



Cisco Subscriber Edge Services Manager Installation Guide

SESM 3.3

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco Subscriber Edge Services Manager Installation Guide
Copyright © 2002-2005 Cisco Systems, Inc. All rights reserved.



About This Guide ix

Document Objectives	ix
Audience	ix
Document Organization	x
Document Conventions	x
Related Documentation	xi
Obtaining Documentation	xii
Cisco.com	xii
Documentation CD-ROM	xii
Ordering Documentation	xii
Documentation Feedback	xiii
Obtaining Technical Assistance	xiii
Cisco TAC Website	xiii
Opening a TAC Case	xiii
TAC Case Priority Definitions	xiv
Cisco Developer Support Program	xiv
Program Benefits	xiv
Contacting Cisco Developer Support	xv
Obtaining Additional Publications and Information	xv

CHAPTER 1

SESM Overview 1-1

Introduction to SESM	1-1
SESM Installation Types	1-3
SESM SPE Installation	1-4
SESM RADIUS Installation	1-4
SESM Installation Options	1-5
SESM Typical Installation	1-5
SESM Custom Installation	1-5
SESM Demo Installation	1-6
SESM Installation Scenarios	1-6
New SESM Installation	1-6
Upgrading From a Previous SESM Release	1-6

CHAPTER 2**Before You Begin 2-1**

- System Requirements 2-1
- Memory Requirements for Running SESM Applications 2-2
 - Memory Requirements for SESM Web Applications 2-2
 - Memory Requirements for RDP 2-3
 - Memory Requirements for DNS Proxy 2-3
- Performance Considerations 2-4
- Java Software Considerations 2-4
 - JRE Requirements 2-4
 - JDK Requirements 2-4
 - Solaris Patch Requirements 2-5
- Installing and Configuring Related Components 2-5
- Gathering Information Required for the SESM Installation 2-6
- Obtaining the SESM Installation Image File 2-7
 - Downloading Software from the Cisco Website 2-7
 - Uncompressing the Image 2-7
- Obtaining a SESM License Number 2-8
- Gaining Required Privileges for Installation 2-8

CHAPTER 3**Configuring the Selection Services Gateway to Work with SESM 3-1**

- Introduction 3-1
- Configuring SSG to Work with SESM 3-2
 - Configuring the Port-Bundle Host Key Feature on SSG 3-4
 - Configuring the SSG to Match the Installed SESM Captive Portal 3-5
 - Configuring the SSG TCP Redirect Features 3-5
 - Configuring SSG and Port-Bundle Host Key to Work with Captive Portal 3-6
 - Defining Captive Portal Groups 3-6
 - Defining Port Lists 3-7
 - Configuring Unauthenticated User Redirection 3-7
 - Configuring Unauthorized Service Redirection 3-8
 - Configuring Initial Logon Redirection 3-10
 - Configuring Advertising Redirection 3-11
 - Configuring Prepaid Redirection 3-12
- Example SSG Configuration for Working With SESM 3-12

CHAPTER 4**Configuring the Servers in Your Deployment for SESM 4-1**

- Configuring an LDAP Directory to Work with SESM 4-1
 - Choosing a Suitable LDAP Directory 4-2
 - Installing and Configuring Novell eDirectory Version 8.7 to Work with SESM 4-2
 - Installing and Configuring Sun ONE (iPlanet) to Work with SESM 4-5
 - Extending the Directory Schema and Loading Initial RBAC Objects 4-7
 - Loading Sample SESM Data 4-7
- Configuring Cisco Access Registrar for SESM Deployments 4-8

CHAPTER 5**Installing and Uninstalling SESM 5-1**

- Installation Methods and Logging Options 5-1
 - GUI Mode Installation 5-1
 - Console Mode Installation 5-2
 - Silent Mode Installation 5-2
 - SESM Installation Logging Feature 5-3
 - Commands to Start Installation 5-3
- Running the Installation Program 5-4
 - Installing a Licensed Version 5-5
 - Installing an Evaluation Version 5-5
- Responding to Installation Program Prompts 5-6
- Installation Results 5-20
- Uninstalling a SESM Installation 5-22
- What's Next 5-22
 - Post-Installation Configuration Tasks 5-23
 - Creating Profiles 5-23
 - Running SESM Applications 5-23
 - Customizing SESM Applications 5-23

CHAPTER 6**Upgrading to SESM 3.3(1) 6-1**

- Upgrading the LDAP Directory with SPE Schema Extensions 6-1
 - Upgrading the LDAP Directory from SESM 3.2(2) 6-1
 - Upgrading the LDAP Directory from SESM 3.1(9) or SESM 3.2(1) 6-2
 - Upgrading the LDAP Directory from SESM 3.1(3), SESM 3.1(5), or SESM 3.1(7) 6-3
- Preserving SESM Customizations and Configurations 6-3

CHAPTER 7**Tuning SESM for Optimal Performance 7-1**

- Platform Patches and Platform Specific Java/J2SE Patches 7-1
- Java Virtual Machine 7-2
 - JVM Memory Allocation 7-2
 - Garbage Collection 7-2
 - Java Version 7-3
- Jetty Web Server 7-3
- SESM Memory Management 7-4
- SESM Cache Settings 7-4
- SSG MBEAN Settings 7-5
- SSG MBEAN Statistics 7-6
- SESM Logging 7-7

APPENDIX A**Example SESM RADIUS Installation A-1**

- Introduction A-1
- Assumptions A-2
- Setting Up a SESM RADIUS Installation A-2
 - Step 1: Installing a SESM RADIUS Installation A-2
 - Step 2: Running SESM Components A-5
 - Step 3: Logging On to a Web Portal A-5
- What to Do Next A-6
 - Finding Further Information A-6
 - Troubleshooting A-6

APPENDIX B**Example SESM SPE Installation B-1**

- Introduction B-1
- Assumptions B-2
- Setting Up a SESM SPE Installation B-3
 - Step 1: Installing a SESM SPE Installation B-3
 - Step 2: Installing CDAT Sample Data B-6
 - Step 3: Starting CDAT and Accessing the CDAT Home Page B-7
 - Step 4: Logging In to CDAT B-7
 - Step 5: Running SESM Components B-8
 - Step 6: Logging On to a Web Portal B-8
- What to Do Next B-9
 - Finding Further Information B-9
 - Troubleshooting B-9

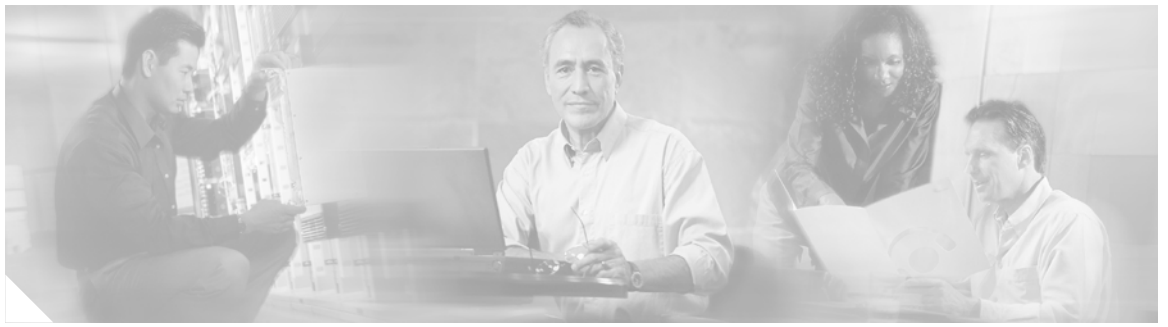
APPENDIX C**Configuration File Changes in SESM 3.3(1) C-1**

nwsp.xml file	C-2
rdp.xml file	C-6
webproxy.xml	C-8
captiveportal.xml	C-10
wsg.xml	C-12
nwsp.web-jetty.xml	C-13
webproxy.web-jetty.xml	C-14
captive.web-jetty.xml	C-14
Additional Changes	C-15

APPENDIX D**SESM Performance Information D-1**

NWSP Performance	D-1
NWSP iPass Servlet Performance	D-2
WSG Performance	D-3
Captive Portal Performance	D-4
Web Proxy Performance	D-6
RDP Performance	D-7
DNS Proxy Performance	D-8

INDEX



About This Guide

This preface introduces *Cisco Subscriber Edge Services Manager Installation Guide*. The preface contains the following sections:

- [Document Objectives](#)
- [Audience](#)
- [Document Organization](#)
- [Document Conventions](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Document Objectives

This guide contains installation prerequisites and procedures for all of the Cisco Subscriber Edge Services Manager (SESM) software components. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their end users (subscribers) with a single web interface for accessing multiple Internet Protocol (IP) services and value-added features.

Audience

This guide is intended for administrators, web developers, and others who are responsible for installing SESM applications.

Document Organization

This guide contains the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	SESM Overview	Provides information on SESM and its installation options.
Chapter 2	Before You Begin	Provides information on the hardware and software requirements for SESM.
Chapter 3	Configuring the Selection Services Gateway to Work with SESM	Provides information on the minimum required configuration for the Cisco Service Selection Gateway (SSG) to work with SESM.
Chapter 4	Configuring the Servers in Your Deployment for SESM	Provides information on how to configure the servers in your deployment for use with SESM.
Chapter 5	Installing and Uninstalling SESM	Provides information on how to install the SESM software and bundled components, including the Security Policy Engine (SPE).
Chapter 6	Upgrading to SESM 3.3(1)	Provides information on how to upgrade SESM from previous releases.
Chapter 7	Tuning SESM for Optimal Performance	Provides information on how to ensure optimal performance for SESM.
Appendix A	Example SESM RADIUS Installation	Provides an example of how to install and configure a SESM RADIUS installation.
Appendix B	Example SESM SPE Installation	Provides an example of how to install and configure a SESM SPE installation.
Appendix C	Configuration File Changes in SESM 3.3(1)	Describes the changes in configuration files in SESM 3.3(1).
Appendix D	SESM Performance Information	Provides guidelines to help you achieve optimal performance for SESM.
Index		

Document Conventions

The following conventions are used in this guide:

- *Italic* font is used for parameters for which you supply a value, emphasis, and to introduce new terms.
- **Bold** font is used for user entry and command names.
- `Computer` font is used for examples.



Note

Means reader take note. Notes contain helpful suggestions or references to materials not contained in this guide.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for SESM 3.3 includes:

- *Release Notes for Cisco Subscriber Edge Services Manager 3.3(1)*
- *Cisco Subscriber Edge Services Manager Introduction Guide*
- *Cisco Subscriber Edge Services Manager Installation Guide*
- *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*
- *Cisco Subscriber Edge Services Manager Web Portals Guide*
- *Cisco Subscriber Edge Services Manager Profile Management Guide*
- *Cisco Subscriber Edge Services Manager Web Services Gateways Guide*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Subscriber Edge Services Manager SDK Programmer Guide*
- *Cisco Subscriber Edge Services Manager Troubleshooting Guide*

Documentation for SESM is online at:

<http://www.cisco.com/univercd/cc/td/doc/solution/sesm/index.htm>

Documentation for the Cisco SSG is online at:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/ssg/
- <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/>

Information related to configuring the SSG authentication, authorization, and accounting features is included in:

- *Cisco IOS Security Configuration Guide:*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/sec_vcg.htm
- *Cisco IOS Security Command Reference*

If you are including the Cisco Access Registrar (a RADIUS server) in your SESM deployment, see the documentation for Cisco Access Registrar (AR) online at:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Cisco Developer Support Program

The Developer Support Program was developed to provide formalized support for Cisco interfaces to accelerate the delivery of compatible solutions to Cisco customers. The program web site at <http://www.cisco.com/go/developersupport> provides a central resource point for all your development needs.

Program Benefits

- Product and document downloads
- Bug reports
- Sample scripts
- Frequently Asked Questions
- Access to Developer Support Engineers

Many of the product and document downloads are accessible with a Cisco.com guest level login. However, as a member of the program, you will get access to all the program benefits listed above to promote your development efforts. The subscription also provides the ability to open support cases using the same infrastructure and processes used by Cisco Technical Assistance Center (TAC).

Our Subscription membership is fee-based. The Developer Support Agreement, with the subscription fees and list of supported interfaces, is available on the Developer Support Web site.

**Note**

The Cisco TAC does NOT provide support for this API/interface under standard hardware or software support agreements. All technical support for this API/interface, from initial development assistance through API troubleshooting/bugs in final production apps, is provided by Cisco Developer Support and requires a separate Developer Support contract. When opening cases, a Developer Support contract number must be provided in order to receive support.

Contacting Cisco Developer Support

You can contact Cisco Developer Support using the following:

- Email: developer-support@cisco.com
- Web: <http://www.cisco.com/go/developersupport>

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *The Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqumagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>



SESM Overview

This chapter provides a brief overview of the Cisco Subscriber Edge Services Manager (SESM), and installation options. This chapter contains the following sections:

- [Introduction to SESM, page 1-1](#)
- [SESM Installation Types, page 1-3](#)
- [SESM Installation Options, page 1-5](#)
- [SESM Installation Scenarios, page 1-6](#)

Introduction to SESM

Cisco Subscriber Edge Services Manager (SESM) provides on-demand value-added services and access control at the network edge. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM solutions to provide value-added services to their subscriber base and management capabilities to their administrators.

SESM contains:

- **Sample web portal applications** that you can install and configure for demonstration purposes or as a starting point for customizations:
 - New World Service Provider (NWSP) portal—Provides a fully functional web portal for network services. Developers can use the NWSP web components as a starting point for designing and creating a SESM web application.
 - Wireless Access Protocol (WAP) portal—Provides a subset of the SESM functionality for WAP subscribers. It is designed specifically for deployment in the mobile wireless industry.
 - Personal Digital Assistant (PDA) portal—Provides a subset of the SESM functionality for subscribers using a PDA or other handheld device.
 - subscriber portal—provides example web pages to demonstrate deployment in the public wireless LAN (PWLAN), broadband, and metropolitan WAN (MWAN) markets.
- **Captive portal solution applications:**
 - Captive Portal application—A gateway application for use with the Service Selection Gateway (SSG) and other applications in a captive portal solution. The default configuration for this application redirects subscriber browsers to either the Message Portal application or the NWSP application.
 - Message Portal application—A SESM application that produces sample greetings and advertising pages to demonstrate SESM captive portal features.

- **Web Services Gateway (WSG)**— A SESM application that enables third-party web portals and subscriber management systems to integrate with the SESM and SSG solution using Simple Object Access Protocol over HTTP (SOAP/HTTP).
- **Application Manager (AM)**—A web-based tool through which administrators can view and change configuration attributes for running applications.

Software components included in the Cisco SESM installation package for SESM SPE installations are:

- **RADIUS Data Proxy (RDP) server**—A RADIUS server that can transform RADIUS requests into Security Policy Engine (SPE) API calls to work with SPE extensions. This server can also read and processes profiles in Merit format.
- **Cisco Distributed Administration Tool (CDAT)**—A web-based tool from which administrators can maintain data in the SESM container in an Lightweight Directory Access Protocol (LDAP) directory.
- **SPE component**—This component provides the interface between SESM applications and the SPE directory.

Additional software components included in the SESM installation package are:

- Java Runtime Environment (JRE)—JRE version 1.4.2 is included in the SESM installation image. The installation process always installs this version.
- J2EE (Java 2 Platform, Enterprise Edition) components:

- Sun example Java Management Extensions (JMX) server—This is a fully functional JMX server from Sun Microsystems. SESM depends on the JMX server for internal object configuration. For more information about JMX technology and its related JMX MBean standards, see:

<http://java.sun.com/products/JavaManagement/>

The sample SESM portal applications and CDAT are installed with configuration files and startup scripts that are ready to run using the Jetty webserver and the Sun example JMX server. RDP is installed with configuration files and a startup script that is ready to run using the JMX server.

- Jetty webserver—Jetty is a J2EE-compliant server package from Mort Bay Consulting that is released under an open source license. The license puts few restrictions on usage of Jetty. For more information about the Jetty server, see:

<http://jetty.mortbay.org/>

- JSP engine—The Jasper Java Server Pages (JSP) engine from Apache Software Foundation, Servlets Version 2.3 and JSP Version 1.2.
- JNDI—The Java Naming and Directory Interface (JNDI) from Sun Microsystems is a standard extension to the Java platform, providing a unified interface to multiple naming and directory services in the enterprise. For more information, see:

<http://java.sun.com/products/jndi>

Figure 1-1 shows the software included in the SESM package.

Figure 1-1 SESM Package Contents

	* SESM Sample Applications	SESM Management Applications	Software Bundled with SESM	Core Applications
SESM-RADIUS				
SESM-SPE				

120693

* Includes SESM platform development kit

SESM Installation Types

SESM provides the following installation types:

- [SESM SPE Installation, page 1-4](#)
- [SESM RADIUS Installation, page 1-4](#)

SESM SPE Installation

In a SESM SPE installation, the Cisco Subscriber Policy Engine (SPE) is installed, which provides the libraries and directory schema extensions that enable queries to an LDAP directory for authentication and authorization information.

SESM web applications deployed in a SESM SPE installation require access to an LDAP-compliant directory. Typically, you would use the SESM SPE installation because you require the self-care features that are provided, such as service subscriptions, firewalls, subaccounts, or notification of personal account details.

You must also use the SESM SPE installation if you want to use the SESM Trusted ID Authorization feature.

The SESM SPE installation includes the following items:

- Cisco SPE AUTH library—The AUTH library implements a role-based access control (RBAC) authorization model. The RBAC model allows administrators to manage groups of subscribers, rather than individuals. Using the RBAC model, administrators define roles, which have specific privileges, and groups, which have assigned roles. Individual subscribers are then assigned to a group and inherit the roles of that group.
- Cisco SPE DESS library—The directory-enabled service selection (DESS) library provides the framework for using the RBAC model in an LDAP directory.
- Files containing the directory schema extensions. The install program can optionally apply these extensions to your LDAP directory.
- Files containing sample RBAC data.

If your LDAP directory is configured and running, the installation program can communicate with the LDAP directory using the communication parameters that you provide, and can perform the following required tasks:

- Extend the directory schema with the SPE extensions. These extensions are the LDAP classes and attributes that will hold the SESM subscriber profiles, service profiles, and policy information.
- Install top-level RBAC objects that are required before administrators can log into CDAT to create additional RBAC objects and before you can install the SESM sample data.

If the installation program does not perform these tasks, you must do them at a later time by running the installation program again, before running the SESM web application or CDAT.

To configure an LDAP directory to work with SESM, see [Configuring an LDAP Directory to Work with SESM, page 4-1](#). For information about the RBAC model, the DESS and AUTH extensions to an LDAP directory, and how to develop subscriber and service profile information in the RBAC model, see *Cisco Subscriber Edge Services Manager Profile Management Guide*.

SESM RADIUS Installation

The SESM RADIUS installation does not support the self-care features provided by a SESM SPE installation. Typically, you would use the SESM RADIUS installation when you want to use an existing RADIUS server with SESM and do not require self-care features.

In a SESM RADIUS installation, the SESM web application and SSG query a RADIUS server for authentication and authorization information.

SESM RADIUS installation works with any RADIUS server that accepts Cisco SSG vendor-specific attributes (VSAs). Cisco VSAs define the subscriber and service profile information required in the SESM deployments. The RADIUS protocol is based on a client server model. This uses a RADIUS server and a multiple dial-in Network Access Server (NAS) devices are the clients. Before communication can occur, each client must be configured on the RADIUS server. One RADIUS server to consider in your deployment is the Cisco Access Registrar, a carrier class RADIUS platform that is fully tested with SESM. For information about configuring Cisco Access Registrar to work with SESM, see the AR documentation. See [Related Documentation, page xi](#) for the link to the AR documentation.

For more information about RADIUS, see RFC 2865. For more information about RADIUS accounting, see RFC 2866.

SESM Installation Options

SESM provides the following installation options:

- [SESM Typical Installation, page 1-5](#)
- [SESM Custom Installation, page 1-5](#)
- [SESM Demo Installation, page 1-6](#)

SESM Typical Installation

A SESM typical installation installs all the following components in the same directory on the same machine:

- Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model.
- Captive portal solution applications—Includes the Captive Portal and Message Portal applications.
- Jetty—Includes the Jetty webserver, Jetty web proxy application, the JMX server, and JNDI.
- RDP—Installed only when installation type is SPE evaluation or SPE license.
- CDAT—Installed only when installation type is SPE evaluation or SPE license.
- Application Manager—Installed for all installation types.
- SPE—Installed only when installation type is SPE evaluation or SESM-SPE license.
- Tools—Includes utilities for testing, development, and small-scale production environments.

SESM Custom Installation

A SESM custom installation allows you to choose the components to install and configure from a checklist. Choose this option to:

- Install WSG.
- Reinstall one of the SESM components.
- Distribute the SESM components among different workstations.

SESM Demo Installation

In a SESM Demo installation, the SESM web application simulates the actions of a SESM application in a RADIUS or an SPE installation. It is not configured to communicate with an SSG, RADIUS server, or LDAP directory. It uses a local copy of a merit RADIUS file to obtain profile information.

Typically you would use this installation when you want to demo SESM features without the SSG, RADIUS server, or LDAP directory components.

**Note**

If you install a SESM Demo installation and later want to run the portals in a RADIUS or SPE installation, we recommend that you run another SESM installation for a RADIUS or SPE installation. Otherwise, you must make extensive adjustments to configuration attributes in the MBeans.

SESM Installation Scenarios

- [New SESM Installation, page 1-6](#)
- [Upgrading From a Previous SESM Release, page 1-6](#)

New SESM Installation

If you are installing SESM for the first time, you will need to:

- Prepare for installation. See [Chapter 2, “Before You Begin.”](#)
- Configure SSG to work with SESM. See [Chapter 3, “Configuring the Selection Services Gateway to Work with SESM.”](#)
- For a SESM SPE installation, configure the LDAP server to work with SESM. See [Chapter 4, “Configuring the Servers in Your Deployment for SESM.”](#)
- Install SESM. See [Chapter 5, “Installing and Uninstalling SESM.”](#)

Upgrading From a Previous SESM Release

When you upgrade from a previous release of SESM, you can preserve all your configurations and web portal customizations from the previous release.

If you are upgrading a SESM SPE installation, you must update your LDAP directory.

For information on upgrading SESM, see [Chapter 6, “Upgrading to SESM 3.3\(1\).”](#)



Before You Begin

This chapter describes system requirements for SESM, and describes the tasks required before you install SESM. The chapter contains the following topics:

- [System Requirements, page 2-1](#)
- [Memory Requirements for Running SESM Applications, page 2-2](#)
- [Performance Considerations, page 2-4](#)
- [Java Software Considerations, page 2-4](#)
- [Installing and Configuring Related Components, page 2-5](#)
- [Gathering Information Required for the SESM Installation, page 2-6](#)
- [Obtaining the SESM Installation Image File, page 2-7](#)
- [Obtaining a SESM License Number, page 2-8](#)
- [Gaining Required Privileges for Installation, page 2-8](#)

System Requirements

SESM applications can run on operating systems that support the Java Runtime Environment (JRE). [Table 2-1](#) lists the minimum system requirements for running SESM in a production environment.

Table 2-1 *Operating System and Hardware Requirements*

Operating System	Hardware
<ul style="list-style-type: none">• Solaris Version 8 or 9	<ul style="list-style-type: none">• Sun Fire V210 (or later version) Single or Dual CPU, 1002 MHz SUNW UltraSPARC-IIIi processor 2 GB RAM• Sun Blade 2000 Single or Dual CPU, 1200 MHz SUNW UltraSPARC-III+ processor 2 GB RAM
<ul style="list-style-type: none">• Windows 2000 with Service Pack 4 or later	<ul style="list-style-type: none">• Pentium 4 (or equivalent) processor
<ul style="list-style-type: none">• Red Hat Enterprise Linux ES3• Red Hat Enterprise Linux AS	<ul style="list-style-type: none">• Sun Cobalt Dual CPU, 1.4 GHz 2 GB RAM

**Note**

If you intend to use SESM for large scale configuration of whitelists and locations, we recommend as a minimum, SUN V250, with Dual CPU, and 2GB memory.

**Note**

SESM Application Manager (AM) uses applets; hence the client machine requires Java Virtual Machine (JVM) to run AM.

The temporary disk space required for a SESM installation is approximately 50 MB on any system, regardless of the installation options you choose.

Memory Requirements for Running SESM Applications

This section describes how to calculate memory requirements for SESM applications:

- [Memory Requirements for SESM Web Applications, page 2-2](#)
- [Memory Requirements for RDP, page 2-3](#)
- [Memory Requirements for DNS Proxy, page 2-3](#)

Memory Requirements for SESM Web Applications

This section describes how to calculate the memory requirements for the following SESM web applications:

- Captive Portal
- NWSP
- Web Proxy
- WSG

The following equation calculates the RAM required for running a single SESM web application:

$$Java\ Heap = Base + M(t) * N(t) + M(cu) * N(cu) + K(conf) * S(conf)$$

where:

- *JavaHeap* is the amount of Java virtual memory to reserve for use by the SESM application. This is a predefined block of memory, reserved at application startup. The SESM generic start script (jetty/bin/start.sh) sets the JavaHeap using an argument to the JAVA command. The following line is near the end of the start script:

```
$JAVA -Xms64m -Xmx64m
```

The -Xms argument is the initial memory to reserve. The -Xmx argument is the maximum memory to reserve. We recommend using the same numeric value for both.

- *Base* is base memory required for each web application.
- *M(t)* is memory required per thread.
- *N(t)* is number of threads.
- *M(cu)* is memory required per user.
- *N(cu)* is number of concurrent users.

- $K(conf)$ is additional configuration memory per MB of configuration file (locations and whitelists).
- $S(conf)$ is size of configuration file in MB.

We recommend that you use the following values to calculate memory requirements for each SESM web application:

- Base memory for each web application—10 MB.
- Memory required per thread—50 KB.
- Memory required per user:
 - SESM SPE installation—70 KB.
 - SESM RADIUS installation—70 KB.
- Additional memory required per MB configuration file—15 MB



Note

The memory required for threads and users must be converted to MB.

Memory Requirements for RDP

The following equation calculates the RAM required for running RDP:

$$Java\ Heap = Base + M(t) * N(t)$$

where:

- *JavaHeap* is the amount of Java virtual memory to reserve for use by the SESM application. This is a predefined block of memory, reserved at application startup. The SESM generic start script (jetty/bin/start.sh) sets the JavaHeap using an argument to the JAVA command. The following line is near the end of the start script:

```
$JAVA -Xms64m -Xmx64m
```

The -Xms argument is the initial memory to reserve. The -Xmx argument is the maximum memory to reserve. We recommend using the same numeric value for both.

- *Base* is base memory required for each web application.
- $M(t)$ is memory required per thread.
- $N(t)$ is number of threads.

We recommend that you use the following values to calculate memory requirements for RDP:

- Base memory—5 MB.
- Memory required per thread size—10 KB.

