



Lucent Security Management Server (LSMS)

Release 9.1

Installation Guide

260-100-018R9.1
CC109630764
Issue 1
August 2006

Lucent Technologies - Proprietary

This document contains proprietary information of Lucent Technologies and is not to be disclosed or used except in accordance with applicable agreements.

Copyright © 2006 Lucent Technologies
Unpublished and Not for Publication
All Rights Reserved

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies and the business management owner of the material.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

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. Lucent Technologies 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 Lucent Technologies Account Team.

Ordering Information

The ordering number for this information product is 260-100-018R9.1.

Technical Support

In the continental United States, when you need additional technical assistance, the Lucent Technologies 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-LUCENT8 (1-866-582-3688).

Outside the United States, contact your Local Customer Support (LCS) or the support organization designated by your 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@lucent.com.

Contents

	About this information product	v
	Purpose	v
	How to use this information product	v
	Supported Brick devices	vi
	Related information	vi
	How to order	vii
	Safety information	vii
	How to comment	vii
1	Safety Information	1
	Structure of hazard statements	1
2	LSMS on a <i>Windows</i>® Server Platform	3
	Overview	3
	Introduction	4
	Hardware Requirements	6
	Software Requirements	7
	Pre-Installation Requirements (Clean Installations)	8
	To Install the LSMS Application (Clean Installation)	11
	To Manually Un-Install LSMS	17
	To Upgrade the LSMS Software	18
	What To Do Next	23
3	LSMS on a <i>Solaris</i>® Server Platform	25
	Overview	25
	Introduction	26
	Hardware Requirements	28
	Software Requirements	29
	Pre-Installation Requirements (Clean Installations)	30

Contents

To Install the LSMS Application (Clean Installation)	32
To Manually Un-Install LSMS	37
To Upgrade the LSMS Software	38
What To Do Next	42

Index	43
--------------	-----------

About this information product

Purpose

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

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

How to use this information product

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

This *Installation Guide* is organized as follows:

Chapter Title	Description
Chapter 2, “LSMS on a <i>Windows®</i> Server Platform”	Describes how to install the LSMS application on a host running <i>Microsoft®</i> 2000 Professional, 2000 Server, XP Professional, or Server 2003. Includes hardware and software requirements, pre-installation requirements, and detailed installation procedures for a new and upgrade installation for both a Primary LSMS and redundant LSMS configurations. Also provides post-installation configuration requirements and how to access the LSMS application on your PC desktop. Also provides a procedure for manually un-installing the LSMS from a de-commissioned server as needed.

Chapter Title	Description
Chapter 3, “LSMS on a Solaris® Server Platform”	Describes how to install the LSMS application on a host running the Sun® Solaris® 2.8, 2.9, or 2.10 operating system. Describes hardware and software requirements for installing LSMS on a Solaris® server platform, pre-installation requirements, and and detailed installation procedures for a new and upgrade installation for both a Primary LSMS and redundant LSMS configurations. Also provides post-installation configuration requirements and how to access the LSMS application on your PC desktop. Also provides a procedure for manually un-installing the LSMS from a de-commissioned server as needed.

Supported Brick devices

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

- Model 20 Brick device
- Model 50 Brick device
- Model 150 Brick device
- Model 350 Brick device
- Model 1100/1100A Brick device
- Model 700 Brick device
- Model 1200 Standard and HS Brick device

Some of the above Brick device models require a specific patch of the current LSMS release in order to be fully supported. For details about the LSMS patch release required for a specific Brick device model, refer to the *User's Guide* for the Brick device model or check out the **VPN Firewall Portfolio** link on the following website for specific LSMS patch release information: <http://www.lucent.com/security/>

