the box checked and click **Finish**, the Configuration Assistant is displayed.

If you un-check the box before clicking **Finish**, the Configuration Assistant is not displayed, and the system returns to the *Windows*® desktop.

Configuration Assistant

The Configuration Assistant allows you to set certain system-wide parameters. You can open the Configuration Assistant now to change SMS system parameters now, or keep the default parameter settings and modify them at a later point.

For additional details about the Configuration Assistant, refer to the *SMS Administration Guide*.

END OF STEPS

□

To Manually Un-Install SMS

When to use

This procedure is not required or recommended for upgrading to the current “official” SMS release that you purchased. As part of its software upgrade program, the SMS automatically installs, upgrades to the current release, and un-installs the previous SMS release.

However, if you have installed an Evaluation copy of the SMS software, you should manually un-install the Evaluation copy using this procedure before upgrading to an “official” SMS release. You should skip Step 2 of this procedure if you want to preserve your configuration data.

This procedure can be used, for example, to manually un-install the SMS software from a de-commissioned server.

Task

Complete the following steps to manually un-install the SMS.

1 The SMS can be un-installed via the **Add or Remove Programs** utility of the *Windows*® **Control Panel** by selecting **Alcatel-Lucent Security Management Server** and clicking **Remove**.

2 For final removal, you can move to backup or delete the contents of the SMS directory (Example: *c:\isms\lmf\*).

END OF STEPS

□

To Upgrade the SMS Software

When to use

Use this procedure to upgrade to the current SMS software release.

Before you begin

Before you begin this procedure, it is recommended that you perform a manual backup of the Primary SMS database in the event of a system failure during the upgrade installation.

For instructions on how to perform a manual backup of the SMS database, refer to the *Manual Backup* section of the *SMS Administration Guide*.

Should you need to restore the backed up Primary SMS database, refer to the *To Restore SMS Data on a Primary SMS* section in the *SMS Administration Guide*.

Procedure

Use the following procedure to upgrade to the current SMS software release.

1 With the CD-ROM in the drive, open the *Windows*® Explorer and locate this directory on the CD-ROM:

Windows

2 Double-click the file *LSMS-9.4.xxx.exe* where *xxx* is the build number of the software.

This is the installation program. Windows that indicate the progress of the unpacking and setup during these processes are displayed first.

Result: Upon completion of these processes a Welcome window is displayed.

3 Read the text in the Welcome window, and when you are finished, click **Next** to continue with the installation.

4 Scroll through the Software License Agreement, and if it is acceptable, click **Yes** to proceed.

Result: The Installation Key window is displayed.

5 Enter the installation key applicable to this SMS that you obtained from the VPN Firewall Product Registration and Support website (https://vpn-firewall-brick.alcatel-lucent.com) and

click **Next**. Refer to the "Obtain the SMS installation keys" (p. 8) section for the types of installation keys available.

Result: The Select Program Folder window is displayed.

6 Select the folder in which the SMS application will appear on the *Windows*® **Start** menu. The default is **Alcatel-Lucent Security Management Server .**

It is recommended that you accept the default. Click **Next** to accept the default, or type a different folder name and click **Next**.

Result: The What You Should Know about this Release window is displayed.

7 Read the Release Notes, which gives important information regarding this release. When finished, click **Next**.

Result: A message window is displayed, indicating that a previous version of the SMS already exists on the host.

8 Click **OK**.

Result: The old SMS files are removed. The Uninstall Programs screen is displayed.

9 When the uninstall process is completed, click **OK**.

Result: Installation of the files will now begin. While the files are being installed, a progress screen will indicate the status of the installation.

10 When the installation is complete, click **OK**.

Result: The SMS Web Server Configuration window is displayed.

11 The SMS Web Server Configuration window allows you to select the type of web server to be installed and the port to be used:

- **Type**. Enter the type of web server. The value for **Type** defaults to the value specified during the initial installation of the SMS. The choices are **HTTP** and **HTTPS**, which relies on a digital certificate and is substantially more secure. If administrators will be logging into the SMS remotely, it is a good idea to use **HTTPS**. (To obtain and install a digital certificate, refer to the *Digital Certificates* section in the *SMS Policy Guide*.)
- **Port**. Enter the web server port. The value for **Port** defaults to the value specified during the initial installation of the SMS. The standard port value for HTTP is **80**; the standard port value for HTTPS is **443**. If you are using **HTTPS**, or if port 80 is already in use, you can change the port value.
  Click **OK** to retain the current values for **Type** and **Port**, or enter new values and click **OK**.

  Important! The values for the Web Server **TYPE** and **PORT** can be changed using the SMS Configuration Assistant after successful completion of the software upgrade.

  Result: The **Select SMS Type** field is displayed next.

12 The Select SMS Type window shows the following information:

- **SMS IP Address**. The application is able to detect all of the available IP addresses configured on the machine. The value of this field defaults to the one chosen during the initial installation of the SMS. If you wish to change the default address, choose the desired address from the drop down box.
- **SMS Name**. This field displays the SMS Machine name. The value of this field defaults to the one chosen during the initial installation of the SMS. Change this field value if desired.
- **SMS Type**. Based on the installation key entered, either **Primary SMS Secondary SMS**, or **Compute Server SMS** is selected and the others are grayed out.
- **Primary SMS**. This field is displayed if you are upgrading a Secondary SMS or Compute Server SMS with the IP Address of the associated SMS (Primary for Secondary SMS or Home SMS for Compute Server).

13 If the upgrade installation is for a Primary SMS, go to Step 14. If the upgrade installation is for a Secondary SMS or a Compute Server, the system prompts you for the IP adddress of the Primary SMS or the SMS to which the Compute Server will home. The program performs the additional steps required. If you are upgrading a secondary or Compute Server, the SMS services are initialized. After all SMS services are started, go to Step 16.

Result: The Upgrade Options window is displayed.

14 Select one of the following upgrade types (this prompt is displayed only if you are upgrading a Primary SMS):

- **Normal upgrade**. If you know an Admin ID and password from the previous version of the SMS, click the radio button for this option. You will be prompted to enter the Admin ID and password.
- **Forgot password**. If you forgot the Admin password from the previous release — but know the master key — select this option. You will be prompted to create a new password.
- **Forgot master key**. If you forgot the Admin password from the previous release — and do not know the master key — choose this option. You will have to create a new password for each administrator, and then make new USB drives or floppies and reboot each Brick from a USB drive or floppy.

15 After selecting one of the upgrade types, click **Continue**.

Result: The upgrade installation program proceeds to the final phase of the upgrade. The SMS services are initialized. While the services are starting, a progress bar indicates the status of the services initialization.

16 **Important!** In some cases, even if the installation is successfully completed, you may receive the following message:

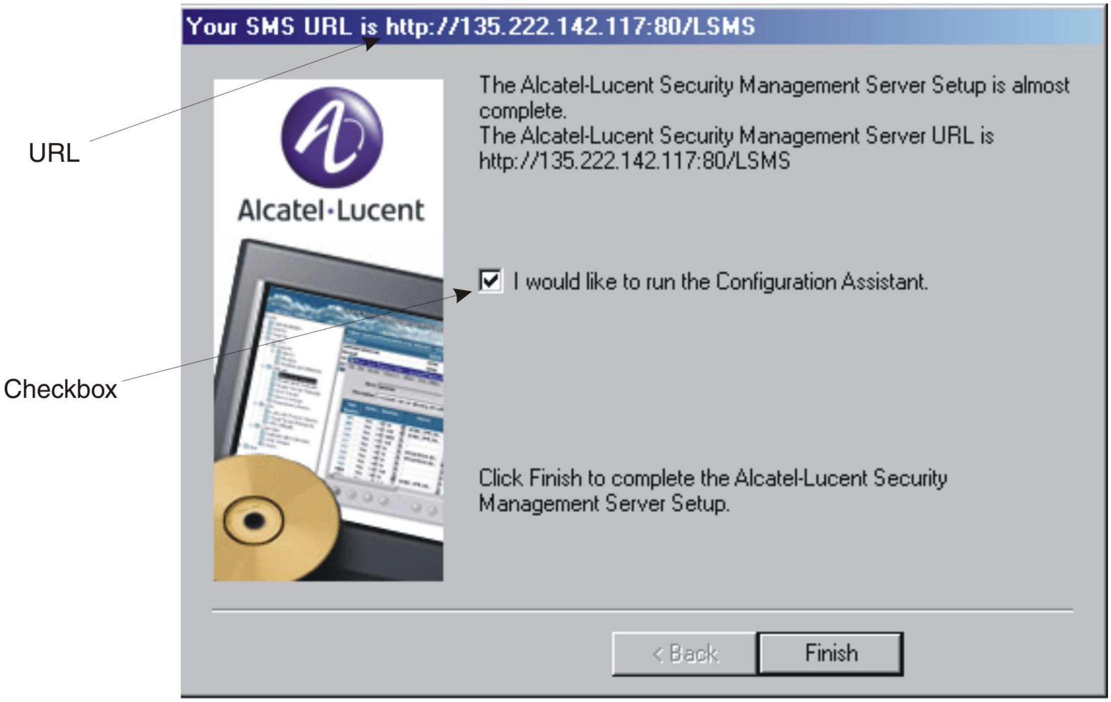
`This program might not have installed correctly`

followed by a series of options. If this occurs, choose

`This program installed correctly` to proceed with the installation.

When all SMS services have been successfully started, click **OK** to continue.

Result: If the installation is successful, a window similar to the following is displayed.



Your SMS URL is http://135.222.142.117:80/LSMS

The Alcatel-Lucent Security Management Server Setup is almost complete.
The Alcatel-Lucent Security Management Server URL is http://135.222.142.117:80/LSMS

☑ I would like to run the Configuration Assistant.

Click Finish to complete the Alcatel-Lucent Security Management Server Setup.

The URL of the SMS is shown at the top of the window. It consists of the IP address and port entered, and the directory that contains the SMS software. You will need this URL in order for your administrators to download the SMS Remote Navigator from a browser to their remote machines (see the *Remote Administration* section in the *SMS Administration Guide*).

By default, the box labeled **I would like to run the Configuration Assistant** is checked. If you leave the box checked and click **Finish**, the Configuration Assistant is displayed.

If you un-check the box before clicking **Finish**, the Configuration Assistant is not displayed, and the system returns to the *Windows*® desktop.

Configuration Assistant

The Configuration Assistant allows you to set certain system-wide parameters. You can open the Configuration Assistant now to change SMS system parameters now, or keep the default parameter settings and modify them at a later point.

For additional details about the Configuration Assistant, refer to the *SMS Administration Guide* .

END OF STEPS

□

What To Do Next

Overview

Congratulations! You have successfully installed or upgraded the required software and have a working SMS running the current software release. The installation accomplished the following:

1. It placed an entry called **Alcatel-Lucent Security Management Server** in the Programs folder on the *Windows*® Start menu.

   This entry enables you to:

   - Run the SMS application using the SMS Navigator or, if previously installed, the SMS Remote Navigator
   - Open the local SMS Log Viewer
   - Access the four SMS utilities (Configuration Assistant, New Feature Setup, SMS Service Status, and SMS Schedule Editor)
   - Start and stop the SMS services
   - Restart SMS services
2. It created an SMS Administrator account with full privileges that you or another administrator, can use to log into the SMS and begin work.

You are now ready to begin deploying Brick devices in your network as firewalls and VPN tunnel endpoints. The best place to begin is the *Getting Started* chapter in the *SMS Administration Guide*.

The *Getting Started* chapter in the *SMS Administration Guide* explains how to log on and off the SMS, and describes the basics about using the SMS software in detail. It also provides guidelines for setting up the objects using the SMS interface and explains where to find information in the SMS documents to enable you to perform basic tasks.

If you have purchased any optional feature licenses, run the New Feature Setup utility on the Primary SMS to install the optional feature installation keys to enable the features. For more information about the New Feature Setup utility, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

□

3 SMS on a *Microsoft*® *Vista*® Server Platform

Overview

Purpose

This chapter explains how to install or upgrade the SMS application on a *Microsoft*® *Vista*® server platform. It also includes a procedure for manually un-installing the SMS as needed.

Contents

Introduction	26
Hardware Requirements	29
Software Requirements	30
Pre-Installation Requirements (Clean Installations)	31
To Install the SMS Application (Clean Installations With Server Running *Microsoft*® *Vista*®)	33
To Manually Un-Install SMS	39
To Upgrade the SMS Software	40
What To Do Next	44

Introduction

Overview

The SMS application can be installed on a host running *Microsoft*® *Vista*®.

On *Microsoft*® *Vista*® hosts, Release 9.4 is can be installed as a first time (clean) installation or as an upgrade. The host may already be running the *Microsoft*® *Vista*® operating system when the SMS application is installed, or the host operating system may be converted from *Microsoft*® *Windows*® to *Vista*™ before the SMS application is installed.

This chapter provides step-by-step instructions for installing the SMS application as:

- a Primary SMS. Use this procedure to install a single SMS or the first SMS in a multi-site SMS redundancy configuration
- a Secondary SMS associated with a Primary SMS in a redundant pair or as part of a multi-site SMS redundancy configuration
- a Compute Server associated with a Primary or Secondary SMS

  Important! If *Vista*® User Account Control (UAC) is enabled (which is the default), and you run the SMS application using a *Vista*® standard user or administrator account, you may be prompted via screens for permission or credentials (such as a valid local administrator password) to run any SMS function/feature after it is installed. *Vista*® UAC is designed to prevent unauthorized access of your computer by users or malicious software programs, with changes in the *Vista*® operating system that can restrict standard user accounts or administrator accounts, without permission or authorization, from performing certain activities or running applications.

  If this is the case, respond to the UAC screen prompt by allowing the SMS application to be run or by entering a valid administrator password, based on what is requested.

  If you encounter prompting for permission to run the SMS application each time after it is installed, it may be advisable to disable *Vista*® UAC, depending on the security requirements of your local operational environment.

Upgrades

CAUTION

Service-disruption hazard

Security Precaution

It is highly recommended that the SMS server be protected with a VPN Firewall and that as little as possible be put on the same trusted subnet as the SMS.

SMS configurations

The SMS can be deployed in one of the following configurations:

- A Primary SMS (stand-alone configuration)
- A Primary SMS and Secondary SMS (in a redundant configuration)

- A Primary SMS and up to three Secondary SMSs (Multi-Site configuration)
- A Primary SMS and up to three Secondary SMSs, each with up to five Compute Servers (Compute Server configuration)

Multi-Site SMS configuration

A multi-site SMS configuration consists of a Primary SMS and up to three Secondary SMSs. The Primary SMS and Secondary SMS (s) share the same database, which is updated periodically across the network. The Primary SMS and Secondary SMS(s) are simultaneously active, synchronizing status and configuration at the same time.

Compute servers

To maximize scalability of the SMS/Brick security solution, the SMS provides the option of adding a separate set of servers called Compute Servers (CSs), which are associated with a Primary or Secondary SMS and act as collection points for Brick log traffic. Using a CS to collect Brick log data frees up computing resources on the SMS itself and extends the number of Brick devices and total log traffic that can be handled. Each Brick device managed by the SMS can be homed to one of the associated CSs or the managing SMS for logging purposes.

Up to five CSs can be configured for a Primary or Secondary SMS.

Implementing Primary SMS/Secondary SMS configurations

During the installation of the Secondary SMS, there is a point at which the Secondary SMS attempts to contact the Primary SMS to replicate the Primary SMS database on the Secondary SMS. If the Secondary SMS cannot contact the Primary SMS, correct the problem and retry the operation on the Secondary SMS.

For reasons of security, we strongly recommend that you deploy a Brick device ″in front″ of the Primary and Secondary SMS(s) to protect all servers.

To ensure that the Primary SMS and Secondary SMS(s) can contact each other through both Brick devices, follow the course of action outlined below when you order the installation:

1. Install the Primary SMS first. The two installation procedures in this chapter provide step-by-step instructions for a new installation and an upgrade installation.
2. Once the Primary SMS is operational, use it to configure two Bricks and assign the pre-configured ruleset *administrativezone* to the ports that will be connected to the SMS. Refer to the *Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports* section in the *SMS Administration Guide* for instructions on how to do this.
3. Connect the Primary SMS to the port on one Brick, and the host that will be the Secondary SMS to the port on the other. Then, deploy the two Bricks: the primary SMS and the host that will be the Secondary SMS in the network.

4. To ensure that the Primary SMS and remote host can communicate, add a ping rule (*dir=both, source=**, *dest=**, *service=ping_request,action=pass*) to the *administrativezone* ruleset, and then ping the host from the SMS. Once the ping is successful, remove the rule for security reasons. (Refer to the *Brick Zone Rulesets* section in the *SMS Policy Guide* for instructions on how to create a rule.)
5. When you have established that the two SMS servers can communicate, install the Secondary SMS.

□

Hardware Requirements

Minimum hardware requirements

The host on which you install the SMS application that is running on the *Microsoft*® *Vista*® operating system must meet the following minimum hardware requirements:

- 800 MHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB of RAM
- Swap space at least as large as the amount of RAM
- 20 GB hard drive that has at least 15 GB of available disk space for the *Vista*® operating system and at least 1 GB free space on an NTFS partition for the SMS software
- Internal or external DVD/CD drive
- 3.5 inch floppy drive, USB port, or serial port. For information on the hardware required to boot specific Lucent Brick device models, consult the *User's Guide* for the specific Brick or contact your Alcatel-Lucent customer support team representative.
- Ethernet interface card
- Video card capable of 1024 x 768 resolution (65,535 colors)

  Important! Because of the memory requirements of SMS R9.4, older Brick 20 models with only 8 MB of RAM may not be able to be configured with all features.

  To verify the amount of RAM on the Brick device, log into the Brick device via the remote console and run the `display mem` command.

If you are managing many Brick devices, supporting many IPSec clients, or generating large amounts of audit data, you may require additional memory. See the *Sizing Guidelines* appendix in the *SMS Administration Guide* to help you determine how much additional memory you may need.

One optional piece of equipment you may want to consider is a modem. Having a modem in the host allows you to set up alarms that page an administrator when a problem is encountered. If you decide to add a modem, it must be Hayes-compatible and configured so that it cannot accept incoming calls and cannot be shared by other services, such as a Remote Access Server.

□

Software Requirements

Required software components

The following software is required to run the SMS application on a *Microsoft*® *Vista*® platform:

- *Windows*® *Vista*® with Service Pack 1 or 2
- A hard drive with at least one NTFS partition. The drive can have the FAT file system installed, but it must have at least one NTFS partition to hold the SMS software.

In addition, the following software is not required, but is highly recommended:

- A browser such as *Microsoft*® *Internet Explorer*® or Firefox to view SMS reports and display the on-line help.
- Adobe Acrobat Reader. This application is required to display the on-line manuals.

Security patches

It is strongly recommended that you install security patches on a regular basis to keep security on your machine up-to-date. Use caution when installing service packs. It is not guaranteed that the current SMS software can be installed or run with new service packs.

□

Pre-Installation Requirements (Clean Installations)

Overview

Before you proceed with the actual installation of the SMS application for the first time on a host, some pre-installation steps are required:

1. Resolve potential web server port conflicts.
2. Install Adobe Acrobat Reader.
3. Obtain the SMS installation keys.

Resolve potential web server port conflicts

The SMS application contains a web server which will conflict with any existing web server currently active on the host machine. If there is another web server running on the SMS host (such as *Microsoft*® Internet Information Server or Apache), you must either:

- Shut the web server down
- Check system services and set the Startup Type to Manual or Disabled rather than Automatic so that the web server will not start up when the OS is rebooted.

Port 80 is the default SMS web server port. In the event that another web server is already using port 80 (such as Apache), you must either change the port on that web server or select a different port when configuring the SMS web server.

Install Adobe Acrobat Reader

Adobe Acrobat Reader is required to view the on-line documentation that is provided with the application. A copy of this application can be downloaded from the Adobe website, http://www.adobe.com.

Obtain the SMS installation keys

To install the SMS application, two keys are required:

- *Software license key*
  The software license key is provided with the product. You will need this key to register the product and to obtain the installation key, which is required to perform the installation.
- *Installation key*
  The installation key is required to install the product.

For complete instructions on how to register a software license key and obtain an installation key, refer to Appendix A, “Registering SMS Software License Keys and Obtaining Installation Keys”.

There are six categories of installation keys available, depending on the type of installation you are performing. The six categories are:

- Primary SMS (Clean Install)
- Upgrade for Primary SMS

- Secondary SMS associated with a Primary SMS (Clean Install)
- Upgrade for Secondary SMS associated with a Primary SMS
- Compute Server SMS (Clean Install)
- Upgrade for Compute Server SMS

The installation key that you enter, which sets parameters affecting the operation of the SMS, cannot be changed.

You will be prompted to enter the software installation key during the installation process. If you have purchased any optional feature licenses, refer to the procedure "To register a software license key and obtain an installation key for upgrade or feature option" (p. 101) in Appendix A, "Registering SMS Software License Keys and Obtaining Installation Keys" for instructions on how to register these license keys and obtain installation keys that you will use to enable these features on your SMS. Optional features are enabled after the software installation/upgrade is complete, using the New Feature Setup utility.

To enable optional features, run the New Feature Setup utility on the Primary SMS after you finish the software installation process and enter your optional feature installation keys. Optional features enabled on the Primary SMS are also automatically enabled on all associated Secondary and Compute Server SMS machines. It may be necessary to restart services to enable some features.

For more information on New Feature Setup, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

Software patches and documentation updates

It is a good idea to check the VPN Firewall Product Registration and Support website (https://vpn-firewall-brick.alcatel-lucent.com) periodically for patches and documentation updates issued since you purchased the product.

If you are installing the SMS application for the first time, the installation keys that you will receive are only for an initial installation of the current software release. If you are upgrading from an earlier release of the SMS software, these installation keys are only for an upgrade to the current software release. When installing a patch version of the SMS application, you do not need an installation key.