Memory Requirements for DNS Proxy

The DNS Proxy application requires 64 MB RAM.

Performance Considerations

Many factors affect performance of SESM applications including:

- Subscriber load.
- JSP page contents.
- Size of user profiles.
- Size of SESM configuration files (for whitelists and location definitions).

Deployment sites might have additional critical factors affecting the design and development of a robust network.

[Appendix D, “SESM Performance Information”](#) provides SESM performance test results to help you plan your SESM deployment.

[Chapter 7, “Tuning SESM for Optimal Performance”](#) provides guidelines to help you achieve optimal performance for SESM.

Java Software Considerations

This section describes the SESM requirements regarding Java Runtime Environment (JRE) and Java Development Kit (JDK). The section includes the following topics:

- [JRE Requirements, page 2-4](#)
- [JDK Requirements, page 2-4](#)
- [Solaris Patch Requirements, page 2-5](#)

JRE Requirements

A JRE is included in the SESM installation image. The installation process automatically installs this bundled version. JRE version 1.4.2 is required for SESM.



Note

To use a different version of JRE or JDK, you should either define a `JDK_HOME` environment variable or edit the start scripts to explicitly point to it. For more information about determining a JVM at application startup, see *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*.

JDK Requirements

A JDK (Version 1.4.2 required) must be installed on any system that web developers will use to create or modify the Java Server Pages (JSPs) for a customized SESM application. The JDK is necessary for recompiling the changed JSPs. See *Subscriber Edge Services Manager Web Developer Guide* for more information. You can obtain JDK Version 1.4.2 from the Sun Java website.

On systems that you will use to customize the SESM application, we recommend that you install the JDK before you install SESM.

Solaris Patch Requirements

On older Solaris platforms, you might need to apply Solaris operating system upgrades (patches). To determine if the system requires patches:

-
- Step 1** Go to the Sun Microsystems Java site:
<http://www.sun.com/software/solaris/jre/index.html>
- Step 2** Start downloading the JRE. After you log in, a list of download options appears, including the necessary patches for your operating system version.
- Step 3** Download the readme file, which contains instructions on how to apply patches.
-

Installing and Configuring Related Components

**Note**

Skip this section if you plan to install a SESM Demo installation.

The SESM installation program can configure the SESM applications to communicate with other required components in a SESM deployment: Service Selection Gateways (SSGs), RADIUS servers, or SPE databases, such as an LDAP directory.

**Note**

If you do not provide correct communication information for SSG and RADIUS servers during the installation, we recommend that you reinstall to ensure that the SESM application works correctly.

To prepare for a SESM installation, we recommend the following procedure before you run the SESM installation program:

-
- Step 1** Configure the SSG on the Cisco platform.
For information on configuring the SSG to work with SESM, see [Chapter 3, “Configuring the Selection Services Gateway to Work with SESM.”](#)
- Step 2** For a SESM RADIUS installation, install and configure a RADIUS server. One RADIUS server to consider in your deployment is the Cisco Access Registrar, a carrier class RADIUS platform that is fully tested with SESM.
For information on configuring Cisco Access Registrar to work with SESM, see the Cisco Access Registrar (AR) documentation. See [Related Documentation, page xi](#) for the link to the AR documentation.
- Step 3** For an SPE installation, install an LDAP directory. Make sure it is running during installation. This allows the SESM installation program to update the directory with required extensions.
For information on configuring an LDAP directory to work with SESM, see [Configuring an LDAP Directory to Work with SESM, page 4-1](#).
-

Gathering Information Required for the SESM Installation

Table 2-2 contains the information you need to know before running the SESM installation program. It shows the attributes whose values you should be prepared to enter during SESM installation.

To gather the Service Selection Gateway (SSG) information, use the **show run** command on the SSG platform and examine the output for the commands provided in the Explanation column in Table 2-2.

Table 2-2 Required Attributes for Installation

Installation	Component	Attribute	Explanation	Example value
RADIUS and SPE	SSG	SSG port number	Port that SSG uses to listen for requests from SESM applications.	1812
		SSG shared secret	Shared secret used for communication between SSG and SESM applications.	cisco
		Port-bundle host key bundle length	Uniquely identifies each edge session on the SSG host.	
	SSG-to-client mapping	SSG address	Hostname or IP address of the SSG platform.	1.2.3.5
	These values are required only when port-bundle host key is not used (bundle length is 0).	Client subnet	One client subnet that is handled by this SSG. This is the subnet for the devices, such as PCs or WAP phones, you want to use to test the SESM deployment.	50.0.0.0
		Subnet mask	Mask that can be applied to subscriber IP addresses to derive their subnet.	255.0.0.0
	RADIUS or RDP server	Primary AAA server IP address or hostname		
		Primary AAA server port		
		Secondary AAA server IP address or hostname		
		Secondary AAA server port		
		Shared secret		

Table 2-2 Required Attributes for Installation (continued)

Installation	Component	Attribute	Explanation	Example value
SPE only	Profile passwords	Service password		
		Service group password		
	SPE database server (for example, LDAP directory)	Directory address	IP address or the hostname of the system on which the LDAP directory server is running.	1.2.3.4
		Directory port	Port on which the LDAP directory server listens.	389
		Directory admin user	User ID within Novell Directory Server (NDS) that has permissions to extend the directory schema.	cn=admin, ou=sesm, o=cisco
		Directory admin password	Password for the directory administrator. This is the password you entered during directory installation and configuration.	admin
	SPE directory container	Container name	Identifies the structure within the SPE database that holds the SESM data	ou=sesm,o=cisco
		Container user ID		cn=admin, ou=sesm, o=cisco
		Container password		

Obtaining the SESM Installation Image File

The installation images for SESM are available from the product CD-ROM or from the Cisco website. This section contains the following topics:

- [Downloading Software from the Cisco Website, page 2-7](#)
- [Uncompressing the Image, page 2-7](#)

Downloading Software from the Cisco Website

If you purchased a contract that allows you to obtain the SESM software from the Cisco website, you can access the Cisco images from the CCO Software Center, you must have a valid Cisco user ID and password.

See *Release Notes for Cisco Subscriber Edge Services Manager 3.3(1)* for the download location on Cisco.com.

Uncompressing the Image

Copy and uncompress the .tar or .zip file to a temporary directory to obtain the following files:

- The installation executable file—A .bin or .exe file, depending on the system you are using.
- Files used for a silent mode installation—These are .iss and .properties files. Refer to [Silent Mode Installation, page 5-2](#) for information about silent mode.

Table 2-3 shows the names of the compressed and executable files (Note that “x.x.x” is used to denote version number).

Table 2-3 Installation Image Filenames

Operating System	Compressed Filename	Executable Installation Filename
Solaris	sesm-x.x.x-pkg-sol-k9.tar	sesm_sol.bin
Linux	sesm-x.x.x-pkg-linux-k9.tar	sesm_linux.bin
Windows	sesm-x.x.x-pkg-win32-k9.zip	sesm_win.exe

Obtaining a SESM License Number

You must install a licensed version of SESM using a license number before you deploy SESM in a production environment.

The license number is available on the License Certificate that is shipped with a purchased product. If you purchased the product and have not yet received the CD-ROM and License Certificate, you can choose the evaluation option during installation. However, be sure to reinstall using your license number when you receive the certificate.

The license number is important when you are requesting technical support for SESM from Cisco.

After installation, you can see your license number and the software version in the licensenum.txt file under the installation directory.



Note

You can install an evaluation version of SESM without a license number. An evaluation version provides full software functionality and does not have an expiration period. However, you must install a licensed version using a license number before deploying SESM in a production environment.

Gaining Required Privileges for Installation

You must have the following privileges to install SESM:

- On Solaris and Linux—No special privileges required. However, if you do not run the installation program as root, you cannot install to a location that has been created by root.
- On Windows—Run the installation program as a member of the Administrators group.
- The installation program writes to parts of the filesystem or Windows registry that are accessible only to a privileged user. The outcome of the installation is unpredictable if you are not privileged.



Note

You must have write privileges to the intended SESM installation directory.



Configuring the Selection Services Gateway to Work with SESM

This chapter describes the minimum required configuration for the Cisco Service Selection Gateway (SSG) to work with SESM. This chapter contains the following topics:

- [Introduction, page 3-1](#)
- [Configuring SSG to Work with SESM, page 3-2](#)
- [Configuring the Port-Bundle Host Key Feature on SSG, page 3-4](#)
- [Configuring the SSG to Match the Installed SESM Captive Portal, page 3-5](#)
- [Configuring the SSG TCP Redirect Features, page 3-5](#)
- [Example SSG Configuration for Working With SESM, page 3-12](#)



Note

For more information about configuring SSG, including optional features and a more detailed explanation of the required configurations described in this chapter, see the SSG documentation. See [Related Documentation, page xi](#) for an online link to SSG documentation.

Introduction

All SESM implementations work with and require a Cisco gateway such as SSG. The SSG is a feature in the Cisco IOS software running on a Cisco device. The SSG provides authentication, service connection, connection management, and SESM session capabilities. The SESM portals provide the subscriber's interface to SSG for those services.

For more information about SSG and SESM applications, see *Cisco Subscriber Edge Services Manager Introduction Guide*.

Before configuring SESM you need to configure the SSG using the information in this chapter.

A sample configuration is provided in [Example SSG Configuration for Working With SESM, page 3-12](#).

Configuring SSG to Work with SESM

To configure SSG to work with SESM:

- Step 1** Using a suitable terminal, log into your router and obtain the IOS command prompt.
- Step 2** To verify that the Cisco IOS software running on the platform is a version that supports the SSG feature, enter the following at the command line prompt:

```
show version
```

The version number is now displayed.

- Step 3** To enable SSG, at the IOS command prompt, enter the following command in global configuration mode:

```
ip cef
ssg enable
```



Note The Cisco Express Forwarding (CEF) feature is required for SSG.

- Step 4** To identify the network where the SESM portal is running, enter:

```
ssg default-network IPaddress mask
```

Where *IPaddress* and *mask* identify the network on which the SESM portal is running.

- Step 5** To specify the password that SSG uses to query the RADIUS server for service profiles, enter:

```
ssg service-password serviceProfilePassword
```

Where *serviceProfilePassword* matches the password in the service profiles. The default password used in SESM configurations and sample data files is servicecisco.

- Step 6** To configure the port on which the SSG will listen for SESM requests, enter:

```
ssg radius-helper auth-port port
```

Where *port* is the port on which all requests from SESM portals arrive. The default port used in SESM configurations is 1812.

- Step 7** To specify the shared secret for password encryption between SSG and the SESM portal, enter:

```
ssg radius-helper key password
```

Where *password* matches the password configured on the SESM portal. The default password used in SESM configurations is cisco.

- Step 8** To set the SSG cache subscriber profiles to be obtained during authentication, enter:

```
ssg profile-cache
```



Note In SESM RADIUS installations, profile caching is required. Subscriber profiles are included in access-accept replies to authentication requests. The SSG must cache the profile obtained during the authentication stage to make the profile available later when the SESM application queries the SSG.

**Note**

For SESM SPE installations, profile caching is not required. Subscriber profiles are obtained from the directory separately from the authentication stage. The memory saved by turning off the profile caching increases the scalability of the SSG host device.

- Step 9** To configure the SSG to perform RADIUS authentication, enter the following (minimum configuration shown):

```
aaa new-model
aaa authentication login default none
aaa authentication ppp default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa session-id common
```

**Note**

In a SESM SPE installation, the RADIUS server is the SESM RADIUS Data Proxy (RDP) server.

- Step 10** To configure communication between SSG and the RADIUS server, enter:

```
radius-server host ipAddress auth-port authPort acct-port acctPort key password
```

where:

ipAddress is the address of the RADIUS server. In SPE mode, this is the address of the RDP.

authPort is the port SSG uses for authentication requests. The standard is 1812.

acctPort is the port SSG uses for accounting requests. This is optional in SESM deployments. The standard is 1813.

password is the RADIUS shared secret for password encryption

**Note**

When you deploy SESM with iPass support, the accounting requests for iPass users must be proxied to the iPass RADIUS Server. See *Cisco Subscriber Edge Services Manager Administration and Configuration Guide* for details.

- Step 11** Every service must be bound to an uplink interface. If the service binding is not defined in the next-hop table on the SSG device, use the **ssg bind service** command to bind the service.
- Step 12** If required, configure the SSG port-bundle host key feature as described in [Configuring the Port-Bundle Host Key Feature on SSG, page 3-4](#).
- Step 13** If required, configure the SSG to work with the Captive portal solution installed with your deployment using the procedures given in [Configuring the SSG to Match the Installed SESM Captive Portal, page 3-5](#).
- Step 14** If required, configure the SSG TCP redirect features using the procedures given in [Configuring the SSG TCP Redirect Features, page 3-5](#).

Configuring the Port-Bundle Host Key Feature on SSG

The port-bundle host key feature uses a software token (or key) that *uniquely* identifies each edge session on the SSG host, even when multiple subscribers are using the same IP address. The port-bundle host key feature also provides an SSG IP address in the key.



Note

The host key feature requires Cisco IOS Release 12.2(2)B or later on the SSG device.

The port-bundle host key feature provides the following advantages to SESM portals:

- It allows SESM portal applications to robustly handle overlapping IP addresses, nonroutable IP addresses, and dynamically assigned IP addresses.
- It eliminates the need to explicitly map subscriber subnets to SSGs.

When the port-bundle host key is enabled on the SSG, the SSG rewrites the source port number and IP address of TCP packets whose destination is the default network. The new source port and IP address combination becomes the key that uniquely identifies each session. The new IP address is the SSG IP address. The new port number identifies a specific edge session on the SSG.



Note

For the port-bundle host key mechanism to operate correctly, the SESM web application must reside in the default network with subscribers (PPP or bridged/routed) connected on downstream interfaces.

To configure the SSG for host key operation, enter the following configuration commands at the terminal configuration prompt on the SSG host:

```
ssg port-map enable
ssg port-map source ip loopback 0
ssg port-map destination range lowPort to highPort ip SESMaddress
```

The **ssg port-map source ip** command configures the IP addresses for use as the IP portion of the host key. Each configured address allows for approximately 4000 host keys, if the default port bundle length of 4 is used. This address becomes the source IP address for all upstream TCP packets from SSG to the SESM web application (and conversely, the destination address for all downstream TCP packets from the SESM web application to the SSG). Although you can explicitly configure these addresses, the safest way to configure them is by using a loopback interface, as shown in the configuration commands, because these IP addresses must be recognized as corresponding to a local interface or loopback.



Note

If you use the interface that is configured to give SSG access to the default network as one of the interfaces in the **ssg port-map source ip** command, that interface cannot also be used as a Telnet interface into the SSG host.

The **ssg port-map destination range** command defines the address and ports of the SESM web application, where:

lowPort is the lowest SESM port

highPort is the highest SESM port

SESMaddress is the IP address of SESM

If only one SESM port is available, *highPort* should have the value *lowPort* + 1. For example:

```
ssg port-map destination range 10100 to 10101 ip 10.0.3.1
```

Configuring the SSG to Match the Installed SESM Captive Portal

To demonstrate the complete capabilities of the captive portal solution, you must run it with a fully configured SSG.

To configure the SSG TCP redirect features to work with the configuration parameters that you just installed on the SESM side:

Step 1 Make sure that basic SSG functionality is enabled and configured, as described in [Configuring SSG to Work with SESM, page 3-2](#).

Step 2 Open the ssgconfig.txt file in a text editor. The file location is:

```
captiveportal
config
  ssgconfig.txt
```

The ssgconfig.txt file contains all of the Cisco IOS software commands required to configure the four types of TCP redirection that the captive portal reference implementation can support and demonstrate. The commands in this file configure SSG to match the default values presented during the captive portal installation. The file includes example IP addresses.



Note The installation displays default inputs for captive portal group names and port numbers. These defaults correspond to values used in the TCP redirect commands in the ssgconfig.txt file. If you change these captive portal group names or port numbers, you must make corresponding changes to the port numbers in the ssgconfig.txt file.

Step 3 Edit ssgconfig.txt:

- You *must* edit the placeholder IP addresses. Change them to the actual network IP addresses you entered during captive portal installation.
- If you changed the displayed defaults for captive portal group names or the incoming port numbers, then you must edit those values in ssgconfig.txt to match the values you entered during captive portal installation.

Step 4 On the SSG host device, enter the contents of ssgconfig.txt to update the Cisco IOS running-config file.

Step 5 Save running-config.

Configuring the SSG TCP Redirect Features

This section summarizes how to configure the Cisco IOS software TCP redirect features on the SSG platform. This section contains the following topics:

- [Configuring SSG and Port-Bundle Host Key to Work with Captive Portal, page 3-6](#)
- [Defining Captive Portal Groups, page 3-6](#)
- [Defining Port Lists, page 3-7](#)
- [Configuring Unauthenticated User Redirection, page 3-7](#)
- [Configuring Unauthorized Service Redirection, page 3-8](#)
- [Configuring Initial Logon Redirection, page 3-10](#)

- [Configuring Advertising Redirection, page 3-11](#)
- [Configuring Prepaid Redirection, page 3-12](#)

For complete information about the SSG TCP redirect features, see the SSG documentation.

Using the `ssgconfig.txt` File

The SESM installation includes a sample configuration file containing Cisco IOS commands for the SSG TCP redirect features. The sample file is located in:

```
captiveportal
  config
    ssgconfig.txt
```

The examples in this section are copied from the `ssgconfig.txt` file. You can edit this file to supply valid IP addresses for your network, and then run the file on your SSG platform to make the example captive portal solution work on your network.

Configuring SSG and Port-Bundle Host Key to Work with Captive Portal

To allow the Captive Portal application to obtain the subscriber name from profiles, the following SSG configurations are required:

1. If the SESM single sign-on feature is turned on, the SSG profile cache feature must also be turned on:

```
ssg profile-cache
```

2. If the SSG port-bundle host key is used, ensure that the destination range configured in the port-mapping command includes the port numbers you assigned during the captive portal configuration, in addition to the port number of the main SESM web application. (The suggested default values that the installation program uses for the Captive Portal configuration are 8090 to 8096.)

Example port-bundle host key port mapping commands:

```
ssg port-map enable
ssg port-map destination range 8080 to 8100 ip 10.0.1.4
ssg port-map source ip Loopback()
```

Defining Captive Portal Groups

When SSG determines that a TCP packet must be redirected, it redirects the packet to a configured captive portal group. A captive portal group consists of one or more web servers running an application that can handle the redirected packet. If you deploy the SESM captive portal solution, the web servers in your captive portal groups are running the SESM Captive Portal application.

Grouping multiple instances of a captive portal application allows the SSG to apply sequential load balancing over the members of the group. The SSG monitors the web servers in the group and redirects packets only to those servers that respond.

You can configure as many captive portal groups as required. For example, you can specify different captive portal groups for each type of redirection, or different destination networks for different services in service redirects.

Use the following command to create a captive portal group and add web servers to the group.

```
ssg tcp-redirect server-group group-name server ip-address port
```

For the SESM example solution to work, you must assign the IP address and port of the SESM captive portal application to all of your server groups. Do this by using the following values in the above command:

- The IP address of the captive portal application.
- The port that you configured in the captiveportal.xml file for the specific type of redirection. The installation program initially sets these ports. [Table 3-1](#) shows the port values that are configured at installation time if you accepted all of the default values during installation.

Table 3-1 Default Redirection Port Values Configured During Installation

Redirection Type	Default Port Value at Installation
Unauthenticated user redirections	8090
Initial logon redirections	8091
Advertising redirections	8092
Unconnected service redirections:	--
default service redirection	8093
Service1	8094
Service2	8095
Service3	8096

Defining Port Lists

A port list refers to the destination ports in the incoming TCP packets. For example, at most sites, ports 80 and 8080 would identify Internet packets, and port 70 would identify FTP packets. If you assign a port list to a captive portal group, you limit redirections to only the traffic arriving on the ports in the port list.



Note

You can associate the same port-list to multiple captive portal groups.

Use the following command to create a port list.

```
ssg tcp-redirect port-list
    port port
    port port
```

The examples in other sections of this chapter include commands that create port lists.

Configuring Unauthenticated User Redirection

Unauthenticated user redirection captures and redirects packets from subscribers who have not logged onto a SESM session (not authenticated).

When a subscriber successfully authenticates, SSG creates an edge session for that subscriber. When an edge session does not exist for the source address of a packet, SSG redirects the packet to the portal group associated with unauthenticated user redirection. The result is that subscribers cannot access any part of the network beyond the default network and configured open gardens without first authenticating.

If you do not configure a captive portal group to handle TCP packets from unauthenticated users, the following occurs:

- SSG discards packets from unauthenticated users, except those that are destined to the default network or open gardens.
- To obtain the SESM logon page, subscribers must enter the URL of the SESM web server.

If a TCP packet is destined to the SSG default network or an open garden network configured on the SSG, it is not a candidate for redirection.

Authentications for PPP Connections

Subscribers who are connecting to SSG over a PPP connection are already authenticated. The SSG accepts this authentication and creates the host object for the subscriber. If the subscriber logs out of SESM but does not log off of the PPP connection, the host object is marked inactive, and then unauthenticated redirection applies. When the PPP subscriber logs back into SESM (reauthenticates), the edge session is active again.

Cisco IOS Configuration Commands

Use the following command to specify which captive portal group will handle unauthenticated user redirections.

```
ssg tcp-redirect redirect unauthenticated-user to server-group
```

For example, the following commands from ssgconfig.txt configure unauthenticated user redirection:

```
ssg tcp-redirect
  server-group userRedirect server 10.0.1.4 8090
  redirect unauthenticated-user to userRedirect
```

The above example:

- Creates a captive portal group named userRedirect.
- Assigns one web server, whose IP address is 10.0.1.4, to the group, with a listener on port 8090. (See [Table 3-1](#) for details about the port number.)
- Associates the userRedirect group with unauthenticated user redirections.
- Applies user redirection to all TCP packets whose source IP address does not have an edge session on the SSG. A port list cannot be assigned to this type of redirection.

Configuring Unauthorized Service Redirection

If a TCP packet is destined to the SSG default network or an open garden network configured on the SSG, it is not a candidate for service redirection. Also, if a packet is destined to a service to which the subscriber is already connected, the packet is not redirected.

Otherwise, service redirection redirects a TCP packet if all the following conditions are true:

- The packet is destined for a service in a configured port-list. For example, you could configure a port-list that makes TCP packets destined for FTP (port 70) and HTTP (port 80) candidates for redirection.
- The packet is destined for a network in a configured network list. For example, you can limit access to specific networks for each service. The SSG rejects packets destined for other networks, unless you configure a default service redirection to redirect the packets destined for other networks.

- The subscriber is not authorized to use the service. Reasons for not being authorized are:
 - Not subscribed to the service
 - Not logged into the service
 - If the SSG prepaid feature is configured, insufficient quota in the account

Cisco IOS Configuration Commands

The following commands from the ssgconfig.txt file configure service redirections. This example:

- Configures three specific service redirections and a default service redirection.
- Applies all of the service redirections to traffic coming into ports 80 and 8080.
- The IP address of the web server in which the SESM Captive Portal application is running is 10.0.1.4.
- Each type of service redirection uses a different port on the same web server. See [Table 3-1](#) for more details about the port number.

```
ssg tcp-redirect
network-list serviceNetwork1
network 1.1.1.0 255.255.255.0
!
network-list serviceNetwork2
network 2.2.2.0 255.255.255.0
!
network-list serviceNetwork3
network 3.3.3.0 255.255.255.0
!
port-list ports
port 80
port 8080
server-group serviceRedirect1
server 10.0.1.4 8094
!
redirect port-list ports to serviceRedirect1
redirect unauthorized-service destination network-list serviceNetwork1 to
serviceRedirect1
!
server-group serviceRedirect2
server 10.0.1.4 8095
!
redirect port-list ports to serviceRedirect2
redirect unauthorized-service destination network-list serviceNetwork2 to
serviceRedirect2
!
server-group serviceRedirect3
server 10.0.1.4 8096
!
redirect port-list ports to serviceRedirect3
redirect unauthorized-service destination network-list serviceNetwork3 to
serviceRedirect3

server-group defaultServiceRedirect
server 10.0.1.4 8093
!
redirect port-list ports to defaultServiceRedirect
redirect unauthorized-service to defaultServiceRedirect
```

Shared Address Spaces

It is possible for some services to share some of their address space. For example, consider an Internet service with allowable networks of 0.0.0.0 and a mask 0.0.0.0. (In effect, any address is permissible.) An IPTV service would have a much smaller network space—for example, 1.2.3.0 with a mask of 255.255.255.0). In this situation, having access to the Internet service should not automatically give access to the IPTV service.

You can configure the SSG to handle the situation described above by configuring a specific service redirection for the narrow address space. This takes precedence over the wider address space, thus ensuring that the specific service redirection occurs. You can also configure a wider address space and exclude specific networks in service profiles.

Specifying Service Redirection Networks in the Service Profile

In Cisco IOS Release 12.2.15BW and later, you can specify a service name as the redirected network for unconnected service redirections. SSG obtains the network information from the service profile.

The following commands redirect to a network specified in the service1 profile.

```
server-group serviceRedirect1
server 10.0.1.4 8094
!
redirect port-list ports to serviceRedirect1
redirect unauthorized-service service service1 to serviceRedirect1
```

Configuring Initial Logon Redirection

The initial logon redirection redirects all subscribers when they first authenticate, which is when SSG first creates the edge session.

Redirected Message Duration

The message duration is the length of time that the redirected page is displayed. Message duration is controlled by:

- A globally set parameter set by the Cisco IOS command described below.
- Subscriber-specific values set in the subscriber profiles. The profile value, if it exists, overrides the global value.



Note The SESM captive portal solution also uses duration parameters. See *Cisco Subscriber Edge Services Manager Administration and Configuration Guide* for more information.

Cisco IOS Configuration Commands for Initial Logon Redirection

Use the following command to specify which captive portal group will handle initial logon redirections and to set the duration of the display.

```
ssg tcp-redirect redirect captive initial default group group-name duration seconds
```

The following commands from ssgconfig.txt configure initial logon redirection:

```
ssg tcp-redirect
port-list ports
    port 80
    port 8080
server-group initialCaptive
```



```
server 10.0.1.4 8091
redirect port-list ports to initialCaptive
redirect captive initial default group initialCaptive duration 10
```

The previous example:

- Creates a port list named ports and a captive portal group named initialCaptive.
- Assigns one web server, whose IP address is 10.0.1.4, to the group, with a listener on port 8091. (See [Table 3-1](#) for details about the port number.)
- Associates the initialCaptive group with initial logon redirections.
- Sets the message captivation to last for 10 seconds. The subscriber profile can override the 10-second duration value. See the *Cisco Subscriber Edge Services Manager Administration and Configuration Guide* for more information.
- Specifies that redirections to the initialCaptive group be applied to TCP packets arriving on the SSG at ports 80 or 8080.