Related information

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

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

Documentation

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

- *Lucent Security Management Server (LSMS) Policy Guide* (260-100-016R9.1), which instructs users how to create security policies and set up VPN tunnels on Lucent Virtual Firewall *Brick*® devices.
- *Lucent Security Management Server (LSMS) Administration Guide* (260-100-017R9.1), which instructs users how to administer the LSMS application.
- *Lucent Security Management Server (LSMS) Installation Guide* (260-100-018R9.1), which instructs users how to install the LSMS application.
- *Lucent Security Management Server (LSMS) Reports, Alarms, and Logs* (260-100-019R9.1), which instructs users how to use log files, configure triggers and actions to generate alarms, and how to compile and view reports.
- *Lucent Security Management Server (LSMS) Tools and Troubleshooting Guide* (260-100-020R9.1), which instructs users how to use the Command Line Interface (CLI) commands.
- *Lucent Security Management Server (LSMS) Technical Overview* (260-100-022R9.1), which provides a general technical description of the Lucent VPN Firewall solution.
- *Lucent Security Management Server (LSMS) What's New for Release 9.1?* (260-100-025R9.1), which provides a summary of new features for the current LSMS product release.

How to order

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

- From the United States, call 888-LUCENT8 (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/) (<http://www.lucent-info.com/comments/enus/>) or email your comments to the Comments Hotline (comments@lucent.com).

1 Safety Information

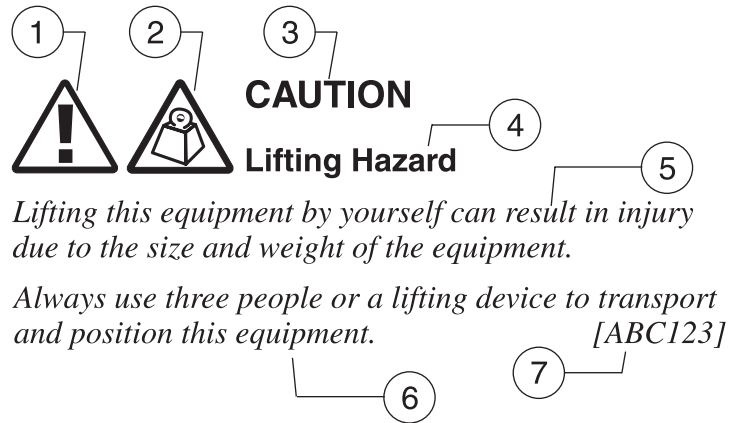
Structure of hazard statements

Overview

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

General structure

Hazard statements include the following structural elements:



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	<p><i>When used with the personal injury symbol:</i></p> <p>Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in personal injury.</p> <p><i>When used without the personal injury symbol:</i></p> <p>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.</p>



2 LSMS on a *Windows*[®] Server Platform

Overview

Purpose

This chapter explains how to install the LSMS application on a *Windows*[®] server platform. It also includes a procedure for manually un-installing the LSMS as needed.

Contents

Introduction	4
Hardware Requirements	6
Software Requirements	7
Pre-Installation Requirements (Clean Installations)	8
To Install the LSMS Application (Clean Installation)	11
To Manually Un-Install LSMS	17
To Upgrade the LSMS Software	18
What To Do Next	23



Introduction

Overview

The LSMS application can be installed on a host running *Microsoft*[®] *Windows*[®] 2000 Professional, *Windows*[®] 2000 Server, XP Professional, or Server 2003.

Release 9.1 can be installed as a first time (clean) installation or as an upgrade.

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

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

Important! The LSMS and all Lucent Virtual Firewall *Brick*[®] devices must have the IKE on the Brick feature enabled before upgrading to the current LSMS release.

Upgrades



CAUTION

Service disruption hazard

Security Precaution

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

LSMS configurations

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

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

Multi-Site LSMS configuration

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

Compute servers

To maximize scalability of the LSMS/Brick security solution, LSMS provides the option of adding a separate set of servers called Lucent Secure Compute Servers (LSCSs), or simply

Compute Servers, which are associated with a Primary or Secondary LSMS and act as collection points for Brick log traffic. Using an LSCS to collect Brick log data frees up computing resources on the LSMS itself and extends the number of Brick devices and total log traffic that can be handled. Each Brick device managed by the LSMS can be homed to one of the associated LSCSs or the managing LSMS for logging purposes.

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

Implementing Primary LSMS/Secondary LSMS Configurations

During the installation of the Secondary LSMS, there is a point at which the Secondary LSMS attempts to contact the Primary LSMS to replicate the Primary LSMS database on the Secondary LSMS. If the Secondary LSMS cannot contact the Primary LSMS, the installation fails.