□

To Install the SMS Application (Clean Installations With Server Running *Microsoft® Vista®*)

When to use

Use this procedure to install the SMS application for the first time on a host that is already running *Microsoft® Vista®*.

Before you begin

Before you begin this task, if you are installing a Secondary or Compute Server SMS, you must first:

1. Install the Primary SMS, using this procedure.
2. Log into the Primary SMS and add the Secondary or Compute Server SMS to the **LSMSs and LSCSs** folder using the exact SMS Name, IP Address, and installation key that will be used to install it. For instructions on how to add a Secondary or Compute Server SMS, refer to the *SMS Administration Guide*.

Procedure

Use the following procedure to install the SMS application for the first time on a host.

1 With the SMS CD-ROM in the drive, open the *Vista®* Explorer and locate this directory on the CD-ROM:

Windows

2 Double-click the file *LSMS-9.4.xxx.exe* where xxx is the build number of the software.

This is the installation program. Windows that indicate the progress of the unpacking and setup during these processes are displayed first.

> **Result:** Upon completion of these processes a Welcome window is displayed.

3 Read the text in the Welcome window, and when you are finished, click **Next** to continue with the installation.

4 Scroll through the Software License Agreement, and if it is acceptable, click **Yes** to proceed.

Result: The Installation Key window is displayed.

5 Enter the installation key applicable to this SMS that you obtained from the VPN Firewall Product Registration and Support website (https://www.lucent-ipsec.com) and click **Next**. Refer to the "Obtain the SMS installation keys" (p. 8) section for the types of installation keys available.

Result: The program verifies the key, and then displays the Choose Destination Location window.

6 The Root Directory for the Alcatel-Lucent Security Management Server window allows you to specify where the SMS software will be installed. The default is: *c:\isms*

Click **Next** to do this, or click the **Browse** button and enter a new destination location before clicking **Next**.

Result: Once you have indicated the directory, the **Where do you want the logs to go?** window is displayed.

The destination directory for the SMS application must reside on an NTFS partition. If not, you will have to select another directory that is on an NTFS partition, or terminate the installation and run the Vista convert utility on the partition on which you want to install the SMS software.

7 The Where do you want the logs to go? window allows you to specify the folder where the SMS logs will be stored. If you chose the default in the previous step, this selection defaults to: *c:\isms\lmf*

You may either accept this selection, or click the **Browse** button and enter a new destination location before clicking **Next**.

After completing the installation, you may elect to redefine the location of the ″log″ directory or even ″ftp″ the logs to another machine. Either of these changes can be done through the SMS Configuration Assistant. Refer to *Using the Configuration Assistant* chapter in the *SMS Administration Guide* for more details.

8 The Select Program Folder window allows you to select the folder in which the SMS application will appear on the *Vista*® Start menu. The default is **SMS Applications**

It is recommended that you accept the default. Click **Next** to do this, or select another directory from the Existing Folders and then click **Next**.

Result: The What You Should Know about this Release window is displayed.

9 Read the Release Notes, which gives important information regarding this release. When finished, click **Next**.

Result: Installation of the files will now begin. While the files are being installed, a progress screen will indicate the status of the installation.

10 When the installation is complete, click **OK**.

Result: The SMS Web Server Configuration window is displayed.

11 The SMS Web Server Configuration window allows you to select the type of web server to be installed and the port to be used:

- **Type**. Enter the type of web server. The choices are **HTTP** (the default) and **HTTPS**, which relies on a digital certificate and is substantially more secure. If administrators will be logging into the SMS remotely, it is a good idea to use **HTTPS**. (To obtain and install a digital certificate, refer to the *Digital Certificates* section in the *SMS Policy Guide*.)
- **Port**. Enter the web server port. The default value is *80*, the standard port for HTTP; *443* is the standard port for HTTPS. If you are using HTTPS, or if port 80 is already in use, you can change the port.

12 After you have made your choices, click **Next** to continue with the installation.

Result: The SNMP Agent Configuration window is displayed.

13 The SMS SNMP Agent Configuration window allows you to choose the port that the SMS SNMP agent will use. The SMS SNMP agent is used for remote monitoring of the SMS and Brick devices.

The default value is *161*, which is the standard port for SNMP. You can change this if port 161 is already in use by another SNMP application.

14 When you have made your choice, click **Next** to continue with the installation.

For more information on how the SMS interacts with SNMP, refer to the *SNMP* appendix in the *SMS Reports, Logs and Alarms Guide*.

15 The Select SMS Type window shows the following information:

- **SMS IP Address**. The application is able to detect all of the available IP addresses configured on the machine. Choose the desired address from the drop down box.
- **SMS Name**. This field defaults to the SMS Machine name, but you may override it and type your own selection.
- **SMS Type**. Based on the installation key entered, either **Primary SMS Secondary SMS**, or **Compute Server SMS** is selected and the others are grayed out.

16 If the installation is a Primary SMS, the installation will proceed immediately to Step 17.

If the installation is either a Secondary SMS or a Compute Server installation, you will be asked to enter the IP address for either the Primary SMS or the SMS to which the Compute Server will home. The program will perform the additional steps required and proceed to Step 20.

If the Secondary SMS cannot contact the Primary SMS, or the Compute Server cannot contact its associated SMS, the installation program prompts you to retry with a different IP address. If you cannot enter a valid IP address, you must terminate the installation program using the Task Manager. The inability to contact the specified IP address may indicate a network problem that must be corrected before proceeding with the installation.

For security reasons, the Secondary SMS must be installed/upgraded within 7 days of installing/upgrading a Primary SMS. After more than 7 days, the installation or upgrade of a secondary will fail because the Primary SMS does not allow the Secondary SMS to copy/replicate the database. To allow database replication, you must open a command line window on the primary, cd to the installation directory, and enter the following command:

```
local\bin\allowSecondarySetup
```

Result For Secondary SMS or Compute Server installations, the SMS services are initialized. Go to Step 20.

17 For Primary SMS installations, the installation program begins to initialize the database.

This process will take several minutes.

A master key is generated and displayed in the lower half of the SMS Setup screen. The purpose of the master key is to protect the root certificate used to authenticate communication between the SMS and the Brick devices that it manages. *Write the master key down and keep it in a secure place*. You will need the key to recover if you should forget the Administrator password and become locked out of the SMS.

Result: The installation program displays the Enter Admin ID window so that you may create an SMS Administrator ID and password.

18 Create an Administrator ID and password by entering information into the following fields:

- **Admin ID**. This is the initial ID used to log into the SMS. It can contain a maximum of 16 characters. Keep a record of the Admin ID in a secure place. You will need it to log into the SMS after installation is complete. Once you log in with this initial ID, other administrator IDs can be created, if desired.
- **Password**. The password is needed to complete the login. Enter the password, and then enter it again for verification purposes. The password can contain up to 42 characters. It is case-sensitive, so you must enter the password exactly the same each time.

19 Click **OK** to accept your choice.

Result: When the initial installation is complete, the ″Initial Installation Complete″ notification is displayed. You must click **Continue** at the bottom of the dialog box for the installation to proceed.

Result: The SMS services are initialized. While the services are starting, a progress bar indicates the status of the effort.

20 **Important!** In some cases, even if the installation is successfully completed, you may receive the following message:

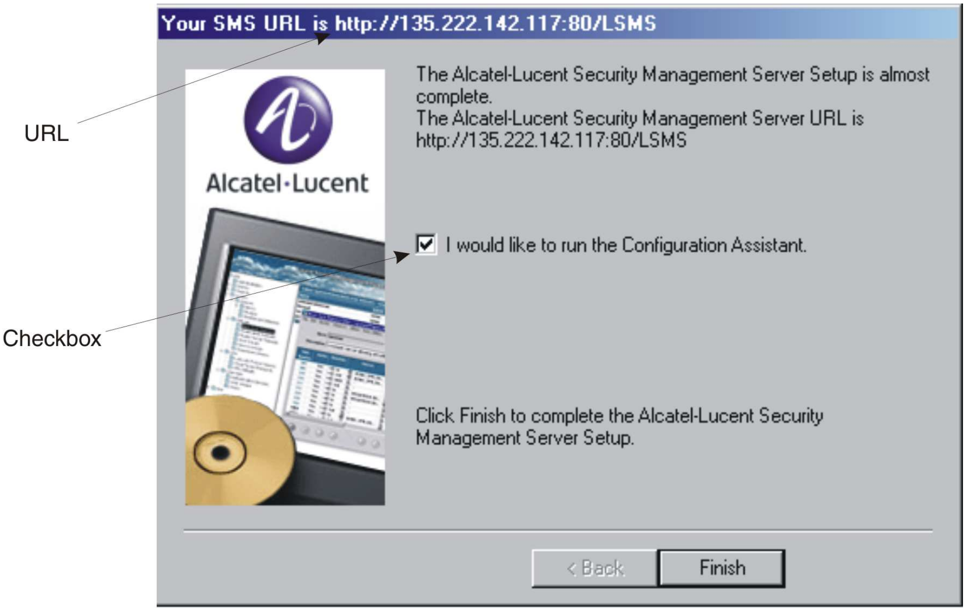
`This program might not have installed correctly`

followed by a series of options. If this occurs, choose

`This program installed correctly` to proceed with the installation.

When all SMS services have been successfully started, click **OK** to continue.

Result: If the installation is successful, a window similar to the following is displayed.



Your SMS URL is http://135.222.142.117:80/LSMS

The Alcatel-Lucent Security Management Server Setup is almost complete.
The Alcatel-Lucent Security Management Server URL is http://135.222.142.117:80/LSMS

☑ I would like to run the Configuration Assistant.

Click Finish to complete the Alcatel-Lucent Security Management Server Setup.

The URL of the SMS is shown at the top of the window. It consists of the IP address and port entered, and the directory that contains the SMS software. You will need this URL in order for your administrators to download the SMS Remote Navigator from a browser to their remote machines (see the *Remote Administration* chapter in the *SMS Administration Guide*).

By default, the box labeled **I would like to run the Configuration Assistant** is checked. If you leave the box checked and click **Finish**, the Configuration Assistant is displayed.

If you un-check the box before clicking **Finish**, the Configuration Assistant is not displayed, and the system returns to the *Vista*® desktop.

Configuration Assistant

The Configuration Assistant allows you to set certain system-wide parameters. You can open the Configuration Assistant now to change SMS system parameters now, or keep the default parameter settings and modify them at a later point.

For additional details about the Configuration Assistant, refer to the *SMS Administration Guide*.

END OF STEPS

□

To Manually Un-Install SMS

When to use

This procedure is not required or recommended for upgrading to the current “official” SMS release that you purchased. As part of its software upgrade program, the SMS automatically installs, upgrades to the current release, and un-installs the previous SMS release.

However, if you have installed an Evaluation copy of the SMS software, you should manually un-install the Evaluation copy using this procedure before upgrading to an “official” SMS release. You should skip Step 2 of this procedure if you want to preserve your configuration data.

This procedure can be used, for example, to manually un-install the SMS software from a de-commissioned server.

Task

Complete the following steps to manually un-install the SMS.

1 The SMS can be un-installed via the **Add or Remove Programs** utility of the *Vista*®**Control Panel** by selecting **Alcatel-Lucent Security Management Server** and clicking **Remove**.

2 For final removal, you can move to backup or delete the contents of the SMS directory (Example: *c:\isms\lmf\*).

END OF STEPS

□

To Upgrade the SMS Software

When to use

Use this procedure to upgrade to the current SMS software on a host that is already running *Microsoft*® *Vista*®.

Before you begin

Before you begin this task, if you are upgrading a Secondary or Compute Server SMS, you must first upgrade the Primary SMS using this procedure.

Procedure

Use the following procedure to upgrade to the current SMS software release.

1 Manually back up the current SMS database to a USB drive or *ftp* server using the `backup` database utility. For instructions on how to perform a manual backup of the SMS database, refer to the *Manual Backup* section of the *SMS Administration Guide*.

2 Insert the current SMS release CD-ROM into the server's CD/DVD drive.

3 With the SMS CD-ROM in the drive, open the *Vista*® Explorer and locate this directory on the CD-ROM:

Windows

4 Double-click the file *LSMS-9.4.xxx.exe* where *xxx* is the build number of the software.

This is the installation program. Windows that indicate the progress of the unpacking and setup during these processes are displayed first.

Result: Upon completion of these processes a Welcome window is displayed.

5 Read the text in the Welcome window, and when you are finished, click **Next** to continue with the installation.

6 Scroll through the Software License Agreement, and if it is acceptable, click **Yes** to proceed.

Result: The Installation Key window is displayed.

7 Enter the installation key applicable to this SMS that you obtained from the VPN Firewall Product Registration and Support web site (https://www.lucent-ipsec.com) and click **Next**. Refer to the "Obtain the SMS installation keys" (p. 8) section for the types of installation keys available.

Result: The Select Program Folder window is displayed.

8 Select the folder in which the SMS application will appear on the *Vista*® **Start** menu. The default is **SMS Applications**.

It is recommended that you accept the default. Click **Next** to accept the default, or type a different folder name and click **Next**.

Result: The What You Should Know about this Release window is displayed.

9 Read the Release Notes, which gives important information regarding this release. When finished, click **Next**.

Result: A message window is displayed, indicating that a previous version of the SMS already exists on the host.

10 Click **OK**.

Result: The old SMS files are removed. The Uninstall Programs screen is displayed.

11 When the uninstall process is completed, click **OK**.

Result: Installation of the files will now begin. While the files are being installed, a progress screen will indicate the status of the installation.

12 When the installation is complete, click **OK**.

Result: The SMS Web Server Configuration window is displayed.

13 Select one of the following upgrade types (this prompt is displayed only if you are upgrading a Primary SMS):

- **Normal upgrade**. If you know an Admin ID and password from the previous version of the SMS, click the radio button for this option. You will be prompted to enter the Admin ID and password.
- **Forgot password**. If you forgot the Admin password from the previous release — but know the master key — select this option. You will be prompted to create a new password.
- **Forgot master key**. If you forgot the Admin password from the previous release — and do not know the master key — choose this option. You will have to create a new password for each administrator, and then make new USB drives or floppies and reboot each Brick from a USB drive or floppy.

14 After selecting one of the upgrade types, click **Continue**.

Result: The upgrade installation program proceeds to the final phase of the upgrade. The SMS services are initialized. While the services are starting, a progress bar indicates the status of the services initialization.

15 **Important!** In some cases, even if the installation is successfully completed, you may receive the following message:

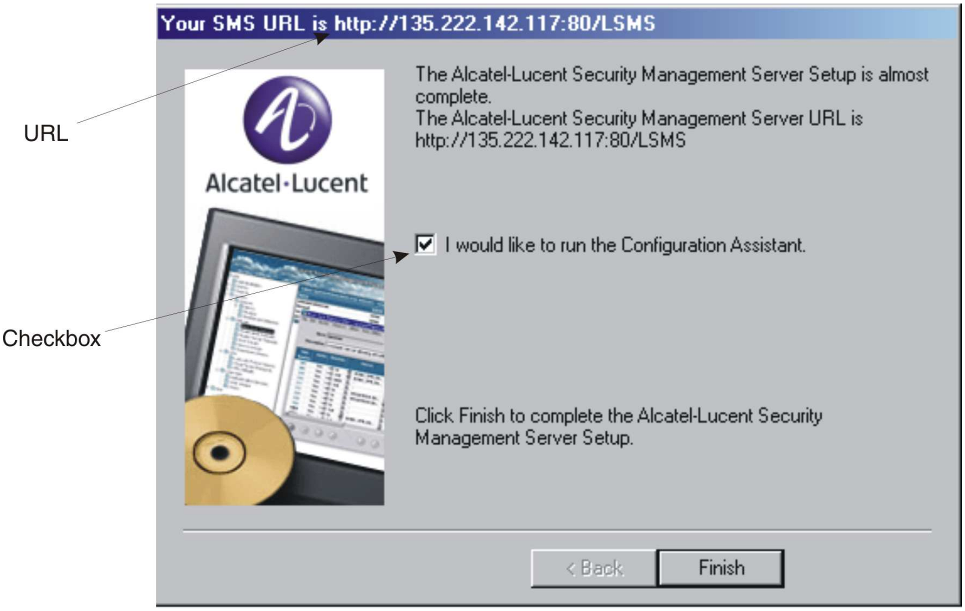
`This program might not have installed correctly`

followed by a series of options. If this occurs, choose

`This program installed correctly` to proceed with the installation.

When all SMS services have been successfully started, click **OK** to continue.

Result: If the installation is successful, a window similar to the following is displayed.



Your SMS URL is http://135.222.142.117:80/LSMS

The Alcatel-Lucent Security Management Server Setup is almost complete.
The Alcatel-Lucent Security Management Server URL is http://135.222.142.117:80/LSMS

☑ I would like to run the Configuration Assistant.

Click Finish to complete the Alcatel-Lucent Security Management Server Setup.

The URL of the SMS is shown at the top of the window. It consists of the IP address and port entered, and the directory that contains the SMS software. You will need this URL in order for your administrators to download the SMS Remote Navigator from a browser to their remote machines (see the *Remote Administration* chapter in the *SMS Administration Guide*).

By default, the box labeled **I would like to run the Configuration Assistant** is checked. If you leave the box checked and click **Finish**, the Configuration Assistant is displayed.

If you un-check the box before clicking **Finish**, the Configuration Assistant is not displayed, and the system returns to the *Vista*® desktop.

Configuration Assistant

The Configuration Assistant allows you to set certain system-wide parameters. You can open the Configuration Assistant now to change SMS system parameters now, or keep the default parameter settings and modify them at a later point.

For additional details about the Configuration Assistant, refer to the *SMS Administration Guide* .

END OF STEPS

□

What To Do Next

Overview

Congratulations! You have successfully installed or upgraded the required software and have a working SMS running the current software release. The installation accomplished the following:

1. It placed an entry called **Alcatel-Lucent Security Management Server** in the Programs folder on the *Vista*® Start menu.

   This entry enables you to:

   - Run the SMS application using the SMS Navigator or, if previously installed, the SMS Remote Navigator
   - Open the local SMS Log Viewer
   - Access the four SMS utilities (Configuration Assistant, New Feature Setup, SMS Service Status, and SMS Schedule Editor)
   - Start and stop the SMS services
   - Restart SMS services
2. It created an SMS Administrator account with full privileges that you or another administrator, can use to log into the SMS and begin work.

You are now ready to begin deploying Brick devices in your network as firewalls and VPN tunnel endpoints. The best place to begin is the *Getting Started* chapter in the *SMS Administration Guide*.

The *Getting Started* chapter in the *SMS Administration Guide* explains how to log on and off the SMS, and describes the basics about using the SMS software in detail. It also provides guidelines for setting up the objects using the SMS interface and explains where to find information in the SMS documents to enable you to perform basic tasks.

If you have purchased any optional feature licenses, run the New Feature Setup utility on the Primary SMS to install the optional feature installation keys to enable the features. For more information about the New Feature Setup utility, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

□

4 SMS on a *Sun*® *Solaris*® Server Platform

Overview

Purpose

This chapter explains how to install or upgrade the SMS application on a *Sun*® *Solaris*® server platform. It also includes a procedure for manually de-installing the application if necessary.

Contents

Introduction	46
Hardware Requirements	48
Software Requirements	49
Pre-Installation Requirements (Clean Installations)	50
To Install the SMS Application (Clean Installation)	53
To Manually Un-Install SMS	58
To Upgrade the SMS Software	59
What To Do Next	64

□

Introduction

Overview

CAUTION

Service-disruption hazard

SMS only supported on SPARC processors.

The SMS is only supported on SPARC processors that are running Solaris® *Release 9 or 10. For additional requirements, refer to the "Hardware Requirements" (p. 48) section.*

The SMS application is not supported on a Solaris® *server that has the Internet Protocol Multiple Path (IPMP) feature enabled.*

Upgrades

CAUTION

Service-disruption hazard

Security Precaution

It is highly recommended that the SMS server be protected with a Brick device and that as little as possible be put on the same trusted subnet as the SMS.

SMS configurations

The SMS can be deployed in one of the following configurations:

- A Primary SMS (stand-alone configuration)
- A Primary SMS and Secondary SMS (in a redundant configuration)
- A Primary SMS and up to three Secondary SMSs (Multi-Site configuration)
- A Primary SMS and up to three Secondary SMSs, each with up to five Compute Servers (Compute Server configuration)

Multi-Site SMS configuration

A multi-site SMS configuration consists of a Primary SMS and up to three Secondary SMSs. The Primary SMS and Secondary SMS (s) share the same database, which is updated periodically across the network. The Primary SMS and Secondary SMS(s) are simultaneously active, synchronizing status and configuration at the same time.

Compute servers

To maximize scalability of the SMS/Brick security solution, the SMS provides the option of adding a separate set of servers called Compute Servers (CSs), which are associated with a Primary or Secondary SMS and act as collection points for Brick log traffic. Using a CS to collect Brick log data frees up computing resources on the SMS itself and extends the number of Brick devices and total log traffic that can be handled. Each Brick device managed by the SMS can be homed to one of the associated CSs or the managing SMS for logging purposes.

Up to five Compute Servers can be configured for a Primary or Secondary SMS.

Implementing Primary SMS/Secondary SMS configurations

During the installation of the Secondary SMS, there is a point at which the Secondary SMS attempts to contact the Primary SMS to replicate the Primary SMS database on the Secondary SMS. If the Secondary SMS cannot contact the Primary SMS, correct the problem and retry the operation on the Secondary SMS.

For reasons of security, we strongly recommend that you deploy a Brick device ″in front″ of the Primary and Secondary SMS(s) to protect all servers.