Configuring Advertising Redirection

Advertising redirection redirects browsers to a configured page at timed intervals throughout the SESM session.

Message Duration and Frequency

The length of time that the message is displayed (the duration) and the frequency of the intervals are controlled by:

- Globally set parameters set by the Cisco IOS command described below.
- Subscriber-specific values set in the subscriber profiles. The profile value, if it exists, overrides the global value.

The frequency is approximate, because redirection can occur only when a TCP packet is initiated by the subscriber.



Note

The Message Portal application also accepts a duration attribute. See *Cisco Subscriber Edge Services Manager Administration and Configuration Guide* for more information.

Cisco IOS Configuration Commands for Advertising Redirection

Use the following command to specify which captive portal group will handle advertising redirections, and to set the duration and frequency of the display. The valid range for duration and frequency is 1 to 65,536 seconds.

```
ssg tcp-redirect redirect captive advertising default group group-name duration seconds
frequency seconds
```

The following commands from ssgconfig.txt configure initial logon redirection:

```
ssg tcp-redirect
port-list ports
port 80
port 8080
server-group advertisingCaptive
server 10.0.1.4 8092
redirect port-list ports to advertisingCaptive
```

```
redirect captive advertising default group advertisingCaptive duration 5
frequency 60
```

The previous example:

- Creates a port list named `ports` and a captive portal group named `advertisingCaptive`.
- Assigns one web server, whose IP address is 10.0.1.4, to the group, with a listener on port 8092.
In the reference implementation, this must be the IP address of the web server for the SESM captive portal application. The port must match the port you configured for advertising redirections in the `captiveportal.xml` file.
- Associates the `advertisingCaptive` group with advertising redirections.
- Sets captivation to last for 5 seconds and to occur every 60 seconds. The subscriber profile can override the duration and frequency. See *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*.
- Specifies that redirections to the `advertisingCaptive` group be applied to TCP packets arriving on the SSG at ports 80 or 8080.

Configuring Prepaid Redirection

Prepaid redirection is valid if the SSG Prepaid feature is implemented. The prepaid redirection specifies what happens when the prepaid quota is exhausted. This feature is available in Cisco IOS Release 12.2.8B and later.

Configure a default prepaid redirection group as follows:

```
ssg tcp-redirect
server-group PREPAID_REDIR_DEFAULT
server 10.0.1.4 8099
!
redirect prepaid-user to PREPAID_REDIR_SERVER
```

You can also configure a prepaid redirection group on a per service basis instead of a default as follows:

```
ssg tcp-redirect
server-group PREPAID_REDIR_SERVICE1
server 10.0.1.4 8100
```

Configure the per-service redirection in a service profile using the Z subattribute code. For example:

```
Z;PREPAID_REDIR_SERVICE1
```

Example SSG Configuration for Working With SESM

The following annotated configuration example shows how to configure SSG to work with SESM applications.

```
c7200-1#sho run
Building configuration...

Current configuration : 4499 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```

!
hostname c7200-1
!
boot system flash disk0:c7200-g4js-mz.v122_4_b_throttle

```

The following lines configure AAA authentication.

```

aaa new-model
!
!
aaa authentication login default none
aaa authentication ppp default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa session-id common
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
!
!ip cef
!
!

```

The following lines enable and configure SSG to communicate with the SESM web application.

```

!!
ssg enable

ssg default-network 192.168.254.16 255.255.255.248
ssg service-password servicecisco
ssg radius-helper auth-port 1812
ssg radius-helper key cisco
ssg accounting interval 999999
ssg profile-cache

```

The following lines configure the SSG port-bundle host key feature.

```

ssg port-map enable
ssg port-map destination range 8080 to 8080 ip <sesmIPaddress>
ssg port-map destination range 8443 to 8443 ip <sesmIPaddress>
>
ssg port-map source ip Loopback0
!
!
ssg bind service passthrough1 FastEthernet4/0
ssg bind service proxy1 FastEthernet4/0
ssg bind service tunnell1 FastEthernet4/0
ssg bind direction downlink FastEthernet1/0
ssg bind direction downlink Ethernet3/2
!

```

The following lines configure a RADIUS proxy server.

```

ssg radius-proxy
client-address 192.167.254.26 key cisco
address-pool 10.0.0.1 10.0.0.200
!

```

The following lines configure SSG TCP redirections.

```

ssg tcp-redirect
network-list Unauth-Service-pass
network 10.60.60.0 255.255.255.128
!
network-list Unauth-Service-prox
network 10.61.61.0 255.255.255.128

```

```

!
network-list Unauth-Service-tunn
  network 10.62.62.0 255.255.255.128
!
port-list ports
  port 80
  port 8080
!
server-group Unauth-User
  server 192.168.254.21 8090
!
server-group Initial
  server 192.168.254.21 8091
!
redirect port-list ports to Initial
!
server-group Advertisement
  server 192.168.254.21 8092
!
redirect port-list ports to Advertisement
!
server-group Unauth-Service-pass
  server 192.168.254.21 8094
!
redirect port-list ports to Unauth-Service-pass
redirect unauthorized-service destination network-list Unauth-Service-pass to
Unauth-Service-pass
!
server-group Unauth-Service-prox
  server 192.168.254.21 8095
!
redirect port-list ports to Unauth-Service-prox
redirect unauthorized-service destination network-list Unauth-Service-prox to
Unauth-Service-prox
!
server-group Unauth-Service-tunn
  server 192.168.254.21 8096
!
redirect port-list ports to Unauth-Service-tunn
redirect unauthorized-service destination network-list Unauth-Service-tunn to
Unauth-Service-tunn
!
server-group Advertisement
!
redirect unauthenticated-user to Unauth-User
redirect captivate initial default group Initial duration 1
redirect captivate advertising default group Advertisement duration 5 frequency 600
!
!

```

The following lines configure the device interfaces.

```

interface Loopback0
  ip address 10.2.2.1 255.255.255.0
  no ip mroute-cache
!
interface FastEthernet0/0
  ip address 10.0.3.20 255.255.255.128
  no ip mroute-cache
  duplex half

```

```
no cdp enable
!
interface FastEthernet1/0
ip address 192.168.254.25 255.255.255.248
no ip mroute-cache
duplex half
no cdp enable
!
interface ATM2/0
no ip address
no ip mroute-cache
shutdown
no atm ilmi-keepalive
atm voice aal2 aggregate-svc upspeed-number 0
!
interface Ethernet3/0
ip address 10.10.10.1 255.255.255.0
no ip mroute-cache
duplex half
no cdp enable
!
interface Ethernet3/1
ip address 192.168.254.20 255.255.255.248
no ip mroute-cache
duplex half
no cdp enable
!
interface Ethernet3/2
ip address 192.168.254.4 255.255.255.248
no ip mroute-cache
duplex half
no cdp enable
!
interface Ethernet3/3
ip address 10.5.5.2 255.255.255.0
no ip mroute-cache
shutdown
duplex half
no cdp enable
!
interface FastEthernet4/0
ip address 172.16.59.1 255.255.255.0
no ip mroute-cache
duplex half
no cdp enable
!
ip default-gateway 192.168.254.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.52.199.1
ip route 10.0.12.0 255.255.255.128 10.10.10.2
ip route 10.1.0.0 255.255.0.0 10.0.4.1
ip route 10.50.0.0 255.255.0.0 10.52.199.1
ip route 192.168.254.100 255.255.255.255 10.52.199.1
ip route 172.19.60.0 255.255.255.128 10.59.59.2
ip route 172.18.61.0 255.255.255.128 10.59.59.2
ip route 172.17.62.0 255.255.255.128 10.59.59.2
ip route 172.16.70.0 255.255.255.0 10.59.59.2
ip route 192.168.0.0 255.255.0.0 10.52.199.1
no ip http server
ip pim bidir-enable
!
```

The following lines configure communication between SSG and a RADIUS server.

```
radius-server host 192.168.254.100 auth-port 1812 acct-port 1813 timeout 10 retransmit 3
key cisco
radius-server retransmit 3
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
call rsvp-sync
!
mgcp profile default
dial-peer cor custom
gatekeeper
shutdown
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password cisco
end
c7200-1#
```



Configuring the Servers in Your Deployment for SESM

The SESM solution integrates with any one or a combination of the following options to obtain subscriber and service data:

- SESM SPE installation—An SPE database (LDAP directory) accessed through the Cisco SPE application programming interface (API).
- SESM RADIUS installation—An authentication, authorization, and accounting (AAA) database managed and accessed by a RADIUS server.

This chapter provides information on how to configure the servers in your deployment for use with SESM. The chapter contains the following topics:

- [Configuring an LDAP Directory to Work with SESM, page 4-1](#)
- [Configuring Cisco Access Registrar for SESM Deployments, page 4-8](#)

Configuring an LDAP Directory to Work with SESM

We recommend that you start the SPE database server (for example, the LDAP directory) before installing SESM, although this is optional. The installation program prompts you for connection information to the SPE database and then tries to connect to the database using the values that you provide. When the database server is running, the installation program's successful connection is your verification that the attribute values you provided are correct.

This section describes how to install, configure, and extend LDAP directories to work with a SESM SPE installation. Topics in this section are:

- [Choosing a Suitable LDAP Directory, page 4-2](#)
- [Installing and Configuring Novell eDirectory Version 8.7 to Work with SESM, page 4-2](#)
- [Installing and Configuring Sun ONE \(iPlanet\) to Work with SESM, page 4-5](#)
- [Extending the Directory Schema and Loading Initial RBAC Objects, page 4-7](#)
- [Loading Sample SESM Data, page 4-7](#)



Note

For full installation instructions for the LDAP directories, please see the product documentation.

Choosing a Suitable LDAP Directory

SESM is verified to run with the following LDAP directories:

- Novell eDirectory Version 8.7 on Solaris Version 7 or 8.
- Sun ONE (iPlanet) Directory Server Version 5.2 on Solaris Version 8.

Installing and Configuring Novell eDirectory Version 8.7 to Work with SESM

To install and configure Novell eDirectory Version 8.7 to work with SESM, perform the following steps. These instructions assume that you are installing NDS on a Solaris machine.

Step 1 Log on as superuser.

Step 2 Download a copy of NDS8.7 onto the target platform. This can be the SESM server itself, if it has sufficient memory. For example, place the download bundle into the following location:

```
/opt/cisco/nds/edir87_solaris_full.tar.gz
```

Step 3 Unzip or untar the downloaded bundle by entering:

```
cd /opt/cisco/nds
gunzip edir87_solaris_full.tar.gz
```

This produces the files edir87_solaris_full.tar, tar xvf edir87_solaris_full.tar and several directories in the location of the tar-file, one of which is called Solaris.

Ensure that there is a directory called Licenses that contains an .nfk file and an .nlf file. If these files are not present, copy them from the same location as the NDS8.7 installation bundle.

Step 4 Change directory into the Solaris/setup directory and run the installation script (must be superuser) by entering:

```
cd /opt/cisco/nds/Solaris/setup/
./nds-install
```

The installation starts and you are prompted to agree to the license agreement.

```
%% Do you accept the terms of the Novell eDirectory license agreement [y,n,?,q]
```

Step 5 At the installer prompt, enter **y** to agree and continue.

Step 6 At the following prompt, enter **1,2,3** to install all components:

```
~~~~~
%% List of Novell eDirectory components available to install

%% 1 Novell eDirectory Server
%% 2 Novell eDirectory Administration Utilities
%% 3 Management Console for Novell eDirectory (ConsoleOne)
%% Select the components you wish to install [?, q] : 1,2,3
~~~~~
```

Step 7 At the following prompt, enter the path of the license files for example, /opt/cisco/nds/licenses/. These should be obtained as part of the NDS download process:

```
~~~~~
%% Enter the path to License File (.nfk): /opt/cisco/nds/licenses/
~~~~~
```


The program installs the set of required packages.

- Step 8** At the following prompt, select **3** to install all languages.

```
~~~~~
The following is a list of languages that are available to install.
1 English
2 French
3 All
Select the languages you wish to install [?,q]: 3
~~~~~
```

- Step 9** At the following prompt, select **8** to install all snap-ins.

```
~~~~~
The following are all the available snapin you can choose to install
0 NONE
1 ICE Snapin
2 Index Manager Snapin
3 LDAP Snapin
4 SLP Snapin
5 WAN Manager Snapin
6 PKI Snapin
7 Filtered Replica Snapin
8 All
Select the snapin(s) you wish to install [?,q]:
~~~~~
```

- Step 10** At the following prompt, enter **y** to install the Java Runtime Environment. This means ConsoleOne will be configured to use a suitable JRE, which will save configuration time.

```
~~~~~
Do you wish to install Java Runtime Environment [y,n,?,q] y
~~~~~
```

The installation of the LDAP Directory should then complete successfully and should display the following information:

```
~~~~~
%% Novell eDirectory Server packages successfully installed.

%% Novell eDirectory Administration Utilities packages successfully installed.
%% Use "ndsconfig" to configure Novell eDirectory Server.
%% Please update following environment variables to use LDAP tools from Novell -
PATH=/usr/ldaptools/bin:$PATH
MANPATH=/usr/ldaptools/man:$MANPATH:/usr/share/man

%% Please go through ../readme.txt carefully before using the product.
~~~~~
```

- Step 11** Create the container and admin user by entering (must be superuser):

```
ndsconfig new -t MYNAME-SESM -n ou=sesm.o=cisco -a cn=admin.ou=sesm.o=cisco
```

Where:

-t = the tree name.
 -n = container.
 -a = admin user.

- Step 12** At the following prompts, enter your password. Reenter the password to confirm when prompted.

```
Enter the password for cn=admin.ou=sesm.o=cisco:
Re-enter the password for cn=admin.ou=sesm.o=cisco:
```

A series of messages is displayed on completion of this process.

Step 13 Enable the *Allow Clear Text Passwords* (NDS Version 8.5) or *Require TLS for Simple Binds with Password* (NDS Version 8.7) attribute:

- a. Start ConsoleOne. Run the following file:

```
/usr/ConsoleOne/bin/ConsoleOne &
```

- b. Log in (authenticate) to the NDS Directory as follows if the Login window does not appear:

- Click on the **NDS** icon in the tree.
- From the menu, select **File Authenticate**.

- c. In the Login window, use the following values:

```
Login name: admin
Password: cisco
Tree: SESM
Context: ou=sesm.o=cisco
```

- d. Click **Enter**.

Upon successful authentication, the SESM icon appears in the right-hand panel. You can now enable the required attribute as follows:

- e. In the left panel, expand the NDS tree to the sesm object level:

```
NDS
  SESM
    cisco
      sesm
```

- f. In the left panel, click **sesm** to select it.
- g. In the right panel, right-click the **LDAP Group object**.
- h. Select **Properties** from the pop-up menu now displayed.
- i. For NDS version 8.7, the **Allow Clear Text Passwords** option was replaced by **Require TLS for Simple Binds with Password**. This option must be unchecked.
- j. Click **Apply**.
- k. Click **Close**.
- l. Exit ConsoleOne and proceed to SESM installation.

Step 14 Extend the directory schema and load initial RBAC objects using the procedure given in [Extending the Directory Schema and Loading Initial RBAC Objects, page 4-7](#).

Step 15 Load SESM sample data as required using the procedures given in [Loading Sample SESM Data, page 4-7](#).

Step 16 Configuration is now complete.

Installing and Configuring Sun ONE (iPlanet) to Work with SESM

To install and configure Sun ONE (iPlanet) to work with SESM, perform the following steps. These instructions assume that you are installing Sun ONE Version 5.2 SP1 on a Solaris Version 8 system.

-
- Step 1** Log on as superuser.
- Step 2** If you have a tar file, expand it.
- Step 3** Run the setup file. Follow the instructions in the setup program.
- Step 4** At the prompt, enter the fully qualified name of the computer on which you are installing Sun ONE.
- Step 5** When the program displays the following prompt, select the **SunOne Servers** option.
- ```

1. SunOne Servers
 Installs iPlanet Servers with the integrated iPlanet Console onto your computer.
2. SunOne Server Console
 Installs iPlanet Console as a stand-alone Java application on your computer.
```
- Step 6** In response to subsequent prompts asking you which components to install, select all components.
- Step 7** At the prompt, select **New instance will be the configuration directory server**.
- Step 8** At the prompt, select **Store data in the new directory server**.
- Step 9** At the following prompt, we recommend that you enter the standard server port 389, rather than accepting the random default port. You must know this port number later in this procedure and also during SESM installation. Select suffix **o=cisco**. Leave the server identifier as is.
- Step 10** At the following prompt, accept the default value of **admin** for the directory administrator.
- ```

iPlanet configuration directory server
administrator ID [admin]:
Password:
Password (again):
```
- Enter the password of your choice. You must enter this admin ID and password later in this procedure and also during SESM installation.
- Step 11** Leave the administration domain as is, then click **Next**.
- Step 12** At the following prompt, accept the default value of **Directory Manager**.
- ```

Directory Manager DN [cn=Directory Manager]:
Password:
Password (again):
```
- Enter the password of your choice. This username and password has privileges to update the directory schema. You must enter this Directory Manager DN and password later in this procedure and also during SESM installation.
- Step 13** At the prompt, select **Don't Populate**.
- Step 14** At the following prompt, enter any port number. The configuration examples later in this procedure use the value 390.
- ```

Administration port [15197]:390
```
- The installation begins. After successful installation, the Sun ONE server might start automatically. If it does not, start it as described in [Step 15](#).
- Step 15** Start the directory server by running the following:
- ```

/usr/iplanet/servers/start-admin
slapd-cd-sv210-sesm3/start-slapd
```

**Step 16** Start the console by running the following:

```
/usr/iplanet/servers/startconsole
```

A login window appears.

**Step 17** Log in by entering:

```
User ID:cn=Directory Manager
Password:
AdminURL:http://hostname:390
```

The Sun ONE Console window appears.

**Step 18** Expand the folders in the console window until the Directory Server object appears. Select **Directory Server**, then click **Open** at the top right corner of the window.

An Sun ONE Directory Server window appears.

**Step 19** Right-click the **cisco** folder. Select **New Org Unit** from the pop-up menu.

**Step 20** In the Name field, enter **sesm**, then click **OK**.

**Step 21** Right-click the **sesm** object. Select **New User** from the pop-up menu. The Create New User window appears.

**Step 22** Enter appropriate values in the following fields. In the UserID field, enter **admin**.

```
First Name:
Last Name:
Common Name:
UserID: admin
Password:
```

Click **OK**.

**Step 23** Right-click the **sesm** object. Select **Set Access Permissions** from the pop-up menu. The Manage Access Control window for ou=sesm, o=cisco appears.

**Step 24** Click **New**. The Edit ACI window for ou=sesm, o=cisco appears.

**Step 25** Enter any value for ACI Name. Click **Add**. The Add User & Group window appears.

**Step 26** Enter **admin** in the search field. Click **Search**: The admin user appears in the top window.

**Step 27** Select **admin**, then click **Add**. The admin user appears in the bottom window. Click **OK**.

**Step 28** Click **Targets**. Click **This Entry**. Click **OK**.

**Step 29** Click **OK** in the Manage Access Control window.

**Step 30** Exit Sun ONE and go to the SESM installation.

**Step 31** Extend the directory schema and load initial RBAC objects using the procedure given in [Extending the Directory Schema and Loading Initial RBAC Objects, page 4-7](#).

**Step 32** Load SESM sample data as required using the procedures given in [Loading Sample SESM Data, page 4-7](#).

Configuration is now complete.

---

## Extending the Directory Schema and Loading Initial RBAC Objects

To use the SESM installation process to extend the directory schema and load initial RBAC objects, follow these procedures:

- 
- |               |                                                                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Make sure the LDAP directory server is running.                                                                                                                                                                                                                                                                                   |
| <b>Step 2</b> | Make sure you know the following user IDs and passwords: <ul style="list-style-type: none"><li>• A user ID and password that allows you to update the directory schema.</li><li>• A user ID and password that allows you to update the container (organization and organizational unit) that you created for SESM data.</li></ul> |
| <b>Step 3</b> | Run the SESM installation program on a server that has network access to the LDAP directory.                                                                                                                                                                                                                                      |
| <b>Step 4</b> | If you select Custom when the installation program prompts for setup type, select <b>SPE</b> when the installation program prompts for the components to install.                                                                                                                                                                 |
| <b>Step 5</b> | When the installation program prompts for directory connection information, provide correct information to access the directory. This includes the names of the organization and organizational unit you created to hold the SESM data.                                                                                           |
| <b>Step 6</b> | When the installation program displays the options, click <b>Update schema</b> and <b>Install RBAC</b> .                                                                                                                                                                                                                          |
- 

## Loading Sample SESM Data

The SESM installation includes sample data that you can load into the LDAP directory after the SPE extensions are applied. The sample data includes a new\_subscribers group, which is required for self registration for the NWSP web application.

The sample data is located in:

```
dess-auth
 schema
 samples
 DESSusecasedata.ldf
```

To load the sample data, follow instructions in the following file:

```
dess-auth
 schema
 README.SESM.LDIF.html
```

**Note**

If you do not want to install the sample data, or if you installed the sample data and then cleared it from the LDAP directory, you must manually define a new\_subscribers group through CDAT.

# Configuring Cisco Access Registrar for SESM Deployments

For information about configuring Cisco Access Registrar (AR) to work with SESM, see [Related Documentation, page xi](#) for the link to the Cisco Access Registrar documentation.

If you want to use the SESM Trusted ID authorization feature, you will need to perform additional configuration in AR. For more information about the Trusted ID authorization feature, see the AR documentation.



## Installing and Uninstalling SESM

This chapter describes how to install and uninstall the Cisco Subscriber Edge Services Manager (SESM) software and bundled components, including the Security Policy Engine (SPE). The chapter contains the following topics:

- [Installation Methods and Logging Options, page 5-1](#)
- [Running the Installation Program, page 5-4](#)
- [Responding to Installation Program Prompts, page 5-6](#)
- [Installation Results, page 5-20](#)
- [Uninstalling a SESM Installation, page 5-22](#)
- [What's Next, page 5-22](#)



**Note**

Before you begin to install, read the information in the preceding chapters.

### Installation Methods and Logging Options

You can install SESM using the following installation methods:

- [GUI Mode Installation](#)
- [Console Mode Installation](#)
- [Silent Mode Installation](#)
- [SESM Installation Logging Feature, page 5-3](#)
- [Commands to Start Installation, page 5-3](#)

### GUI Mode Installation

GUI mode installation is an interactive installation method that communicates with you by displaying interactive windows. GUI mode is the default installation mode. To use this mode, run the installation image. No command line options are required unless you want to run the logging option.

See [Commands to Start Installation, page 5-3](#), for the commands required to start the installation in GUI mode.

## Console Mode Installation

Console mode installation is a text-only, question and answer interactive installation method. To run in console mode, use the `-console` option on the command line.

See [Commands to Start Installation, page 5-3](#), for the commands required to start the installation in console mode.

## Silent Mode Installation

Silent mode installation is a text-only noninteractive method. This method, also known as batch mode, is useful for multiple installations. Before you begin the installation, prepare the files that contain your installation and configuration information. The installation program obtains all input from the response file.

To run in silent mode, you must first prepare the configuration information normally gathered during the installation process in two files:

- InstallShield properties file (.iss file)—This file defines values related to the installation. It includes the name of the .properties file. This file is specified as an argument on the command line when you start the installation.
- Java system properties file (.properties file)—This file defines values related to application configuration.

Examples of the .iss and .properties files are included in the installation download. Before you start the installation, you must modify both files to match your requirements.

To prepare for silent mode:

---

**Step 1** Open the .properties and .iss files in any text editor.




---

**Note** Before you begin, you might need to obtain write access to the files.

---

**Step 2** Edit the values for each parameter in the file. [Table 5-1 on page 5-7](#) describes each parameter. Save and close the file.

**Step 3** To turn on the installation logging feature for a silent mode installation, open the .iss file in any text editor. Remove the first pound sign (#) from the following line:

```
-log # @all
```

**Step 4** Save and close the file.

---

To run the installation in silent mode, use the `-option fileName` argument on the command line when you start the installation image. See [Commands to Start Installation, page 5-3](#), for the commands required to start the installation in Silent mode.



## SESM Installation Logging Feature

The installation logging feature logs all messages during installation. You can select to have messages appear on the console or send all messages to a file named log.txt.

You can use the installation logging feature with any installation method.

The -log option on the installation command line turns on the installation logging feature.

See [Commands to Start Installation, page 5-3](#), for the commands required to start the installation with logging.

## Commands to Start Installation

For a new installation, the default installation directories are:

- On Solaris and Linux: /opt/cisco/sesm\_3.3.1
- On Windows: C:\Program Files\cisco\sesm\_3.3.1



### Note

If the installation program finds an existing SESM installation on the machine, the default installation directory is the directory of the current installation. You must change the default installation directory, or backup the current installation and uninstall, before you continue to install in the default directory. Do not install SESM in the same directory as an existing SESM installation.

### Solaris machines

Change directories to the location of the installation image, and enter one of the following commands, as required:

- GUI mode installation, no logging:

```
solaris> sesm_sol.bin
```

- GUI mode installation, with logging:

```
solaris> sesm_sol.bin -log [#] @ALL
```

Where:

# sends logging messages to a file named log.txt. If # is omitted, messages are sent to the console.

@ALL means log all messages, which is the recommended procedure.

- Console mode installation, no logging:

```
solaris> sesm_sol.bin -console
```

- Console mode installation, with logging:

```
solaris> sesm_sol.bin -log [#] @ALL -console
```

Where:

# sends logging messages to a file named log.txt. If # is omitted, messages are sent to the console.

@ALL indicates to log all messages, which is the recommended procedure.

- Silent mode (first prepare the configuration information, as described in [Silent Mode Installation, page 5-2](#)):

```
solaris> imageName -options issFileName
```

Where:

*imageName* is the name of the downloaded installation image, for example **sesm\_sol.bin**.

*issFileName* is the name of the install shield properties file you prepared, for example **mysesm.iss**.

### Windows Machines

Open a command prompt window, change directories to the location of the image, and enter one of the following commands, as required:

- GUI mode, no logging:

```
C:\> sesm_win.exe
```

(Alternatively, you can double-click the installation image filename.)

- GUI mode, with logging:

```
C:\> sesm_win.exe -options -log [#] @ALL
```

Where:

# sends logging messages to a file named log.txt. If # is omitted, messages are sent to the console.

@ALL means log all messages, which is the recommended procedure.

- Console mode, no logging:

```
C:\> sesm_win.exe -console
```

- Console mode, with logging:

```
C:\> sesm_win.exe -options -log [#] @ALL -console
```

Where:

# sends logging messages to a file named log.txt. If # is omitted, messages are sent to the console.

@ALL means log all messages, which is the recommended procedure.