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

To ensure that the Primary LSMS and Secondary LSMS(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 LSMS 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 LSMS is operational, use it to configure two Bricks and assign the pre-configured ruleset *administrativezone* to the ports that will be connected to the LSMS. Refer to the *Configuring Brick Ports* section in the *LSMS Administration Guide* for instructions on how to do this.
3. Connect the Primary LSMS to the port on one Brick, and the host that will be the Secondary LSMS to the port on the other. Then, deploy the two Bricks: the primary LSMS and the host that will be the Secondary LSMS in the network.
4. To ensure that the Primary LSMS 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 LSMS. Once the ping is successful, remove the rule for security reasons. (Refer to the *Brick Zone Rulesets* section in the *LSMS Policy Guide* for instructions on how to create a rule.)
5. When you have established that the two LSMS servers can communicate, install the Secondary LSMS.



Hardware Requirements

Minimum hardware requirements

Regardless of which operating system you are running, the host on which you install the LSMS 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 device or the following website: <http://www.lucent.com/security>.
- Ethernet interface card
- Video card capable of 1024 x 768 resolution (65,535 colors).

Important! Because of the memory requirements of LSMS R9.1, 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 *Appendix B. Sizing Guidelines* in the *LSMS 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 LSMS application on a Microsoft *Windows*® platform:

- *Windows*® 2000 Professional and Service Pack 4 or higher, *Windows*® 2000 Server and Service Pack 4 or higher, Windows XP Professional and Service Pack 1 or Service Pack 2, 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 LSMS software.

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

- A browser (either *Microsoft*® Internet Explorer 5.5 or later or Netscape Navigator 4.7 or later). This is needed to view LSMS reports and display the on-line help.
- Adobe Acrobat 4.05 or later. This program is required to display the on-line manuals.

Installations on *Windows*® 2000 Server or Server 2003 platforms

If you are installing the LSMS application on *Windows*® 2000 Server or Server 2003 platforms, do not install Terminal Server in *Windows*®. An error message is generated when attempting to install LSMS 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 LSMS 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 LSMS 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 LSMS 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 LSMS application contains a web server which will conflict with any existing web server currently active on the LSMS. If there is another web server running on the LSMS host (such as *Microsoft*[®] Internet Information Server or Apache), you must either:

- Shut the web server down
or
- Select a different port for the LSMS web server when prompted by the installation program

Port 80 is the default. In the event that another web server is already using port 80 (such as IIS), that server can be reassigned to a different port so the LSMS can use port 80.

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 LSMS installation keys

To install the LSMS application, two keys are required:

- *Software license key*
The software license key is found on the CD-ROM case. You will need this key to register the product and to obtain the installation key (see below), which is required to perform the installation.
- *Installation key*
The installation key is required to install the product. To obtain this key, access the Lucent security web site at <http://www.lucent.com/security/>. Click **IP Service Product Registration and Support**, then click **Register Now**. You can also call Lucent Security Customer Care at 1-866-LUCENT-8 to register.

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

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

The installation key that you enter, which sets parameters affecting the operation of the LSMS, 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, register these license keys on the Lucent security website and obtain installation keys that you will use to enable these features on your LSMS. 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 LSMS after you finish the software installation process and enter your optional feature installation keys. Optional features enabled on the Primary LSMS are also automatically enabled on all associated Secondary and Compute Server LSMS 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 *LSMS Administration Guide*.

Software patches and documentation updates

It is a good idea to check the Lucent security web site periodically for patches and documentation updates issued since you purchased the product. The URL is:
<http://www.lucent.com/security/>

If you are installing the LSMS 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 LSMS software, these installation keys are only for

an upgrade to the current software release. When installing a patch version of the LSMS application, you do not need an installation key.



To Install the LSMS Application (Clean Installation)

When to use

Use this procedure to install the LSMS 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 LSMS, you must first:

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

Procedure

Use the following procedure to install the LSMS 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 *lsmis-9.1.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 LSMS that you obtained from the Lucent web site and click **Next**. Refer to the [“Obtain the LSMS installation keys”](#) (p. 9) 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 Lucent Security Management Server window allows you to specify where the LSMS software will be installed. The default is: *c:\users\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 LSMS 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 LSMS software.