To ensure that the Primary SMS and Secondary SMS(s) can contact each other through both Brick devices, follow the course of action outlined below when you order the installation:

1. Install the Primary SMS first. The two installation procedures in this chapter provide step-by-step instructions for a new installation and an upgrade installation.
2. Once the Primary SMS is operational, use it to configure two Bricks and assign the pre-configured ruleset *administrativezone* to the ports that will be connected to the SMS. Refer to the *Configuring Brick Ports* section in the *SMS Administration Guide* for instructions on how to do this.
3. Connect the Primary SMS to the port on one Brick, and the host that will be the Secondary SMS to the port on the other. Then, deploy the two Bricks: the primary SMS and the host that will be the Secondary SMS in the network.
4. To ensure that the Primary SMS and remote host can communicate, add a ping rule (*dir=both, source=*, dest=*, service=ping_request*,*action=pass*) to the *administrativezone* ruleset, and then ping the host from the SMS. Once the ping is successful, remove the rule for security reasons. (Refer to the *Brick Zone Rulesets* section in the *SMS Policy Guide* for instructions on how to create a rule.)
5. When you have established that the two SMS servers can communicate, install the Secondary SMS.

□

Hardware Requirements

Minimum hardware requirements

Regardless of which operating system you are running, the workstation on which you install the SMS application must meet the following minimum hardware requirements:

- A Sun Ultra SPARC 5 (330 MHz processor or better)
- 500 MB free disk space in the partition where the SMS application is to be installed
- 50 MB of free space in the root partition
- 512 MB of RAM
- Swap space at least as large as the amount of RAM
- CD-ROM drive
- 3.5 inch floppy drive, USB port, or serial port. For information on the hardware required to boot specific Brick models, consult the *User's Guide* for the specific Brick model or contact your Alcatel-Lucent customer support team representative.
- *Ethernet*™ interface card
- Video card capable of 1024 x 768 resolution (65,535 colors)

  Important! Because of the memory requirements of SMS R9.4, older Brick 20 models with only 8 MB of RAM may not be able to be configured with all features.

  To verify the amount of RAM on the Brick device, log into the Brick device via the remote console and run the `display mem` command.

If you are managing many appliances, supporting many IPSec clients, or generating large amounts of audit data, you may require additional memory. Refer to the *Sizing Guidelines* appendix in the *SMS Administration Guide* to help you determine how much additional memory you may need.

One optional piece of equipment you may want to consider is a modem. Having a modem in the host allows you to set up alarms that page an administrator when a problem is encountered. If you decide to add a modem, it must be Hayes-compatible and configured so that it cannot accept incoming calls and cannot be shared by other services, such as a Remote Access Server.

□

Software Requirements

Required software components

To run the SMS application on a *Solaris*® platform, you need *Solaris*® Release 9 or 10. In order to ensure that all the necessary libraries have been loaded, the machine must be installed with the *Solaris*® ″Developer Support″ package (or greater).

In addition, the following software is not required, but is highly recommended:

- A browser such as *Microsoft*™ *Internet Explorer*® or Firefox to view SMS reports and display the on-line help.
- Adobe Acrobat Reader. This application is required to display the on-line manuals.

□

Pre-Installation Requirements (Clean Installations)

Overview

Before you proceed with the actual installation of the SMS application for the first time on a host, some pre-installation steps are required:

1. Install the patch cluster.
2. Resolve potential web server port conflicts.
3. Obtain the SMS installation keys.

Install the patch cluster

Check the Sun website for any critical bug fixes or security patches for your *Solaris*® version, and install the appropriate patch cluster.

Resolve potential web server port conflicts

The SMS application includes a web server. If there is another web server running on the host machine (such as Apache), you must either:

- Shut the web server down
  Note: If there is an entry in the /etc/inittab file to automatically start your web server, you must remove or disable this entry so that it does not conflict with the SMS server.
  or
- Select a different port for the SMS web server when prompted by the installation program

Port 80 is the default SMS web server port. In the event that another web server is already using port 80 (such as Apache), you must either change the port on that web server or select a different port when configuring the SMS web server.

Obtain the SMS installation keys

To install the SMS application, two keys are required:

- *Software license key*
  The software license key is provided with the product. You will need this key to register the product and to obtain the installation key, which is required to perform the installation.
- *Installation key*
  The installation key is required to install the product.

For complete instructions on how to register a software license key and obtain an installation key, refer to Appendix A, “Registering SMS Software License Keys and Obtaining Installation Keys”.

There are six categories of installation keys available, depending on the type of installation you are performing. The six categories are:

- Primary SMS (Clean Install)
- Upgrade for Primary SMS
- Secondary SMS associated with a Primary SMS (Clean Install)
- Upgrade for Secondary SMS associated with a Primary SMS
- Compute Server SMS (Clean Install)
- Upgrade for Compute Server SMS

The installation key that you enter, which sets parameters affecting the operation of the SMS, cannot be changed.

You will be prompted to enter the software installation key during the installation process. If you have purchased any optional feature licenses, refer to the procedure "To register a software license key and obtain an installation key for upgrade or feature option" (p. 101) in Appendix A, "Registering SMS Software License Keys and Obtaining Installation Keys" for instructions on how to register these license keys and obtain installation keys that you will use to enable these features on your SMS. Optional features are enabled after the software installation/upgrade is complete, using the New Feature Setup utility.

To enable optional features, run the New Feature Setup utility on the Primary SMS after you finish the software installation process and enter your optional feature installation keys. Optional features enabled on the Primary SMS are also automatically enabled on all associated Secondary and Compute Server SMS machines. It may be necessary to restart services to enable some features.

For more information on New Feature Setup, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

Software patches and documentation updates

It is a good idea to check the VPN Firewall Product Registration and Support website (https://vpn-firewall-brick.alcatel-lucent.com) periodically for patches and documentation updates issued since you purchased the product.

If you are installing the SMS application for the first time, the installation keys that you will receive are only for an initial installation of the current software release. If you are upgrading from an earlier release of the SMS software, these installation keys are only for an upgrade to the current software release. When installing a patch version of the SMS application, you do not need an installation key.

Running OS firewall and security software and the SMS

If you have enabled OS firewall or security software on a host that is also running the SMS application, it must be configured to allow the SMS services to run and to allow access to ports that the SMS uses to communicate with Brick devices and other SMSs/Compute Servers (CSs). For a list of ports that are used by the SMS to communicate with other components in the Alcatel-Lucent VPN Firewall Solution, refer to the *VPN Firewall Solution Ports* appendix in the *SMS Administration Guide*.

□

To Install the SMS Application (Clean Installation)

When to use

Use this procedure to install the SMS application for the first time on a host.

Before you begin

Before you begin this task, if you are installing a Secondary or Compute Server SMS, you must first:

1. Install the Primary SMS, using this procedure.
2. Log into the Primary SMS and add the Secondary or Compute Server SMS to the **LSMSs and LSCSs** folder using the exact SMS Name, IP Address, and installation key that will be used to install it. For instructions on how to add a Secondary or Compute Server SMS, refer to the *SMS Administration Guide*.

Procedure

Complete the following steps to install the SMS application for the first time on a host.

1 Login as user `root`.

2 With the CD-ROM in the drive and a terminal window displayed, enter:

cd /cdrom/cdrom0/Solaris

Result: The system changes to the directory on the CD-ROM that contains the installation script.

3 Enter `sh installLSMS .` to begin the installation.

Result: The installation program displays a series of prompts.

4 Press **[Enter]**to display the license agreement and type Y to accept these terms and conditions.

5 Press **[Enter]** to display the installation notes and type **Y** to accept the terms of the notes.

6 Enter the installation key as provided.

7 Press **[Enter]** to install the SMS application in the default directory (*/opt/isms*), or enter a different directory and press **[Enter]**.

8 Press **[Enter]** to store the SMS log files in the default directory (*/opt/isms/lmf*), or enter a different directory and press **[Enter]**.

After completing the installation, you may elect to redefine the location of the log directory or even *ftp* the logs to another machine. Either of these changes can be done through the SMS Configuration Assistant. Refer to *Using the Configuration Assistant* chapter in the *SMS Administration Guide* for more details.

Result: The installation program asks whether you want to configure the SMS web server for HTTP or HTTPS.

9 Press **[Enter]** to configure the web server for HTTP, or enter **HTTPS** and press **[Enter]**.

HTTPS relies on a digital certificate, and is, therefore, substantially more secure. If administrators will be logging into the SMS remotely, it is a good idea to use HTTPS.

To obtain and install a digital certificate, see the *Digital Certificates* section in the *SMS Policy Guide.*

Result: The installation program prompts for entry of the port that the web server will be listening on.

The default is *80*, which is the standard port for HTTP. *443* is the standard port for HTTPS.

10 Press **[Enter]** to use port *80*, or enter another port and press **[Enter]**.

Result: The installation program displays a series of prompts that ask if the system is already running the *Solaris*® SNMP Agent, if you want to use the SMS SNMP Agent, or you would like to run both SNMP Agents.

11 Choose one of the SNMP Agent options.

Result: The installation program asks for the port number if the system is already running the *Solaris*® SNMP Agent.

The SMS SNMP Agent provides the ability to monitor the SMS and firewall appliances remotely.

The default port is *161*, which is the standard port for SNMP.

12 Depending on whether the system is already running the *Solaris*® SNMP Agent, accept the default port for the SMS SNMP Agent or define another port, as needed.

Result: The installation program prompts you to define an SNMP Read Community.

13 Accept the SNMP Read Community default **(public)**, or modify as needed.

The SNMP values in steps 11 to 13 can be modified after the installation using the SMS Configuration Assistant.

For additional information on how the SMS interacts with SNMP, refer to the *Simple Network Management Protocol (SNMP)* chapter in the *SMS Administration Guide*.

For additional information about the SMS Configuration Assistant, refer to the *Using the Configuration Assistant* chapter in the *SMS Administration Guide*.

Result: The installation program displays the following message:

```
This package contains scripts which will be
executed with super-user
permission during the process
of installing this package.
```

14 Enter **Y** to proceed with the installation.

Result: The installation program begins to copy files to the target directory and echoes each of the file copies to the console window.

When all of the files have been copied, the installation program prompts you to indicate whether this is a Primary, Secondary, or Compute Server SMS.

As of Release 8.0, the SMS type is pre-determined by the installation key that is used.

The system prompts you to enter the IP address to be used by the SMS.

15 Enter **1** and press **[Enter]** to accept the default, or enter another IP address and press **[Enter]**.

Result: The installation program displays a prompt that shows the default name of the SMS machine.

If a Secondary or Compute Server SMS is being installed, the system prompts for the IP address of the Primary SMS so the SMS database can be accessed. Enter the IP address.

If you are installing a Secondary SMS or Compute Server, skip to Step 20.

16 For Primary SMS installations, the installation program begins to initialize the database.

This process will take several minutes.

For Primary SMS installations, a master key is generated and displayed in the lower half of the SMS Setup screen. The purpose of the master key is to protect the root certificate used to authenticate communication between the SMS and the Brick devices that it manages. Write the master key down and keep it in a secure place. You will need the key to recover if you should forget the Administrator password and become locked out of the SMS.

17 Press **[Enter]** to continue with the installation.

Result: If you are installing a Primary SMS, the installation program prompts you to create an SMS Administator ID.

This is the Admin ID that you or another administrator uses to log into the SMS.

A valid Admin ID contains a maximum of 16 characters. Keep a record of the Admin ID in a secure place. You will need this ID to log into the SMS after the installation is completed.

18 Enter the Admin ID and press **[Enter]**.

Result: The installation program prompts you to enter a password.

A valid password contains up to 42 characters. The password is case-sensitive. Keep a record of the password, which will be required to log into the SMS after the installation is completed.

19 Enter the password and press **[Enter]**, then enter the password a second time and press **[Enter]**.

Result: The installation program displays a message indicating that the initial setup is complete.

20 **Important!** In some cases, even if the installation is successfully completed, you may receive the following message:

```
This program might not have installed correctly
```

followed by a series of options. If this occurs, choose

`This program installed correctly` to proceed with the installation.

Press **[Enter]** to continue with the installation.

Result: The remaining files are installed and all SMS services are started.

When the installation is completed, the *Solaris*® command prompt is displayed.

END OF STEPS

Configuration Assistant

The Configuration Assistant is a utility that allows you to set or modify certain system-wide parameters which affect the SMS application's operation and performance. You can open the Configuration Assistant after the SMS installation has completed to change SMS parameters now, or keep the default parameter settings and modify them at a later point. Note that the SMS services or the SMS Navigator may have to be restarted for some changes to take effect.

For additional details about the Configuration Assistant, refer to the *Using the Configuration Assistant* chapter in the *SMS Administration Guide*.

□

To Manually Un-Install SMS

When to use

This procedure is not required or recommended for upgrading to the current “official” SMS release that you purchased. As part of its software upgrade program, the SMS automatically installs, upgrades to the current release, and un-installs the previous SMS release.

However, if you have installed an Evaluation copy of the SMS software, you should manually un-install the Evaluation copy using this procedure before upgrading to an “official” SMS release. You should skip Step 2 of this procedure if you want to preserve your configuration data.

This procedure can be used, for example, to manually un-install the SMS software from a de-commissioned server.

Task

Complete the following steps to manually un-install the SMS.

1. Login as user root.

2. In a Terminal window, run the command `pkgrm LUsms`.

3. For final removal, you can backup or delete the contents of the SMS directory (Example: *c:/opt/isms/lmf*

END OF STEPS

□

To Upgrade the SMS Software

When to use

Use this procedure to upgrade the SMS to the current software release.

Before you begin

Before you begin this procedure, it is recommended that you perform a manual backup of the Primary SMS database in the event of a system failure during the upgrade installation.

For instructions on how to perform a manual backup of the SMS database, refer to the *Manual Backup* section of the *SMS Administration Guide*.

Should you need to restore the backed up Primary SMS database, refer to the *To Restore SMS Data on a Primary SMS* section in the *SMS Administration Guide*.

Procedure

Complete the following steps to upgrade the SMS to the current software release.

1 Log in as user `root`.

2 With the CD-ROM in the drive and a terminal window displayed, enter:

cd /cdrom/cdrom0/Solaris

> **Result:** The system changes to the directory on the CD-ROM that contains the installation script.

3 Enter `sh installLSMS` to begin the installation.

> **Result:** The installation program displays a series of prompts.

4 Press **[Enter]** to display the license agreement and enter `Y` to accept these terms and conditions.

> **Result** The installation program will display a warning indicating that you should only upgrade to the current software release after the IKE on the Brick feature has been enabled on the SMS and all Bricks.

5 If you are ready to upgrade, enter `Y` to proceed.

6 Press **[Enter]** to display the installation notes and type **Y** to accept the terms of the notes.

7 Enter the installation key as provided after registering the license key.

Result The installation program displays a message indicating a previous version of the SMS is installed, and prompts you to upgrade.

8 Enter `Y` to proceed, and enter `Y` a second time when the program prompts you to remove the previous version of the SMS. Enter `Y` a third time when the program warns that the script will be executed as super-user.

Result The previous version of the SMS is removed.

9 During an upgrade, the install directory defaults to the value specified during the initial installation of the SMS. Press **[Enter]** to keep the default directory, or enter a different directory and press **[Enter]**.

10 During an upgrade, the logs directory defaults to the value specified during the initial installation of the SMS. Press **[Enter]** to keep the default directory, or enter a different directory and press **[Enter]**.

11 The installation program defaults to the the Web Server **TYPE** entered during the initial installation of the SMS. Press **[Enter]** to accept the default, or manually enter `HTTP` or `HTTPS` to change the web server type.

`HTTPS` relies on a digital certificate, and is, therefore, substantially more secure. If administrators will be logging into the SMS remotely, it is a good idea to use `HTTPS`.

To obtain and install a digital certificate, see the *Digital Certificates* section in the *SMS Policy Guide*.

Important! The values for the Web Server **TYPE** and **PORT** can be changed using the SMS Configuration Assistant after successful completion of the software upgrade.

Result: The installation program prompts for entry of the port that the web server will be listening on.

.

12 The installation program defaults to the value that was entered during the initial installation of the SMS. Press **[Enter]** to accept the default, or manually enter another port value and press **[Enter]**.

`80` is the standard port for HTTP; `443` is the standard port for HTTPS.

Result: After configuration of the web server is complete, the installation program displays the following message:

```
This package contains scripts which
will be executed with super-user permission
during the process of installing this package.
```

13 Enter **Y** to proceed with the installation.

Result: The installation program begins to copy files to the target directory and echoes each of the file copies to the console window.

When all of the files have been copied, the installation program prompts you to indicate whether this is a Primary, Secondary, or Compute Server SMS.

As of Release 8.0, the SMS type is pre-determined by the installation key that is used. The installation program displays a prompt that shows the default name of the SMS machine.

14 Press **[Enter]** to accept the default, or type another name for the SMS and press **[Enter]**.

Result: If you are upgrading a Primary SMS, the installation program starts to upgrade the SMS database. Upgrade of the SMS database may take several minutes.

If you are upgrading a Secondary or Compute Server SMS, the remaining files and settings are now installed and all SMS services are started. If the upgrade installation is for a Secondary SMS or a Compute Server, the system prompts you for the IP address of the Primary SMS or the SMS to which the Compute Server will home. When the installation is completed, the *Solaris*® command prompt is displayed. The upgrade is complete at this point.

If you are upgrading a Primary SMS, go to Step 15.

15 If you are upgrading a Primary SMS, the installation program prompts you to select the type of upgrade:

- 1 - Normal Upgrade
- 2 - If you forgot the Admin password
- 3 - If you forgot the master key

Result: The installation program prompts you to enter the SMS Admin ID.

16 Enter the SMS Admin ID and press **[Enter]**.

Result: The installation program prompts you to enter the Admin ID password.

17 Enter the password and press **[Enter]**.

In some cases, even if the installation is successfully completed, you may receive the following message:

```
This program might not have installed correctly
```

followed by a series of options. If this occurs, choose

`This program installed correctly` to proceed with the installation.

The remaining files and settings are now installed and all SMS services are started.

When the installation is completed, the *Solaris*® command prompt is displayed.

END OF STEPS

Configuration Assistant

The Configuration Assistant allows you to set certain system-wide parameters. You can open the Configuration Assistant now to change SMS system parameters now, or keep the default parameter settings and modify them at a later point.

For additional details about the Configuration Assistant, refer to the *SMS Administration Guide*.

□

What To Do Next

Overview

Congratulations! You have successfully installed or upgraded the required software and have a working SMS running the current software release. The installation accomplished the following:

1. It placed an entry called **Alcatel-Lucent Security Management Server** in the Application menu of the Common Desktop Environment (CDE). This menu is accessed by right-clicking on the desktop, and it enables you to:
   - Run the SMS application using the SMS Navigator or, if previously installed, the SMS Remote Navigator
   - Open the local SMS Log Viewer
   - Access the four SMS utilities (Configuration Assistant, New Feature Setup, SMS Service Status, and SMS Schedule Editor)
   - Start and stop the SMS services
   - Restart SMS services
2. It created an SMS Administrator account with full privileges that you, or another administrator, can use to log into the SMS and begin work.

   If you are using CDE, Workspace menu items have been added for your convenience. To see the new menu items, update the Workspace menu and restart the Workspace Manager by doing the following:

   a. Right-click to bring up the Workspace menu.

   b. Select **Tools > Desktop Controls > Extras > Restore Workspace Menu**.

You are now ready to begin deploying Brick devices in the network as firewalls and VPN tunnel endpoints. The best place to begin is the *Getting Started* chapter in the *SMS Administration Guide.*

The *Getting Started* chapter in the *SMS Administration Guide* explains how to log on and off the SMS, and describes the basics about using the SMS software in detail. It also provides guidelines for setting up the objects using the SMS interface and describes where to find information in the SMS documents to enable you to perform basic tasks.

If you have purchased any optional feature licenses, run the New Feature Setup utility on the Primary SMS to install the optional feature installation keys to enable the features. For more information about the New Feature Setup utility, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

□

5 SMS on a Linux Server Platform

Overview

Purpose

This chapter explains how to install or upgrade the SMS application on a Linux server platform. It also includes a procedure for manually de-installing the application if necessary.

Contents

Introduction	66
Minimum Hardware/Software Requirements	68
Pre-Installation Requirements (Clean Installations)	69
To Install the SMS Application (Clean Installation)	72
Post-Installation Steps	78
To Manually Un-Install SMS	79
To Upgrade the SMS Software	80
What To Do Next	84

□

Introduction

Overview

The SMS application can be installed on a host running Red Hat Enterprise Linux 4 (RHEL4) or Red Hat Enterprise Linux 5 (RHEL5).

> **Important!** If you are migrating from a *Windows*® or *Solaris*® server platform to a Linux host running SMS Release 9.4, and want to use the configuration database from a prior SMS release, you must manually back up the SMS database to a USB drive or *ftp* server using the `backup` database utility. Only SMS Release 9.2 and Release 9.3 database structures are supported on a Linux host running SMS Release 9.4. For additional pre-installation steps that must be followed, refer to the section "Pre-installation steps for Linux installations" (p. 72).

Upgrades

CAUTION

Service-disruption hazard

Security Precaution

It is highly recommended that the SMS server be protected with a Brick device and that as little as possible be put on the same trusted subnet as the SMS.

SMS configurations

The SMS can be deployed in one of the following configurations:

- A Primary SMS (stand-alone configuration)
- A Primary SMS and Secondary SMS (in a redundant configuration)
- A Primary SMS and up to three Secondary SMSs (Multi-Site configuration)
- A Primary SMS and up to three Secondary SMSs, each with up to five Compute Servers (Compute Server configuration)

Multi-Site SMS configuration

A multi-site SMS configuration consists of a Primary SMS and up to three Secondary SMSs. The Primary SMS and Secondary SMS (s) share the same database, which is updated periodically across the network. The Primary SMS and Secondary SMS(s) are simultaneously active, synchronizing status and configuration at the same time.