- Silent mode, (first prepare the configuration information, as described in [Silent Mode Installation, page 5-2](#)):

```
C:\> sesm_win.exe -options mysesm.iss
```

## Running the Installation Program

The following sections describe how to run the installation program:

- [Installing a Licensed Version, page 5-5](#)
- [Installing an Evaluation Version, page 5-5](#)

## Installing a Licensed Version

To install a licensed version of SESM software, do the following:

- 
- Step 1** Obtain the license number from the License Certificate that is shipped with the product CD-ROM after you purchase the product.
- Step 2** Obtain the software package from the product CD or the Cisco Web page, and uncompress the software package as described in [Obtaining the SESM Installation Image File, page 2-7](#).



**Note** The software package must match the license you purchased. For example, if you purchased a SESM RADIUS installation license for 50000 users, your license number works only with the SESM software package labeled for SESM RADIUS installation for 50000 users.

---

- Step 3** Start the installation program as described in [Commands to Start Installation, page 5-3](#).
- Step 4** When the installation program prompts for the Installation Type and License Number, select the Licensed option and enter your license number.
- The installation program can detect from your license number whether to install a SESM RADIUS installation or a SESM SPE installation.
- Step 5** When the installation program prompts for the Setup Type, select one of the following:
- Typical or Custom—To install and configure SESM and SPE components for communication with other network components in a fully configured deployment, for testing, development, and production.
  - Demo—To install and configure a demonstration version of SESM, which simulates SESM portal activity but does not communicate with other network components. If you are installing the SESM SPE package, a Demo installation does not install the SPE components. You can perform another installation at a later time to obtain the SPE components.
- Step 6** Continue to answer prompts from the installation program, as described in [Responding to Installation Program Prompts, page 5-6](#).
- 

## Installing an Evaluation Version

You can install an evaluation version of SESM without a license number. An evaluation version provides full software functionality and does not have an expiration period.



**Note** You must install a licensed version using a license number before deploying SESM in a production environment.

---

To install an evaluation version of SESM software:

- 
- Step 1** Obtain the software package from the product CD or the Cisco Web page, and uncompress the software package as described in the [Obtaining the SESM Installation Image File, page 2-7](#).
- You can use any of the SESM packages for evaluation installations.
- Step 2** Start the installation as described in [Commands to Start Installation, page 5-3](#).

- Step 3** When the installation program prompts for the Installation Type and License Number, select one of the following:
- SESM RADIUS evaluation—To evaluate a SESM RADIUS installation.
  - SESM SPE evaluation—To evaluate a SESM SPE installation.
- Leave the license number field blank.
- Step 4** When the installation program prompts for the Setup Type, select one of the following:
- Typical or Custom—To install and configure SESM components for communication with other network components in a fully configured deployment, for testing, evaluation, and development.
  - Demo—To install and configure a demonstration version of SESM, which simulates SESM portal activity but does not communicate with other network components. If you chose SESM SPE in Step 4, the Demo installation does not install the SPE components.
- Step 5** Continue to answer prompts from the installation program, as described in [Responding to Installation Program Prompts, page 5-6](#).
- 

## Responding to Installation Program Prompts

[Table 5-1](#) describes the attributes that the installation program prompts for during the installation process.

After installation, you can change the value of configuration attributes by editing configuration files or by using the CDAT Application Management interface.

**Table 5-1** *SESM Installation and Configuration Parameters*

| Category                        | Field                                | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General installation parameters | Installation type and license number | <p>Select the type of installation:</p> <ul style="list-style-type: none"> <li>• <b>RADIUS Evaluation</b>—Select this option to evaluate SESM in a RADIUS deployment. You do not need a license number, there is no expiration time associated with the evaluation, and the functionality is the same as that of licensed installation.</li> <li>• <b>SPE Evaluation</b>—Select this option to evaluate SESM in an SPE deployment. You do not need a license number, there is no expiration time associated with the evaluation, and the functionality is the same as that of licensed installation.</li> <li>• <b>Licensed</b>—If you purchased a SESM license, select this option and enter the license number provided by Cisco.</li> </ul> <p>The installation program interprets the license number you enter and proceeds with the SESM RADIUS or SESM SPE installation, whichever matches the license you purchased. A RADIUS installation license will not allow you to install SPE libraries or RDP.</p> <p><b>Note</b> Obtain your SESM license number from the License Certificate shipped with the CD-ROM or otherwise provided to you by your Cisco account representative. If you have not yet received a Certificate, select one of the Evaluation modes.</p> <p>The licensenum.txt file in your root installation directory records your license number and the version of the software you installed. This information is important when you access Cisco technical support for this product.</p> |
|                                 | License agreement                    | Read the displayed license agreement to ensure that you agree with the terms of the license. You must accept the agreement to proceed with installation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                                 | Installation directory               | <p><b>Note</b> You must have write privileges to the installation directory.</p> <p>To specify the installation directory, do one of the following:</p> <ul style="list-style-type: none"> <li>• Accept the displayed default installation directory.</li> <li>• Click <b>Browse</b> to find a location.</li> <li>• Enter the directory name in the box.</li> </ul> <p>For a new installation, the default installation directories are:</p> <ul style="list-style-type: none"> <li>• On Solaris and Linux: /opt/cisco/sesm_3.3.1</li> <li>• On Windows: C:\Program Files\cisco\sesm_3.3.1</li> </ul> <p><b>Note</b> If the installation program finds an existing SESM installation on the machine, the default installation directory is the directory of the current installation. You must change the default installation directory, or backup the current installation and uninstall, before you continue to install in the default directory. Do not install SESM in the same directory as an existing SESM installation.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 5-1 SESM Installation and Configuration Parameters (continued)

| Category                                       | Field      | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General installation parameters<br>(continued) | Setup type | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Typical—(Default) Installs all of the following components in the same directory on the same machine: <ul style="list-style-type: none"> <li>– Captive portal solution applications—Includes the Captive Portal and Message Portal applications.</li> <li>– Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model.</li> <li>– Jetty—Includes the Jetty web server, Jetty web proxy application, the JMX server, and JNDI.</li> <li>– Application Manager—Installed for all installation types.</li> <li>– RDP—Installed only when installation type is SPE evaluation or SPE license.</li> <li>– CDAT—Installed only when installation type is SPE evaluation or SPE license.</li> <li>– SPE—Installed only when installation type is SPE evaluation or SESM SPE license.</li> <li>– Tools—Includes utilities for testing, development, and small-scale production environments. Installed for all installation types.</li> </ul> </li> <li>• Custom—Allows you to select the components to install and configure from a checklist. Select this option to: <ul style="list-style-type: none"> <li>– Install WSG.</li> <li>– Reinstall a component.</li> <li>– Distribute the SESM components among different workstations.</li> </ul> </li> <li>• Demo—Installs and configures the NWSP, WAP, and PDA applications to run in Demo mode. The configuration files are not set up to communicate with an SSG, a RADIUS server, or an LDAP directory. Select this option when those components are not available.</li> </ul> <p><b>Note</b> If you install SESM Demo, and later want to run the portals in a RADIUS or SPE installation, we recommend that you run the SESM installation again for a SESM RADIUS or SESM SPE installation. Otherwise, you must make extensive adjustments to configuration attributes in the MBeans.</p> <p>The SESM Demo installation simulates the actions of SESM deployments in both SESM RADIUS and SESM SPE installations. It uses a local copy of a Merit RADIUS file to obtain profile information.</p> <p>The difference between a demo installation and a typical installation is the contents of the configuration files. (The JMX MBeans are configured differently.) In addition, a demo installation does not install the SPE component.</p> |

**Table 5-1** *SESM Installation and Configuration Parameters (continued)*

| Category                                                                                                | Field                       | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration and Deployment                                                                            | Web Application Host        | <p>Specify the IP address or hostname of the host on which the SESM web portal applications will run. In a Demo installation, you can use the default value localhost.</p> <p><b>Note</b> In SESM SPE and SESM RADIUS installations, this value must be a real IP address. You cannot use the values localhost or 127.0.0.1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                                                                         | Web Application Port Number | <p>Specify the port on which the container (the J2EE web server) for the SESM portal applications will listen for HTTP requests from subscribers. The installation program updates the application startup scripts for NWSP, WAP, and PDA to use this value. If you want to run these applications simultaneously, you must edit the start scripts to ensure that each application uses a different port.</p> <p>The displayed default value is port 8080.</p> <p><b>Tip</b> Each web server running on the same machine must listen on its own unique port. If another web server or another instance of the SESM portal application is listening on 8080, change this value.</p> <p>The application startup script uses the application port number to derive two other port numbers:</p> <ul style="list-style-type: none"> <li>A secure socket listener (SSL) port is derived as follows: <math display="block">\text{application port} - 80 + 443</math> <p>For example, when the application port is 8080, the SSL port is:</p> <math display="block">8080 - 80 + 443 = 8443</math> </li> <li>A management console port is derived as follows: <math display="block">\text{application port} + 100</math> <p>For example, when the application port is 8080, the management port is:</p> <math display="block">8080 + 100 = 8180</math> </li> </ul> |
| <p><b>Note</b> If you are running a SESM Demo installation, you are finished with the installation.</p> |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 5-1 SESM Installation and Configuration Parameters (continued)

| Category                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Field                | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SSG details</b><br><br><b>Tip</b> Use the <b>show run</b> command on the SSG host device to determine how SSG is configured.                                                                                                                                                                                                                                                                                                                          | SSG port number      | Specify the port that SSG uses to listen for RADIUS requests from SESM applications. This value must match the value that was configured on the SSG host with the following command:<br><br><pre>ssg radius-helper &lt;authenticationPort&gt;</pre> Default: 1812.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                          | SSG shared secret    | Specify the shared secret used for communication between SSG and SESM applications. This value must match the value that was configured on the SSG host with the following command:<br><br><pre>ssg radius-helper key &lt;secret&gt;</pre> Default: cisco.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                          | SSG port bundle size | Enter the number of bits that SSG uses for port bundling when the port-bundle host key feature is enabled. This value must match the value that was configured on the SSG host with the following command:<br><br><pre>ssg port-map &lt;length&gt;</pre> We recommend using the value 4.<br><br>A value of 0 indicates that the SSG is not using the port-bundle host key mechanism.<br><br><b>Note</b> The port-bundle host key feature was introduced in Cisco IOS Release 12.2(2)B. If you are using an earlier release, use a value of 0 in this field.<br><br>Default: 0.<br><br>For more information about port bundle host key, see <a href="#">Configuring the Port-Bundle Host Key Feature on SSG, page 3-4</a> . |
| <b>Note</b> If you set the port bundle size to 0, you must associate SSGs to client subnets. The following category of parameters lets you associate one client subnet for one SSG. You must manually edit the configuration file to: <ul style="list-style-type: none"> <li>Associate additional non host key SSG.</li> <li>Add more client subnets to this SSG.</li> <li>Override the global values you specified in the previous category.</li> </ul> |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| One non host key SSG                                                                                                                                                                                                                                                                                                                                                                                                                                     | SSG address          | Enter the hostname or IP address of the SSG host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Client subnet        | Enter one client subnet address handled by this SSG, for example, 177.52.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Subnet mask          | Enter the mask that can be applied to subscriber IP addresses to derive their subnet, for example, 255.255.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Note</b> If you are running a SESM RADIUS installation, then the installation prompts you for the following RADIUS server information. If you are running a SESM SPE installation, skip the following two categories and continue with the Data store type selection category later in this table.                                                                                                                                                    |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



**Table 5-1** *SESM Installation and Configuration Parameters (continued)*

| Category                                                                                                                                                                                                                                                                                      | Field                     | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS server details                                                                                                                                                                                                                                                                         | Primary AAA server IP     | Enter the IP address or the hostname of the primary RADIUS server.<br>Default: localhost.                                                                                                                                                                                                                                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                               | Primary AAA server port   | Enter the port number on the primary RADIUS server host that the RADIUS server listens on.<br>Default: 1812.                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                                                                                                                                                                                                               | Secondary AAA server IP   | Enter the IP address or the hostname of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the value used for the primary server.<br>Default: localhost.                                                                                                                                                                                                                                                                      |
|                                                                                                                                                                                                                                                                                               | Secondary AAA server port | Enter the port number on the secondary RADIUS server host that the RADIUS server listens on. If you are not using a secondary RADIUS server, enter the value used for the primary server.                                                                                                                                                                                                                                                                     |
|                                                                                                                                                                                                                                                                                               | Shared secret             | Enter the shared secret used between the RADIUS server and SESM. If you are using a primary and a secondary server, the shared secret must be the same for both servers.<br>Default: cisco.                                                                                                                                                                                                                                                                   |
| Passwords                                                                                                                                                                                                                                                                                     | Service password          | Enter the password that the SESM application uses to request service profiles from RADIUS. It must match the service password used in the service profiles in the RADIUS database.<br><br>This password must also match the value that was configured on the SSG host with the following command:<br><br><code>ssg service-password &lt;password&gt;</code><br><br>The service password value must be the same on all of your SSGs.<br>Default: servicecisco. |
|                                                                                                                                                                                                                                                                                               | Service group password    | Enter the password that the SESM application uses to request service group profiles from RADIUS. It must match the service group password values used in the service group profiles in the RADIUS database.<br>Default: groupcisco.                                                                                                                                                                                                                           |
| <b>Note</b> If you are running a SESM SPE installation, then the installation prompts you for the following directory server information. If you are running a SESM RADIUS installation, skip the following categories and continue with the Captive Portal installation later in this table. |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Data store type selection                                                                                                                                                                                                                                                                     | Data store type           | Select the default value of Directory Server. This is the only Data Store Type that is supported for SESM.                                                                                                                                                                                                                                                                                                                                                    |
|                                                                                                                                                                                                                                                                                               | Vendor name               | Only two Directory Server vendors are supported: <ul style="list-style-type: none"> <li>• Novell Directory Server</li> <li>• Sun ONE (iPlanet)</li> </ul>                                                                                                                                                                                                                                                                                                     |

Table 5-1 SESM Installation and Configuration Parameters (continued)

| Category                     | Field                         | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password Encryption Panel    | SPE Installation Type         | Select the default value of Fresh SPE Installation. This is the only SPE installation type that is supported for SESM.                                                                                                                                                                                                                                                                                                                 |
|                              | Master Password               | Enter a password and verify it in the Master Password (Repeat) field. Make a note of this password for future reference.                                                                                                                                                                                                                                                                                                               |
|                              | Password Encryption Algorithm | Select <b>SHA</b> .                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Naming attribute             | inetorgPerson                 | <p>This window appears only when the Datastore selected is iPlanet. Change the component in distinguished name (dn) that allows access to the SESM container, if required. The default is unique identifier (uid).</p> <p><b>Note</b> When the Datastore selected is not iPlanet, the naming attribute is automatically set to common name (cn).</p>                                                                                   |
| Directory server information | Directory address             | <p>Enter the IP address or the hostname of the system on which the directory server is running.</p> <p>Default: localhost.</p>                                                                                                                                                                                                                                                                                                         |
|                              | Directory port                | Enter the port on which the directory server listens.                                                                                                                                                                                                                                                                                                                                                                                  |
|                              | Directory admin user          | <p>Enter a user ID that has permissions to extend the directory schema. Use cn or uid as appropriate. For example:</p> <ul style="list-style-type: none"> <li>For NDS, enter:<br/><code>cn=admin, ou=sesm, o=cisco</code></li> <li>For Sun ONE or iPlanet, enter:<br/><code>cn=Directory Manager</code></li> </ul> <p><b>Note</b> The default configuration by the Sun ONE installation process uses cn for the directory manager.</p> |
|                              | Directory admin password      | <p>Enter the password for the directory administrator. This is the password you entered during directory installation and configuration. For example:</p> <ul style="list-style-type: none"> <li>For NDS, enter the password you specified for the admin user during installation.</li> <li>For Sun ONE or iPlanet, enter the password you entered for the Directory Manager user during Sun ONE installation.</li> </ul>              |
|                              | Directory container           | <p>Enter the organization and organizational unit that will hold the SESM service, subscriber, and policy information. Use the following format:</p> <p><code>ou=orgUnit, o=org</code></p> <p>For example, the installation program's default values are:</p> <p><code>ou=sesm, o=cisco</code></p> <p>The above defaults are the values used in the sample data file that comes with CDAT.</p>                                         |

Table 5-1 SESM Installation and Configuration Parameters (continued)

| Category                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Field               | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | DESS AdminUser      | <p>Enter a user ID that has permissions to access and create objects in the organization and organizational unit named above. Use cn or uid as appropriate. For example:</p> <ul style="list-style-type: none"> <li>For NDS, the container administrator is the same as the directory administrator you entered on the previous window:<br/><code>cn=admin,ou=sesm,o=cisco</code></li> <li>For Sun ONE or iPlanet, the container administrator is not the same as the directory administrator. You created this container administrator after Sun ONE installation.<br/><code>uid=yourAdmin,ou=sesm,o=cisco</code></li> </ul>                                                                                                                                                                                                                                           |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | DESS Admin Password | Enter the password associated with the DESS Admin user ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p><b>Note</b> The installation program tries to access the directory server and the container, using the information you provided. If access fails, the installation program displays a window with the header “Warning—Please confirm these options.” Verify that the information you entered is correct, and also verify that the directory server is running. If the directory is not running, you can continue installing SPE components by clicking the <b>Ignore</b> button on the warning window. However, if you click <b>Ignore</b>, the installation program can not update the directory for SESM use. You must perform the updates at a later time before you run SESM web applications or CDAT.</p> |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| RDP<br>Configures RDP to<br>SSG communication                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | RDP host            | <p>Enter the IP address or hostname on which the RDP will run.</p> <p>Default: localhost.</p> <p><b>Note</b> Use a routable IP address. Do not use the values localhost or 127.0.0.1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Port number         | <p>Enter the port on which the RDP will listen.</p> <p>Default: 1812.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Shared secret       | <p>Enter the shared secret to be used for communication between the SSGs and RDP when the restricted client feature is turned off. This value must match the value configured on the SSG host devices, using the following command:</p> <pre>radius-server key &lt;SharedSecret&gt;</pre> <p>When the restricted client feature is turned off, the shared secret must be the same on all SSGs.</p> <p>When the restricted client feature is turned on, this attribute is ignored. Instead, you configure a specific shared secret for each client (each SSG). See <a href="#">Chapter 3, “Configuring the Selection Services Gateway to Work with SESM”</a> for more information.</p> <p>The Add Client option (the option appears in a few windows after this one) lets you select whether to turn the restricted client feature on or off.</p> <p>Default: cisco.</p> |

Table 5-1 SESM Installation and Configuration Parameters (continued)

| Category    | Field             | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | Service password  | <p>Enter the password that RDP uses to request service profiles from the directory. This value must match two other configured values:</p> <ul style="list-style-type: none"> <li>This password must match the value that was configured on the SSG host with the following command:<br/> <pre>ssg service-password &lt;password&gt;</pre> <p>The service-password value must be the same on all the SSGs that communicate with this RDP server.</p> </li> <li>This value must also match the service password value you entered for the SESM portal. See <a href="#">Passwords, page 5-11</a>.</li> </ul> <p>Default: servicecisco.</p> |
|             | Group password    | <p>Enter the password that RDP uses to request service group profiles from the directory.</p> <p>This password must match the group password value you entered for the SESM portal. See <a href="#">Passwords, page 5-11</a>.</p> <p>Default: groupcisco.</p>                                                                                                                                                                                                                                                                                                                                                                            |
|             | Next hop password | <p>Enter the password that SSG uses to request next hop tables from RDP.</p> <p>This password must match the value that was configured on the SSG host with the following command:<br/> <pre>ssg next-hop download &lt;nextHopTableName password&gt;</pre> <p>The service password value must be the same on all of the SSGs that communicate with this RDP server.</p> <p>Default: nexthopcisco.</p> </p>                                                                                                                                                                                                                               |
| RDP Options | Proxy mode        | <p>Select this option to run RDP in proxy mode. RDP has two modes:</p> <ul style="list-style-type: none"> <li>Proxy mode—In this mode, RDP forwards authentication requests to a RADIUS server. RDP uses the SPE API to send authorization requests to the directory.</li> <li>Default (non-proxy) mode—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the SPE API to send authorization requests to the LDAP directory.</li> </ul>                                                                                                                                              |
|             | Add client        | <p>Select this option if you want to turn on the RDP restricted client feature, which allows RDP to service requests only from a preconfigured list of clients. The RDP clients are SSGs.</p> <p>If you check this option, the installation program prompts for configuration information for one client. You can add more clients by adding elements to the allowedClients attribute in the RADIUSServerSocket MBean.</p> <p>The default is unchecked, which allows the RDP to accept requests from any client (any SSG).</p>                                                                                                           |

**Table 5-1** *SESM Installation and Configuration Parameters (continued)*

| Category                                                                                                                                                                                                                                                                                                                                                             | Field             | Explanation                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If you select the RDP Proxy mode option, the installation prompts you for the following RADIUS server information.                                                                                                                                                                                                                                                   |                   |                                                                                                                                                                                                                         |
| AAA Server Details                                                                                                                                                                                                                                                                                                                                                   | Primary IP        | Enter the IP address or the hostname of the primary AAA server that you want RDP to communicate with.<br>Default: localhost                                                                                             |
|                                                                                                                                                                                                                                                                                                                                                                      | Primary port      | Enter the port number on the primary RADIUS server host that the RADIUS server listens on.<br>Default: 1812                                                                                                             |
|                                                                                                                                                                                                                                                                                                                                                                      | Secondary IP      | Enter the IP address or the hostname of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the value used for the primary server.<br>Default: localhost                                 |
|                                                                                                                                                                                                                                                                                                                                                                      | Secondary port    | Enter the port number on the secondary RADIUS server host that the RADIUS server listens on. If you are not using a secondary RADIUS server, enter the value used for the primary server.<br>Default: 1812              |
|                                                                                                                                                                                                                                                                                                                                                                      | Shared secret     | Enter the shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers.<br>Default: cisco.                                                                                 |
| <b>Note</b> If you select the RDP Add client option, the installation program prompts you for the following information about one RDP client. You can add more clients by adding elements to the allowedClients attribute in the RDP MBean, RADIUSServerSocket component. See <i>Cisco Subscriber Edge Services Manager Administration and Configuration Guide</i> . |                   |                                                                                                                                                                                                                         |
| RDP Client                                                                                                                                                                                                                                                                                                                                                           | Client IP address | Enter the IP address of the SSG.                                                                                                                                                                                        |
|                                                                                                                                                                                                                                                                                                                                                                      | Shared Secret     | Enter the shared secret used for SSG to RDP communication. This value must match the value configured on the SSG, using the following command:<br><br><pre>radius-server key &lt;SharedSecret&gt;</pre> Default: cisco. |

**Table 5-1** *SESM Installation and Configuration Parameters (continued)*

| Category                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Field                       | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> The Captive Portal configuration information you enter in the following parameters must match TCP redirect configuration values on the SSG. The easiest way to ensure that values match in both places is to accept all of the default values presented by the installation process. Then configure the SSG based on the example captiveportal/config/ssgconfig.txt file. See <a href="#">Chapter 3, “Configuring the Selection Services Gateway to Work with SESM”</a> for more information. |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Captive Portal Server Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Captive portal host         | Enter the IP address or hostname on which the captive portal solution will run.<br>Default: localhost                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Captive portal port number  | Enter the port number on which the first listener in the captive portal web server will listen.<br><br>This installation program sets up the captiveportal.jetty.xml file to create seven listeners in the web server, as follows: <ul style="list-style-type: none"> <li>Subscriber redirection listener.</li> <li>Initial logon redirection listener.</li> <li>Advertising redirection listener.</li> <li>Default service redirection listener.</li> <li>Three service redirection listeners.</li> </ul> Later in this installation procedure, you are prompted for a port number for each of these listeners. The port you enter now is used as the default value for the first listener.<br><br><b>Note</b> If you use the same port number for more than one listener, some redirections will not work.<br><br>Default: 8090 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Install Message Portal      | Select this option if you want to install the Message Portal application. The Message Portal application is an example of an SESM portal that provides content for: <ul style="list-style-type: none"> <li>Initial logon redirections.</li> <li>Advertising redirections.</li> </ul> For those redirection types, the default URIs displayed later in this installation procedure refer to pages in the Message Portal application.<br><br>Default: Selected                                                                                                                                                                                                                                                                                                                                                                      |
| If you select the Message Portal option above, the installation program prompts you for the following information.                                                                                                                                                                                                                                                                                                                                                                                        |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Message Portal Server Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Message Portal Port Number  | Enter the port number on which the Message Portal web server will listen. The Message Portal web server has one listener.<br>Default: 8085                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Redirect after message page | Select this option if you want the Message Portal application to redirect the subscriber to the originally requested URL after the message duration time elapses. If you do not select this option, the subscriber must enter an URL to leave the message page.<br><br>Default: Selected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 5-1** *SESM Installation and Configuration Parameters (continued)*

| Category                         | Field                                          | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Main web server configuration    | Host                                           | <p>Enter the hostname or IP address of the web server for the NWSP or other application that will respond to:</p> <ul style="list-style-type: none"> <li>• Unauthenticated user redirection.</li> <li>• Default unconnected service redirection.</li> <li>• Specific unconnected service redirections.</li> <li>• Error handling due to captive portal misconfiguration (if a port that is not configured for redirection was used).</li> </ul> <p>This value becomes the default for the serviceportal.host system property in the captiveportal.xml file.</p> <p>Default: localhost</p>                                                                               |
|                                  | Port                                           | <p>Enter the port number on which the web server named above will listen.</p> <p>This value becomes the default for the serviceportal.port system property in the captiveportal.xml file.</p> <p>Default: 8080</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Unauthenticated User Redirection | Enable                                         | Check this box to configure unauthenticated user redirections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | Port In                                        | <p>Enter the port that the web server for the Captive Portal application will listen on for unauthenticated user redirections received from the SSG. The installation program displays the value that you entered earlier in the Captive Portal Port Number field. You can accept this default value.</p> <p><b>Note</b> You must configure the SSG TCP redirect feature to send unauthenticated user redirections to this port.</p> <p>Default: 8090</p>                                                                                                                                                                                                               |
|                                  | URL Out: Host<br>URL Out: Port<br>URL Out: URI | <p>These fields define the URL to which browsers are redirected for unauthenticated user redirections. The default values refer to the NWSP application.</p> <ul style="list-style-type: none"> <li>• Host—Enter the name or IP address for the web server that contains the content application for unauthenticated user redirections.<br/>Default: localhost</li> <li>• Port—Enter the listener port number for this content application. The default is the port number you entered for the NWSP application.<br/>Default: 8080</li> <li>• URI—The absolute page name you want the subscriber to see. The default is /home, which is the NWSP logon page.</li> </ul> |