- 7 The Where do you want the logs to go? window allows you to specify the folder where the LSMS logs will be stored. If you chose the default in the previous step, this selection defaults to: *c:\users\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 LSMS Configuration Assistant. Refer to *Using the Configuration Assistant* in the *LSMS Administration Guide* for more details.

- 8 The Select Program Folder window allows you to select the folder in which the LSMS application will appear on the Windows Start menu. The default is: **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 LSMS Web Server Configuration window is displayed.

.....

11 The LSMS 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 LSMS remotely, it is a good idea to use **HTTPS**. (To obtain and install a digital certificate, refer to the *Digital Certificates* section in the *LSMS 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 LSMS SNMP Agent Configuration window allows you to choose the port that the LSMS SNMP agent will use. The LSMS SNMP agent is used for remote monitoring of the LSMS and *Brick*[®] firewall appliances.

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 LSMS interacts with SNMP, refer to *Appendix A - SNMP* in the *LSMS Reports, Logs and Alarms Guide*.

.....

15 The Select LSMS Type window shows the following information:

- **LSMS 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.
 - **LSMS Name.** This field defaults to the LSMS Machine name, but you may override it and type your own selection.
 - **LSMS Type.** Based on the installation key entered, either **Primary LSMS**, **Secondary LSMS**, or **Compute Server LSMS** is selected and the others are grayed out.
-

16 If the installation is a Primary LSMS, the installation will proceed immediately to [Step 17](#).

If the installation is either a Secondary LSMS or a Compute Server installation, you will be asked to enter the IP address for either the Primary LSMS or the LSMS to which the

.....

Compute Server will home. The program will perform the additional steps required and proceed to [Step 20](#).

If the Secondary LSMS cannot contact the Primary LSMS, or the Compute Server cannot contact its associated LSMS, 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 LSMS must be installed/upgraded within 7 days of installing/upgrading a Primary LSMS. After more than 7 days, the installation or upgrade of a secondary will fail because the Primary LSMS does not allow the Secondary LSMS 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 LSMS or Compute Server installations, the LSMS services are initialized. Go to [Step 20](#).

- 17 For Primary LSMS 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 LSMS Setup screen. The purpose of the master key is to protect the root certificate used to authenticate communication between the LSMS 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 LSMS.

Result: The installation program displays the Enter Admin ID window so that you may create an LSMS 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 LSMS. 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 LSMS 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 LSMS services are initialized. While the services are starting, a progress bar indicates the status of the effort.

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

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



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

END OF STEPS



To Manually Un-Install LSMS

When to use

This procedure is not required or recommended for upgrading to the current LSMS release. As part of its software upgrade program, the LSMS automatically installs, upgrades to the current release, and un-installs the previous LSMS release.

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

Task

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

- 1 The LSMS can be un-installed via the **Add or Remove Programs** utility of the *Windows*[®] **Control Panel** by selecting **Lucent Security Management Server** and clicking **Remove**.
 - 2 For final removal, you can move to backup or delete the contents of the LSMS directory (Example: *c:\users\isms\lmsf*).
-

END OF STEPS



To Upgrade the LSMS Software

When to use

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

Procedure

Use the following procedure to upgrade to the current LSMS 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-9.1.xxx.exe* where *xxx* is the build number of the software.

This is the installation program. Windows indicating 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 LSMS that you obtained from the Lucent web site and click **Next**. Refer to the “[Obtain the LSMS installation keys](#)” (p. 9) section for the types of installation keys available.

Result: The Select Program Folder window is displayed.

- 6 Select the folder in which the LSMS application will appear on the *Windows*[®] **Start** menu. The default is **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 warning window is displayed, indicating that you should only upgrade to the current LSMS software release after enabling the IKE on the Brick feature in the previous release and on all Bricks. Then, a message window is displayed, indicating that a previous version of the LSMS already exists on the host.

.....

- 8 Click **OK**.

Result: The old LSMS 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 LSMS Web Server Configuration window is displayed.

.....