Compute servers

To maximize scalability of the SMS/Brick security solution, the SMS provides the option of adding a separate set of servers called Compute Servers (CSs), which are associated with a Primary or Secondary SMS and act as collection points for Brick log traffic. Using a CS to collect Brick log data frees up computing resources on the SMS itself and extends the number of Brick devices and total log traffic that can be handled. Each Brick device managed by the SMS can be homed to one of the associated CSs or the managing SMS for logging purposes.

Up to five Compute Servers can be configured for a Primary or Secondary SMS.

Implementing Primary SMS/Secondary SMS configurations

During the installation of the Secondary SMS, there is a point at which the Secondary SMS attempts to contact the Primary SMS to replicate the Primary SMS database on the Secondary SMS. If the Secondary SMS cannot contact the Primary SMS, correct the problem and retry the operation on the Secondary SMS.

For reasons of security, we strongly recommend that you deploy a Brick device ″in front″ of the Primary and Secondary SMS(s) to protect all servers.

To ensure that the Primary SMS and Secondary SMS(s) can contact each other through both Brick devices, follow the course of action outlined below when you order the installation:

1. Install the Primary SMS first. The two installation procedures in this chapter provide step-by-step instructions for a new installation and an upgrade installation.
2. Once the Primary SMS is operational, use it to configure two Bricks and assign the pre-configured ruleset *administrativezone* to the ports that will be connected to the SMS. Refer to the *Configuring Brick Ports* section in the *SMS Administration Guide* for instructions on how to do this.
3. Connect the Primary SMS to the port on one Brick, and the host that will be the Secondary SMS to the port on the other. Then, deploy the two Bricks: the primary SMS and the host that will be the Secondary SMS in the network.
4. To ensure that the Primary SMS and remote host can communicate, add a ping rule (*dir=both, source=**, *dest=**, *service=ping_request*,*action=pass*) to the *administrativezone* ruleset, and then ping the host from the SMS. Once the ping is successful, remove the rule for security reasons. (Refer to the *Brick Zone Rulesets* section in the *SMS Policy Guide* for instructions on how to create a rule.)
5. When you have established that the two SMS servers can communicate, install the Secondary SMS.

□

Minimum Hardware/Software Requirements

Minimum hardware requirements

The host on which you install the SMS application that is running the Linux RHEL4 or RHEL5 operating system must meet the following minimum hardware requirements:

- 2 GHz dual-core or greater processor
- At least 1GB of RAM
- Swap space at least as large as the amount of RAM
- 1 GB or greater free disk space in */tmp*
- 1GB or greater free disk space in the partition where the SMS application is to be installed
- USB 2.0 port. Alcatel-Lucent approved USB floppy drives are supported for hosts with only USB ports.
- Ethernet interface card
- Video card capable of 1024 x 768 resolution (65,535 colors)

  Important! A floppy drive is only required if managing Alcatel-Lucent *VPN Firewall Brick*™ Model 20, 80, or 1100/1100A Security Appliances. A USB port is required for managing all other Brick models.

Minimum software requirements

The following software is required to run the SMS application on a Linux server platform:

- Red Hat Enterprise Linux 4 (RHEL4) or Red Hat Enterprise Linux 5 (RHEL5)
- A browser such as *Microsoft*™ *Internet Explorer*® or Firefox to view SMS reports and online help
- Adobe Acrobat Reader. This application is used to display the on-line manuals.

□

Pre-Installation Requirements (Clean Installations)

Overview

Before you proceed with the actual installation of the SMS application for the first time on a host, some pre-installation steps are required:

1. Resolve potential web server port conflicts.
2. Install Adobe Acrobat Reader
3. Obtain the SMS installation keys.

Resolve potential web server port conflicts

The SMS application includes a web server. If there is another web server running on the host machine (such as Apache), you must either:

- Shut the web server down
  Note: If there is an entry in the /etc/inittab file to automatically start your web server, you must remove or disable this entry so that it does not conflict with the SMS server.
  or
- Select a different port for the SMS web server when prompted by the installation program

Port 80 is the default SMS web server port. In the event that another web server is already using port 80 (such as Apache), you must either change the port on that web server or select a different port when configuring the SMS web server.

Install Adobe Acrobat Reader

Adobe Acrobat Reader is required to view the on-line documentation that is provided with the application. A copy of this application can be downloaded from the Adobe website, http://www.adobe.com.

Obtain the SMS installation keys

To install the SMS application, two keys are required:

- *Software license key*
  The software license key is provided with the product. You will need this key to register the product and to obtain the installation key, which is required to perform the installation.
- *Installation key*
  The installation key is required to install the product.

For complete instructions on how to register a software license key and obtain an installation key, refer to Appendix A, “Registering SMS Software License Keys and Obtaining Installation Keys”.

There are six categories of installation keys available, depending on the type of installation you are performing. The six categories are:

- Primary SMS (Clean Install)
- Upgrade for Primary SMS
- Secondary SMS associated with a Primary SMS (Clean Install)
- Upgrade for Secondary SMS associated with a Primary SMS
- Compute Server SMS (Clean Install)
- Upgrade for Compute Server SMS

The installation key that you enter, which sets parameters affecting the operation of the SMS, cannot be changed.

You will be prompted to enter the software installation key during the installation process. If you have purchased any optional feature licenses, refer to the procedure "To register a software license key and obtain an installation key for upgrade or feature option" (p. 101) in Appendix A, "Registering SMS Software License Keys and Obtaining Installation Keys" for instructions on how to register these license keys and obtain installation keys that you will use to enable these features on your SMS. Optional features are enabled after the software installation/upgrade is complete, using the New Feature Setup utility.

To enable optional features, run the New Feature Setup utility on the Primary SMS after you finish the software installation process and enter your optional feature installation keys. Optional features enabled on the Primary SMS are also automatically enabled on all associated Secondary and Compute Server SMS machines. It may be necessary to restart services to enable some features.

For more information on New Feature Setup, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

Software patches and documentation updates

It is a good idea to check the VPN Firewall Product Registration and Support website (https://vpn-firewall-brick.alcatel-lucent.com) periodically for patches and documentation updates issued since you purchased the product.

If you are installing the SMS application for the first time, the installation keys that you will receive are only for an initial installation of the current software release. If you are upgrading from an earlier release of the SMS software, these installation keys are only for an upgrade to the current software release. When installing a patch version of the SMS application, you do not need an installation key.

Running OS firewall and security software and the SMS

If you have enabled OS firewall or security software on a host that is also running the SMS application, it must be configured to allow the SMS services to run and to allow access to ports that the SMS uses to communicate with Brick devices and other SMSs/Compute Servers (CSs). For a list of ports that are used by the SMS to communicate with other components in the Alcatel-Lucent VPN Firewall Solution, refer to the *VPN Firewall Solution Ports* appendix in the *SMS Administration Guide*.

□

To Install the SMS Application (Clean Installation)

When to use

Use this procedure to install the SMS application for the first time on a host.

Pre-installation steps for Linux installations

Before proceeding with the actual installation, some preliminary steps must be taken to prepare the host environment:

1. If you are migrating from a previous SMS release on a *Windows*® or *Solaris*® server to Release 9.4 installed for the first time on a Linux host, manually back up the current SMS database to a USB drive or *ftp* server using the `backup` database utility. For instructions on how to perform a manual backup of the SMS database, refer to the *Manual Backup* section of the *SMS Administration Guide*.
2. In the backup directory which contains the files that you just backed up, edit the *config.ini* file to ensure that:
   - the root directory statement (`Rootdir=`) has the correct directory path where the SMS will be installed on the Linux host.
   - the root Document statement (`DocumentRoot=`) has the correct directory path where the SMS on-line documents will be stored on the Linux host.
   - the root log statement (`logDir=`) has the correct directory path where the SMS logs will be stored on the Linux host.
   - the operating system statement (`OS=`) is set to UNIX.

   The following shows an example of how these directory path statements should be defined in the *config.ini* file:

   ```
   Rootdir=/opt/isms/lmf
   DocumentRoot=/opt/isms/lmf/httpdocs/LSMS
   logDir=/opt/isms/lmf
   OS=UNIX
   ```

After checking the directory path statements and making any necessary modifications, write and save the *config.ini* file.

> **Important!** The SMS GUI requires X-Windows software to be running. If you are running the Linux OS software at Level 3, you must change the run level from Level 3 to Level 5 before installing the SMS software; switching the Linux OS to run at Level 5 will automatically start the X-Windows services required for the SMS GUI. After the SMS installation has been successfully completed, you can change the Linux run level back to Level 3 if desired.

Procedure

Complete the following steps to install the SMS application for the first time on a host.

1 Log in as user `root`.

2 With the CD-ROM in the drive, locate this directory on the CD-ROM:

Linux

3 Enter `./lsms-9.4.xxx.bin`, where *xxx* is the build number of the software, to start the installation program.

> **Result** The installation program is started. The first in a series of screens is displayed, with an introduction to the InstallAnywhere installation program and some general tips about how to use the program. It also advises you to quit any programs that are running before continuing with the installation of the SMS application.

4 Click **Next** to proceed to the next installation screen.

> **Result** The next screen displays the license agreement and usage terms of the SMS application software, and asks if you accept the terms of the license agreement.

5 Accept the terms of the license agreement to proceed with the installation and click **Next** to proceed to the next installation screen.

> **Result** The next screen displays the default destination directory/folder where the SMS will be installed, with options to choose another directory/folder to install the product or restore the default directory/folder entry.

6 Leave the default directory/folder for installing the SMS application or click **Choose** to display a Browse window and choose a different destination directory/folder for installing the application.

To restore the original default directory/folder entry, click **Restore Default Folder**.

After entering the destination directory/folder for where the SMS application will be installed, click **Next** to proceed to the next installation screen.

> **Result** The next screen displays the default destination directory/folder where the SMS log files will be stored, with options to choose another directory/folder for storing the log files or restore the default directory/folder entry.

7 Leave the default directory/folder for storing the SMS log files or click **Choose** to display a Browse window and choose a different destination directory/folder for where the log files will be stored.

To restore the original default directory/folder entry, click **Restore Default Folder**.

After entering the destination directory/folder for where the log files will be stored, click **Next** to proceed to the next installation screen.

> **Result** The next screen displays the installation release notes about the major features and enhancements in the release.

---

8 Review the installation release notes and click **Next** to proceed to the next installation screen.

> **Result** The next screen displays information about the installation and log files folder and information about disk space requirements for the installation.

---

9 Review the information provided and click **Next** to proceed to the next installation screen.

> **Result** The next screen displays a field for entering the installation key for the SMS release being installed.

---

10 In the **Installation Key** field, enter the installation key and click **Next** to proceed to the next installation screen.

> **Result** The next screen displays options for configuring the SMS web server for HTTP or HTTPS. The web server is used for downloading and displaying the SMS reports and online documentation.

---

11 Choose **HTTP** (the default) or **HTTPS** for the web server.

HTTPS relies on a digital certificate, and is, therefore, substantially more secure. If administrators will be logging into the SMS remotely, it is recommended that HTTPS is used.

To obtain and install a digital certificate, refer to the *Digital Certficates* section of the *SMS Policy Guide*.

After selecting the web server configuration, click **Next** to proceed to the next installation screen.

> **Result** The next screen prompts you to enter the port on which the web server will be listening.

---

12 Leave the default web server listening port or enter a new port value.

Port `80` is the standard port for HTTP. Port `443` is the standard port for HTTPS.

After entering the web server listening port, click **Next** to proceed to the next installation screen.

Result The next screen asks if the operating system is already running the SNMP Agent on the Linux machine.

13 An SMS SNMP Agent will be installed as part of the application. If there is already a Linux OS SNMP Agent or some other third party SNMP Agent software installed on this machine, you must specify the port so SMS can communicate with this agent.

Choose **Yes** (the default) if the Linux OS SNMP Agent or some other third party SNMP Agent software is running on this machine.

Choose **No** if the SMS SNMP Agent will be the only SNMP Agent on this machine.

Result If you choose **Yes**, the next screen displayed asks for the listening port for the SNMP Agent on the Linux machine. Click **Next** and go to Step 14.

If you choose **No**, click **Next** and go to Step 15.

14 If you chose **Yes** in Step 13, enter the listening port number for the Linux machine SNMP Agent.

The default port is **161**, which is the standard port for SNMP.

After entering the port number, click **Next** to proceed to the next installation screen.

The next screen prompts for the listening port number for the SMS SNMP Agent.

15 Enter the listening port number for the SMS SNMP Agent.

The default port for SNMP Agents is **161**. If there is a Linux OS SNMP Agent running on port 161, then the SMS SNMP Agent must be configured on a different port (such as **8161**).

After entering the port number, click **Next** to proceed to the next installation screen.

The next screen prompts you to specify the SNMP Read Community “community string”, which is used to authenticate NMS hosts that access the Linux host or SMS for management or configuration data.

16 Accept the SNMP Read Community default, **public**, or modify as needed.

Additional details about configuring the SNMP Agent software on the SMS and operating system are provided in the *Using the Configuration Assistant* and *Simple Network Management Protocol (SNMP)* chapters in the *SMS Administration Guide*.

17 Click **Install** at the bottom of the SNMP Read Community installation screen.

Result The installation of the SMS commences as a background process.

An SMS Setup screen is displayed, which prompts you for the IP address and name of the SMS host to be used. The program defaults to installing a Primary SMS for the first time on a new host.

18 Enter another IP address or leave the default IP address. Enter the name of the SMS host.

Click **OK**.

Result For Primary SMS installations, the installation program begins to initialize the database. This process will take several minutes.

If a Secondary or Compute Server SMS is being installed, the system prompts for the IP address of the Primary SMS so the SMS database can be accessed. Enter the IP address.

If you are installing a Primary SMS, a Provide Administrator ID screen is displayed, prompting you to enter an Admin ID and password.

19 Enter the Admin ID and password. Re-enter the password and click **OK**.

Result For Primary SMS installations, a master key is generated and displayed at the lower half of the SMS setup screen. The purpose of the master key is to protect the root certificate used to authenticate communication between the SMS and Brick devices that it manages. Write the master key down and keep it in a secure place. You will need this key to recover the system if you should forget the Administrator password and are locked out of the SMS.

A series of messages is displayed, indicating that the initial setup is complete.

20 Click **Continue** to continue with the installation.

Result The remaining files are installed and all SMS services are started.

21 Click **Next** to complete the installation process.

Result If the installation is successful, a screen is displayed indicating that the SMS has been successfully installed to the directory path specified during the installation procedure.

22 Click **Done** to quit the installer (program).

END OF STEPS

Configuration Assistant

The Configuration Assistant is a utility that allows you to set or modify certain system-wide parameters which affect the SMS application's operation and performance. You can open the Configuration Assistant after the SMS installation has completed to change SMS parameters now, or keep the default parameter settings and modify them at a later point.

For additional details about the Configuration Assistant, refer to the *Using the Configuration Assistant* chapter in the *SMS Administration Guide*.

□

Post-Installation Steps

Post-installation steps for migrating SMS database from *Windows*® or *Solaris*® server

If you performed a manual backup of the SMS database that was migrated from a *Windows*® or *Solaris*® server from a previous SMS release (following the instructions in the "Pre-installation steps for Linux installations" (p. 72) section), before restoring the SMS database for use with the new SMS release just installed on the Linux server, verify that the required modifications to the various path statements in the *config.ini*described in the section "Pre-installation steps for Linux installations" (p. 72) have been made. If not, make any necessary changes in the *config.ini* file under the backup directories and save it.

Restore the previously backed up database using the `restore` utility. For instructions on how to restore the SMS database, refer to the *To Restore SMS Data on a Primary SMS* procedure in the *SMS Administration Guide*. Before running the `restore` utility, stop all SMS services from the installation root directory by entering `./stopServices`. When the database restore is complete, restart the SMS services from the installation root directory by enter `./startServices`.

□

To Manually Un-Install SMS

When to use

This procedure is not required or recommended for upgrading to the current “official” SMS release that you purchased. As part of its software upgrade program, the SMS automatically installs, upgrades to the current release, and un-installs the previous SMS release.

However, if you have installed an Evaluation copy of the SMS software, you should manually un-install the Evaluation copy using this procedure before upgrading to an “official” SMS release. You should skip Step 3 of this procedure if you want to preserve your configuration data.

This procedure can be used, for example, to manually un-install the SMS software from a de-commissioned server.

Task

Complete the following steps to manually un-install the SMS.

1 Login as user `root` and `cd` to the directory */opt/isms/Uninstall_ALSMS*

Note: if you have chosen a non-default installation path, then `cd` to the directory `<LSMS ROOT>/Uninstall_ALSMS`

2 Run the command `./Uninstall_ALSMS`.

3 For final removal, you can backup or delete the contents of the SMS directory (Example: */opt/isms/lmf*).

END OF STEPS

□

To Upgrade the SMS Software

When to use

Use this procedure to upgrade the SMS to the current software release.

Before you begin

Before you begin this procedure, it is recommended that you perform a manual backup of the Primary SMS database in the event of a system failure during the upgrade installation.

For instructions on how to perform a manual backup of the SMS database, refer to the *Manual Backup* section of the *SMS Administration Guide*.

Should you need to restore the backed up Primary SMS database, refer to the *To Restore SMS Data on a Primary SMS* section in the *SMS Administration Guide*.

Procedure

Complete the following steps to upgrade to the current SMS release.

1 Log in as user `root`.

2 With the CD-ROM in the drive, locate this directory on the CD-ROM:

Linux

3 Enter `./lsms-9.4.xxx.bin`, where *xxx* is the build number of the software, to start the installation program.

Result The installation program is started. The first in a series of screens is displayed, with an introduction to the InstallAnywhere installation program and some general tips about how to use the program. It also advises you to quit any programs that are running before continuing with the installation of the SMS application.

4 Click **Next** to proceed to the next installation screen.

Result The next screen displays the license agreement and usage terms of the SMS application software, and asks if you accept the terms of the license agreement.

5 Accept the terms of the license agreement to proceed with the installation and click **Next** to proceed to the next installation screen.

Result The next screen displays the directory/folder where the SMS is currently installed. If the installer is unable to determine the current installation directory/folder, the default installation directory/folder is displayed.

6 If the displayed directory/folder for installing the SMS application is not correct, click **Choose** to display a Browse window and the directory/folder where the SMS application is currently installed.

After entering the destination directory/folder for where the SMS application will be installed, click **Next** to proceed to the next installation screen.

Result The next screen displays the default directory/folder where the SMS log files are currently stored, with options to choose another directory/folder for storing the log files or to restore the default directory/folder entry.

7 Leave the default directory/folder for storing the SMS log files or click **Choose** to display a Browse window and choose a different destination directory/folder for where the log files will be stored.

To restore the original default directory/folder entry, click **Restore Default Folder**.

After entering the destination directory/folder for where the log files will be stored, click **Next** to proceed to the next installation screen.

Result The next screen displays the upgrade installation release notes about the major features and enhancements in the release.

8 Review the upgrade installation release notes and click **Next** to proceed to the next installation screen.

Result The next screen displays information about the installation and log files folder and information about disk space requirements for the installation.

9 Review the information provided and click **Next** to proceed to the next installation screen.

Result The next screen displays a field for entering the installation key for the SMS release being installed.

10 In the **Installation Key** field, enter the installation key and click **Next** to proceed to the next installation screen.

Result The next screen displays a message that a previous version of SMS was found and asks if you would like to continue with the upgrade.

11 Choose **Yes** and click **Next** to proceed with the upgrade.

Result The uninstaller is launched. The uninstaller removes the previous version of the SMS software while preserving all of the configuration data.

12 Click **Uninstall** to remove the previous version of SMS software.

Result The Cleanup SMS Services window is displayed, the SMS services are stopped, and old software is removed.

13 Click **Enter** to continue.

Result The Uninstall Complete summary screen is displayed.

14 Click **Done** to dismiss the uninstaller and continue with the installation of the new SMS release.

Result The installation of the SMS commences as a background process.

An SMS Setup screen is displayed with the IP address, SMS Name, and SMS Type of the host being upgraded.

15 Click **OK**.

Result If the upgrade installation is for a Primary SMS, the Upgrade Options window is displayed. Go to Step 16.

If the upgrade installation is for a Secondary SMS or a Compute Server, the system prompts for the IP address of the Primary SMS or the SMS to which the Compute Server will home. Enter the IP address and click **OK**. The remaining SMS steps are completed. Go to Step 18.

16 Select one of the following upgrade types (this prompt is displayed only if you are upgrading a Primary SMS) and click **OK**.

- Normal upgrade. If you know the Admin ID and password from the previous version of the SMS, click the radio button for this option. You will be prompted to enter the Admin ID and password.
- Forgot password. If you forgot the Admin password from the previous release – but know the master key – select this option. You will be prompted to create a new password.
- Forgot master key. If you forgot the Admin password from the previous release – and do not know the master key – choose this option. You will have to create a new password for each administrator, and then make new USB drives or boot floppies and reboot each Brick from a floppy or USB drive.

Result The prompt for Admin ID and Password (for normal upgrade) or other onscreen instructions are displayed (for other upgrade types).

17 Enter the Admin ID and Password and click **OK** or follow the onscreen instructions for the upgrade type selected. The remaining SMS Setup steps are performed.

Result The status of the SMS Setup steps are displayed.

18 Click **Continue** to dismiss the SMS Setup window and continue with the installation.

Result The final configuration upgrades are performed and summarized on the SMS Setup summary window.

19 Click **Next** to complete the installation process.

Result The SMS Services are started. When all SMS services have been successfully started, the Install Complete window is displayed.