**Table 5-1** *SESM Installation and Configuration Parameters (continued)*

| Category                | Field                                          | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initial Captivation     | Enable                                         | Check this box to configure initial logon redirections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                         | Port In                                        | Enter the port that the Captive Portal web server will listen on for initial logon redirections.<br><br><b>Note</b> You must configure the SSG TCP redirect feature to send initial logon redirections to this port.<br><br>Default: 8091                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                         | URL Out: Host<br>URL Out: Port<br>URL Out: URI | These fields define the URL to which browsers are redirected for initial logon redirections. The default values refer to the Message Portal application.<br><ul style="list-style-type: none"><li>Host—Enter the name or IP address for the web server that contains the content application for initial logon redirections.<br/>Default: localhost</li><li>Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application.<br/>Default: 8085</li><li>URI—The absolute page name you want the subscriber to see. The default is /initial, which is the Message Portal greeting page.</li></ul>    |
|                         | Duration                                       | The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL.<br>Default: 15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Advertising Captivation | Enable                                         | Check this box to configure advertising redirections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                         | Port In                                        | Enter the port that the Captive Portal web server will listen on for advertising redirections.<br><br><b>Note</b> You must configure the SSG TCP feature to send advertising redirections to this port.<br><br>Default: 8092                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                         | URL Out: Host<br>URL Out: Port<br>URL Out: URI | These fields define the URL to which browsers are redirected for advertising redirections. The default values refer to the Message Portal application.<br><ul style="list-style-type: none"><li>Host—Enter the name or IP address for the web server that contains the content application for advertising redirections.<br/>Default: localhost</li><li>Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application.<br/>Default: 8085</li><li>URI—The absolute page name you want the subscriber to see. The default is /advertising, which is the Message Portal advertising page.</li></ul> |
|                         | Duration                                       | The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL.<br>Default: 15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



Table 5-1 SESM Installation and Configuration Parameters (continued)

| Category                                    | Field                                                                                               | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unconnected Service Redirection             | Enable                                                                                              | Check this box to configure service redirections, including a default service redirection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                             | Default Service Redirect Port In                                                                    | Enter the port that the Captive Portal web server will listen on for default service redirections. Default service redirections are used for services whose address does not belong to the destination network of any of the specific service redirections.<br><br><b>Note</b> You must configure the SSG TCP feature to send default service redirections to this port.<br><br>Default: 8093                                                                                                                                                                                                                                                                                                                                                |
|                                             | First Service Redirect Port In<br>Second Service Redirect Port In<br>Third Service Redirect Port In | Enter the ports that the Captive Portal web server will listen on for service redirections for Service1, Service2, and Service3.<br><br><b>Note</b> You must configure the SSG TCP feature to send redirections to these ports.<br><br>Defaults: 8094, 8095, 8096                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                             | URL Out                                                                                             | Enter the URL to which browsers are redirected for any type of service redirection. The default value refers to the NWSP application, as follows: <ul style="list-style-type: none"> <li>The host and port values are the ones you entered earlier for the service application.</li> <li>The page name is /serviceRedirect, which is a generalized NWSP page. Configuration parameters in nwsp.xml define more specific pages.</li> </ul> This installation program assumes that the same URL is used for all service redirections. You can change this default configuration in the captiveportal.xml file. There is no requirement that all service redirections use the same page, port, or application.<br><br>Default: http://localhost |
| Details for Unconnected Service Redirection | Pass Service Names                                                                                  | Select this option if you want the Captive Portal application to pass the service names to the content application that handles service redirections (NWSP in the default configuration). NWSP uses the service name to connect to the service.<br><br>If you do not check this option, NWSP displays the page specified in the serviceNotGivenURI attribute in nwsp.xml. (The default installation setting for the serviceNotGivenURI attribute is the NWSP status page.)                                                                                                                                                                                                                                                                   |
|                                             | Redirect Service Names                                                                              | Provide the service name as specified in the service profile. The default values provided in the installation program match services in the sample data installed with SESM.<br><br>Default: service1, service2, service3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| CDAT                                        | CDAT host                                                                                           | Enter the IP address or hostname on which the CDAT application will run.<br><br>Default: localhost<br><br><b>Note</b> Use a routable IP address. Do not use the values localhost or 127.0.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                             | CDAT port number                                                                                    | Enter the port number on which the CDAT web server will listen.<br><br>The default is 8081.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 5-1** SESM Installation and Configuration Parameters (continued)

| Category                                                                                                                                                                                                                                               | Field                              | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Management Web Server Configuration                                                                                                                                                                                                        | Application Management Port Number | Enter the port number on which the Application Management web server will listen.<br>Default: 8082.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| The installation program installs the components on your system. When it is finished installing the files, and if it successfully connected to your LDAP directory, it displays the following additional prompts about modifications to the directory. |                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LDAP directory modifications                                                                                                                                                                                                                           | Extend schema                      | <p>Select this option if:</p> <ul style="list-style-type: none"> <li>You are installing the current SESM release for the first time.</li> <li>You installed a new LDAP directory.</li> <li>If this update was not yet performed on the database for the current SESM release.</li> <li>If you are not sure about any of the above. There are no negative consequences to running the extensions multiple times.</li> </ul> <p>The extensions include the objects and attributes for SPE. For more information about the extensions, see <i>Cisco Subscriber Edge Services Manager Profile Management Guide</i>.</p> <p><b>Note</b> After installing a SESM SPE installation, you must extend the directory schema at some time before running the SESM application and before logging into CDAT to create objects in the directory. See <i>Cisco Subscriber Edge Services Manager Profile Management Guide</i> for more information.</p> |
|                                                                                                                                                                                                                                                        | Install RBAC                       | <p>Select this option if you want the installation program to load the top-level RBAC objects. You need to perform this operation only once per container in a directory.</p> <p>Some initial top-level rules and roles must be created in the directory before an administrator can log into CDAT and create additional objects. If you do not select this option, you must install RBAC objects later, before running SESM and before logging into CDAT to create objects in the directory. See <a href="#">Extending the Directory Schema and Loading Initial RBAC Objects, page 4-7</a> for more information.</p> <p>See <a href="#">Loading Sample SESM Data, page 4-7</a> for information about loading sample data after the SPE extensions are applied.</p>                                                                                                                                                                      |

## Installation Results

The Cisco SESM installation directory contains the following subdirectories and files:

- \_jvm—(Optional) This directory contains the JRE that is shipped with SESM.
- \_uninst—This directory contains the utility to uninstall the components you just installed. To uninstall components, run the executable file in this directory.
- apmgmt—This directory contains the Application Manager application and configuration files.
- captiveportal—This directory contains the SESM Captive Portal application and configuration files.
- cdat (SESM SPE installation only)—This directory contains the CDAT application and configuration files.

- **dess-auth** (SESM SPE installation only)—This directory contains the SPE DESS and AUTH libraries, SPE DESS schema, and sample data. The schema subdirectory contains the README.SESM.LDIF.html file, which explains how to manually update the LDAP directory with the SPE schema, load initial RBAC objects, and load sample data.
- **docs**—This directory contains the apidoc directory, which holds the Java documentation for the SESM application programmer interface (API).
- **jetty**—This directory contains the following subdirectories:
  - **bin**—Contains start scripts for SESM applications running in Jetty containers; includes a start script for the Jetty web proxy application.
  - **config**—Contains configuration files that control Jetty servlets.
  - **lib**—Contains the Jetty server class libraries.
- **libs**—This directory contains the SESM class libraries.
- **messageportal**—This directory exists only if you chose the Install Message Portal option during the installation.
- **nwsp, pda, wap, and sp**—These directories contain the following subdirectories:
  - **config**—Contains a configuration file for the portal application and a demo data file.
  - **docs**—Contains the application javadoc files.
  - **webapp**—Contains the Web application, including libraries, JSPs, images, and the WEB-INF directory, which includes J2EE configuration files, such as web.xml and web-jetty.xml.
- **rdp**—This directory contains startup scripts, configuration files, and libraries for the RDP application.
- **redist**—This directory contains libraries from third-party companies that Cisco is redistributing. It includes the Jasper JSP framework, the JMX framework, and the JAXP XML parser framework. It also includes test tools.
- **tools**—This directory contains the following scripts and utilities that developers can use to:
  - Precompile customized SESM JSPs.
  - Configure and start the Bundled RADIUS server.
  - Configure and start the Bundled Proxy server.
  - Simulate an SSG for testing and development purposes.
- **webproxy**—A placeholder directory for log files created by the web proxy application.
- **wsg**—This directory contains the SESM Web Services Gateway (WSG) application and configuration files, and the startup script for the WSG client example application.
- **licensenum.txt**—This file contains the license number that you used during installation and the version number of the SESM software that you installed.
- **readme** file.

# Uninstalling a SESM Installation

If you plan to install SESM into a directory in which a previous SESM installation already exists, you must first uninstall the existing SESM installation. You must use the SESM uninstall utility provided with the SESM product to ensure the complete removal of the previous installation. (You can successfully install SESM in a different directory without removing the first installation.)



## Note

Do not uninstall SESM by manually deleting the contents of the installation directory. If you do so, and then try to reinstall into the same directory, the installation might not be complete. If the installation is incomplete, see *Cisco Subscriber Edge Services Manager Troubleshooting Guide* for information.

The **uninstall** utility is located in the following directory:

```
installDir
 _uninst
 uninstall.bin or uninstall.exe
```

The **uninstall** utility does the following:

- Lets you choose the components to uninstall.
- Verifies the installation directory that is being uninstalled.
- Uninstalls the SESM components. It does not remove the installation directory, only the contents under the installation directory.

**Step 1** Stop all SESM application processes before uninstalling SESM.

**Step 2** Run the uninstall utility.

**Step 3** After running the **uninstall** utility, manually remove any remaining subdirectories under the installation directory.

You can now reinstall one or more SESM components into the same directory.

## What's Next

This chapter describes how to proceed with SESM configuration, testing, and development after installation. The chapter includes the following topics:

- [Post-Installation Configuration Tasks, page 5-23](#)
- [Creating Profiles, page 5-23](#)
- [Customizing SESM Applications, page 5-23](#)
- [Running SESM Applications, page 5-23](#)

## Post-Installation Configuration Tasks

This section lists some configuration tasks that might be required after you install SESM applications.

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | If you have not already done so, install and configure other software components required for your SESM solution, such as RADIUS servers, an LDAP directory, and SSGs. See <a href="#">Chapter 3, “Configuring the Selection Services Gateway to Work with SESM”</a> and <a href="#">Chapter 4, “Configuring the Servers in Your Deployment for SESM”</a> for information about configuring these components to work in SESM deployments. |
| <b>Step 2</b> | <p>If the SSG port-bundle host key feature is not used on the SSGs, add configuration information for additional SSGs.</p> <p>The SESM installation program caters to use of a single SSG or multiple SSGs with the host key feature. For multiple SSG support without the host key feature, you must configure the mappings between the SSG and client subnets. See <i>Cisco Subscriber Edge Services Manager Web Portals Guide</i>.</p> |
| <b>Step 3</b> | If you installed the RDP server and turned on the restricted client feature, you might need to add more SSGs to the RDP's client list. The installation program accepts information for one client. See <i>Cisco Subscriber Edge Services Manager Profile Management Guide</i> .                                                                                                                                                          |
- 

## Creating Profiles

SESM deployments depend on valid information in subscriber and service profiles. For procedures about maintaining profiles and information about profile content, see the following:

- For SESM RADIUS installations:
  - *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*
  - Your RADIUS server vendor documentation
- For SESM SPE installations:
  - *Cisco Subscriber Edge Services Manager Profile Management Guide*
  - Your SPE database vendor documentation

## Running SESM Applications

To start or stop a SESM application, you must run the associated start or stop script. For information about the start and stop scripts for SESM applications, see *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*.

## Customizing SESM Applications

This section points you to information about changing the installed applications.

### Customizing the SESM Web Portals

For information about changing the SESM web portal pages, and compiling or precompiling those pages, see *Cisco Subscriber Edge Services Manager Web Developer Guide*.

For information about configuring a SESM web portal application, see *Cisco Subscriber Edge Services Manager Web Portals Guide*.

### **Customizing the Captive Portal Solution**

For information about customizing the captive portal solution:

- To change captivation configuration, and to change the URLs that are displayed as a result of the captivation, see *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*.
- To change the look of the JSPs that are displayed after captivation, or to create new captivation content applications, see *Cisco Subscriber Edge Services Manager Web Developer Guide*. The captive portal content applications are SESM web portals.

### **Setting Up a Testing Environment**

For information about setting up a testing environment, see *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*.



## Upgrading to SESM 3.3(1)

---

This chapter describes how to upgrade SESM from previous releases and preserve your customizations and configurations. In a SESM SPE installation, you must also upgrade your LDAP directory with the SPE schema extensions. This chapter contains the following topics:

- [Upgrading the LDAP Directory with SPE Schema Extensions, page 6-1](#)
- [Preserving SESM Customizations and Configurations, page 6-3](#)

## Upgrading the LDAP Directory with SPE Schema Extensions

In a SESM SPE installation, you must upgrade your LDAP directory with the SPE schema extensions:

- [Upgrading the LDAP Directory from SESM 3.2\(2\), page 6-1](#)
- [Upgrading the LDAP Directory from SESM 3.1\(9\) or SESM 3.2\(1\), page 6-2](#)
- [Upgrading the LDAP Directory from SESM 3.1\(3\), SESM 3.1\(5\), or SESM 3.1\(7\), page 6-3](#)



**Note**

---

We recommend that you make a backup of your LDAP directory before you upgrade it.

---

## Upgrading the LDAP Directory from SESM 3.2(2)

To upgrade the LDAP directory in a SESM SPE installation from SESM 3.2(2) to SESM 3.3(1), you need only extend the SPE schema using the SESM SPE installation application.

### Extending SPE Schema

You can choose to extend the SPE schema while installing SESM, or you can run the installation program with the Custom option after installing SESM.




**Note**

---

If you use the custom installation just to extend schema, you should install SESM in a directory separate from the directory in which SESM is already installed.

---

To use the SESM installation process to extend the directory schema:

- 
- Step 1** Make sure the LDAP directory server is running.
- Step 2** Make sure you know the following user IDs and passwords:
- A user ID and password that enables you to update the directory schema
  - A user ID and password that enables you to update the container (organization and organizational unit) that you created for SESM data.
- Step 3** Run the SESM installation program on a server that has network access to the LDAP directory.
- 
-  **Note** If you are using the custom installation, when the installation program prompts for the components to install, you can deselect all components except SPE.
- 
- Step 4** When the installation program prompts for directory connection information, provide correct information to access the directory. This includes the names of the organization and organizational unit you created to hold the SESM data.
- Step 5** When the installation program displays the LDAP Directory Modifications window, check the Extend Schema check box.
- 

For more details about the installation program prompts, see [Responding to Installation Program Prompts, page 5-6](#).

## Upgrading the LDAP Directory from SESM 3.1(9) or SESM 3.2(1)

To upgrade the LDAP directory in a SESM SPE installation from SESM 3.1(9) or SESM 3.2(1) to SESM 3.3(1):

- 
- Step 1** Extend the SPE schema, as described in [Extending SPE Schema, page 6-1](#).
- Step 2** Update the LDAP data so that for each rule, you add the attribute **policyKeyword = CISCO\_AZN**. You can do this by creating an LDIF file and using the `ldapmodify` command to update the LDAP data. Taking as an example goldrule from the sample data, the contents of the LDIF file will be:

```
dn: cn=goldrule,ou=sesm,o=cisco
changetype: modify
add: policyKeyword
policyKeyword: CISCO_AZN
```

Repeat this for each rule. To update the LDAP data, use the following command:

```
ldapmodify -h <ipaddress> -p <port> -c -v -D "<container_administrator>" -w <password> -f <ldif_file>
```

---



## Upgrading the LDAP Directory from SESM 3.1(3), SESM 3.1(5), or SESM 3.1(7)

If you are upgrading from SESM 3.1(3), 3.1(5), or 3.1(7), you must install the new SPE schema extensions and RBAC objects, using the SESM SPE installation program.

- 
- Step 1** Export the data from the LDAP directory.
  - Step 2** Reinstall the LDAP directory, and configure the LDAP directory to work with SESM, as described in [Configuring an LDAP Directory to Work with SESM, page 4-1](#).
  - Step 3** Install a SESM SPE installation. See [Chapter 5, “Installing and Uninstalling SESM.”](#)
  - Step 4** When the installation program displays the LDAP Directory Modifications window, check **Extend Schema**, and **Install RBAC**.
  - Step 5** Import your LDAP data back into the LDAP directory.
  - Step 6** Update the LDAP data so that for each rule, you add the attribute “policyKeyword = CISCO\_AZN”.  
You can do this by creating an LDIF file and using the “ldapmodify” command to update the LDAP data. Taking as an example “goldrule” from the sample data, the contents of the LDIF file will be:

```
dn: cn=goldrule,ou=sesm,o=cisco
changetype: modify
add: policyKeyword
policyKeyword: CISCO_AZN
```

You must repeat this for each rule; then to update the LDAP data, use the following command:

```
ldapmodify -h <ipaddress> -p <port> -c -v -D "<container_administrator>" -w <password>
-f <ldif_file>
```

---

## Preserving SESM Customizations and Configurations

This section describes how to upgrade from SESM 3.1(9) and later to SESM 3.3(1) and preserve your previous SESM installation customizations, including changes to configuration files and customized web applications.

The order of work is:

- [Install SESM 3.3\(1\) in a separate location from the current SESM installation, page 6-3](#)
- [Migrate the previous SESM configurations to SESM 3.3\(1\), page 6-4](#)
- [Migrate your customized SESM 3.2\(2\) web application to SESM 3.3\(1\), page 6-4](#)

### Install SESM 3.3(1) in a separate location from the current SESM installation



#### Note

If you are upgrading from SESM 3.1(3), 3.1(5), or 3.1(7) and have already installed SESM 3.3(1) as part of the procedure to upgrade your LDAP directory, skip this procedure and continue to [Migrate the previous SESM configurations to SESM 3.3\(1\), page 6-4](#).

---

We recommend that you install SESM into a new directory without removing the previous installation. You will then still have a reference version to compare with, and you can transfer customized settings from the previous version to the new version.

When the installation program finds an existing SESM installation on the machine, the default installation directory is the directory of the current installation. If you do not want to remove the previous installation, you must change the default installation directory. See [Chapter 5, “Installing and Uninstalling SESM”](#) for instructions on installing SESM.

If you plan to install SESM into a directory in which a previous SESM installation already exists:

- 
- Step 1** Ensure that a backup copy of your previous SESM installation is stored in a safe location. If you want to migrate your NWSP application to the new installation, you will need to copy files from this location later.
- Step 2** Uninstall the previous release of SESM using the SESM uninstallation utility provided with the SESM product to ensure that the previous installation is completely removed. See [Uninstalling a SESM Installation, page 5-22](#).
- 

### Migrate the previous SESM configurations to SESM 3.3(1)

Use any of the following methods to migrate previous SESM configurations:

- When the application is running, use Agent View or Application Manager to change the attributes to the values used in the previous installation. Be sure to use the Apply and Store operations to persist the new values across application restarts.
- When the application is not running, edit the XML configuration files to change the attribute values to the values used in the previous installation.
- Back up the SESM 3.3(1) configuration files, then copy your SESM 3.2(2) configuration files to the SESM 3.3(1) installation directory.

The SESM 3.3(1) configuration files include new and enhanced MBeans. If you copy your SESM 3.2(2) configuration files to SESM 3.3(1), you will need to manually merge the SESM 3.3(1) enhancements from the backed up files. See [Appendix C, “Configuration File Changes in SESM 3.3\(1\)”](#) for details of the changes to configuration files.

Start the NWSP web application to verify the SESM configuration. If you are running a Demo installation, you can log into the web application using the username **golduser** and the password **cisco**. After verifying that you can use the SESM web application, stop the server.

### Migrate your customized SESM 3.2(2) web application to SESM 3.3(1)



#### Note

See [Appendix C, “Configuration File Changes in SESM 3.3\(1\)”](#) for:

- Changes to configuration files.
  - Changes to web.xml file.
  - Details of the new and enhanced JSP files.
- 

To migrate your customized web application:

- 
- Step 1** If your customized SESM 3.2(2) web application is called nwsp or sp, back up the corresponding SESM 3.3(1) web application directory.
- Step 2** Copy your customized web application from the SESM 3.2(2) web application directory to SESM 3.3(1).

- Step 3** SESM 3.3(1) includes enhancements to the libraries in the WEB-INF/lib folder. Copy the new jar files from the WEB-INF/lib folder in the unmodified SESM 3.3(1) nwsp directory (in the installation directory or backup location) to your web application WEB-INF/lib folder.
- Step 4** Merge new and enhanced JSP files with the JSP files in webapp/pages in your web application.
- Step 5** If your web application contains customized JSPs in webapp/decorators:
- Use a **diff** utility to compare your web application's files in all files in webapp/decorators with the same files in the unmodified SESM 3.3(1) nwsp directory (in the installation directory or backup location).
  - Using the **diff** output from step a, merge the SESM 3.3(1) JSP file enhancements with your customizations in all files in webapp/decorators.
- If your web application does not contain customized JSPs in webapp/decorators, copy the JSPs from the unmodified SESM 3.3(1) nwsp directory (in the installation directory or backup location) to your web application.
- Step 6** If your web application's web.recompile.xml file is customized in any way, merge the enhancements in the SESM 3.3(1) web.recompile.xml file with your customizations. If your web application's web.recompile.xml file is not customized, copy the web.recompile.xml from the unmodified SESM 3.3(1) nwsp directory (in the installation directory or backup location) to your web application.
- Step 7** If you modified JSPs in the migration process, compile the JSPs using the precompile.sh script. This creates a web.xml file based on your customized web.recompile.xml file in WEB-INF. For information on how to use the precompile.sh script, see *Cisco Subscriber Edge Services Manager Web Developer Guide*.
- Step 8** If your customized web application is not called nwsp or sp, copy the following files from the installation location of the SESM 3.3(1) software (/install\_dir/):
- In */install\_dir/jetty/bin*, copy startNWSP.sh to startMYWEBAPP.sh. Edit the startMYWEBAPP.sh file and replace APP=nwsp with APP=mywebapp. (For a SESM installation on a Windows platform, the suffix of the start file is .cmd.)
  - In */install\_dir/jetty/config*, copy nwsp.jetty.xml to mywebapp.jetty.xml. Edit the mywebapp.jetty.xml file and replace nwspkeystore with mywebappkeystore. Also, replace any comments that refer to NWSP.
  - In */install\_dir/jetty/config*, copy nwsp.web-jetty.xml to mywebapp.web-jetty.xml.
- Step 9** In */install\_dir/jetty/config*, copy mywebappkeystore from your previous installation into this directory.
- Step 10** Update the web application configuration file in one of the following ways:
- Add changes and enhancements from the unmodified SESM 3.3(1) nwsp.xml file to your web application configuration file.
  - Copy the unmodified SESM 3.3(1) nwsp.xml file from the nwsp/config/ directory to your web application directory, and rename the nwsp.xml file to mywebapp.xml. Update mywebapp.xml with the customized web application configuration, as described in [Migrate the previous SESM configurations to SESM 3.3\(1\)](#), page 6-4.
- Step 11** Recompile and rerun the web application.
-





## Tuning SESM for Optimal Performance

---

This chapter describes how to ensure optimal performance for SESM. The information in this chapter is relevant to both RADIUS and SPE deployments, but for SPE deployments, there are additional considerations, which this chapter does not cover (for example, configuring the SPE component).

This chapter contains the following topics:

- [Platform Patches and Platform Specific Java/J2SE Patches, page 7-1](#)
- [Java Virtual Machine, page 7-2](#)
- [Jetty Web Server, page 7-3](#)
- [SESM Memory Management, page 7-4](#)
- [SESM Cache Settings, page 7-4](#)
- [SSG MBEAN Settings, page 7-5](#)
- [SSG MBEAN Statistics, page 7-6](#)
- [SESM Logging, page 7-7](#)

### Platform Patches and Platform Specific Java/J2SE Patches

Ensure that the platform running SESM applications conforms to the system requirements described in [Chapter 2, “Before You Begin”](#) and is kept up to date with the latest available patches from the supplier. This must include general operating system patches and Java (J2SE)-specific patches.

For Sun/Solaris platforms, patch updates can be controlled and automated using the Sun Patch Manager. For more details, see the Sun website.

Without the Patch Manager, comparing installed patches with the latest available patches can be difficult. One approach is to keep a copy of the latest installed patch clusters. On a regular basis, visit the Sun website and compare the size of the latest available patch cluster files or read the associated readme for details.

The failsafe approach is to always install the latest available patch clusters, which can be downloaded from the Sun website.

# Java Virtual Machine

- [JVM Memory Allocation, page 7-2](#)
- [Garbage Collection, page 7-2](#)
- [Java Version, page 7-3](#)

## JVM Memory Allocation

SESM is a suit of Java applications, all of which, individually, run within a Java Virtual Machine (JVM). The amount of memory available to the JVM, and hence the application, is controlled by the Java options, -Xms and -Xmx, which are passed to the JVM at startup.

By default, the amount of memory allocated to the JVM for each of the SESM web applications is set to 64 MB. This is set in the start script, <install-directory>/jetty/bin/start.sh.



### Note

The start script, start.sh, is common to all SESM web applications. If you are running multiple SESM applications on the same server, it might be necessary to modify the SESM start scripts to allocate different amounts of memory to different applications

The amount of memory allocated to the JVM depends on many factors, such as the level of load or throughput to be supported, functions and features supported by the application, the type of resources requested by the client, and content of JSPs. For guidelines on estimating required memory and CPU for the SESM web portal see [Chapter 2, “Before You Begin.”](#)

The use of swap space degrades performance of the application, so you must ensure that only physical memory is used by the JVM. To do so, take into account the memory requirements of the OS and any other applications running on the same platform, and deduct this from the amount of physical memory on the machine before you allocate memory to the JVM.

The Java -Xms option sets the initial size of the Java heap. The -Xmx option sets the maximum size of the Java heap. Both should be set to the same value for optimal performance.

It is important to note that if the JVM is allowed to run out of memory, the results are unpredictable and can be catastrophic. It is therefore essential that you configure the system to prevent this from occurring. The Jetty logs should be monitored for OutOfMemory exceptions. If any instance of this exception is found, you must reconfigure.

## Garbage Collection

The JVM has its own methods of memory management including a process called Garbage Collection. When a Java application releases an object, the memory that object occupied does not become immediately available for re-use. The Garbage Collector is responsible for reclaiming the memory from unused objects

The behavior of the Garbage Collection process can be modified using Java Garbage Collection options at start-up. It is recommended to use the default behavior. However, The Garbage Collection mechanism within Java is continually being improved and new releases of JVM might contain improvements or new Garbage Collection options that will improve performance. Further information on the garbage collector specific to Java 1.4.2 is available on the Sun website for Java developers.