- 11 The LSMS 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 LSMS. The choices are **HTTP** and **HTTPS**, which relies on a digital certificate and is substantially more secure. If administrators will be logging into the LSMS remotely, it is a good idea to use **HTTPS**. (To obtain and install a digital certificate, refer to the *Digital Certificates* section in the *LSMS Policy Guide*.)
- **Port.** Enter the web server port. The value for **Port** defaults to the value specified during the initial installation of the LSMS. 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 LSMS Configuration Assistant after successful completion of the software upgrade.

.....

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

12 The Select LSMS Type window shows the following information:

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

13 If the upgrade installation is for a Primary LSMS, go to [Step 14](#). If the upgrade installation is for a Secondary LSMS or a Compute Server, the system prompts you for the IP address of the Primary LSMS or the LSMS to which the Compute Server will home. The program performs the additional steps required. If you are upgrading a secondary or Compute Server the LSMS services are initialized. After all LSMS 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 LSMS):

- **Normal upgrade.** If you know an Admin ID and password from the previous version of the LSMS, 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 floppies and reboot each unit from a 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 LSMS services are initialized. While the services are starting, a progress bar indicates the status of the services initialization.

- 16 When all LSMS services have been successfully started, click **OK** to continue.

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



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

END OF STEPS



What To Do Next

Overview

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

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

This entry enables you to:

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

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



3 LSMS on a *Solaris*[®] Server Platform

Overview

Purpose

This chapter explains how to install the LSMS application on a *Solaris*[®] server platform. It also includes a procedure for manually de-installing the application if necessary.

Contents

Introduction	26
Hardware Requirements	28
Software Requirements	29
Pre-Installation Requirements (Clean Installations)	30
To Install the LSMS Application (Clean Installation)	32
To Manually Un-Install LSMS	37
To Upgrade the LSMS Software	38
What To Do Next	42



Introduction

Overview



CAUTION

Service disruption hazard

LSMS only supported on SPARC processors.

The LSMS is only supported on SPARC processors that are running Solaris® Release 2.8, 2.9, or 2.10. For additional requirements, refer to the “[Hardware Requirements](#)” (p. 28) section.

Upgrades



CAUTION

Service disruption hazard

Security Precaution

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

Important! The LSMS and all Lucent Virtual Firewall *Brick*® devices must have the IKE on the Brick feature enabled before upgrading to the current LSMS release.

LSMS configurations

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

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

Multi-Site LSMS configuration

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

Compute servers

To maximize scalability of the LSMS/Brick security solution, LSMS provides the option of adding a separate set of servers called Lucent Secure Compute Servers (LSCSs), or simply Compute Servers, which are associated with a Primary or Secondary LSMS and act as collection points for Brick log traffic. Using an LSCS to collect Brick log data frees up

computing resources on the LSMS itself and extends the number of Brick devices and total log traffic that can be handled. Each Brick device managed by the LSMS can be homed to one of the associated LSCSs or the managing LSMS for logging purposes.

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

Implementing Primary LSMS/Secondary LSMS Configurations

During the installation of the Secondary LSMS, there is a point at which the Secondary LSMS attempts to contact the Primary LSMS to replicate the Primary LSMS database on the Secondary LSMS. If the Secondary LSMS cannot contact the Primary LSMS, the installation fails.

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

To ensure that the Primary LSMS and Secondary LSMS(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 LSMS 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 LSMS is operational, use it to configure two Bricks and assign the pre-configured ruleset *administrativezone* to the ports that will be connected to the LSMS. Refer to the *Configuring Brick Ports* section in the *LSMS Administration Guide* for instructions on how to do this.
3. Connect the Primary LSMS to the port on one Brick, and the host that will be the Secondary LSMS to the port on the other. Then, deploy the two Bricks: the primary LSMS and the host that will be the Secondary LSMS in the network.
4. To ensure that the Primary LSMS 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 LSMS. Once the ping is successful, remove the rule for security reasons. (Refer to the *Brick Zone Rulesets* section in the *LSMS Policy Guide* for instructions on how to create a rule.)
5. When you have established that the two LSMS servers can communicate, install the Secondary LSMS.