20 Click **Done** to quit the installer.

END OF STEPS

□

What To Do Next

Overview

Congratulations! You have successfully installed the required software and have a working SMS running the current software release. The installation accomplished the following:

1. It placed an entry called **Alcatel-Lucent Security Management Server** in the Linux menus.

   This entry enables you to:

   - Run the SMS application using the SMS Navigator
   - Open the local SMS Log Viewer
   - Access the four SMS utilities (Configuration Assistant, New Feature Setup, SMS Service Status, and SMS Schedule Editor)
   - Start and stop the SMS services
   - Restart SMS services
2. It created an SMS Administrator account with full privileges that you or another administrator, can use to log into the SMS and begin work.

You are now ready to begin deploying Brick devices in your network as firewalls and VPN tunnel endpoints. The best place to begin is the *Getting Started* chapter in the *SMS Administration Guide*.

The *Getting Started* chapter in the *SMS Administration Guide* explains how to log on and off the SMS, and describes the basics about using the SMS software in detail. It also provides guidelines for setting up the objects using the SMS interface and explains where to find information in the SMS documents to enable you to perform basic tasks.

If you have purchased any optional feature licenses, run the New Feature Setup utility on the Primary SMS to install the optional feature installation keys to enable the features. For more information about the New Feature Setup utility, refer to the *New Feature Setup* section in the *SMS Administration Guide*.

□

A Registering SMS Software License Keys and Obtaining Installation Keys

Overview

Purpose

This appendix provides instructions on how to register the SMS product and software license key, and obtain an installation key, which is needed to install a new or upgraded SMS release or feature option.

Contents

To Register a Software License Key and Obtain an Installation Key	86

□

To Register a Software License Key and Obtain an Installation Key

When to use

Use this set of procedures to register a software license key that comes with the SMS software or feature option key and to obtain an installation key for installing the software or feature option.

Separate procedures explain how to register a license key and obtain an installation key for the first time as a new user, how to register a license key and obtain an installation key for a software upgrade or feature option using a previously obtained installation key, and obtaining an installation key online through the VPN Firewall Product Registration and Support website, https://vpn-firewall-brick.alcatel-lucent.com.

Before you begin

Before you begin any of these procedures, make sure that you have the software license key that you received with the SMS software or feature option. You will need this key to register the product and obtain an installation key, which is required to perform the installation.

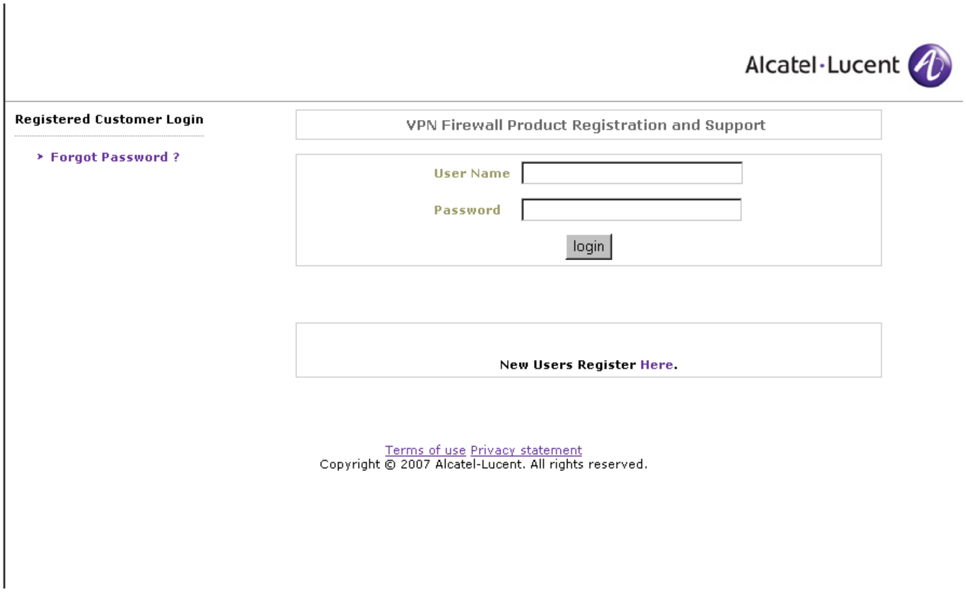
To register a software license key and obtain an installation key as a new user

Complete the following steps to register a software license key and obtain an installation key as a new user.

1 Go to https://vpn-firewall-brick.alcatel-lucent.com

Result The VPN Firewall Product Registration and Support Login page is displayed (Figure A-1, “VPN Firewall Product Registration and Support Login Page” (p. 87)).

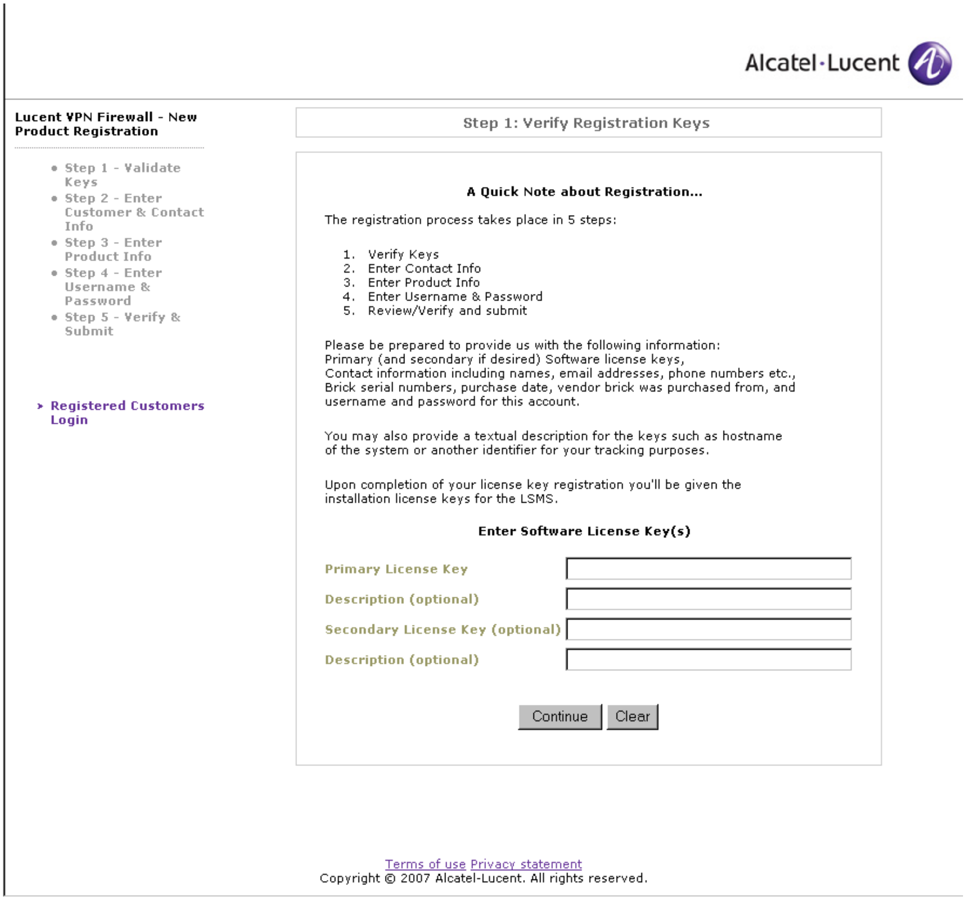
Figure A-1 VPN Firewall Product Registration and Support Login Page


Alcatel·Lucent
Registered Customer Login
› Forgot Password ?
VPN Firewall Product Registration and Support
User Name
Password
login
New Users Register Here.
Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

2 In the text at the bottom of the page **New Users Register Here**, click on the hyperlink word **Here**.

Result The first in a series of registration web pages is displayed for new users (Figure A-2, “Registration Web Page for New Users (Step 1: Verify Registration Keys)” (p. 88)).

Figure A-2 Registration Web Page for New Users (Step 1: Verify Registration Keys)



Alcatel·Lucent

Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys
- Step 2 - Enter Customer & Contact Info
- Step 3 - Enter Product Info
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

› Registered Customers Login

Step 1: Verify Registration Keys

A Quick Note about Registration...

The registration process takes place in 5 steps:

1. Verify Keys
2. Enter Contact Info
3. Enter Product Info
4. Enter Username & Password
5. Review/Verify and submit

Please be prepared to provide us with the following information:
Primary (and secondary if desired) Software license keys,
Contact information including names, email addresses, phone numbers etc.,
Brick serial numbers, purchase date, vendor brick was purchased from, and
username and password for this account.

You may also provide a textual description for the keys such as hostname of the system or another identifier for your tracking purposes.

Upon completion of your license key registration you'll be given the installation license keys for the LSMS.

Enter Software License Key(s)

Primary License Key

Description (optional)

Secondary License Key (optional)

Description (optional)

Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

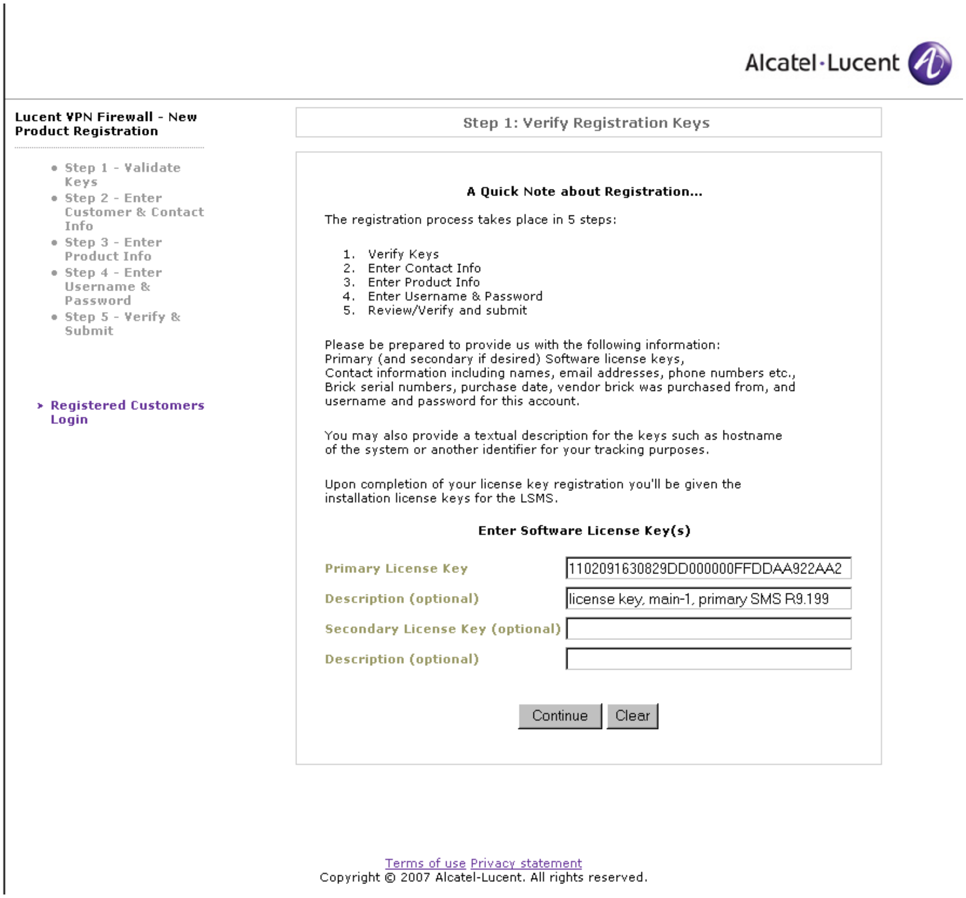
This web page is for entering the software license key that was provided when you purchased the product. Optionally, you can enter some text which describes the Primary and/or Secondary SMS or CS for which you are obtaining an installation key, such as server name, location, software release/version, or any other information that will help you associate the installation key with the specific machine or software release being installed.

3 Enter the software license key information for the Primary SMS (and Secondary SMS, if desired).

In the **Description (optional)** field, enter any descriptive information that would help identify the machine or software version for which the installation key is being obtained. The **Description** field is optional.

Figure A-3, “Verify Registration Keys Information (Example)” (p. 89) shows a sample entry.

Figure A-3 Verify Registration Keys Information (Example)



Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys
- Step 2 - Enter Customer & Contact Info
- Step 3 - Enter Product Info
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

› Registered Customers Login

Step 1: Verify Registration Keys

A Quick Note about Registration...

The registration process takes place in 5 steps:

1. Verify Keys
2. Enter Contact Info
3. Enter Product Info
4. Enter Username & Password
5. Review/Verify and submit

Please be prepared to provide us with the following information:
Primary (and secondary if desired) Software license keys,
Contact information including names, email addresses, phone numbers etc.,
Brick serial numbers, purchase date, vendor brick was purchased from, and
username and password for this account.

You may also provide a textual description for the keys such as hostname of the system or another identifier for your tracking purposes.

Upon completion of your license key registration you'll be given the installation license keys for the LSMS.

Enter Software License Key(s)

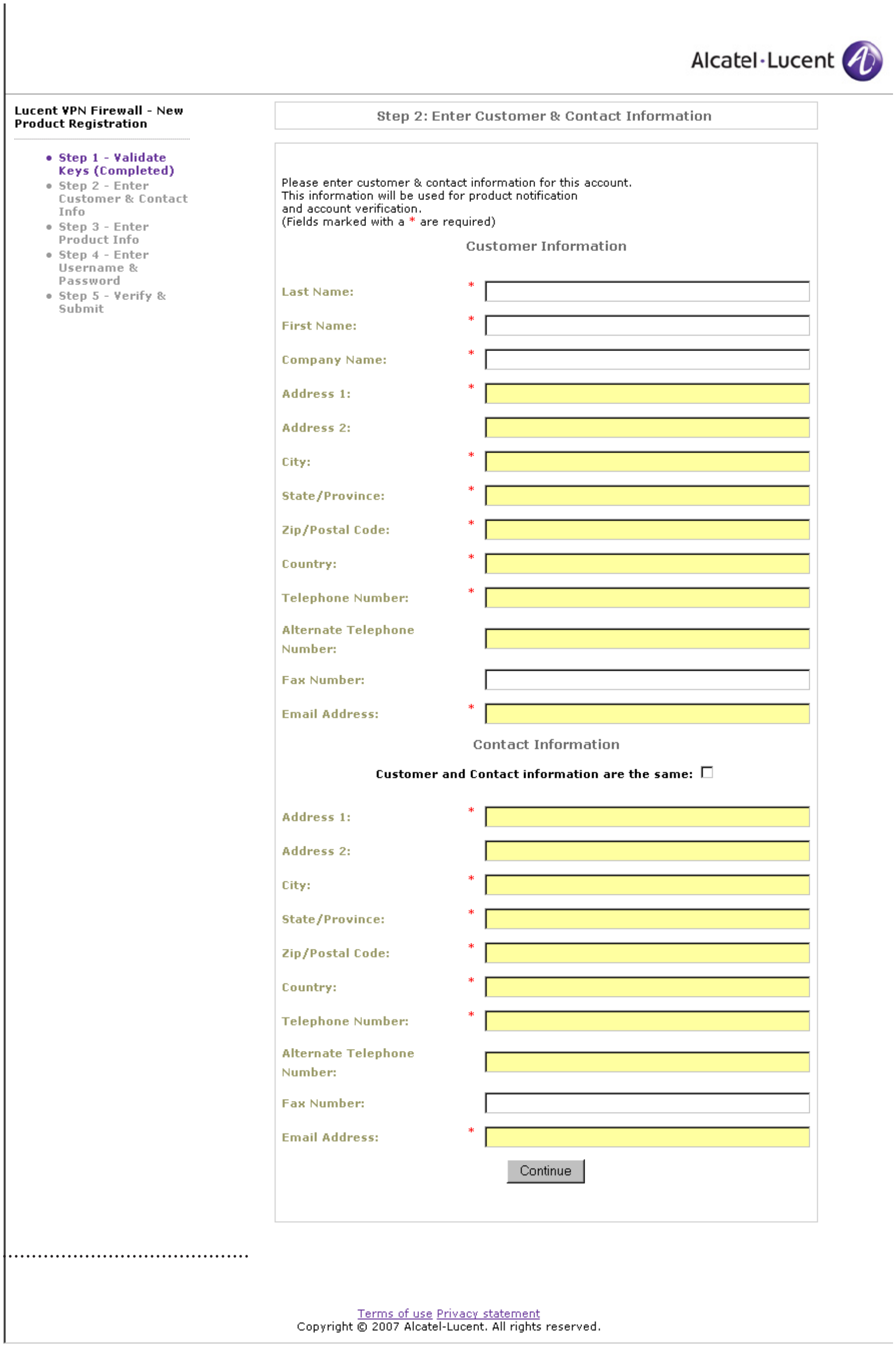
Primary License Key	1102091630829DD000000FFDDAA922AA2
Description (optional)	license key, main-1, primary SMS R9.199
Secondary License Key (optional)	
Description (optional)	

Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

4 Click **Continue** to proceed to the next registration web page.

Result The Customer Contact Information web page is displayed (Figure A-4, “Registration Web Page for New Users (Step 2: Enter Customer & Contact Info)” (p. 90)).

Figure A-4 **Registration Web Page for New Users (Step 2: Enter Customer & Contact Info)**



Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys (Completed)
- Step 2 - Enter Customer & Contact Info
- Step 3 - Enter Product Info
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

Step 2: Enter Customer & Contact Information

Please enter customer & contact information for this account.
This information will be used for product notification
and account verification.
(Fields marked with a * are required)

Customer Information

Last Name: *
First Name: *
Company Name: *
Address 1: *
Address 2:
City: *
State/Province: *
Zip/Postal Code: *
Country: *
Telephone Number: *
Alternate Telephone Number:
Fax Number:
Email Address: *

Contact Information

Customer and Contact information are the same: ☐

Address 1: *
Address 2:
City: *
State/Province: *
Zip/Postal Code: *
Country: *
Telephone Number: *
Alternate Telephone Number:
Fax Number:
Email Address: *

Continue

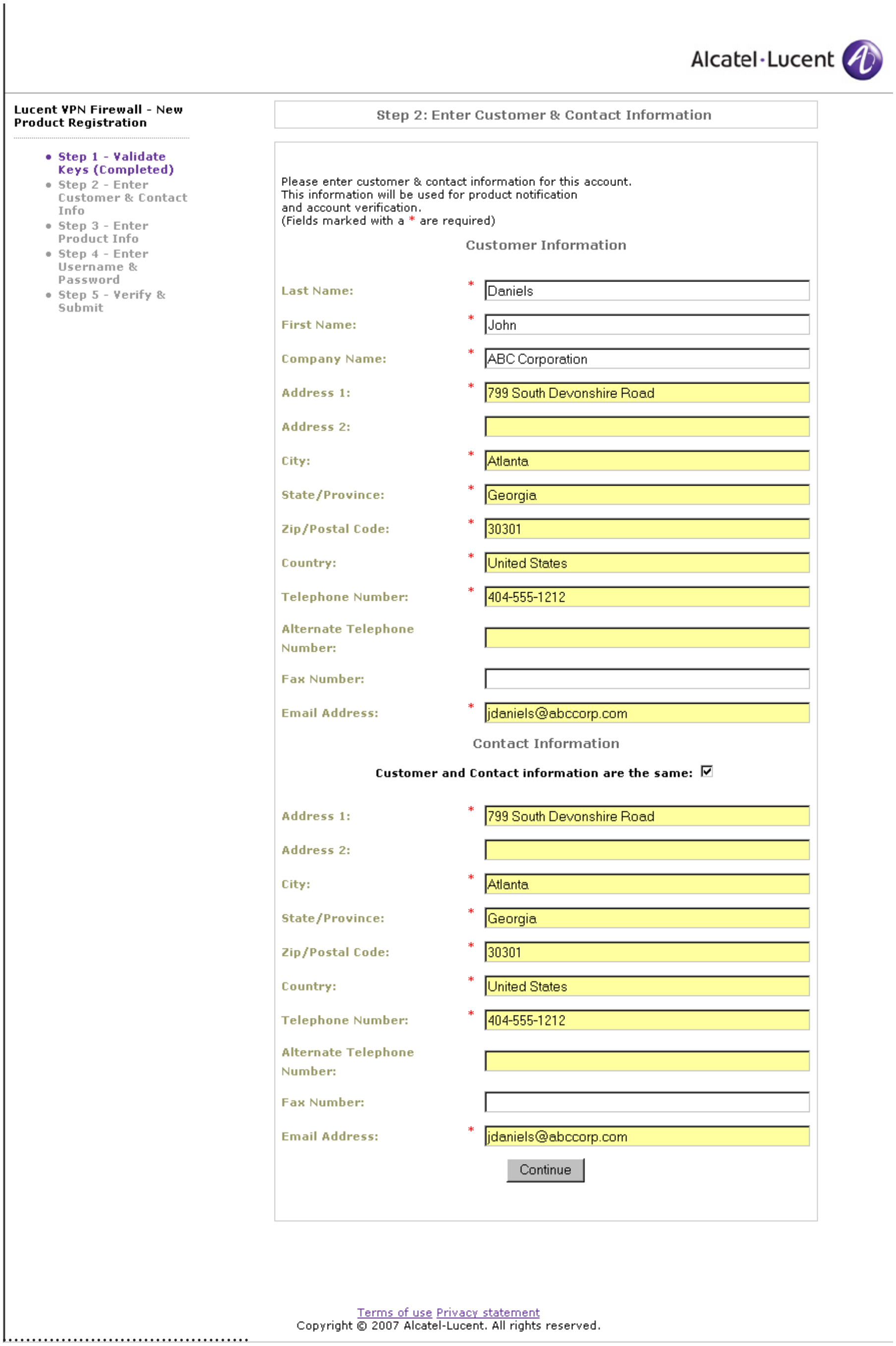
Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

This web page is for entering key customer contact information. Fields that are marked with an asterisk (*) require an entry.

5 Enter your customer information and key contact information if a specific person should be contacted about this product installation. Click the checkbox **Customer and Contact information are the same** if the general customer information and key contact information is the same. The Contact fields at the bottom of the page will be filled in with the same information that was entered at the top of the page.