## Java Version

With each release of SESM, the latest mature version of Java—Java Runtime Environment (JRE)—is bundled with the SESM install image. It is recommended that you use this version, even if you must replace the JRE with a Java Development Kit (JDK).

Newer versions of Java often provide improvements in performance and Garbage Collection. Upgrading to later versions of SESM will ensure that you benefit from these improvements. However, if you do not want to upgrade SESM, you can upgrade just the JVM.

Different versions of JVM can be downloaded with installation instructions from the Sun website for Java developers.

## Jetty Web Server

Jetty is the default web server bundled with SESM, developed by Mort Bay Consulting, partners of Core Developers Network.

Some of the more important aspects of Jetty attributes and settings, are detailed here, but further and more detailed information can be found at the Mort Bay Consulting and Core Developers Network websites. For further details on optimizing Jetty, refer to the Jetty Optimization Guide on the Core Developers Network website.

Jetty MBeans are exposed via the SESM Application Manager (AM), which enables both monitoring and modifying the behavior of Jetty during runtime. Monitoring of the behavior is enhanced by Jetty's support of statistics collection, again available via AM.

Collecting statistics can, in some circumstances, affect the performance. Refer to the Statistics section of the Jetty Optimization Guide for details.

### **maxThreads**

This limits the number of threads that can be allocated to connections for HTTP listeners, and effectively limits the number of simultaneous users of the server and consequently memory usage.

The number of simultaneous users depends on the client browsers used and the version of HTTP they are based on. The latest and most commonly used browsers are based on HTTP-1.1 and use persistent connections.

It is important to note that this is the main control limiting the load on the web server and web application, and must be set according to the memory and CPU available.

If OutOfMemory exceptions are occurring, you must either reduce maxThreads or increase the amount of memory allocated to the JVM.

### **minThreads**

This is the minimum number of unused threads to keep within the thread pool, which enables Jetty to respond to a sudden increase in the load with little latency. A HTTP listener is considered to be low on resources when less than minThreads threads are available for allocation to the thread pool.

For optimal performance, a good rule of thumb is to set minThreads to 20% of maxThreads.

### **maxIdleTimeMs**

This is effectively the maximum time a connection will be maintained without receiving requests. When this timer expires, the thread/connection will be released. Consequently, associated resources/memory will also be released, which will then be available for garbage collection.

Reducing the value of `maxIdleTimeMs`, reduces the time during which resources are needlessly in use. But this must be weighed up against the overhead of reestablishing a connection.

The value of this attribute is determined to a large extent by what the average subscriber is expected to do at the web portal, for example, go to the web portal, log in, and activate a service. If you assume that most subscribers would achieve these tasks within one minute, then that is a good value for this attribute.

#### **lowResourcePersistTimeMS**

This is effectively the maximum time a connection will be maintained without receiving requests, when Jetty is low on resources. It is recommended to leave this attribute at its default value.

#### **lowOnResources**

This is a condition or state that Jetty enters when less than `minThreads` are available for allocation to the thread pool on which, `maxIdleTimeMs` is replaced by `lowResourcePersistTimeMS`.

## SESM Memory Management

When a new session is created, it is stored in a cache. To prevent memory filling up with sessions, the cache is managed as follows:

- The cache contains a configurable number of sessions stored in a hard cache. The hard cache will not hold any more sessions than its configured limit. The default size of the hard cache is 2000 sessions.
- When the hard cache is full, older sessions are pushed into a soft cache. Depending on how the garbage collector is implemented, Java memory management can remove sessions from the soft cache, if memory is low.
- Older sessions can be removed from either cache once they have reached the configurable session timeout value. This prevents old sessions remaining in low usage systems, and the data going stale. You can change the session timeout to remove unused sessions quicker or slower, using the `sessionCachePeriod` attribute in the SESM MBean.
- To manage session memory, change the hard cache size using the `sessionCacheSize` attribute in the SESM MBean. 2000 sessions generally fit easily into the default 64 MB of memory.

## SESM Cache Settings

The following attributes are in the SESM MBean, which also provides statistics such as the number of active sessions and active authenticated sessions.

#### **sessionCachePeriod**

This is the maximum period a SESM session will remain idle. Decreasing the value of this attribute means that SESM sessions will be aged out sooner, freeing resources and memory. This must be weighed against the overhead of (re)creating SESM sessions.

As with the value of the Jetty attribute `maxIdleTimeMs`, you should consider the expected average client behavior when determining the value of this attribute.

#### **profileCachePeriod**

This is the maximum period a service profile, obtained from the RADIUS/AAA server, will remain idle. In addition, this is the frequency with which SESM sessions are checked for `sessionCachePeriod`.



# SSG MBEAN Settings

## THROTTLE

This determines the maximum number of outstanding RADIUS access-requests from the SESM web portal to SSG. RADIUS packets are identified by an identification field in the RADIUS packet. When the SESM web portal receives a response from SSG, it uses the identification, in the received RADIUS packet to determine to which request it corresponds.

The identification field is an octet; therefore the maximum value that can be applied to THROTTLE is 255.

The value of this attribute is applied to each SSG socket created by the SESM Web Portal. In the case where client subnets are mapped to SSGs, the maximum number of SSG sockets will be equal to the number of SSGs in the network

When a port-bundle host key is used (hence no client subnet mappings to SSGs), the maximum number of SSG Sockets will be equal to the sum of all source IP addresses in the port map configurations of all the SSGs in the network.

It is important to note that when THROTTLE number of requests are outstanding, if further access-requests are made to the SSG, these requests will be buffered by virtue of the Java thread being placed in the Wait state, until the requests outstanding drops below THROTTLE.

Under heavy load, this buffering can grow significantly, resulting in large delays in communication with SSG. Even when load has reduced or been removed, the buffer might take some time to clear.

The only protection against excessive buffering is again the maxThreads parameter in Jetty.

## RETRIES

This is the number of attempts the SESM web portal will make in sending an access-request to the SSG, if it does not receive a response.



### Note

The name of this attribute is misleading. If RETRIES is set to 1, and no response to an access-request is received, it will not resend the request.

This value is set to 3 by default but it is recommended that you set it to 1. This is because the RADIUS configuration on the gateway device (SSG) would typically be set to resend access-requests to the RADIUS server when it does not receive a response. Therefore, if both SESM and the gateway are configured to resend, a cascade will result.

It is important to note, however, that not every access-request from the SESM web portal to the gateway will result in an access-request from the gateway to the RADIUS server, for example, the SESM web portal sends access-requests to the gateway requesting the status of a particular host. Also, service activation requests from the SESM web portal to the gateway will not result in an access-request from the gateway to the RADIUS server if the gateway already has the service profile cached.

## TIMEOUTSECS

This is the time, in seconds, that the SESM web portal will wait for a response to an access-request sent to the gateway. The value of this attribute must be consistent with the RADIUS configuration on the gateway device. The following example is a section of a RADIUS configuration on a gateway device.

```
radius-server retransmit 3
radius-server timeout 10
```

TIMEOUTSECS must be greater than retransmit \* timeout, which, in this example is 30 seconds.

# SSG MBEAN Statistics

Any bottleneck in communication between the SESM web portal and the gateway will significantly affect overall performance. Such a bottleneck could exist for a number of reasons. Statistics provided in the SSG MBean can help determine the cause of the bottleneck.

**numSent**

This represents the number of access-request RADIUS packets sent by the SESM web application to the SSG.

**numReceived**

This represents the number of access-accept and access-reject RADIUS packets received by the SESM web application. Under perfect conditions, this number should follow numSent.

**numExceptions**

This represents input and output errors when RADIUS packets are sent and received.

**numRetries**

This represents the number of times a response to an access-request was not received within the period defined by TIMEOUTSECS. If this number is high compared to numSent, it might be an indication that either the SSG or the RADIUS server is not able to handle the load, or is slow in responding.

Try increasing the value of TIMEOUTSECS. If this does not solve the problem, you must investigate further and determine whether the SSG routers or RADIUS server are under too much load.

**numDiscarded**

This represents the number of RADIUS packets discarded because they arrived after the period defined by TIMEOUTSECS. If this number is high, try increasing the value of TIMEOUTSECS.

**numInvalid**

This represents the number of invalid RADIUS packets received because of an invalid authentication field or invalid packet length.

**numCollisions**

This represents the number of times the SESM web application tried to send an access-request to the SSG, but was not able to because the number of requests pending was equal to the value defined by THROTTLE.

If the value of numCollisions is high, try increasing the value of THROTTLE, to a maximum of 255. However, increasing the value of THROTTLE will increase the load on the SSG routers and on the RADIUS server, which could result in the number of numRetries and/or numDiscarded going up.

# SESM Logging

SESM web applications and the Jetty web server produce logging information that is sent to log files on disk. This can have a significant affect on performance.

Write access to disk is slow compared to CPU speed. If logging information is being generated faster than it can be written to disk, the logging information itself uses up memory. This can also result in Java threads entering a Wait state because of the Thread Safe implementation of logging.

It is recommended that in production, you do not set the logging levels higher than the default settings. Reducing the level of logging for both Jetty and the web application, can improve performance.





## Example SESM RADIUS Installation

---

This appendix provides an example of how to install and configure a SESM RADIUS installation. This appendix contains the following sections:

- [Introduction, page A-1](#)
- [Assumptions, page A-2](#)
- [Setting Up a SESM RADIUS Installation, page A-2](#)
- [What to Do Next, page A-6](#)



### Note

---

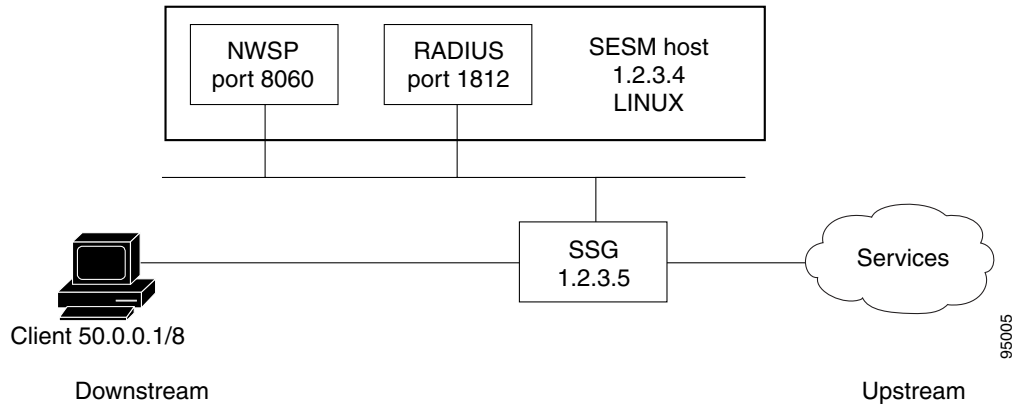
Before you install and set up SESM, you must perform the tasks described in [Chapter 2, “Before You Begin.”](#)

---

## Introduction

This quick start example describes how to run the SESM RADIUS installation on a Linux platform. It takes the you to a point where you can login and configure the services provided by SESM. You can then perform basic authentication for subscribers and service activation. The SESM RADIUS installation supports the following features in the New World Service Provider portal (NWSP):

- Dynamic bandwidth selection
- Dynamic service activation
- Session status
- Changing language settings for messages

**Figure A-1 Block Diagram for RADIUS Example**

This example uses the GUI version of the installer running on a Linux platform to access the SESM installation options. For the purposes of this example, the Port-Bundle Host Key feature is enabled.

## Assumptions

The instructions in this chapter assume the following:

- You have performed the tasks described in [Chapter 2, “Before You Begin.”](#)
- You are using the SESM Bundled RADIUS server as the RADIUS server for this quick start solution.
- You are installing all SESM components on the same system.
- You are not installing the SESM Captive Portal solution.

## Setting Up a SESM RADIUS Installation

### Step 1: Installing a SESM RADIUS Installation

To install a SESM RADIUS installation, proceed as follows:

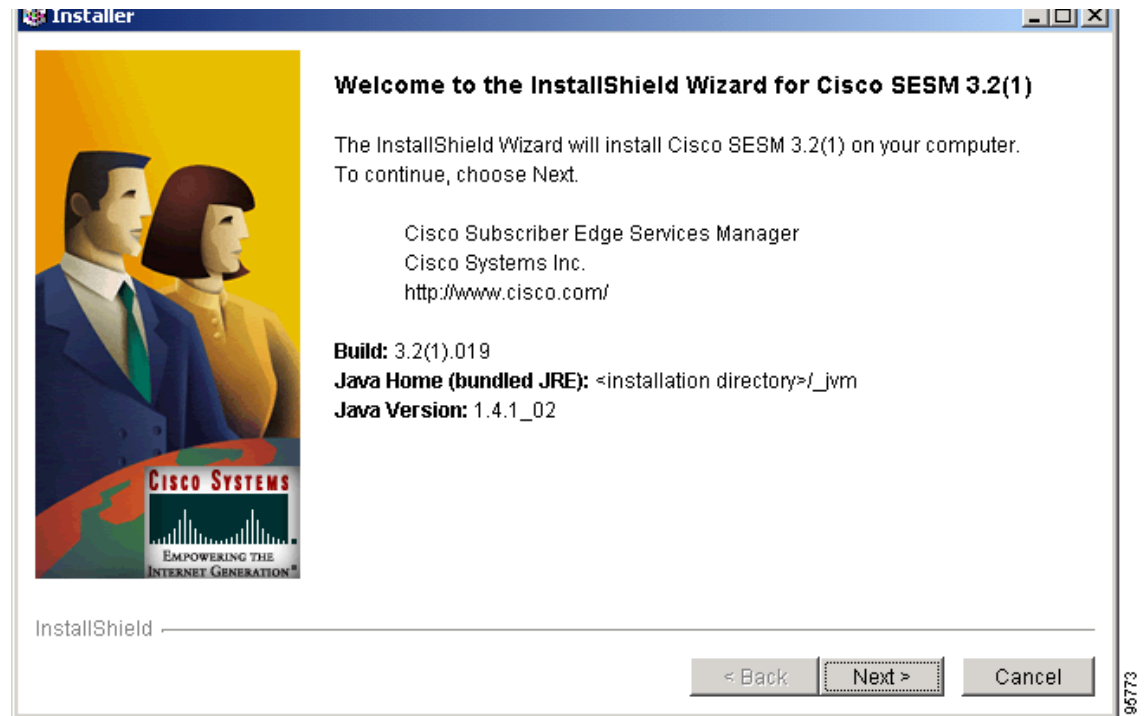
**Step 1** At the command line, change directory into the location of the SESM image.

**Step 2** Run the InstallShield Wizard by entering the following at the command line:

```
sesm_sol.bin
```

The InstallShield Wizard is now displayed.

Figure A-2 The InstallShield Wizard Screen



- Step 3** Within the InstallShield Wizard, step through the screens using the **Next** button and selecting the settings provided in [Table A-1](#) to perform the installation.

**Note**

This installation does not install the Captive Portal solution.  
This installation installs RDP in default (not Proxy) mode.  
This installation assumes that you are installing all SESM components on the same system.

**Table A-1** Installing a SESM RADIUS Installation

| InstallShield Wizard Screen                                                                                                                                                                                                                                | Field                                | Value                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General installation parameters                                                                                                                                                                                                                            | Installation type and license number | <b>Evaluation - RADIUS mode</b>                                                                                                                                                                                                                                                                                    |
|                                                                                                                                                                                                                                                            | License agreement                    | <b>Agree</b>                                                                                                                                                                                                                                                                                                       |
|                                                                                                                                                                                                                                                            | Installation directory               | <p><b>Note</b> You must have write privileges to the installation directory.</p> <p>Accept the displayed default installation directory, click <b>Browse</b> to find a location, or type the directory name in the box.</p> <p>The default installation directory for Solaris is:</p> <p>/opt/cisco/sesm_x.x.x</p> |
|                                                                                                                                                                                                                                                            | Setup Type                           | <b>Typical</b>                                                                                                                                                                                                                                                                                                     |
| Configuration and Deployment                                                                                                                                                                                                                               | Web Application Host                 | Accept the default.                                                                                                                                                                                                                                                                                                |
|                                                                                                                                                                                                                                                            | Web Application Port Number          | Accept the default.                                                                                                                                                                                                                                                                                                |
|                                                                                                                                                                                                                                                            | SSG Deployment Option                | Accept the default.                                                                                                                                                                                                                                                                                                |
| SSG details                                                                                                                                                                                                                                                | SSG port number                      | 1812                                                                                                                                                                                                                                                                                                               |
|                                                                                                                                                                                                                                                            | SSG shared secret                    | cisco                                                                                                                                                                                                                                                                                                              |
|                                                                                                                                                                                                                                                            | SSG port bundle size                 | 4                                                                                                                                                                                                                                                                                                                  |
| If the SSG port bundle length is 0, you must provide the following information.                                                                                                                                                                            |                                      |                                                                                                                                                                                                                                                                                                                    |
| AAA Server Details                                                                                                                                                                                                                                         | Primary IP                           | 1.2.3.4                                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                            | Primary Port                         | 1812                                                                                                                                                                                                                                                                                                               |
|                                                                                                                                                                                                                                                            | Secondary IP                         | 1.2.3.4                                                                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                                                                                            | Secondary Port                       | 1812                                                                                                                                                                                                                                                                                                               |
|                                                                                                                                                                                                                                                            | Shared Secret                        | cisco                                                                                                                                                                                                                                                                                                              |
| Service and Group Passwords                                                                                                                                                                                                                                | Service Password                     | servicecisco                                                                                                                                                                                                                                                                                                       |
|                                                                                                                                                                                                                                                            | Service Group Password               | groupcisco                                                                                                                                                                                                                                                                                                         |
| Application Management Port                                                                                                                                                                                                                                | Application Management Port          | Accept the default.                                                                                                                                                                                                                                                                                                |
| The installation program installs the components on your system. When it is finished installing the files, and if it has successfully connected to your LDAP directory, it displays the following additional prompts about modifications to the directory. |                                      |                                                                                                                                                                                                                                                                                                                    |



## Step 2: Running SESM Components

To run SESM components under Linux as used in this example, use the commands listed in [Table A-2](#).

**Table A-2** Running SESM components

| For this task                     | Enter this command                                       | Details                                |
|-----------------------------------|----------------------------------------------------------|----------------------------------------|
| Start main portal                 | <code>installDir/jetty/bin/startNWSP.sh &amp;</code>     | Starts NWSP Web Portal.                |
| Start SESM Bundled RADIUS server. | <code>installDir/tools/bin/startAAA.sh 1812 &amp;</code> | Starts the SESM Bundled RADIUS Server. |

## Step 3: Logging On to a Web Portal

To access SESM web portals, follow these procedures:



### Note

This example uses the NWSP Web Portal.



### Note

Note that you will be logging on from a client on the downlink interface on the SSG; That is, a client on the 50.0.0.0/8 network (the client subnet defined in [Step 1: Installing a SESM RADIUS Installation, page A-2](#)).

**Step 1** Start a web browser.

**Step 2** Make sure the web browser has JavaScript enabled.

**Step 3** Go to the URL of the SESM portal application:

```
http://host:port
```

The URL is the host and port number that you specified during the SESM installation process. Default values used during SESM installation are:

```
http://localhost:8080
```

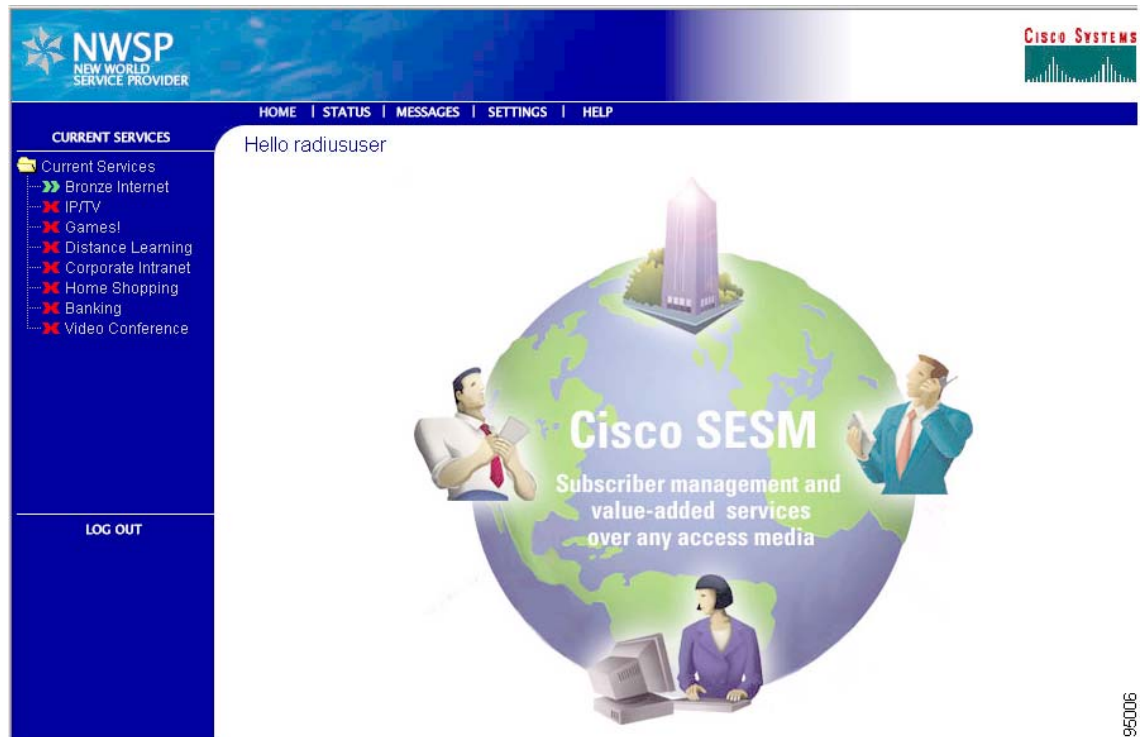
**Step 4** When the SESM portal application's logon page appears, log in using a valid subscriber ID and password as defined in the sample data.

For example:

```
Subscriber IDs: radiususer
Password: cisco
```

The NWSP home page appears as shown in [Figure A-3](#).

Figure A-3 NWSP Home Page



The service selection list (the column on the left side of the window) shows the subscribed services for the logged-on user. The icons in the list have the following meanings:

- Green arrow—Connected service. In the *radiususer* and *golduser* profiles, the Internet service is marked as an automatically connected service; hence the green arrow icon indicating connection immediately after signing on.
- Red X—Unconnected service.

## What to Do Next

### Finding Further Information

For further information about this product, please refer to [Related Documentation](#), page xi.

### Troubleshooting

For information about troubleshooting, refer to the *Cisco Subscriber Edge Services Manager Troubleshooting Guide*.



## Example SESM SPE Installation

---

This appendix provides an example of how to install and configure a SESM SPE installation. This appendix contains the following sections:

- [Introduction, page B-1](#)
- [Assumptions, page B-2](#)
- [Setting Up a SESM SPE Installation, page B-3](#)
- [What to Do Next, page B-9](#)



### Note

---

Before you install and set up SESM, you must perform the tasks described in [Chapter 2, “Before You Begin.”](#)

---

## Introduction

This quick start example describes how to install a SESM SPE installation on a Solaris platform.

The end result will be that the SESM applications will be installed and configured to obtain user and service profiles from an LDAP directory.

You will then be able to login to the Cisco Distributed Administration Tool (CDAT) as an administrator to create users and services. A subscriber will be able to perform basic authentication and service activation using the SESM web portal. The SESM SPE installation supports the following features in the New World Subscriber Portal (NWSP):

- Service subscription\*
- Account self-care\*
- Subaccount creation\*
- Self-registration\*
- Personal firewalls\*
- Dynamic bandwidth selection
- Dynamic service activation
- Session status
- Changing language settings for messages

\*SESM SPE installation only

The diagram illustrates a Solaris-based SSG 1.2.3.5 setup. At the top, a large box represents the Solaris host, containing four sub-components: NWSP port 8080, LDAP (NDS) port 389, RDP port 1812, and SESM host 1.2.3.4 SOLARIS. Below this box is a horizontal line representing a network backbone. A vertical line connects the backbone to the SSG 1.2.3.5 box. To the left of the SSG box is a computer icon representing the Client 50.0.0.1/8. To the right of the SSG box is a cloud icon representing Services. The SSG box is labeled 'SSG 1.2.3.5'. The Client is labeled 'Client 50.0.0.1/8'. The Services cloud is labeled 'Services'. The diagram is labeled 'Downstream' on the left and 'Upstream' on the right.

## Assumptions

- You have performed the tasks described in [Chapter 2, “Before You Begin.”](#)
- You are installing all SESM components on the same system.
- You are not installing the SESM Captive Portal solution.
- You have already installed the LDAP directory. This document contains specific instructions for installing an LDAP directory for a SESM solution.

# Setting Up a SESM SPE Installation

## Step 1: Installing a SESM SPE Installation

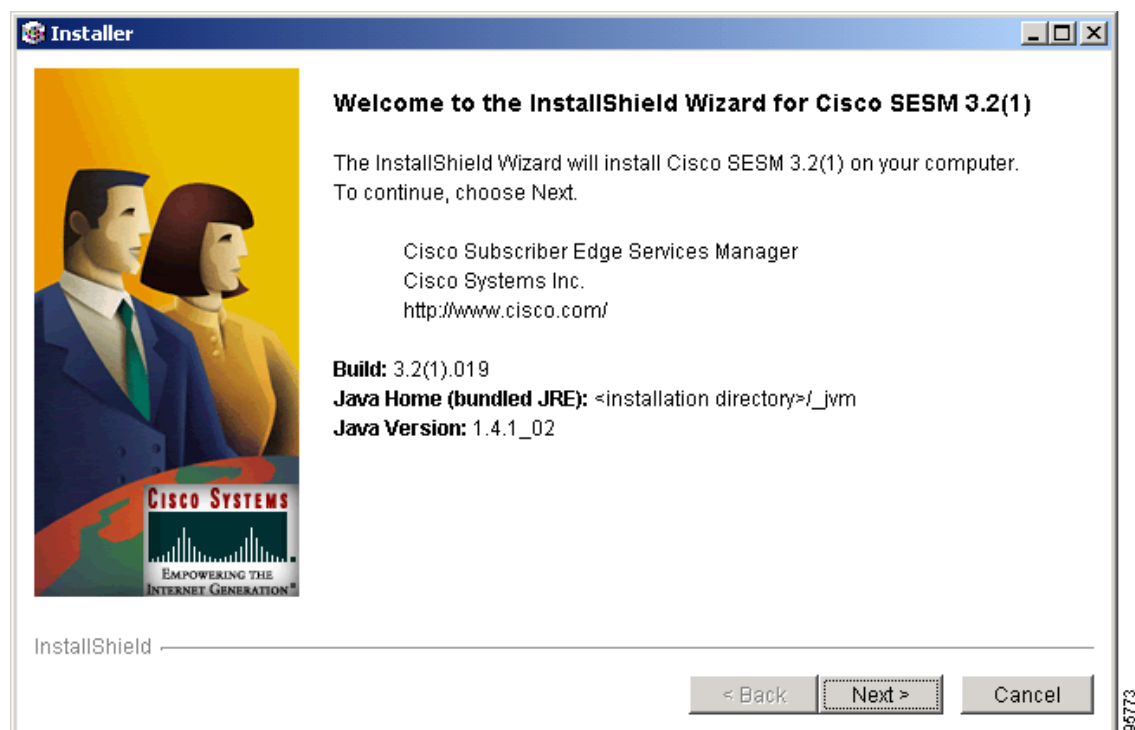
To install a SESM SPE installation, proceed as follows:

- Step 1** At the command line, change directory into the location of the SESM image.
- Step 2** Run the InstallShield Wizard by entering the following at the command line:

```
sesm_sol.bin
```

The InstallShield Wizard is now displayed.