□

Hardware Requirements

Minimum hardware requirements

Regardless of which operating system you are running, the workstation on which you install the LSMS 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 LSMS 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 the following website: <http://www.lucent.com/security>.
- *Ethernet*[™] interface card

Important! Because of the memory requirements of LSMS R9.1, 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 *Appendix B. Sizing Guidelines* in the *LSMS 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 LSMS application on a *Solaris*[®] platform, you need *Solaris*[®] 2.8, 2.9, or 2.10. 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:

- Netscape Navigator 4.7 or later is not required, but is highly recommended. This is needed to view LSMS reports and display the on-line help.
- Adobe Acrobat 4.05 or later. This program is required to display the on-line manuals. This application can be downloaded from the Adobe website, <http://www.adobe.com>.



Pre-Installation Requirements (Clean Installations)

Overview

Before you proceed with the actual installation of the LSMS 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 LSMS 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 LSMS application includes a web server. If there is another web server running on the LSMS host (such as Apache), you must either:

- Shut the web server down
or
- Select a different port for the LSMS web server when prompted by the installation program

Important! 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 LSMS web server.

Port 80 is the default. In the event that another web server is already using port 80 (such as Apache), that server can be reassigned to a different port so the LSMS can use port 80.

Obtain the LSMS installation keys

To install the LSMS application, two keys are required:

- *Software license key*
The software license key is found on the CD-ROM case. You will need this key to register the product and to obtain the installation key (see below), which is required to perform the installation.
- *Installation key*
The installation key is required to install the product. To obtain this key, access the Lucent security web site at <http://www.lucent.com/security/>. Click **IP Service Product Registration and Support**, then click **Register Now**. You can also call Lucent Security Customer Care at 1-866-LUCENT-8 to register.

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

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

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

The installation key that you enter, which sets parameters affecting the operation of the LSMS, 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, register these license keys on the Lucent security website and obtain installation keys that you will use to enable these features on your LSMS. 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 LSMS after you finish the software installation process and enter your optional feature installation keys. Optional features enabled on the Primary LSMS are also automatically enabled on all associated Secondary and Compute Server LSMS 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 *LSMS Administration Guide*.

Software patches and documentation updates

It is a good idea to check the Lucent security web site periodically for patches and documentation updates issued since you purchased the product.

If you are installing the LSMS 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 LSMS software, these installation keys are only for an upgrade to the current software release. When installing a patch version of the LSMS application, you do not need an installation key.



To Install the LSMS Application (Clean Installation)

When to use

Use this procedure to install the LSMS 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 LSMS, you must first:

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

Procedure

Complete the following steps to install the LSMS 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 after registering the license key at <http://www.lucent.com/security>

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

-
- 8 Press **[Enter]** to store the LSMS log files in the default directory (*/opt/isms/lmf/logs*), 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 LSMS Configuration Assistant. Refer to *Using the Configuration Assistant* in the *LSMS Administration Guide* for more details.

Result: The installation program asks whether you want to configure the LSMS 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 LSMS remotely, it is a good idea to use HTTPS.

To obtain and install a digital certificate, see the *Digital Certificates* section in the *LSMS 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 LSMS 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 LSMS SNMP Agent provides the ability to monitor the LSMS 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 LSMS SNMP Agent or define another port, as needed.

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

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

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

For additional information on how the LSMS interacts with SNMP, refer to *Appendix A. SNMP* in the *LSMS Reports, Logs, and Alarms Guide*.

For additional information about the LSMS Configuration Assistant, refer to *Using the Configuration Assistant* in the *LSMS 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 LSMS.

As of Release 8.0, the LSMS 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 LSMS.

- 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 LSMS machine.

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

If you are installing a Secondary LSMS or Compute Server, skip to [Step 20](#).

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

This process will take several minutes.

For Primary LSMS installations, a master key is generated and displayed in the lower half of the LSMS Setup screen. The purpose of the master key is to protect the root certificate used to authenticate communication between the LSMS 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 LSMS.

.....

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

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

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

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

Result: The remaining files are installed and all LSMS 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 LSMS 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 *LSMS Administration Guide*.



To Manually Un-Install LSMS

When to use

This procedure is not required or recommended for upgrading to the current LSMS release. As part of its software upgrade program, the LSMS automatically installs, upgrades to the current release, and un-installs the previous LSMS release.