Figure A-5, “Customer Information and Key Contact Information (Example)” (p. 92) shows a sample entry.

Figure A-5 Customer Information and Key Contact Information (Example)



Alcatel·Lucent
Lucent VPN Firewall - New Product Registration
Step 1 - Validate Keys (Completed)
Step 2 - Enter Customer & Contact Info
Step 3 - Enter Product Info
Step 4 - Enter Username & Password
Step 5 - Verify & Submit

Step 2: Enter Customer & Contact Information

Please enter customer & contact information for this account.
This information will be used for product notification
and account verification.
(Fields marked with a * are required)

Customer Information

Last Name:	*	Daniels
First Name:	*	John
Company Name:	*	ABC Corporation
Address 1:	*	799 South Devonshire Road
Address 2:		
City:	*	Atlanta
State/Province:	*	Georgia
Zip/Postal Code:	*	30301
Country:	*	United States
Telephone Number:	*	404-555-1212
Alternate Telephone Number:		
Fax Number:		
Email Address:	*	jdaniels@abccorp.com

Contact Information

Customer and Contact information are the same: ☑

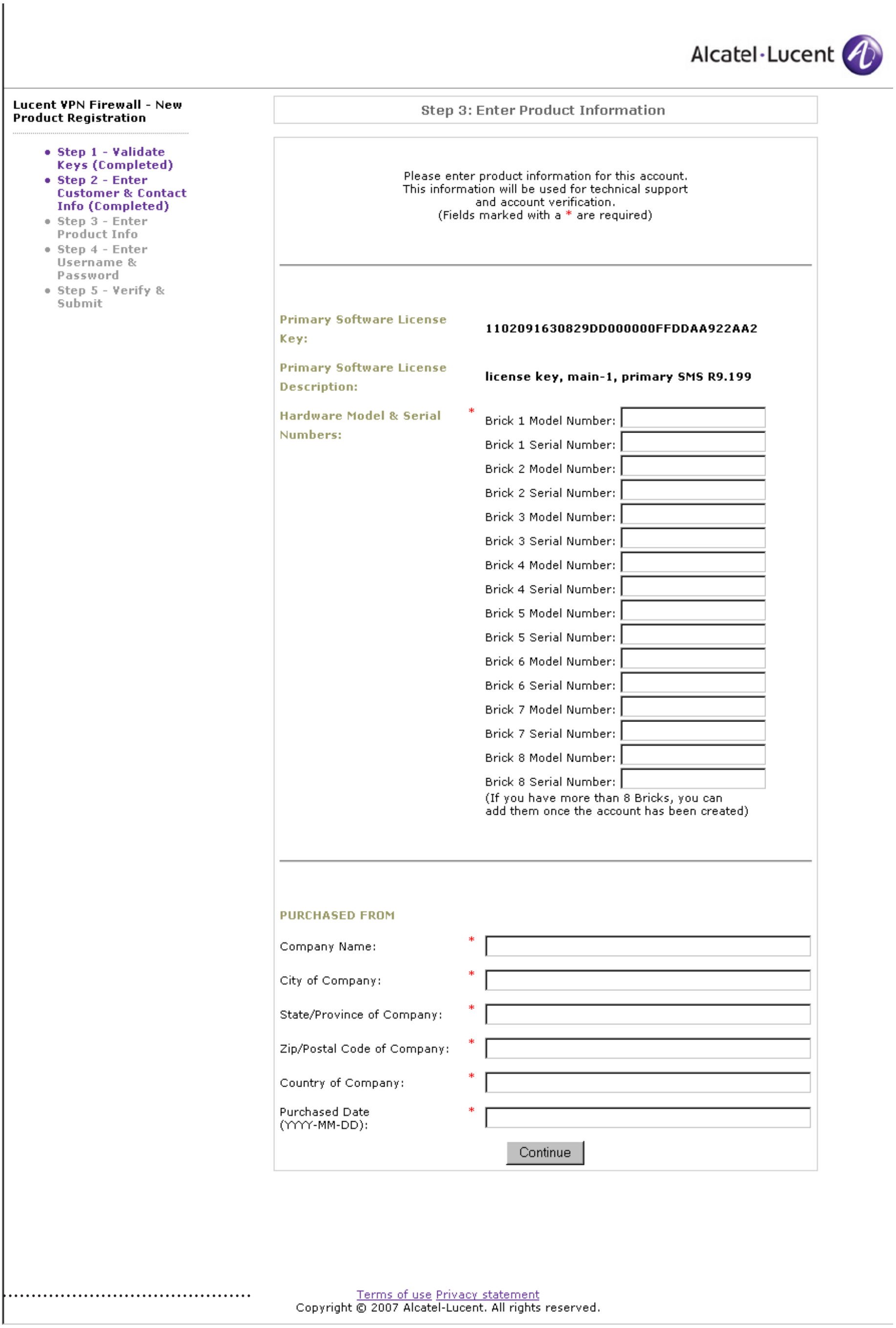
Address 1:	*	799 South Devonshire Road
Address 2:		
City:	*	Atlanta
State/Province:	*	Georgia
Zip/Postal Code:	*	30301
Country:	*	United States
Telephone Number:	*	404-555-1212
Alternate Telephone Number:		
Fax Number:		
Email Address:	*	jdaniels@abccorp.com

Copyright © 2007 Alcatel-Lucent. All rights reserved.

6 Click **Continue** to proceed to the next registration web page.

Result The Product Information registration web page is displayed (Figure A-6, “Registration Web Page for New Users (Step 3: Enter Product Info)” (p. 94)).

Figure A-6 Registration Web Page for New Users (Step 3: Enter Product Info)



Alcatel·Lucent

Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys (Completed)
- Step 2 - Enter Customer & Contact Info (Completed)
- Step 3 - Enter Product Info
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

Step 3: Enter Product Information

Please enter product information for this account.
This information will be used for technical support
and account verification.
(Fields marked with a * are required)

Primary Software License Key: 1102091630829DD000000FFDDAA922AA2

Primary Software License Description: license key, main-1, primary SMS R9.199

Hardware Model & Serial Numbers: *

Brick 1 Model Number:
Brick 1 Serial Number:
Brick 2 Model Number:
Brick 2 Serial Number:
Brick 3 Model Number:
Brick 3 Serial Number:
Brick 4 Model Number:
Brick 4 Serial Number:
Brick 5 Model Number:
Brick 5 Serial Number:
Brick 6 Model Number:
Brick 6 Serial Number:
Brick 7 Model Number:
Brick 7 Serial Number:
Brick 8 Model Number:
Brick 8 Serial Number:
(If you have more than 8 Bricks, you can
add them once the account has been created)

PURCHASED FROM

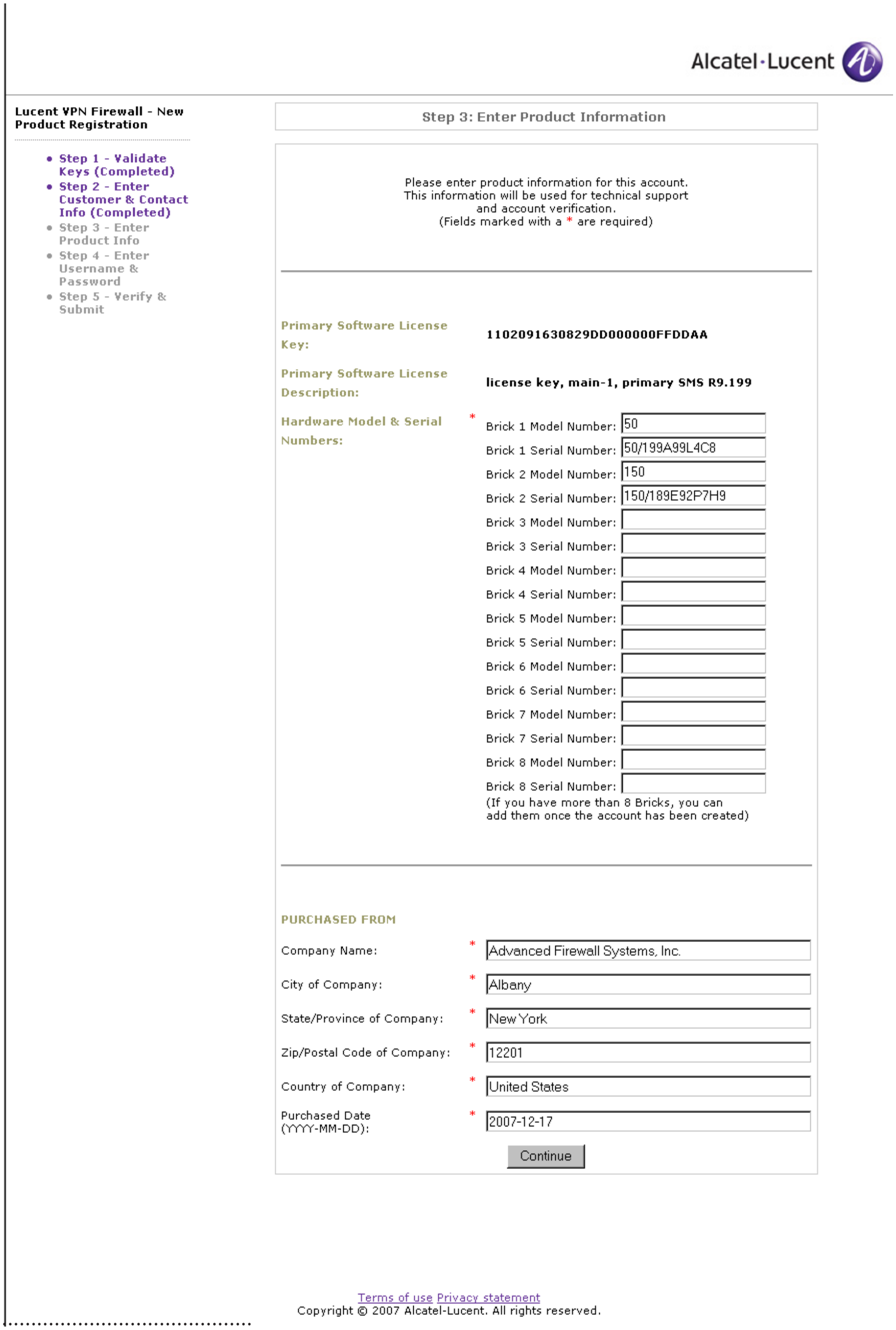
Company Name: *
City of Company: *
State/Province of Company: *
Zip/Postal Code of Company: *
Country of Company: *
Purchased Date (YYYY-MM-DD): *

This page is for recording the Bricks (by model and serial number) associated with this SMS or CS installation and information about the vendor where the Brick(s) were purchased.

7 Enter the Brick data and vendor information.

Figure A-7, “Brick Hardware and Vendor Information (Example)” (p. 96) shows a sample entry.

Figure A-7 Brick Hardware and Vendor Information (Example)



Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys (Completed)
- Step 2 - Enter Customer & Contact Info (Completed)
- Step 3 - Enter Product Info
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

Step 3: Enter Product Information

Please enter product information for this account.
This information will be used for technical support
and account verification.
(Fields marked with a * are required)

Primary Software License Key:		1102091630829DD000000FFDDAA
Primary Software License Description:		license key, main-1, primary SMS R9.199
Hardware Model & Serial Numbers:	*	Brick 1 Model Number: 50
		Brick 1 Serial Number: 50/199A99L4C8
		Brick 2 Model Number: 150
		Brick 2 Serial Number: 150/189E92P7H9
		Brick 3 Model Number:
		Brick 3 Serial Number:
		Brick 4 Model Number:
		Brick 4 Serial Number:
		Brick 5 Model Number:
		Brick 5 Serial Number:
		Brick 6 Model Number:
		Brick 6 Serial Number:
		Brick 7 Model Number:
		Brick 7 Serial Number:
		Brick 8 Model Number:
		Brick 8 Serial Number:
		(If you have more than 8 Bricks, you can add them once the account has been created)

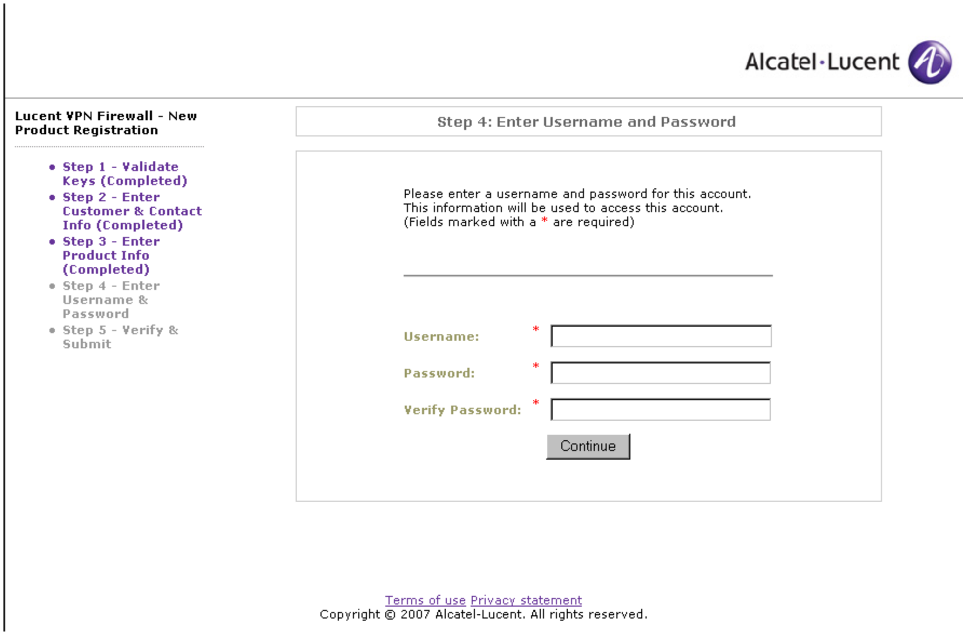
PURCHASED FROM

Company Name:	*	Advanced Firewall Systems, Inc.
City of Company:	*	Albany
State/Province of Company:	*	New York
Zip/Postal Code of Company:	*	12201
Country of Company:	*	United States
Purchased Date (YYYY-MM-DD):	*	2007-12-17

8 Click **Continue** to proceed to the next registration web page.

Result The Username and Password registration web page is displayed (Figure A-8, "Registration Web Page for New Users (Step 4: Enter Username & Password)" (p. 97)).

Figure A-8 Registration Web Page for New Users (Step 4: Enter Username & Password)



Alcatel·Lucent

Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys (Completed)
- Step 2 - Enter Customer & Contact Info (Completed)
- Step 3 - Enter Product Info (Completed)
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

Step 4: Enter Username and Password

Please enter a username and password for this account.
This information will be used to access this account.
(Fields marked with a * are required)

Username: *
Password: *
Verify Password: *

Continue

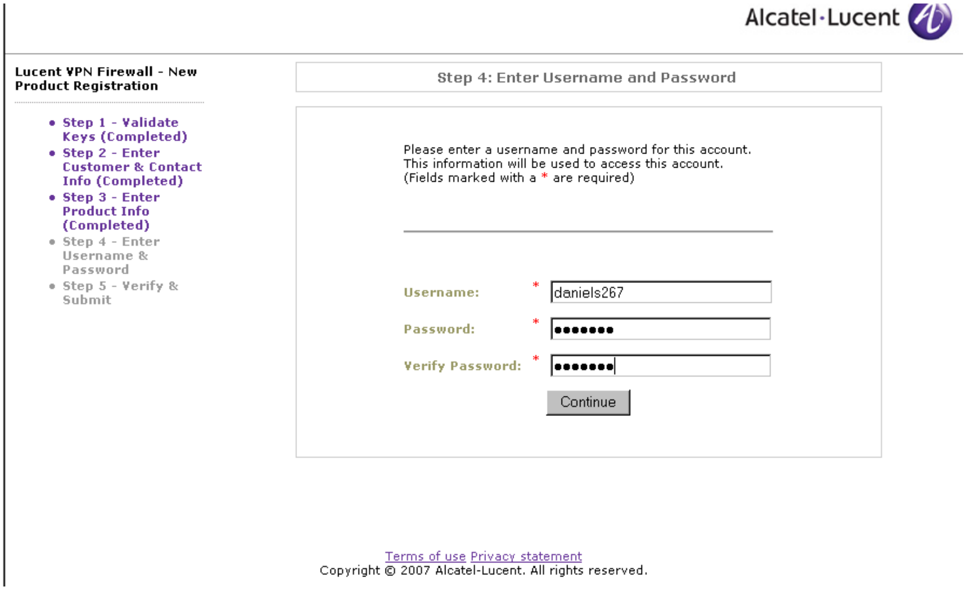
Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

This web page is for entering the username and password that you will use to access this Product Support and Registration website to register additional license keys and obtain additional installation keys.

9 Enter a username, password, and re-enter the password.

Figure A-9, “Username and Password Information (Example)” (p. 98) shows a sample entry.

Figure A-9 Username and Password Information (Example)



Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys (Completed)
- Step 2 - Enter Customer & Contact Info (Completed)
- Step 3 - Enter Product Info (Completed)
- Step 4 - Enter Username & Password
- Step 5 - Verify & Submit

Step 4: Enter Username and Password

Please enter a username and password for this account.
This information will be used to access this account.
(Fields marked with a * are required)

Username: * daniels267

Password: * ●●●●●●●

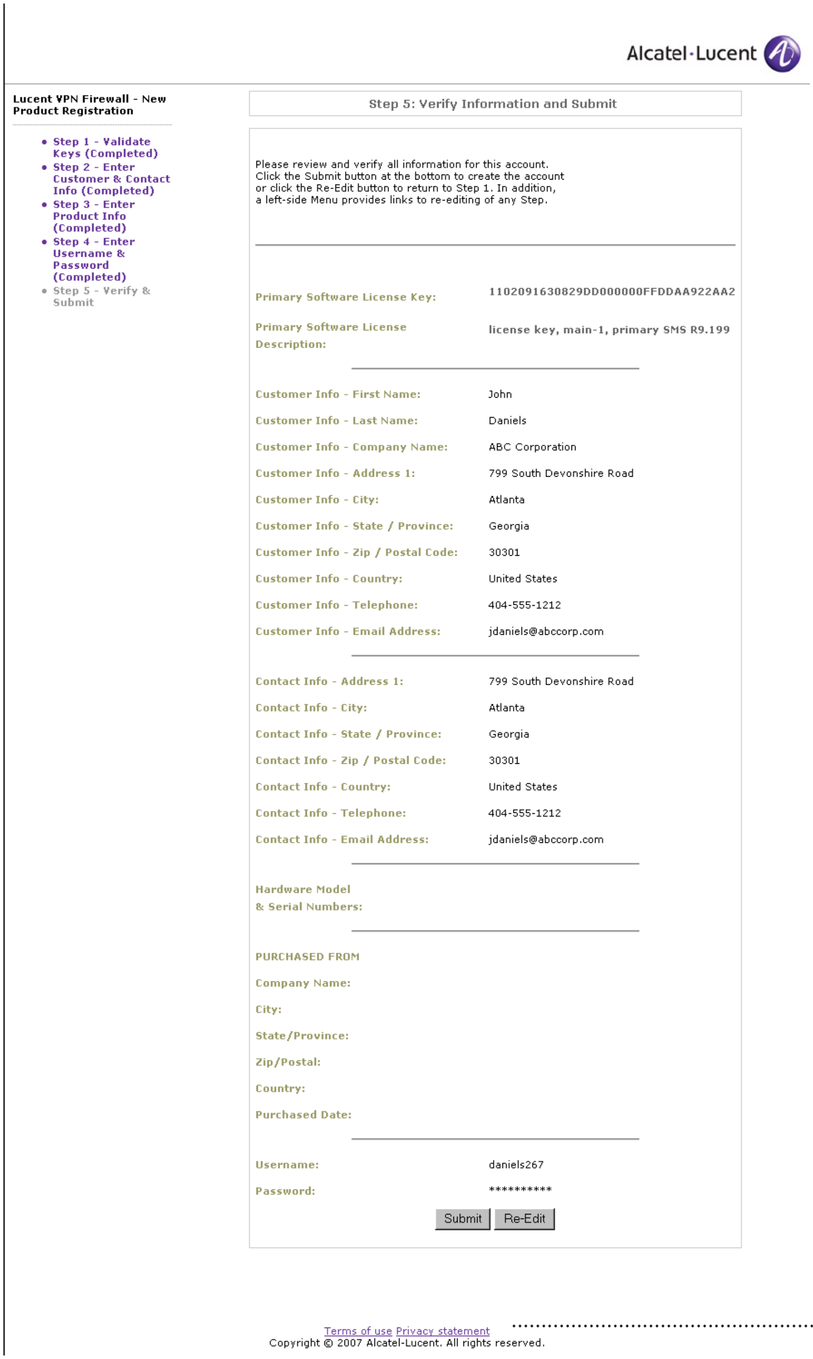
Verify Password: * ●●●●●●●

Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

10 Click **Continue** to proceed to the next registration web page.

Result The Verify Information and Submit registration web page is displayed (Figure A-10, “Registration Web Page for New Users (Step 5: Verify & Submit)” (p. 99)).

Figure A-10 Registration Web Page for New Users (Step 5: Verify & Submit)



Lucent VPN Firewall - New Product Registration

- Step 1 - Validate Keys (Completed)
- Step 2 - Enter Customer & Contact Info (Completed)
- Step 3 - Enter Product Info (Completed)
- Step 4 - Enter Username & Password (Completed)
- Step 5 - Verify & Submit

Step 5: Verify Information and Submit

Please review and verify all information for this account.
Click the Submit button at the bottom to create the account
or click the Re-Edit button to return to Step 1. In addition,
a left-side Menu provides links to re-editing of any Step.