**Figure B-2** The InstallShield Wizard Screen



- Step 3** Within the InstallShield Wizard, step through the screens using the **Next** button and selecting the settings provided in [Table 5-1](#) to perform the installation.



**Note**

This installation does not install the Captive Portal solution.  
This installation installs RDP in default (not Proxy) mode.  
This installation assumes that you are installing all SESM components on the same system.

**Table B-1** Installing a SESM SPE Installation

| InstallShield Wizard Screen                                                     | Field                                | Value                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General installation parameters                                                 | Installation type and license number | <b>Evaluation - SPE mode</b>                                                                                                                                                                                                                                                                                       |
|                                                                                 | License agreement                    | <b>Agree</b>                                                                                                                                                                                                                                                                                                       |
|                                                                                 | Installation directory               | <p><b>Note</b> You must have write privileges to the installation directory.</p> <p>Accept the displayed default installation directory, click <b>Browse</b> to find a location, or type the directory name in the box.</p> <p>The default installation directory for Solaris is:</p> <p>/opt/cisco/sesm_x.x.x</p> |
|                                                                                 | Setup Type                           | <b>Typical</b>                                                                                                                                                                                                                                                                                                     |
| Configuration and Deployment                                                    | Web Application Host                 | Accept the default.                                                                                                                                                                                                                                                                                                |
|                                                                                 | Web Application Port Number          | Accept the default.                                                                                                                                                                                                                                                                                                |
|                                                                                 | SSG Deployment Option                | Accept the default.                                                                                                                                                                                                                                                                                                |
| SSG details                                                                     | SSG port number                      | 1812                                                                                                                                                                                                                                                                                                               |
|                                                                                 | SSG shared secret                    | cisco                                                                                                                                                                                                                                                                                                              |
|                                                                                 | SSG port bundle size                 | 0                                                                                                                                                                                                                                                                                                                  |
| If the SSG port bundle length is 0, you must provide the following information. |                                      |                                                                                                                                                                                                                                                                                                                    |
| One non-host key SSG                                                            | SSG address                          | 1.2.3.5                                                                                                                                                                                                                                                                                                            |
|                                                                                 | Client subnet                        | 50.0.0.0                                                                                                                                                                                                                                                                                                           |
|                                                                                 | Subnet mask                          | 255.0.0.0                                                                                                                                                                                                                                                                                                          |
| Data Store Type Selection                                                       | Data Store Type                      | Directory Server                                                                                                                                                                                                                                                                                                   |
|                                                                                 | Vendor Name                          | Novell Directory Server                                                                                                                                                                                                                                                                                            |
| Password Encryption Panel                                                       | SPE Installation type                | Fresh SPE installation                                                                                                                                                                                                                                                                                             |
|                                                                                 | Master Password                      | cisco                                                                                                                                                                                                                                                                                                              |
|                                                                                 | Master Password (Repeat)             | cisco                                                                                                                                                                                                                                                                                                              |
|                                                                                 | Password Encryption Algorithm        | NONE                                                                                                                                                                                                                                                                                                               |
| Select the naming attribute                                                     | inetOrgPerson                        | cn                                                                                                                                                                                                                                                                                                                 |

**Table B-1** *Installing a SESM SPE Installation (continued)*

| InstallShield Wizard Screen                                                                                                                                                                                                                                                                                                                   | Field                       | Value                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------------------|
| Directory server information                                                                                                                                                                                                                                                                                                                  | Directory address           | 1.2.3.4                  |
|                                                                                                                                                                                                                                                                                                                                               | Directory port              | 389                      |
|                                                                                                                                                                                                                                                                                                                                               | Directory admin user        | cn=admin,ou=sesm,o=cisco |
|                                                                                                                                                                                                                                                                                                                                               | Directory admin password    | admin                    |
|                                                                                                                                                                                                                                                                                                                                               | Directory Container         | ou=sesm,o=cisco          |
|                                                                                                                                                                                                                                                                                                                                               | DESS Admin User             | cn=admin,ou=sesm,o=cisco |
|                                                                                                                                                                                                                                                                                                                                               | DESS Admin Password         | admin                    |
| <b>Note</b> The installation program attempts to access the directory server, using the information you provided. If the attempt is unsuccessful, the installation program displays a window with the header “Warning—Please confirm these options.” Verify the information you entered and also verify that the directory server is running. |                             |                          |
| Enter container information                                                                                                                                                                                                                                                                                                                   | Directory address           | 127.0.0.1                |
|                                                                                                                                                                                                                                                                                                                                               | Directory port              | 389                      |
|                                                                                                                                                                                                                                                                                                                                               | Directory container         | ou=sesm,o=cisco          |
|                                                                                                                                                                                                                                                                                                                                               | Directory user ID           | cn=admin,ou=sesm,o=cisco |
|                                                                                                                                                                                                                                                                                                                                               | Directory password          | admin                    |
| Naming attribute                                                                                                                                                                                                                                                                                                                              | InetorgPerson               | CN (for NDS)             |
| <b>Note</b> The installation program attempts to access the container using the information you provided. If the attempt is unsuccessful, a warning message appears.                                                                                                                                                                          |                             |                          |
| RDP<br>Configures RDP to SSG communication                                                                                                                                                                                                                                                                                                    | RDP host                    | Accept the default.      |
|                                                                                                                                                                                                                                                                                                                                               | Port number                 | Accept the default.      |
|                                                                                                                                                                                                                                                                                                                                               | Shared secret               | Accept the default.      |
|                                                                                                                                                                                                                                                                                                                                               | Service password            | Accept the default.      |
|                                                                                                                                                                                                                                                                                                                                               | Group password              | Accept the default.      |
|                                                                                                                                                                                                                                                                                                                                               | Next hop password           | Accept the default.      |
| RDP Options                                                                                                                                                                                                                                                                                                                                   | Proxy mode                  | Unchecked.               |
|                                                                                                                                                                                                                                                                                                                                               | Add services                | Checked.                 |
|                                                                                                                                                                                                                                                                                                                                               | Add client                  | Unchecked.               |
| CDAT Web Server Configuration                                                                                                                                                                                                                                                                                                                 | CDAT Host                   | Accept the default.      |
|                                                                                                                                                                                                                                                                                                                                               | CDAT Port Number            | Accept the default.      |
| CDAT Web Server Configuration                                                                                                                                                                                                                                                                                                                 | Application Management Port | Accept the default.      |

**Table B-1** Installing a SESM SPE Installation (continued)

| InstallShield Wizard Screen                                                                                                                                                                                                                            | Field         | Value                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------------------------------------------------------------------|
| The installation program installs the components on your system. When it is finished installing the files, and if it successfully connected to your LDAP directory, it displays the following additional prompts about modifications to the directory. |               |                                                                         |
| LDAP directory modifications                                                                                                                                                                                                                           | Extend schema | Click in the check box. Extending the schema is a required step.        |
|                                                                                                                                                                                                                                                        | Install RBAC  | Click in the check box. Installing the RBAC objects is a required step. |

## Step 2: Installing CDAT Sample Data

This section explains how to import the sample data that is provided with the SESM applications. After doing so, you will be able to edit them in CDAT and log in using the NWSP.

To create users and services in CDAT, proceed as follows:

**Step 1** Change directory to:

```
<SESM>/dess-auth/schema/samples
```

**Step 2** At the command line, enter the following:

```
ldapmodify -h IP-address -p port -c -v -D binddn -w passwd -f file
```

where:

- h *IP-address* sets the IP address, for example *127.0.0.1*
- p *port* sets the port on the LDAP server, for example *389*
- c sets continuous operation mode (do not stop on errors)
- v sets run in verbose mode (diagnostics to standard output)
- D *binddn* binds DN, for example *"cn=admin,ou=sesm,o=cisco"*
- w *passwd* binds passwd (for simple authentication), for example *cisco*
- f *file* sets read operations from file *DESSusecasedata.ldf*

**Step 3** The ldapmodify tool will display the output of the command in the terminal window.

**Step 4** On completion of this process, you can use CDAT to look at these objects in the directory, and login as these users to the NWSP.



## Step 3: Starting CDAT and Accessing the CDAT Home Page

This section explains how to start CDAT and access the CDAT home page.

**Note**

Before using CDAT, make sure that cookies are enabled in your browser.

To start CDAT and access the CDAT home page, do the following:

- 
- Step 1** Start CDAT by executing the CDAT startup script.
- For UNIX-based installations, the startup script is `/install_dir/jetty/bin/startCDAT.sh`
  - For Windows-based installations, the startup script is `\install_dir\jetty\bin\startCDAT.cmd`
- Step 2** Open a web browser.
- Step 3** Browse to the CDAT URL, which is:

**`http://host:port`**

For example:

**`http://localhost:8081`**

Port 8081 is the port that is configured, by default, for CDAT. The port number that you specify may be different. This port number is specified in the CDAT startup script (`startCDAT.sh` or `startCDAT.cmd`).

---

## Step 4: Logging In to CDAT

To log in to CDAT for the first time in order to manage an LDAP directory, use the *admin* user name and the password of the directory administrator for the organization and organizational unit where SESM is located. These are the username and password that were specified when the directory was installed.

**Note**

During the directory installation and the CDAT installation, the directory administrator must be specified as the *admin* user ID.

To use the *admin* user name as the first-time CDAT administrator, you must do the following when installing the directory server and the CDAT software:

1. When you install the directory server, set up an *admin* user with the needed permissions to access and create objects in the directory container (organization unit and organization) where the SPE schema extensions and initial RBAC objects will be installed.
2. When you install the CDAT software, select **Install RBAC** to install the initial RBAC objects. When you select **Install RBAC**, the CDAT installation software *expects to find* an admin user ID so that it can grant that user the needed administrator privileges.

Once you are logged into CDAT, you should be able to view, modify, or delete the CDAT sample data.

---

## Step 5: Running SESM Components

To run SESM components under Solaris as used in this example, use the commands listed in [Table B-2](#).

**Table B-2** Running SESM components

| For this task     | Enter this command                                   | Details                        |
|-------------------|------------------------------------------------------|--------------------------------|
| Start main portal | <code>installDir/jetty/bin/startNWSP.sh &amp;</code> | Starts NWSP Web Portal.        |
| Start CDAT        | <code>installDir/jetty/bin/startCDAT.sh &amp;</code> | Starts CDAT directory manager. |
| Run RDP           | <code>installDir/rdp/bin/runrdp.sh &amp;</code>      | Starts RDP process.            |

## Step 6: Logging On to a Web Portal

To access SESM web portals, follow these procedures:



### Note

This example uses the NWSP Web Portal.



### Note

Note that you will be logging on from a client on the downlink interface on the SSG. That is, a client on the 50.0.0.0/8 network (The client subnet defined in [Step 1: Installing a SESM SPE Installation, page B-3](#)).

**Step 1** Start a web browser.

**Step 2** Make sure the web browser has JavaScript enabled.

**Step 3** Go to the URL of the SESM portal application:

```
http://host:port
```

The URL is the host and port number that you specified during the SESM installation process. Default values used during SESM installation are:

```
http://localhost:8080
```

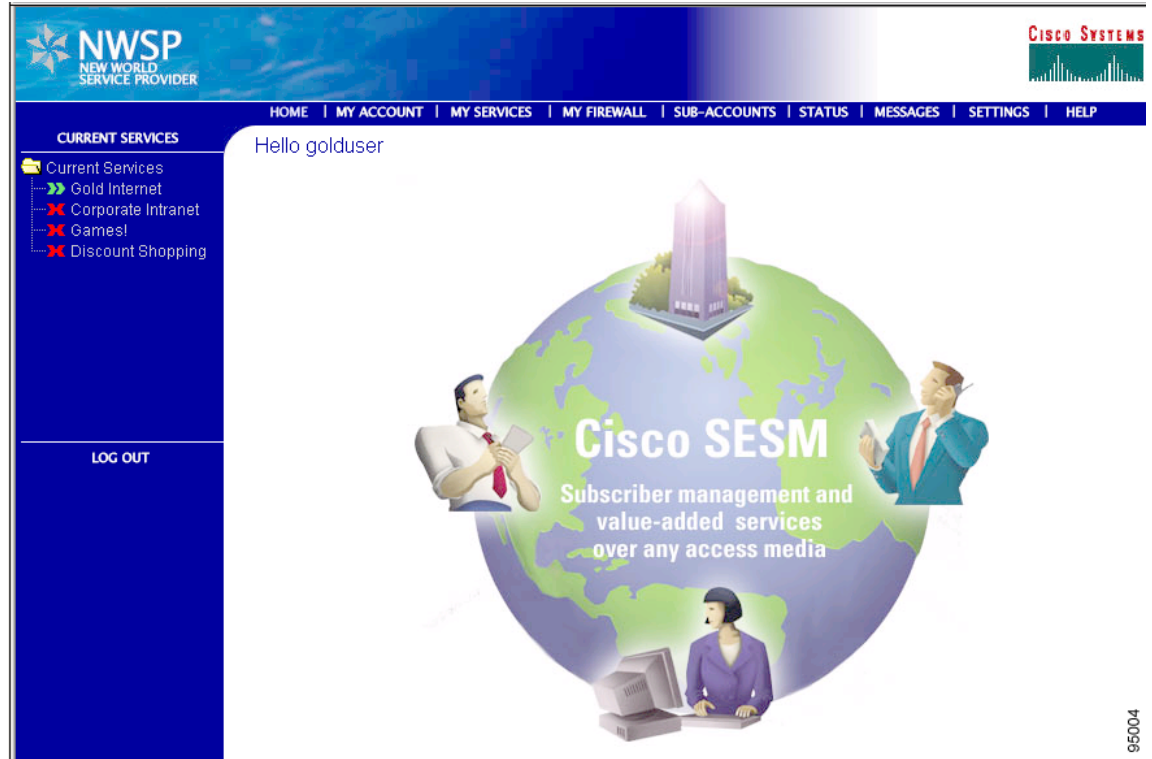
**Step 4** When the SESM portal application's logon page appears, log in using a valid subscriber ID and password defined in the LDAP directory.

For example:

```
Subscriber IDs: golduser, silveruser or bronzeuser
Password: cisco
```

The NWSP home page appears as shown in [Figure B-3](#).

Figure B-3 NWSP Home Page



The service selection list (the column on the left side of the window) shows the subscribed services for the logged-on user. The icons in the list have the following meanings:

- Green arrow—Connected service.
- Red X—Unconnected service.

## What to Do Next

### Finding Further Information

For further information about SESM, see [Related Documentation](#), page xi.

### Troubleshooting

For information on troubleshooting, refer to the *Cisco Subscriber Edge Services Manager Troubleshooting Guide*.





## Configuration File Changes in SESM 3.3(1)

---

This appendix describes the changes in configuration files in SESM 3.3(1). If you migrate configuration files from SESM 3.2(2), you will need to make additional changes to replace configuration clauses that were added and modified in the SESM 3.3(1) configuration files.

The additions and modifications in configuration files are for:

- New features
- Enhancements to existing features
- Bug fixes

The topics in this appendix describe the new and modified configuration sections in the following SESM 3.3(1) configuration files, and other changes:

- [nwsp.xml file, page C-2](#)
- [rdp.xml file, page C-6](#)
- [webproxy.xml, page C-8](#)
- [captiveportal.xml, page C-10](#)
- [wsg.xml, page C-12](#)
- [nwsp.web-jetty.xml, page C-13](#)
- [webproxy.web-jetty.xml, page C-14](#)
- [captive.web-jetty.xml, page C-14](#)
- [Additional Changes, page C-15](#)

# nwsp.xml file

Full path: <install directory>/nwsp/config

Table C-1 shows new sections that have been added to nwsp.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-1 Changes in nwsp.xml**

| MBean                                                                                                    | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Replaces in SESM 3.2(2) |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment this clause to instantiate the file poller   &lt;Instantiate order="10"     Class="com.cisco.sesm.jmx.FilePollerMBean"     jmxname="com.cisco.sesm.jmx:name=FilePoller" /&gt; --&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                             | —                       |
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment and modify this clause to configure the file poller   &lt;Configure jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;     &lt;Set name="pollingInterval" type="int"&gt;3600&lt;/Set&gt;     &lt;Set name="polledFiles"&gt;       &lt;Array class="java.lang.String"&gt;         &lt;Item&gt;configurationfile1.xml&lt;/Item&gt;       &lt;Item&gt;configurationfile2.xml&lt;/Item&gt;       &lt;/Array&gt;     &lt;/Set&gt;   &lt;/Configure&gt;   &lt;Action jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;     &lt;Call name="forcePollingNow" /&gt;   &lt;/Action&gt; --&gt;</pre> | —                       |
| SSG MBean<br>Enhancement to enable changing send and receive buffer sizes, RX_BUF_SIZE/ TX_BUF_SIZE      | <pre>&lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;RX_BUF_SIZE&lt;/Arg&gt;&lt;Arg&gt;3 2767&lt;/Arg&gt; &lt;/Call&gt; &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;TX_BUF_SIZE&lt;/Arg&gt;&lt;Arg&gt;3 2767&lt;/Arg&gt; &lt;/Call&gt;</pre>                                                                                                                                                                                                                                                                                                                                                            | —                       |
| SSG MBean<br>Enhancement to configure time to wait for a RADIUS ID                                       | <pre>&lt;!-- - The time in milliseconds to wait for a RADIUS ID to become available --&gt; &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;ID_TIMEOUT&lt;/Arg&gt;&lt;Arg&gt;50 0&lt;/Arg&gt;&lt;/Call&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                              | —                       |
| SSG MBean                                                                                                | Installed default value for the throttle attribute has been increased to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | —                       |

**Table C-1** Changes in nwsp.xml (continued)

| MBean                                                | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Replaces in SESM 3.2(2)                                                                                                                                                                                                                     |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSGIPPolicy                                          | <pre> &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;TIMEOUTSECS&lt;/Arg&gt;&lt;Arg&gt;6 &lt;/Arg&gt;&lt;/Call&gt;   &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;RETRIES&lt;/Arg&gt;&lt;Arg&gt;2&lt;/Ar g&gt;&lt;/Call&gt;   &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;RX_BUF_SIZE&lt;/Arg&gt;&lt;Arg&gt;3 2767&lt;/Arg&gt;&lt;/Call&gt;   &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;TX_BUF_SIZE&lt;/Arg&gt;&lt;Arg&gt;3 2767&lt;/Arg&gt;&lt;/Call&gt; </pre> | <pre> &lt;Call name="setGlobalAttribute"&gt;&lt; Arg&gt;TIMEOUTSECS&lt;/Arg&gt;&lt;Arg&gt;1 0&lt;/Arg&gt;&lt;/Call&gt;   &lt;Call name="setGlobalAttribute"&gt;&lt; Arg&gt;RETRIES&lt;/Arg&gt;&lt;Arg&gt;3&lt;/Ar g&gt;&lt;/Call&gt; </pre> |
| Location MBean<br>(SSG requirements have<br>changed) | - This requires SSG 12.2(16)B or 12.3(4)T<br>onwards.                                                                                                                                                                                                                                                                                                                                                                                                                              | - This is not<br>available with the SSG in<br>12.2(13)T or 12.2(4)B6.                                                                                                                                                                       |

Table C-1 Changes in nwsp.xml (continued)

| MBean                                                                                                                                                         | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Replaces in SESM 3.2(2) |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <p>IPASS MBean</p> <p>New MBean for the iPass support</p>                                                                                                     | <pre> &lt;!-- Instantiate IPASS MBean ===== ----- --&gt; &lt;Instantiate order="35" class="com.cisco.sesm.ipass.IpassMBean" jmxname="com.cisco.sesm:name=ipass"/&gt;  &lt;Configure jmxname="com.cisco.sesm:name=ipass"&gt;  &lt;!-- - This defines the URLs to be used for redirection for IPASS login and logoff operations - The login URL must be for inside the default network or an - open garden, otherwise the gateway will repeatedly redirect - the request to NWSP, causing a loop condition. - The loginURL must be a secure URL. Be sure to add a listener for the secure login port - in the nwsp.jetty.xml file. --&gt; &lt;Set name="ipassAddLocationToUserName" type="boolean"&gt;true&lt;/Set&gt; &lt;Set name="ipassDefaultLocationName"&gt;Undefined&lt;/Set&gt; &lt;Set name="ipassDefaultLocationID"&gt;N/A&lt;/Set&gt; &lt;Set name="ipassLogonURL"&gt;https://localhost:443/ipass/logon &lt;/Set&gt; &lt;Set name="ipassLogoffURL"&gt;http://127.0.0.1:80/ipass/logoff &lt;/Set&gt; &lt;Set name="ipassUseSESMLocation" type="boolean"&gt;true&lt;/Set&gt; &lt;!-- This value allows RDP and RADIUS handlers to recognize location info attached to user-name principal Please do not change this value untill you definitely need to do so. If this value is changed, location separator in RDP or RADIUS configuration have to changed accordingly as well --&gt; &lt;Set name="ipassLocationSeparator"&gt;###&lt;/Set&gt; &lt;/Configure&gt; </pre> | —                       |
| <p>SESM MBean</p> <p>New attributes for iPass support</p> <p>These attributes should be in all instances of the SESM MBean, but are relevant only in NWSP</p> | <pre> &lt;Set name="ipassOn" type="boolean"&gt;&gt;false&lt;/Set&gt; &lt;!-- ipassProxyIdentity value allows NWSP to recognize transient users and to disallow selfcare for them --&gt; &lt;Set name="ipassProxyIdentity"&gt;IPASS/*.*&lt;/Set&gt; </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —                       |



Table C-1 Changes in nwsp.xml (continued)

| MBean                                                                  | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Replaces in SESM 3.2(2) |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| SESM MBean<br>New attribute for new session management mechanism       | <pre>&lt;!-- - This is the maximum number of sessions that are held in hard - cache. This is cache that isn't cleared by the garbage collector, - only by the timeout mechanism. Once the hard cache is full, - sessions are moved to the soft cache. From there, they can be - removed by the garbage collector when it needs to free up memory. --&gt; &lt;Set name="sessionCacheSize" type="int"&gt;2000&lt;/Set&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                       | —                       |
| SESM MBean<br>Other enhancements for new session management mechanism  | <ul style="list-style-type: none"> <li>• profileCachePeriod has been reduced to 30 seconds.</li> <li>• sessionCachePeriod has been reduced to 2 minutes.</li> <li>• memRequired has been removed from the config. This property is deprecated. It is in the MBean but it doesn't do anything now.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | —                       |
| WebApp MBean<br>New for the Attribute 18 Reply Message Display feature | <pre>&lt;Set&gt; enableReplyMessageDisplay name="enableReplyMessageDisplay" type="boolean"&gt;true&lt;/Set&gt;  &lt;!-- Uncomment and modify this clause to set a delimiter for the reply - message. The delimiter should comply with the pattern of java regular - expression (java.util.regex.Pattern). If the delimiter is valid, it - would split the reply messages into sub strings, so each sub string - is displayed as a separate message in the web portal. - e.g. if we have one message: "This is msg1 ### This is msg2" and the - delimiter is: "###" the web portal would display it as two different - messages: "This is msg1 ", " This is msg2". - The delimiter was added as a workaround to the reply message - concatenation problem in SSG. &lt;Set name="replyMessageDelimiter" type="String"&gt;###&lt;/Set&gt; --&gt;</pre> | —                       |
| WebApp MBean<br>New attribute for trusted ID authorization             | <pre>&lt;!-- Enable the display of the Always On Self-Care flag for the trusted id authorization. --&gt; &lt;Set name="showAllowAlwaysOn" type="boolean"&gt;&gt;false&lt;/Set&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | —                       |

# rdp.xml file

Full path: <install directory>/rdp/config

Table C-2 shows new sections that have been added to rdp.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-2 Changes in rdp.xml**

| MBean                                                                                                    | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Replaces in SESM 3.2(2)                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment this clause to instantiate the file poller   &lt;Instantiate order="10"     Class="com.cisco.sesm.jmx.FilePollerMBean"     jmxname="com.cisco.sesm.jmx:name=FilePoller"/&gt; --&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                           | —                                                                                                                                                                                                                                                                                                                                                      |
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment and modify this clause to configure the file poller   &lt;Configure     jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;     &lt;Set name="pollingInterval"       type="int"&gt;3600&lt;/Set&gt;     &lt;Set name="polledFiles"&gt;       &lt;Array class="java.lang.String"&gt;         &lt;Item&gt;configurationfile1.xml&lt;/Item&gt;       &lt;Item&gt;configurationfile2.xml&lt;/Item&gt;       &lt;/Array&gt;     &lt;/Set&gt;   &lt;/Configure&gt;   &lt;Action     jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;     &lt;Call name="forcePollingNow"/&gt;   &lt;/Action&gt; --&gt;</pre> | —                                                                                                                                                                                                                                                                                                                                                      |
| RDP Handler<br>Enhanced for iPass support                                                                | <pre>&lt;!-- Set the name of the AAA request handler To handle iPass requests, change this to IPASS --&gt; &lt;Set name="aaaHandler"&gt;AAA&lt;/Set&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <pre>&lt;!-- Set the name of the AAA request handler --&gt; &lt;Set name="aaaHandler"&gt;AAA&lt;/Set&gt;</pre>                                                                                                                                                                                                                                         |
| Accounting Listener in the ERP MBean that has the jmxname RDP<br>Enhanced to handle iPass requests       | <pre>&lt;!-- +++++ +++++ --&gt; &lt;!-- Set the accounting request handler. This can be set to: AAA - handle the request locally by logging. PROXY - proxy the request to another server. DOMAINPROXY - proxy the request to another server selected by domain name. IPASS - Handle iPass requests --&gt; &lt;!-- +++++ +++++ --&gt; &lt;Set name="handler"&gt;AAA&lt;/Set&gt;</pre>                                                                                                                                                                                                                                       | <pre>&lt;!-- +++++ +++++ --&gt; &lt;!-- Set the accounting request handler. This can be set to: AAA - handle the request locally by logging. PROXY - proxy the request to another server. DOMAINPROXY - proxy the request to another server selected by domain name. --&gt; &lt;!-- +++++ +++++ --&gt; &lt;Set name="handler"&gt;AAA&lt;/Set&gt;</pre> |