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

Task

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

- 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 LSMS directory (Example:
`c:\opt\isms\lmsf\`

END OF STEPS



To Upgrade the LSMS Software

When to use

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

Procedure

Complete the following steps to upgrade the LSMS 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 LSMS 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 at <http://www.lucent.com/security>

Result The installation program displays a message indicating a previous version of the LSMS 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 LSMS. Enter Y a third time when the program warns that the script will be executed as super-user.

Result The previous version of the LSMS is removed.

- 9 During an upgrade, the install directory defaults to the value specified during the initial installation of the LSMS. 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 LSMS. 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 LSMS. 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 LSMS remotely, it is a good idea to use HTTPS.

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

Important! The values for the Web Server **TYPE** and **PORT** can be changed using the LSMS 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 LSMS. 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 LSMS.

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

.....

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

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

If you are upgrading a Secondary or Compute Server LSMS, the remaining files and settings are now installed and all LSMS services are started. If the upgrade installation is for a Secondary LSMS or a Compute Server, the system prompts you for the IP address of the Primary LSMS or the LSMS 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 LSMS, go to [Step 15](#).

.....

15 If you are upgrading a Primary LSMS, 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 LSMS Admin ID.

.....

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

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

.....

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

Result: The remaining files and settings are now installed and all LSMS services are started.

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

.....
E N D O F S T E P S
.....

Configuration Assistant

The Configuration Assistant allows you to set certain systemwide parameters. You can open the Configuration Assistant now to change LSMS 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 *LSMS Administration Guide*.



What To Do Next

Overview

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

1. It placed an entry called **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 LSMS application using the LSMS Navigator or, if previously installed, the LSMS Remote Navigator
 - Open the local LSMS Log Viewer
 - Access the five LSMS utilities (Configuration Assistant, Certificate Manager, New Feature Setup, LSMS Service Status, and LSMS Schedule Editor)
 - Start and stop the LSMS services
 - Restart LSMS services
2. It created an LSMS Administrator account with full privileges that you, or another administrator, can use to log into the LSMS 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 **Windows > Update Workspace Menu**.
 - c. Select **Windows > Restart Workspace Manager**.

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 *LSMS Administration Guide*.

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



Index

-
- B** Brick devices
 supported, [vi](#)
-
- C** Clean installation
 Solaris® server platform, [32](#)
 Windows® server platform, [11](#)
 Compute servers, [4](#), [26](#)
 Configuration Assistant, [36](#), [41](#)
-
- H** Hardware requirements
 Solaris® server platform, [28](#)
 Windows® server platform, [6](#)
-
- I**
 Installation keys, [8](#), [30](#)
-
- L** LSCS
 See: Lucent Secure Compute Servers (LSCSs)
 LSMS
 software patches, [9](#), [31](#)
 LSMS configurations, [4](#), [26](#)
 Lucent Secure Compute Servers (LSCSs), [4](#), [26](#)
-
- M** Manually un-install LSMS
 Solaris® server platform, [37](#)
 Windows® server platform, [17](#)
-
- N** New Feature Setup utility, [8](#), [30](#)
-
- P** Post-installation steps
 Solaris® server platform, [42](#)
 Windows® server platform, [23](#)
Pre-installation requirements
 Solaris® server platform, [30](#)
 Windows® server platform, [8](#)
-
- S** Software requirements
 Solaris® server platform, [29](#)
 Windows® server platform, [7](#)
 Solaris® server platform
 clean installation, [32](#)
 hardware requirements, [28](#)
 manually un-install LSMS, [37](#)
 post-installation steps, [42](#)
 pre-installation requirements, [30](#)
 software requirements, [29](#)
 upgrade LSMS software, [38](#)
-
- U** Upgrade LSMS software
 Solaris® server platform, [38](#)
 Windows® server platform, [18](#)
-
- W** Windows® 2000 Server
 installations, [7](#)
Windows® 2003 Server
 installations, [7](#)
Windows® server platform
 clean installation, [11](#)
 hardware requirements, [6](#)
 manually un-install LSMS, [17](#)
 post-installation steps, [23](#)
 pre-installation requirements, [8](#)
 software requirements, [7](#)
 upgrade LSMS software, [18](#)
-