Primary Software License Key:	1102091630829DD000000FFDDAA922AA2
Primary Software License Description:	license key, main-1, primary SMS R9.199
Customer Info - First Name:	John
Customer Info - Last Name:	Daniels
Customer Info - Company Name:	ABC Corporation
Customer Info - Address 1:	799 South Devonshire Road
Customer Info - City:	Atlanta
Customer Info - State / Province:	Georgia
Customer Info - Zip / Postal Code:	30301
Customer Info - Country:	United States
Customer Info - Telephone:	404-555-1212
Customer Info - Email Address:	jdaniels@abccorp.com
Contact Info - Address 1:	799 South Devonshire Road
Contact Info - City:	Atlanta
Contact Info - State / Province:	Georgia
Contact Info - Zip / Postal Code:	30301
Contact Info - Country:	United States
Contact Info - Telephone:	404-555-1212
Contact Info - Email Address:	jdaniels@abccorp.com
Hardware Model & Serial Numbers:	
PURCHASED FROM	
Company Name:	
City:	
State/Province:	
Zip/Postal:	
Country:	
Purchased Date:	
Username:	daniels267
Password:	**********

Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

11 Verify that all of the previously entered registration information is correct.

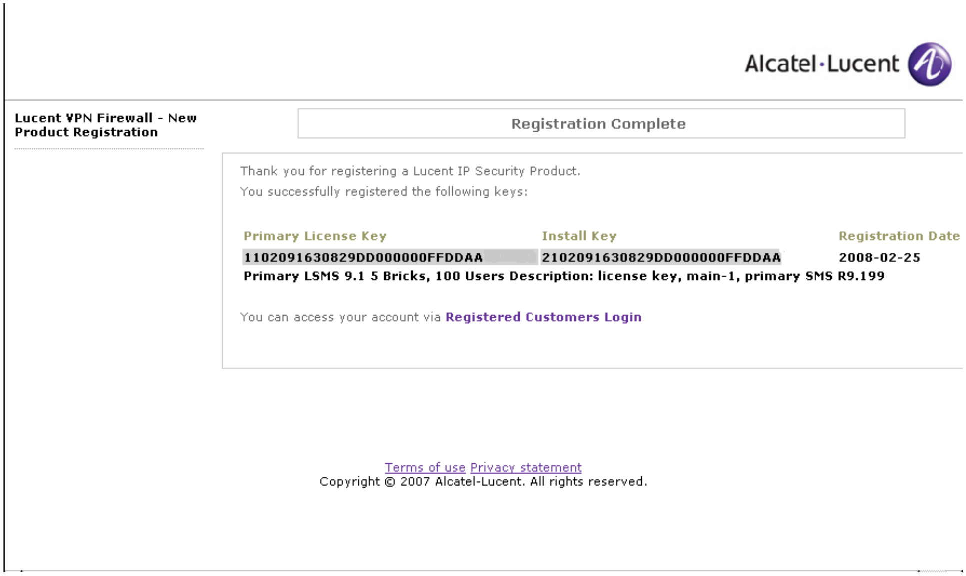
To change any of the previously entered registration information on any web page, click the **Re-Edit** key and then click the bullet item hyperlink at the top left portion of the web page to return to the page where the change(s) must be made.

If the information entered is correct, click the **Submit** button.

Result The Registration Completed registration web page is displayed, showing that the software license key is successfully registered and the installation key that was obtained and should be used to install the SMS application.

Figure A-11, "Registration Completed Page Showing Registered Software License Key and Installation Key Obtained (Example)" (p. 100) shows a sample page.

Figure A-11 **Registration Completed Page Showing Registered Software License Key and Installation Key Obtained (Example)**



Alcatel·Lucent

Lucent VPN Firewall - New Product Registration

Registration Complete

Thank you for registering a Lucent IP Security Product.
You successfully registered the following keys:

Primary License Key	Install Key	Registration Date
1102091630829DD000000FFDDAA	2102091630829DD000000FFDDAA	2008-02-25

Primary LSMS 9.1 5 Bricks, 100 Users Description: license key, main-1, primary SMS R9.199

You can access your account via Registered Customers Login

Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

This license key and installation key information is also available when you log into the Product Registration and Support website and access the **Registered Keys** web page on the site.

END OF STEPS

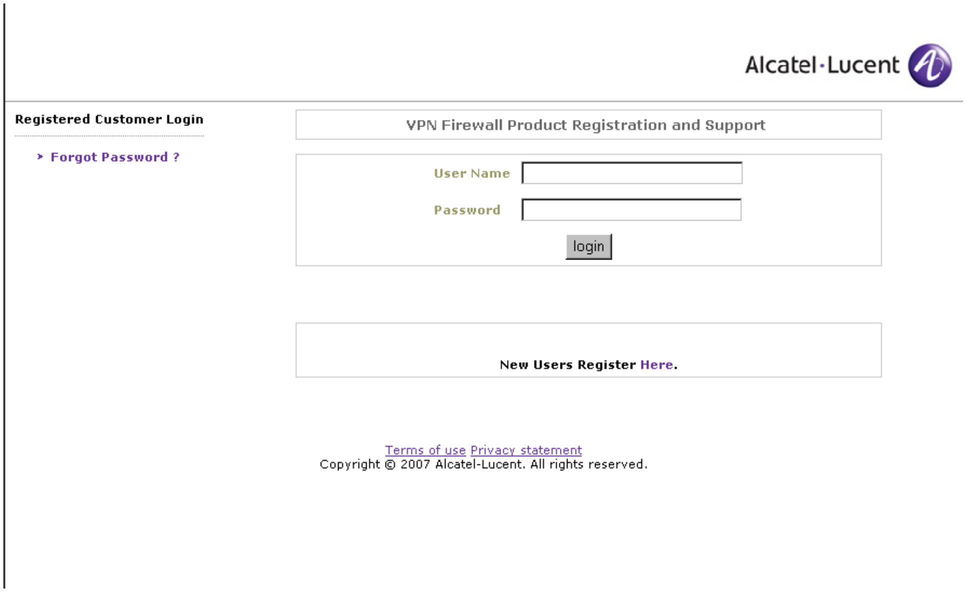
To register a software license key and obtain an installation key for upgrade or feature option

Use this procedure to register a software license key and obtain an installation key for an SMS software upgrade or feature option using a previously registered license key. License keys are “dependent” on each other. For example, if you have installed SMS Release 9.1 on a specific host using an installation key, and want to upgrade the same host to SMS Release 9.2, the upgrade software license key will be dependent on the previously registered license key used to obtain a key to install the Release 9.1 software. Complete the following steps to register a software license key and obtain an installation key for an upgrade or feature option using a previously registered software license key.

1 Go to https://vpn-firewall-brick.alcatel-lucent.com

Result The VPN Firewall Product Registration and Support Login page is displayed (Figure A-12, “VPN Firewall Product Registration and Support Login Page” (p. 101)).

Figure A-12 VPN Firewall Product Registration and Support Login Page

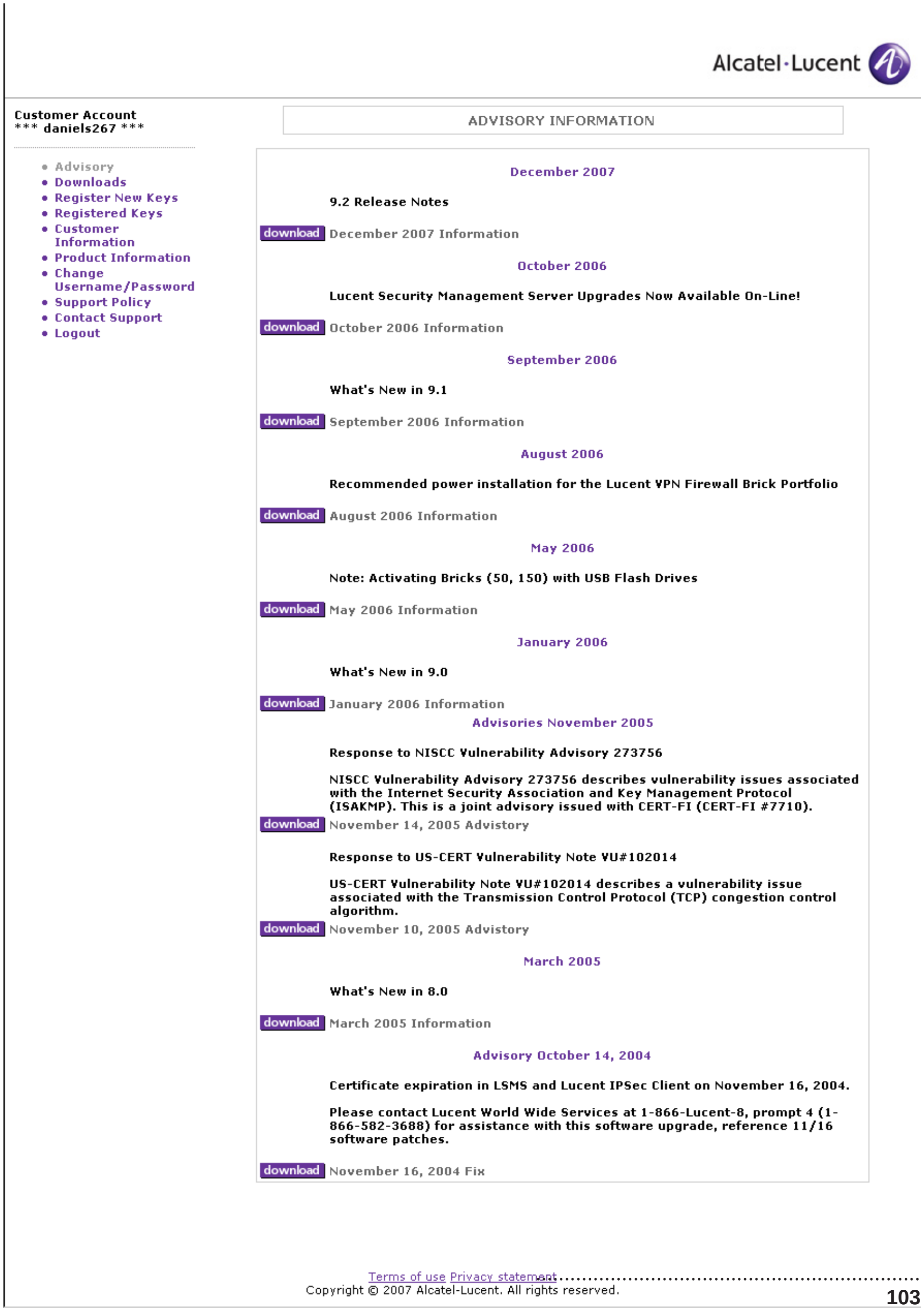

Alcatel·Lucent
Registered Customer Login
Forgot Password ?
VPN Firewall Product Registration and Support
User Name
Password
login
New Users Register Here.
Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

Tip: if you completed the “To register a software license key and obtain an installation key as a new user” (p. 86) procedure and are on the Registration Completed page (Figure A-11, “Registration Completed Page Showing Registered Software License Key and Installation Key Obtained (Example)” (p. 100)), and are ready to register a software license key for an upgrade, you can also bring up the VPN Firewall Product Support and Registration Login page by clicking the **Registered Customers Login** hyperlink text on that page.

2 Log into the VPN Firewall Registration web page by entering your registered username and password (which you created in Step 9 of the “To register a software license key and obtain an installation key as a new user” (p. 86) procedure).

Result The VPN Firewall Registration web page is displayed (Figure A-13, “VPN Firewall Registration Web Page” (p. 103) shows a sample page).

Figure A-13 VPN Firewall Registration Web Page



Customer Account
*** daniels267 ***

- Advisory
- Downloads
- Register New Keys
- Registered Keys
- Customer Information
- Product Information
- Change Username/Password
- Support Policy
- Contact Support
- Logout

ADVISORY INFORMATION

December 2007

9.2 Release Notes

download December 2007 Information

October 2006

Lucent Security Management Server Upgrades Now Available On-Line!

download October 2006 Information

September 2006

What's New in 9.1

download September 2006 Information

August 2006

Recommended power installation for the Lucent VPN Firewall Brick Portfolio

download August 2006 Information

May 2006

Note: Activating Bricks (50, 150) with USB Flash Drives

download May 2006 Information

January 2006

What's New in 9.0

download January 2006 Information

Advisories November 2005

Response to NISCC Vulnerability Advisory 273756

NISCC Vulnerability Advisory 273756 describes vulnerability issues associated with the Internet Security Association and Key Management Protocol (ISAKMP). This is a joint advisory issued with CERT-FI (CERT-FI #7710).

download November 14, 2005 Advistory

Response to US-CERT Vulnerability Note VU#102014

US-CERT Vulnerability Note VU#102014 describes a vulnerability issue associated with the Transmission Control Protocol (TCP) congestion control algorithm.

download November 10, 2005 Advistory

March 2005

What's New in 8.0

download March 2005 Information

Advisory October 14, 2004

Certificate expiration in LSMS and Lucent IPSec Client on November 16, 2004.

Please contact Lucent World Wide Services at 1-866-Lucent-8, prompt 4 (1-866-582-3688) for assistance with this software upgrade, reference 11/16 software patches.

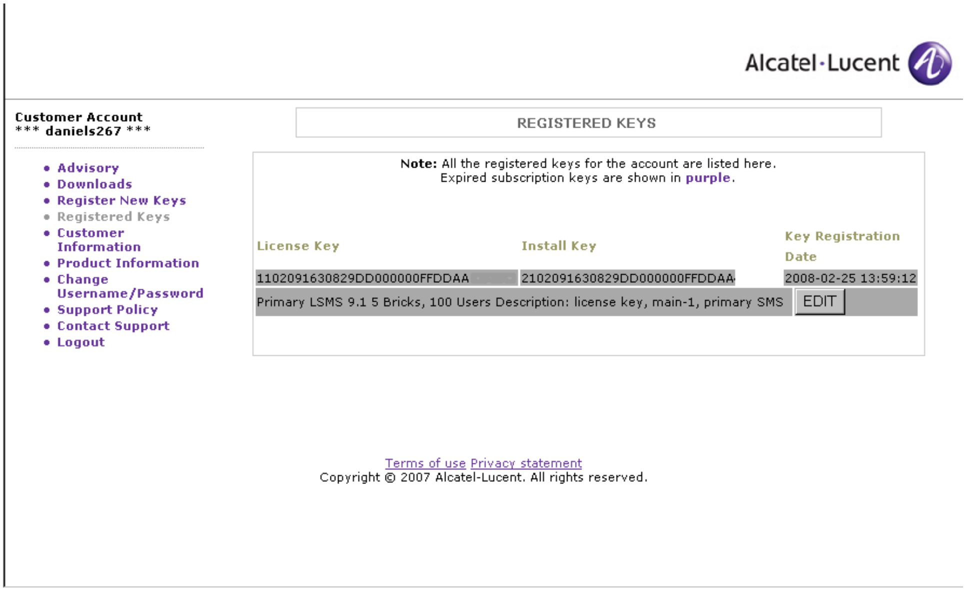
download November 16, 2004 Fix

Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

3 Click on **Registered Keys** to display a list of previously registered keys.

Result The Registered Keys web page is displayed, showing a list of previously registered keys (Figure A-14, “Registered Keys Web Page” (p. 104)).

Figure A-14 Registered Keys Web Page



Note: All the registered keys for the account are listed here.
Expired subscription keys are shown in **purple**.

License Key	Install Key	Key Registration Date
1102091630829DD000000FFDDAA	2102091630829DD000000FFDDAA	2008-02-25 13:59:12
Primary LSMS 9.1 5 Bricks, 100 Users Description: license key, main-1, primary SMS		EDIT

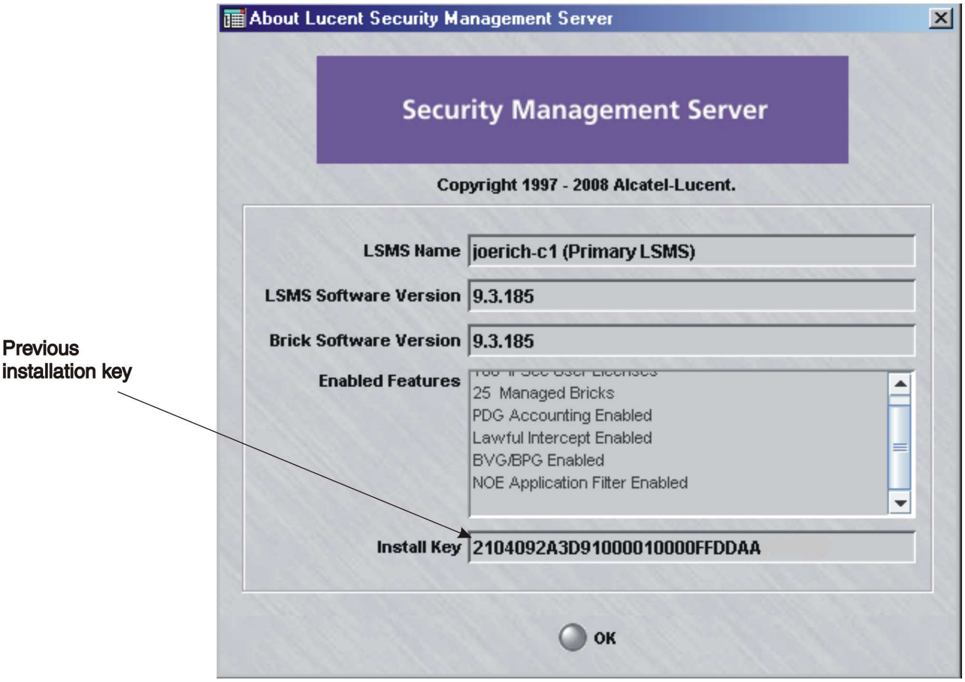
Copyright © 2007 Alcatel-Lucent. All rights reserved.

It is recommended that you print out this page and note which installation key was used to install the previous SMS release on the specific machine that is being upgraded. The new installation key that you will obtain for an upgrade or feature option will depend on the installation key used for the previous release and must be selected when you register a license key and obtain an installation key for the upgrade/feature option.

You can also find out which installation key was used to install the previous SMS release on a host by logging into the SMS GUI on that host and selecting **Help > About** from the menu bar.

The **About** window is displayed, showing general information about the SMS and Brick software version software that is being supported on the SMS host on which you are currently logged in (Figure A-15, “SMS Help > About Window” (p. 105) shows a sample window).

Figure A-15 SMS Help > About Window



About Lucent Security Management Server

Security Management Server

Copyright 1997 - 2008 Alcatel-Lucent.

LSMS Name: joerich-c1 (Primary LSMS)

LSMS Software Version: 9.3.185

Brick Software Version: 9.3.185

Enabled Features:
100 IPSec User Licenses
25 Managed Bricks
PDG Accounting Enabled
Lawful Intercept Enabled
BVG/BPG Enabled
NOE Application Filter Enabled

Install Key: 2104092A3D91000010000FFDDAA

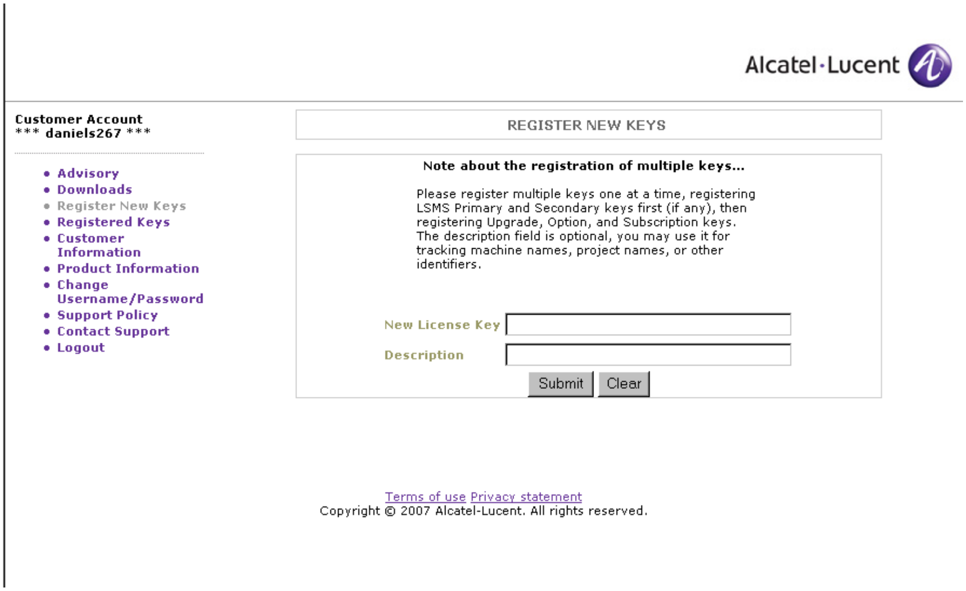
Previous installation key

Click **OK** to close this window.

4 On the **Registered Keys** registration web page (or the VPN Firewall Registration web page, if you are on that page), click on **Register New Keys**.

Result The Register New Keys web page is displayed (Figure A-16, “Register New Keys Web Page” (p. 106)).

Figure A-16 Register New Keys Web Page



Note about the registration of multiple keys...

Please register multiple keys one at a time, registering LSMS Primary and Secondary keys first (if any), then registering Upgrade, Option, and Subscription keys. The description field is optional, you may use it for tracking machine names, project names, or other identifiers.

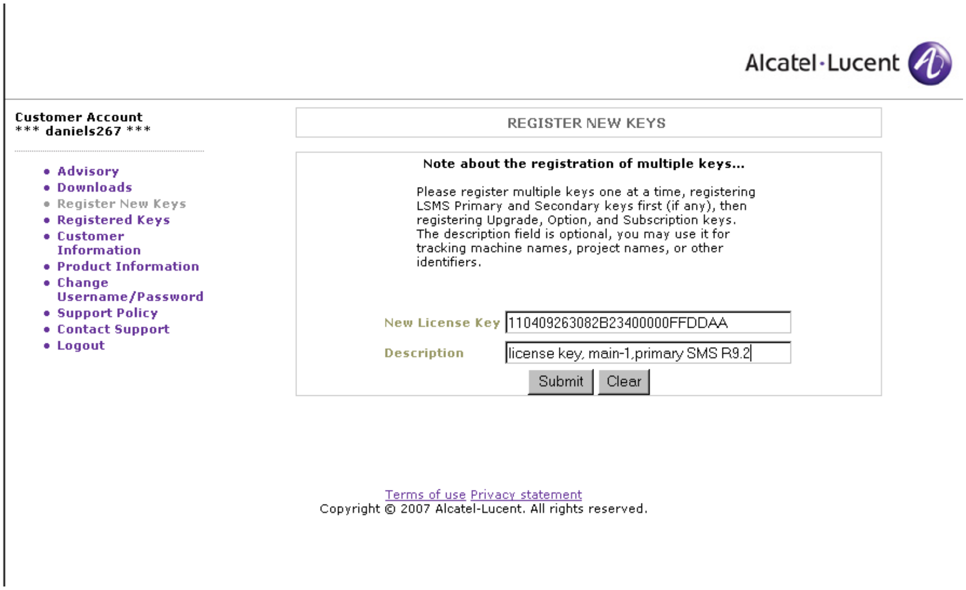
Copyright © 2007 Alcatel-Lucent. All rights reserved.

5 In the **New License Key** field, enter the software license key of the upgrade or feature option.

In the **Description** field, enter any descriptive information that would help identify the machine or software version for which the installation key is being obtained. The **Description** field is optional.

Figure A-17, “Register New Keys Upgrade License Key Entry (Example)” (p. 107) shows a sample entry.

Figure A-17 **Register New Keys Upgrade License Key Entry (Example)**



Note about the registration of multiple keys...

Please register multiple keys one at a time, registering LSMS Primary and Secondary keys first (if any), then registering Upgrade, Option, and Subscription keys. The description field is optional, you may use it for tracking machine names, project names, or other identifiers.

New License Key: 110409263082B23400000FFDDAA

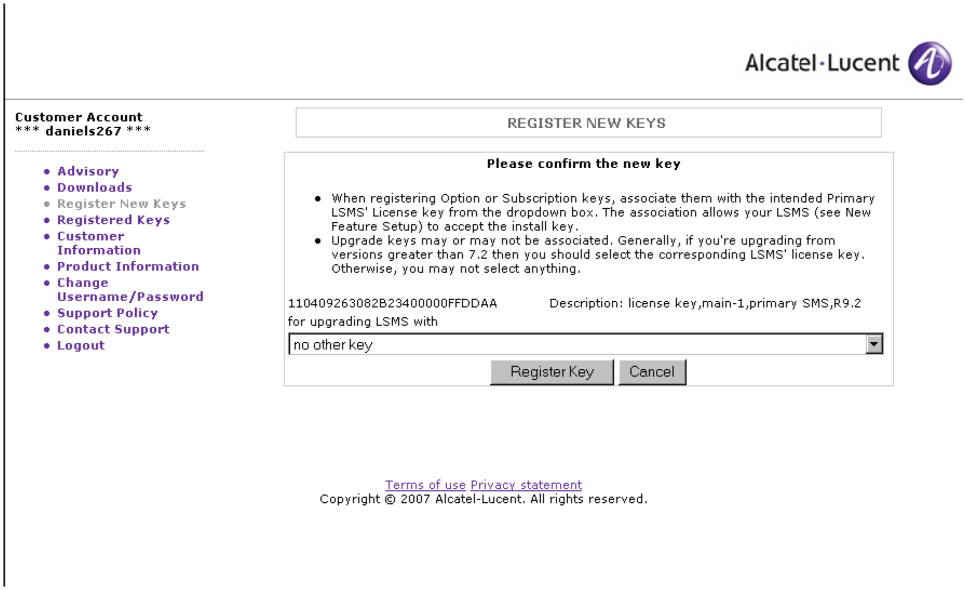
Description: license key, main-1,primary SMS R9.2

Copyright © 2007 Alcatel-Lucent. All rights reserved.

6 Click the **Submit** button.

Result A Register New Keys confirmation window is displayed (Figure A-18, “Register New Keys Confirmation Window” (p. 108)).

Figure A-18 Register New Keys Confirmation Window



Please confirm the new key

- When registering Option or Subscription keys, associate them with the intended Primary LSMS' License key from the dropdown box. The association allows your LSMS (see New Feature Setup) to accept the install key.
- Upgrade keys may or may not be associated. Generally, if you're upgrading from versions greater than 7.2 then you should select the corresponding LSMS' license key. Otherwise, you may not select anything.

110409263082B23400000FFDDAA Description: license key,main-1,primary SMS,R9.2

for upgrading LSMS with

no other key ▼

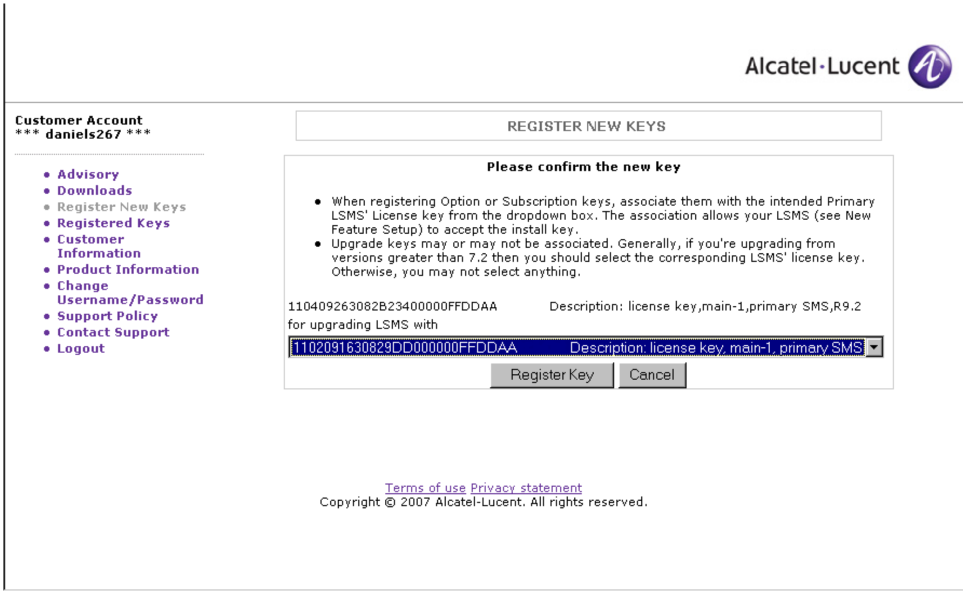
Copyright © 2007 Alcatel-Lucent. All rights reserved.

This window is for associating the previously registered license key that was used to obtain the installation key for the prior SMS release with the software license key for the software upgrade.

7 Click the down arrow to the right of the field below the upgrade license key description and select the previous software license key of the prior release and host machine to be associated with the upgrade license key.

Figure A-19, “Register New Key Confirmation Window, Selecting Associated License Key From Previous Release (Example)” (p. 109) shows an example of selecting an associated license key.

Figure A-19 Register New Key Confirmation Window, Selecting Associated License Key From Previous Release (Example)



Customer Account
***** daniels267 *****

- Advisory
- Downloads
- Register New Keys
- Registered Keys
- Customer Information
- Product Information
- Change Username/Password
- Support Policy
- Contact Support
- Logout

REGISTER NEW KEYS

Please confirm the new key

- When registering Option or Subscription keys, associate them with the intended Primary LSMS' License key from the dropdown box. The association allows your LSMS (see New Feature Setup) to accept the install key.
- Upgrade keys may or may not be associated. Generally, if you're upgrading from versions greater than 7.2 then you should select the corresponding LSMS' license key. Otherwise, you may not select anything.

110409263082B23400000FFDDAA Description: license key,main-1,primary SMS,R9.2

for upgrading LSMS with

1102091630829DD000000FFDDAA Description: license key, main-1, primary SMS

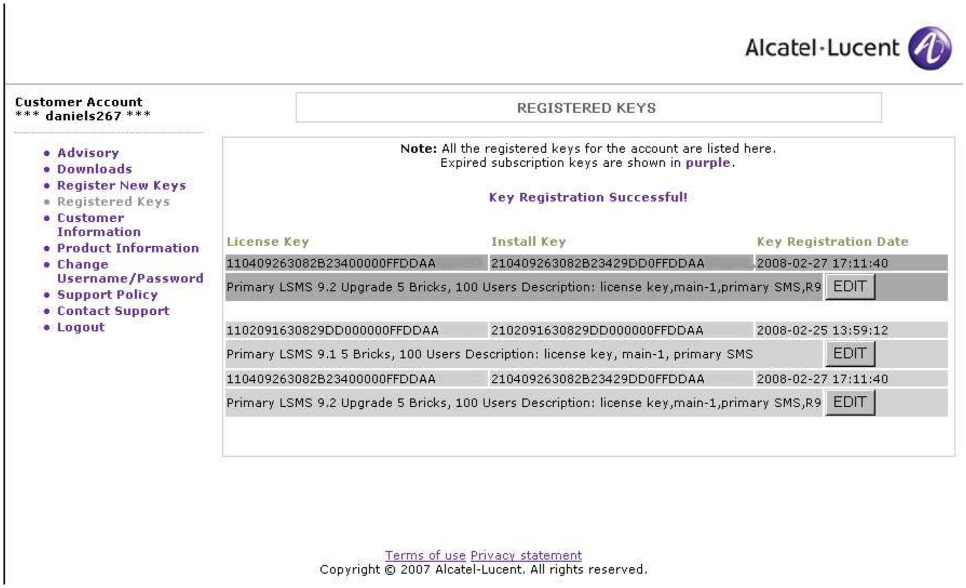
Terms of use Privacy statement
Copyright © 2007 Alcatel-Lucent. All rights reserved.

8 Click the **Register Key** button.

Result A Registration Completed web page is displayed, showing that the upgrade license key was successfully registered and an installation key was obtained for installing the SMS software upgrade.

Figure A-20, "Registration Completed Page, Successful Registration of Upgrade License Key and Installation Key Obtained (Example)" (p. 110) shows a sample window.

Figure A-20 **Registration Completed Page, Successful Registration of Upgrade License Key and Installation Key Obtained (Example)**



Note: All the registered keys for the account are listed here.
Expired subscription keys are shown in **purple**.

Key Registration Successful!

License Key	Install Key	Key Registration Date	
110409263082B23400000FFDDAA	210409263082B23429DD0FFDDAA	2008-02-27 17:11:40	
Primary LSMS 9.2 Upgrade 5 Bricks, 100 Users Description: license key,main-1,primary SMS,R9			EDIT
1102091630829DD000000FFDDAA	2102091630829DD000000FFDDAA	2008-02-25 13:59:12	
Primary LSMS 9.1 5 Bricks, 100 Users Description: license key, main-1, primary SMS			EDIT
110409263082B23400000FFDDAA	210409263082B23429DD0FFDDAA	2008-02-27 17:11:40	
Primary LSMS 9.2 Upgrade 5 Bricks, 100 Users Description: license key,main-1,primary SMS,R9			EDIT

Copyright © 2007 Alcatel-Lucent. All rights reserved.

END OF STEPS

□

B SMS Hardening Guidelines

Overview

Purpose

This appendix provides information on how to harden the server on which the management platform is installed to ensure that the management platform is as secure as possible. The Alcatel-Lucent Security Management Server (SMS) platform is the centralized management platform that is required in order to configure, monitor, and manage the Alcatel-Lucent *VPN Firewall Brick*™ Security Appliances. This management platform is available as a separate application and can be installed on a *Microsoft*® *Windows*®, *Microsoft*® *Vista*®, or *Sun*® Sparc-based *Solaris*® platform. The solution also offers a Remote Navigator capability, which enables a user of a *Windows*®, *Vista*®, or *Solaris*®-based workstation to access the management platform remotely.

The information contained herein are only guidelines and recommendations. Individual network configurations and operational tools may result in differences in actual hardening implementations. In addition, be sure to reference any additional information from the server and underlying operating system manufacturer, along with reference information on any additional applications that may be installed on the management server for more details.

Contents

SMS and Operating System Hardening Guidelines	112

□

SMS and Operating System Hardening Guidelines

General SMS hardening recommendations

For maximum security, Alcatel-Lucent recommends that the management platform (SMS) be placed on its own server in a secure zone protected by an Alcatel-Lucent *VPN Firewall Brick*® Security Appliance. The administrator would then utilize the Alcatel-Lucent SMS platform to configure the *administrativezone* using the pre-defined rulesets (refer to the *Pre-Configured VPN Firewall Brick® Device Zone Rulesets* appendix in the *SMS Policy Guide* for additional information.

In addition to the above recommendation, the underlying operating system on which the SMS is installed should be hardened. This will provide an additional layer of security from internal attacks as well as an added layer of security for networking environments, where the customer is not in a position to deploy a Brick device with an *administrativezone*.

Operating system hardening recommendations

The following are recommendations for hardening the underlying operating system for platforms that are running the Alcatel-Lucent SMS or Remote Navigator applications:

- Ensure that you are running the latest patches from the operating system vendor.
- Implement the hardening guidelines recommended by your operation system platform vendor.
- Ensure that only the required services are running on the platform.
- If additional applications are running on the system being used for the Alcatel-Lucent SMS and/or Remote Navigator products, ensure that the latest patches and any specific hardening guidelines for those other applications are implemented.
- Implement higher security passwords for system login, application login, and remote management capabilities.

Recommended patches

As vulnerabilities may get published frequently, it is recommended that you regularly review the *Sun*® *Solaris*®, *Microsoft*® *Windows*®, and *Microsoft*® *Vista*® support facilities to ensure that new patch updates are downloaded and installed whenever necessary.

General application hardening guidelines

In addition to the general hardening guidelines provided in this appendix, further security information can be found at:

- The Center for Internet Security. This organization provides a wealth of information on securing your platform. The Center for Internet Security’s tools and benchmarks can be found at http://www.cisecurity.org
- Specific guidelines from your hardware and operating system manufacturer. These guidelines can be found (by vendor):
- For *Sun*® *Solaris*®, http://www.cisecurity.org/bench_solaris.html
- For *Microsoft*® *Windows*® and *Vista*®, http://www.cesecurity.org/bench_windows.html

Services and port access

In general, your management platform should enable only the services needed by the applications that are running on the platform. The required services are highly dependent on the specific operational and networking needs of the environment in which you are deploying the SMS, Remote Navigator, and any additional applications that you may be installing on the same platform, along with the specific security requirements that should be followed in your data center.

The following table provides a listing of the services that are required for operating the Alcatel-Lucent SMS and Remote Navigator products.

Port	Service	Type	Port Usage
80	http/httpd	TCP	Used by Alcatel-Lucent SMS for Remote Navigator download and for displaying reports using the SMS Navigator. This is a configurable port and is set at install time with a default value of 80.
900		TCP	Port 900 is used to allow any Brick connected to the Alcatel-Lucent SMS to send audit data to the SMS and rqeuest the application to download the Brick.
7000		TCP	Used by the Alcatel-Lucent SMS to accept connections by the remote/local Alcatel-Lucent SMS Navigator.
7001		TCP	Used by the Alcatel-Lucent SMS Database Utility to accept connections/transactions for its hosted database.

Port	Service	Type	Port Usage
8161-User Configurable		UDP	Used by the Alcatel-Lucent SMS for SNMP traffic - changed from default port of 161 during local installation of the system as system agent is using SNMP port 161. The SMS agent is configured to use 8161 port.
9000		TCP	Port 9000 is used to allow any Brick connected to the Alcatel-Lucent SMS to send audit data to the SMS and request the SMS to download the Brick.
9004	Unknown	TCP	Port 9004 is used to allow other Alcatel-Lucent SMS processes to send audit data to the logger.
9005	Unknown	TCP	Port 9005 is used to allow other RealSecure Engine to communicate to the Alcatel-Lucent SMS and send audit data to the logger.
9007	Unknown	TCP	Port 9007 is used for internal Alcatel-Lucent SMS communications between Admin service and User Auth service.
9008	Unknown	TCP	Port 9008 is used for Alcatel-Lucent SMS communications between Admin service and User Auth service.
9009	Unknown	TCP	Port 9009 is used for internal Alcatel-Lucent SMS communications for setting up scheduled tasks like backup and FTPing of audit logs.
9010	Unknown	TCP	Port used for Firewall User Authentication
9011	Unknown	TCP	Port used for Firewall User Authentication
9012	Unknown	TCP	Used for internal Alcatel-Lucent communications with the Admin service
9019	Unknown	TCP	Used for Alcatel-Lucent SMS CLI communication
9041	Unknown	TCP	Port 9041 is used by Alcatel-Lucent SMS to send alarms
9090	http-admin	TCP	Used in the case of redundant SMS servers for database synchronization

Port	Service	Type	Port Usage
9091	xmitec-xmimail	TCP	Used in the case of redundant SMS servers for database synchronization
9092	Unknown	TCP	Used in the case of redundant SMS servers for database synchronization

As an additional recommendation for hardening the operating system, if the use of multicast packets is not needed on the management platform, disable these functions.

For a *Sun*® *Solaris*®-based system, this can be performed using the following commands while logged in as `root`:

- `/usr/sbin/ndd -set /dev/ip ip_respond_to_echo_multicast 0`
- `/usr/sbin/ndd -set /dev/ip ip6_respond_to_echo_multicase 0`
- `/etc/init.d/network restart`

Application patches

It is recommended that you install the latest patches for all applications that may be installed on the operating system. This includes patches to the Alcatel-Lucent SMS and Remote Navigator products, which are available at the VPN Firewall Product Registration and Support website, https://vpn-firewall-brick.alcatel-lucent.com

Contact the vendor of your other applications for information about how to obtain the latest patches and versions.

Password security

User and administrator access to operating system, remote management (such as SNMP), and applications should be password-enabled using strong password enforcement mechanisms. The Alcatel-Lucent SMS provides strong password enforcement and it is recommended that this capability be enabled on this system. Refer to the *Using the Configuration Assistant* chapter in the *SMS Administration Guide* for information on enabling strong password enforcement.

The Alcatel-Lucent SMS application also includes SNMP-based capabilities to integrate with network management systems. The SNMP facilities are initially configured to a standard *public* community string for access to the SNMP reporting information. While the SNMP agent that is included in the SMS provides read-only access to information, it is recommended to also modify the community string to something that meets your strong password security requirements.

Do the following to modify the Alcatel-Lucent SMS SNMP community string:

1. Log into the Alcatel-Lucent SMS platform as administrator.
2. Bring up the Configuration Assistant.
3. Double-click on the SNMP Agent category.

4. Change the SNMP Read Community String from **public** (the default value) to a custom value
5. Modify the community string on the SNMP management station to match the new community string that you set for the Alcatel-Lucent SMS application

For the operating system and other applications that may be running on the management platform, consult the appropriate guides.

□

C License Terms for Third Party Software

Overview

Purpose

This appendix contains information about licensing terms and agreements for third party software.

□

License terms for third party software

IPMI

Copyright 2006 IronPort Systems, Inc.

All Rights Reserved

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS 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.

Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS 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.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER 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.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS 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.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2008, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS 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.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS 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.

---- Part 7: Fabasoft Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft Software GmbH & Co KG, 2003 oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Fabasoft Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER 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.

□

Index

B Brick devices
supported, xi

C Clean installation
Solaris® server platform, 53
Vista® server platform, 33
Windows® server platform, 10
Compute servers, 4, 27, 46, 66
Configuration Assistant, 57, 63, 77

F Firewall software
and SMS, 51, 70

H Hardening Guidelines
SMS, 111
Hardware requirements
Linux server platform, 68
Solaris® server platform, 48
Vista® server platform, 29
Windows® server platform, 6

I
Installation key
obtain, 86
Installation keys, 8, 31, 50, 69

L Linux server platform
hardware requirements, 68
manually un-install SMS, 79
post-installation steps, 84
pre-installation requirements, 69
software requirements, 68

M Manually un-install SMS
Linux server platform, 79
Solaris® server platform, 58
Vista® server platform, 39
Windows® server platform, 16

N New Feature Setup utility, 8, 31, 50, 69

O Obtain
installation key, 86

P Post-installation steps
Linux server platform, 84
Solaris® server platform, 64
Vista® server platform, 44
Windows® server platform, 23
Pre-installation requirements
Linux server platform, 69
Solaris® server platform, 50
Vista® server platform, 31
Windows® server platform, 8

R Register
software license key, 86

S SMS
hardening guidelines, 111
software patches, 9, 32, 51, 70
SMS configurations, 4, 26, 46, 66
Software license key
register, 86
Software requirements
Linux server platform, 68
Solaris® server platform, 49

Vista® server platform, 30
Windows® server platform, 7
Solaris® server platform
clean installation, 53
hardware requirements, 48
manually un-install SMS, 58
post-installation steps, 64
pre-installation requirements, 50
software requirements, 49
upgrade SMS software, 59

U UAC
See: User Account Control (UAC)
Upgrade SMS software
Linux server platform, 80
Solaris® server platform, 59
Vista® server platform, 40
Windows® server platform, 17
User Account Control (UAC), 26

V *Vista*® server platform
clean installation, 33
hardware requirements, 29
manually un-install SMS, 39
post-installation steps, 44
pre-installation requirements, 31
software requirements, 30
upgrade SMS software, 40
User Account Control (UAC), 26

W *Windows*® 2003 Server
installations, 7
Windows® server platform
clean installation, 10
hardware requirements, 6
manually un-install SMS, 16
post-installation steps, 23
pre-installation requirements, 8
software requirements, 7
upgrade SMS software, 17