Table C-2 Changes in rdp.xml (continued)

| MBean                                                                                                     | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Replaces in SESM 3.2(2) |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <p>New handlers in the ERP MBean that has the jmxname RDP</p> <p>These handlers are for iPass support</p> | <pre> &lt;!-- iPass handlers This section defines the handlers required to handle iPass requests and proxy them to an iPass AAA server --&gt; &lt;Item&gt; &lt;New class="com.cisco.sesm.rdp.IPassDetectionHandler"&gt; &lt;Set name="name"&gt;IPASS&lt;/Set&gt; &lt;Set name="attribute"&gt;USER_NAME&lt;/Set&gt; &lt;Set name="pattern"&gt;IPASS/.*/&lt;/Set&gt; &lt;Set name="noniPassHandler"&gt;AAA&lt;/Set&gt; &lt;Set name="iPassHandler"&gt;LOCEXTRACT&lt;/Set&gt; &lt;/New&gt; &lt;/Item&gt;  &lt;Item&gt; &lt;New class="com.cisco.sesm.rdp.LocationExtractionHandler "&gt; &lt;Set name="name"&gt;LOCEXTRACT&lt;/Set&gt; &lt;Set name="nextHandler"&gt;SERVADD&lt;/Set&gt; &lt;!-- This parameter should not normally be changed. If it is changed, you should also change the corresponding parameter in the web portal. --&gt; &lt;Set name="separator"&gt;###&lt;/Set&gt; &lt;Set name="locationAttribute"&gt;CALLED_STATION_ID&lt;/Set&gt; &lt;Set name="nASPortTypeValue" type="int"&gt;15&lt;/Set&gt; &lt;/New&gt; &lt;/Item&gt;  &lt;Item&gt; &lt;New class="com.cisco.sesm.rdp.ServiceAddFilter"&gt; &lt;Set name="name"&gt;SERVADD&lt;/Set&gt; &lt;Set name="nextHandler"&gt;IPASSPROXY&lt;/Set&gt; &lt;Set name="serviceName"&gt;iPassService&lt;/Set&gt; &lt;Set name="serviceUser"&gt;&lt;/Set&gt; &lt;Set name="servicePassword"&gt;&lt;/Set&gt; &lt;Set name="serviceVisible" type="boolean"&gt;false&lt;/Set&gt; &lt;/New&gt; &lt;/Item&gt;  &lt;Item&gt; &lt;New class="com.cisco.sesm.erp.radius.ProxyHandler"&gt; &lt;Set name="name"&gt;IPASSPROXY&lt;/Set&gt; &lt;/New&gt; &lt;/Item&gt; </pre> | —                       |

**Table C-2** Changes in rdp.xml (continued)

| MBean                                                                                                                                                                                                           | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Replaces in SESM 3.2(2) |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| iPass ProxyHandler                                                                                                                                                                                              | <pre> &lt;!-- iPass PROXY radius socket configuration parameters          --&gt; &lt;Configure   jmxname="com.cisco.sesm:name=RDP,IPASSPROXY=ProxyHa ndler,component=RADIUSClientSocket"&gt;   &lt;Set name="throttle" type="int"&gt;256&lt;/Set&gt;   &lt;Set name="timeOut" type="int"&gt;4000&lt;/Set&gt;   &lt;Set name="maxRetries" type="int"&gt;3&lt;/Set&gt;   &lt;Set name="primaryIP"&gt;127.0.0.1&lt;/Set&gt;   &lt;Set name="primaryPort" type="int"&gt;1816&lt;/Set&gt;   &lt;Set id="IPASSSecret" name="secret"&gt;cisco&lt;/Set&gt;   &lt;Set name="secondaryIP"&gt;127.0.0.1&lt;/Set&gt;   &lt;Set name="secondaryPort" type="int"&gt;1816&lt;/Set&gt;   &lt;Set name="accountingPortOffset" type="int"&gt;1&lt;/Set&gt; &lt;/Configure&gt; </pre> | —                       |
| recvBufSize and<br>sendBufSize<br><br>Enhancement to enable<br>changing send and<br>receive buffer<br>sizes—Located in the<br>AUTH RADIUS listener<br>socket and in the<br>Accounting RADIUS<br>listener socket | <pre> &lt;!-- Desired size of socket receive buffer. 0 = use system default. --&gt; &lt;Set name="recvBufSize" type="int"&gt;32767&lt;/Set&gt; &lt;!-- Desired size of socket transmit buffer. 0 = use system default. --&gt; &lt;Set name="sendBufSize" type="int"&gt;32767&lt;/Set&gt; </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | —                       |
| allowNonSSGUsers<br><br>Enhancement to allow<br>non-SSG users                                                                                                                                                   | <pre> &lt;Set name="allowNonSSGUsers" type="boolean"&gt;false&lt;/Set&gt; </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | —                       |

## webproxy.xml

Full path: <install directory>/webproxy/config

Table C-3 shows new sections that have been added to webproxy.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-3** Changes in webproxy.xml

| MBean                                                                                                                 | Added to SESM 3.3(1)                                                                                                                                                                                               | Replaces in SESM 3.2(2) |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| FilePollerMBean<br><br>New MBean for the file<br>polling feature to<br>dynamically update<br>locations and whitelists | <pre> &lt;!-- Uncomment this clause to instantiate the file poller   &lt;Instantiate order="10"     Class="com.cisco.sesm.jmx.FilePollerMBean"     jmxname="com.cisco.sesm.jmx:name=FilePoller"/&gt; --&gt; </pre> | —                       |

**Table C-3** Changes in webproxy.xml (continued)

|                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |   |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre> &lt;!-- Uncomment and modify this clause to configure the file poller &lt;Configure jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;   &lt;Set name="pollingInterval" type="int"&gt;3600&lt;/Set&gt;   &lt;Set name="polledFiles"&gt;     &lt;Array class="java.lang.String"&gt;       &lt;Item&gt;configurationfile1.xml&lt;/Item&gt;     &lt;Item&gt;configurationfile2.xml&lt;/Item&gt;     &lt;/Array&gt;   &lt;/Set&gt; &lt;/Configure&gt; &lt;Action jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;   &lt;Call name="forcePollingNow" /&gt; &lt;/Action&gt; --&gt; </pre> | — |
| RX_BUF_SIZE/<br>TX_BUF_SIZE<br>Enhancement to enable changing send and receive buffer sizes              | <pre> &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;RX_BUF_SIZE&lt;/Arg&gt;&lt;Arg&gt;32767&lt;/Arg&gt; &lt;/Call&gt; &lt;Call name="setGlobalAttribute"&gt;&lt;Arg&gt;TX_BUF_SIZE&lt;/Arg&gt;&lt;Arg&gt;32767&lt;/Arg&gt; &lt;/Call&gt; </pre>                                                                                                                                                                                                                                                                                                                                      | — |
| AccountWebProxy<br>Handler<br>For whitelist configuration.<br>Migrated from webproxy.web-jetty.xml       | <pre> &lt;Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,WebApplicationContext=0,context=/,AccountWebProxyHandler=0"&gt;   &lt;configuration clauses&gt;   .   .   . &lt;/Configure&gt; </pre>                                                                                                                                                                                                                                                                                                                                                                                | — |

# captiveportal.xml

Full path: <install directory>/captiveportal/config

Table C-4 shows new sections that have been added to captiveportal.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-4** Changes in captiveportal.xml

| MBean                                                                                                    | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Replaces in SESM 3.2(2) |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment this clause to instantiate the file poller   &lt;Instantiate order="10"     Class="com.cisco.sesm.jmx.FilePollerMBean"     jmxname="com.cisco.sesm.jmx:name=FilePoller"/&gt; --&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                           | —                       |
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment and modify this clause to configure the file poller   &lt;Configure     jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;     &lt;Set name="pollingInterval"       type="int"&gt;3600&lt;/Set&gt;     &lt;Set name="polledFiles"&gt;       &lt;Array class="java.lang.String"&gt;         &lt;Item&gt;configurationfile1.xml&lt;/Item&gt;       &lt;Item&gt;configurationfile2.xml&lt;/Item&gt;       &lt;/Array&gt;     &lt;/Set&gt;   &lt;/Configure&gt;   &lt;Action     jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;     &lt;Call name="forcePollingNow"/&gt;   &lt;/Action&gt; --&gt;</pre> | —                       |
| RX_BUF_SIZE/<br>TX_BUF_SIZE<br>Enhancement to enable changing send and receive buffer sizes              | <pre>&lt;Call   name="setGlobalAttribute"&gt;&lt;Arg&gt;RX_BUF_SIZE&lt;/Arg&gt;&lt;Ar g&gt;32767&lt;/Arg&gt; &lt;/Call&gt; &lt;Call   name="setGlobalAttribute"&gt;&lt;Arg&gt;TX_BUF_SIZE&lt;/Arg&gt;&lt;Ar g&gt;32767&lt;/Arg&gt; &lt;/Call&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                     | —                       |
| overrideURLOn toggle                                                                                     | <pre>&lt;!-- - This allows handlers to set a request attribute for the URL - to redirect to, which if set overrides all other forms of redirection, - ie is independent of the listener port. For security reasons, this - should be set to false unless an appropriate handler is in use, which - is the case with the default install (see webapp/WEB-INF/web-jetty.xml - and com.cisco.sesm.jetty.RedirectHandler). --&gt; &lt;Set name="overrideURLOn"   type="boolean"&gt;false&lt;/Set&gt;</pre>                                                                                                                     | —                       |
| SSG MBean                                                                                                | Installed default value for the throttle attribute has been increased to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | —                       |

**Table C-4** Changes in captiveportal.xml (continued)

| MBean                                                                                                                                                              | Added to SESM 3.3(1)                                                                                                                                                                                                                               | Replaces in SESM 3.2(2) |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| RedirectHandler<br>For iPass support                                                                                                                               | <pre>&lt;Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,WebA pplicationContext=0,context=/,RedirectHandler=0"&gt; &lt;configuration clauses&gt; . . . &lt;/Configure&gt;</pre>                                                           | —                       |
| CPProxyHandler<br>For whitelist<br>configuration<br><br>Migrated from<br>captive.web-jetty.xml                                                                     | <pre>&lt;Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,WebA pplicationContext=0,context=/,CPProxyHandler=0"&gt; &lt;configuration clauses&gt; . . . &lt;/Configure&gt;</pre>                                                            | —                       |
| SESM MBean<br><br>New attributes for iPass<br>support<br><br>These attributes should be<br>in all instances of the<br>SESM MBean, but are<br>relevant only in NWSP | <pre>&lt;Set name="ipassOn" type="boolean"&gt;false&lt;/Set&gt; &lt;!-- ipassProxyIdentity value allows NWSP to recognize transient users and to disallow selfcare for them --&gt; &lt;Set name="ipassProxyIdentity"&gt;IPASS/.*&lt;/Set&gt;</pre> | —                       |

# wsg.xml

Full path: <install directory>/wsg/config

Table C-5 shows new sections that have been added to wsg.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-5 Changes in wsg.xml**

| MBean                                                                                                    | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Replaces in SESM 3.2(2) |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment this clause to instantiate the file poller &lt;Instantiate order="10"   Class="com.cisco.sesm.jmx.FilePollerMBean"   jmxname="com.cisco.sesm.jmx:name=FilePoller"/&gt; --&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                    | —                       |
| FilePollerMBean<br>New MBean for the file polling feature to dynamically update locations and whitelists | <pre>&lt;!-- Uncomment and modify this clause to configure the file poller &lt;Configure   jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;   &lt;Set name="pollingInterval"     type="int"&gt;3600&lt;/Set&gt;   &lt;Set name="polledFiles"&gt;     &lt;Array class="java.lang.String"&gt;       &lt;Item&gt;configurationfile1.xml&lt;/Item&gt;     &lt;Item&gt;configurationfile2.xml&lt;/Item&gt;     &lt;/Array&gt;   &lt;/Set&gt; &lt;/Configure&gt; &lt;Action   jmxname="com.cisco.sesm.jmx:name=FilePoller"&gt;   &lt;Call name="forcePollingNow" /&gt; &lt;/Action&gt; --&gt;</pre> | —                       |
| SSG MBean<br>Enhancement to enable changing send and receive buffer sizes, RX_BUF_SIZE/ TX_BUF_SIZE      | <pre>&lt;Call   name="setGlobalAttribute"&gt;&lt;Arg&gt;RX_BUF_SIZE&lt;/Arg&gt;&lt;Ar g&gt;32767&lt;/Arg&gt; &lt;/Call&gt; &lt;Call   name="setGlobalAttribute"&gt;&lt;Arg&gt;TX_BUF_SIZE&lt;/Arg&gt;&lt;Ar g&gt;32767&lt;/Arg&gt; &lt;/Call&gt;</pre>                                                                                                                                                                                                                                                                                                                                        | —                       |
| SSG MBean<br>Enhancement to configure time to wait for a RADIUS ID                                       | <pre>&lt;!-- - The time in milliseconds to wait for a RADIUS ID to become available --&gt; &lt;Call   name="setGlobalAttribute"&gt;&lt;Arg&gt;ID_TIMEOUT&lt;/Arg&gt;&lt;Arg &gt;500&lt;/Arg&gt;&lt;/Call&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                            | —                       |
| SSG MBean                                                                                                | Installed default value for the throttle attribute has been increased to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | —                       |



**Table C-5** Changes in wsg.xml (continued)

| MBean                                                                                                                                                          | Added to SESM 3.3(1)                                                                                                                                                                                                                                                                                                                                                                                                          | Replaces in SESM 3.2(2) |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <p>SESM MBean</p> <p>New attributes for iPass support.</p> <p>These attributes should be in all instances of the SESM MBean, but are relevant only in NWSP</p> | <pre>&lt;Set name="ipassOn" type="boolean"&gt;false&lt;/Set&gt; &lt;!-- ipassProxyIdentity value allows NWSP to recognize transient users and to disallow selfcare for them --&gt; &lt;Set name="ipassProxyIdentity"&gt;IPASS/.*&lt;/Set&gt;</pre>                                                                                                                                                                            | —                       |
| <p>SESM MBean</p> <p>New attribute for new session management mechanism</p>                                                                                    | <pre>&lt;!-- - This is the maximum number of sessions that are held in hard - cache. This is cache that isn't cleared by the garbage collector, - only by the timeout mechanism. Once the hard cache is full, - sessions are moved to the soft cache. From there, they can be - removed by the garbage collector when it needs to free up memory. --&gt; &lt;Set name="sessionCacheSize" type="int"&gt;2000&lt;/Set&gt;</pre> | —                       |
| <p>SESM MBean</p> <p>Other enhancements for new session management mechanism</p>                                                                               | <ul style="list-style-type: none"> <li>• profileCachePeriod has been reduced to 30 seconds.</li> <li>• sessionCachePeriod has been reduced to 2 minutes.</li> <li>• memRequired has been removed from the config. This property is deprecated. It is in the MBean but it does not do anything now.</li> </ul>                                                                                                                 | —                       |

## nwsp.web-jetty.xml

Full path: <install directory>/nwsp/webapp/WEB-INF/

Table C-6 shows new sections that have been added to nwsp.web-jetty.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-6** Changes in nwsp.web-jetty.xml

| MBean         | Added to SESM 3.3(1)                                         | Replaces in SESM 3.2(2) |
|---------------|--------------------------------------------------------------|-------------------------|
| SesmProxyList | <pre>&lt;Item&gt;cd-sv210-sesm3.cisco.com&lt;/Item&gt;</pre> | —                       |

## webproxy.web-jetty.xml

Full path: <install directory>/webproxy/webapp/WEB-INF/

Table C-7 shows new sections that have been added to webprox.web-jetty.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-7** Changes in webproxy.web-jetty.xml

| MBean                                                                                       | Added to SESM 3.3(1) | Replaces in SESM 3.2(2)                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AccountWebProxyHandler<br><br>For whitelist configuration.<br><br>Migrated to webproxy.xml. | —                    | <pre>&lt;Configure jmxname="org.mortbay.jetty:name=Jetty ,Server=0,WebApplicationContext=0,con text=/,AccountWebProxyHandler=0"&gt; &lt;configuration clauses&gt; . . . &lt;/Configure&gt;</pre> |

## captive.web-jetty.xml

Full path: <install directory>/captive/webapp/WEB-INF/

Table C-8 shows new sections that have been added to captive.web-jetty.xml in SESM 3.3(1), and the corresponding sections that have been replaced in the SESM 3.2(2) file, if applicable.

**Table C-8** Changes in captive.web-jetty.xml

| MBean                                                                                  | Added to SESM 3.3(1)                                                                                                                                                               | Replaces in SESM 3.2(2)                                                                                                                                                                  |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RedirectHandler<br><br>For iPass support                                               | <pre>&lt;Call name="addHandler"&gt;   &lt;Arg type="int"&gt;0&lt;/Arg&gt;   &lt;Arg&gt;&lt;New class="com.cisco.sesm.jetty.RedirectHandler "/&gt; &lt;/Arg&gt; &lt;/Call&gt;</pre> | —                                                                                                                                                                                        |
| CPProxyHandler<br><br>For whitelist configuration<br><br>Migrated to captiveportal.xml | —                                                                                                                                                                                  | <pre>&lt;Configure jmxname="org.mortbay.jetty:name=Jetty ,Server=0,WebApplicationContext=0,con text=/,CPProxyHandler=0"&gt; &lt;configuration clauses&gt; . . . &lt;/Configure&gt;</pre> |

# Additional Changes

The following JSP files, and classes were modified to fix bugs.

## Ensuring shape cache is thread safe:

The following JSP files were modified:

- nwsp/webapp/html/3/4/pages/serviceList.jsp
- nwsp/webapp/html/3/4/pages/serviceListGroup.jsp
- nwsp/webapp/pages/serviceList.jsp
- nwsp/webapp/pages/serviceListGroup.jsp

The following Java class was modified:

- com/cisco/sesm/shape/Shape.java

## Captive Portal problems

The following lines have been added to the first half of web.xml:

```
<servlet>
 <servlet-name>RemoveOpenWindow</servlet-name>
 <description>
 Remove the attributes for the pop-up window
 from the HTTP Session after eg cancelling a service.
 </description>
 <servlet-class>
 com.cisco.sesm.navigator.RemoveAttributesDecorator
 </servlet-class>
 <init-param>
 <param-name>names</param-name>
 <param-value>
 openWindowURL
 openWindowName
 </param-value>
 </init-param>
 <init-param>
 <param-name>scope</param-name>
 <param-value>session</param-value>
 </init-param>
 <load-on-startup>1</load-on-startup>
</servlet>
```

The following lines have been added to the second half of the web.xml:

```
<servlet-mapping>
 <servlet-name>RemoveOpenWindow</servlet-name>
 <url-pattern>/cancel/*</url-pattern>
</servlet-mapping>
```

The following JSP files were modified:

- webapp/pages/serviceStart.jsp
- webapp/pages/serviceRedirect.jsp
- webapp/decorators/openWindow.jspf

**Fixing Location Mechanism for PBHK**

The following JSP file was modified:

- webapp/decorators/locationDimension.jsp



## SESM Performance Information

This appendix provides SESM performance test results to help you plan your SESM deployment.

This appendix contains the following sections:

- [NWSP Performance, page D-1](#)
- [NWSP iPass Servlet Performance, page D-2](#)
- [WSG Performance, page D-3](#)
- [Captive Portal Performance, page D-4](#)
- [Web Proxy Performance, page D-6](#)
- [RDP Performance, page D-7](#)
- [DNS Proxy Performance, page D-8](#)



**Note**

These results demonstrate peak performance ability. When planning your deployment, take into account that long-term performance rates will be lower.

## NWSP Performance

This section provides the performance test results for NWSP.

The setup used for these performance tests is described in [Table D-1](#).

**Table D-1 Setup for NWSP Performance Testing**

	<b>Solaris</b>	<b>Linux</b>
SESM server	Sun Fire V210, Dual CPU, 1002 MHz SUNW UltraSPARC-IIIi 1 GB RAM	Linux ES 3.0 HP DL-360, Single CPU, 2.8 GHz, Intel Xeon 1 GB RAM
Heap size	512 MB	512 MB
Threads	<ul style="list-style-type: none"><li>• Max threads—1024</li><li>• Min threads—205</li></ul>	<ul style="list-style-type: none"><li>• Max threads—1024</li><li>• Min threads—205</li></ul>
SESM SSG MBean configuration	<ul style="list-style-type: none"><li>• Timeout—10</li><li>• Retries—3</li></ul>	<ul style="list-style-type: none"><li>• Timeout—10</li><li>• Retries—3</li></ul>
Ulimit in start.sh	4096	4096

Table D-2 shows the results for these performance tests.

**Table D-2 Results for NWSP Performance Testing**

Scenario	Solaris	Linux
Authentication in SESM SPE installation with Sun ONE 5.2 LDAP server with 10000 users.	35 authentication requests per second.	35 authentication requests per second.
Authentication in SESM RADIUS installation.	55 authentication requests per second.	40 authentication requests per second.
Service activation in SESM SPE installation.	30 service activation requests per second.	30 service activation requests per second.
Service activation in SESM RADIUS installation.	40 service activation requests per second.	30 service activation requests per second.



**Note**

Scenario 3 and scenario 4 do not include logoff. SSG was configured to remove host objects after a specified timeout.

## NWSP iPass Servlet Performance

This section provides the performance test results for NWSP iPass servlet.

The setup used for these performance tests is described in Table D-3.

**Table D-3 Setup for NWSP iPass Servlet Performance Testing**

	Solaris	Linux
SESM server	Sun Ultra 10 Single CPU, 440 MHz Ultra-SPARC-III 512 MB RAM	Linux ES 2.1 HP DL-360, Dual CPU, 2.8 GHz 2 GB RAM
Heap size	256 MB	256 MB
Threads	<ul style="list-style-type: none"> <li>Max threads—512</li> <li>Min threads—100</li> </ul>	<ul style="list-style-type: none"> <li>Max threads—1024</li> <li>Min threads—200</li> </ul>
SESM configuration	<ul style="list-style-type: none"> <li>SESM SPE installation with PBHK</li> <li>Default SSG MBean configuration</li> </ul>	<ul style="list-style-type: none"> <li>SESM SPE installation with PBHK</li> <li>Default SSG MBean configuration</li> </ul>

[Table D-4](#) shows the results for these performance tests.

**Table D-4 Results for NWSP iPass Servlet Performance Testing**

Scenario	Solaris	Linux
iPass Smart Client authentication. <b>Note</b> The test setup bypassed SSL.	35 authentications per second.	50 authentications per second.
iPass Smart Client logoff.	40 deauthentications per second.	40 deauthentications per second.

## WSG Performance

This section provides the performance test results for Web Services Gateway (WSG).

The setup used for these performance tests is described in [Table D-5](#).

**Table D-5 Setup for WSG Performance Testing**

	Solaris	Linux
WSG Server	Sun U10 with Solaris 8 Single CPU, 440 MHz Ultra-SPARC-IIIi 1GB RAM	Linux ES 3.0 HP DL-360, Single CPU, 2.8 GHz, Intel Xeon 1 GB RAM
Heap size	256 MB	64 MB
WSG configuration	IPHK with 1 SSG client subnet	IPHK
User profile	<ul style="list-style-type: none"> <li>50000 users on Sun ONE 5.2</li> <li>6 services per user</li> </ul>	<ul style="list-style-type: none"> <li>50000 users on Sun ONE 5.2</li> <li>6 services per user</li> </ul>
Connection pool	50 connections	40 connections

[Table D-6](#) shows the results for these performance tests.

**Table D-6 Results for WSG Performance Testing**

Scenario	Solaris	Linux
Authentication requests in SESM RADIUS installation.	65 requests per second.	210 requests per second.
Authentication requests in SESM SPE installation.	35 requests per second.	150 requests per second.

Table D-7 shows the results for additional performance tests for Solaris.

**Table D-7 Results for WSG Performance Testing on Solaris**

Scenario	Solaris
Service activation requests in SESM RADIUS installation.	50 requests per second.
Service activation requests in SESM SPE installation.	30 requests per second.
Get Status requests in SESM RADIUS installation.	50 requests per second.
Get Status requests in SESM SPE installation.	30 requests per second.

## Captive Portal Performance

This section provides the performance test results for Captive Portal.

The setup used for these performance tests is described in Table D-8.

**Table D-8 Setup for Captive Portal Performance Testing**

	Solaris	Linux
SESM server	Sun Fire V210, Dual CPU, 1002 MHz SUNW UltraSPARC-IIIi 2 GB RAM	Linux ES 2.1 HP DL-360, Dual CPU, 2.8 GHz 2 GB RAM
Heap size	256 MB	512 MB
SESM SSG MBean configuration	<ul style="list-style-type: none"> <li>Timeout—10</li> <li>Retries—3</li> </ul>	<ul style="list-style-type: none"> <li>Timeout—10</li> <li>Retries—3</li> </ul>
Captive Portal configuration	Default configuration	<ul style="list-style-type: none"> <li>Max. threads—1024</li> <li>Min. threads—200</li> </ul> <p><b>Note</b> Specific test cases might have different configurations. These are described where applicable.</p>



Table D-9 shows the results for these performance tests.

**Table D-9 Results for Captive Portal Performance Testing**

Scenario	Solaris	Linux
302 redirect. <ul style="list-style-type: none"> <li>No locations and no whitelists configured.</li> <li>SESM server working with SSG on a Catalyst 10K.</li> </ul>	250 requests per second received from non-web proxy HTTP 1.1 client.	150 requests per second received from non-web proxy HTTP 1.1 client.
IPHK or PBHK location-based whitelist. <ul style="list-style-type: none"> <li>SESM server working with SSG on a Catalyst 10K.</li> <li>Whitelist configuration file contained 5000 whitelists, and 5000 hostgroups—10 with 100 URLs, 4990 with 5 URLs.</li> <li>Location configuration file contained 5000 locations—10 with 100 address ranges, 4990 with 5 address ranges. Each address range has 10 IP addresses.</li> </ul>	100 requests per second received from non-web proxy HTTP 1.1 client: <ul style="list-style-type: none"> <li>50 whitelist mismatch (302 redirects).</li> <li>50 whitelist match (proxy to HTML pages without resources).</li> </ul> <p><b>Note</b> In general, we would expect differences between IPHK and PBHK, because PBHK recalculates the location for every page request (not required for IPHK). However, in our tests there was no significant difference between IPHK and PBHK, because each request came from a different IP whereas in a production environment the same IP would be used for several requests.</p>	120 requests per second received from non-web proxy HTTP 1.1 client: <ul style="list-style-type: none"> <li>60 whitelist mismatch (302 redirects).</li> <li>60 whitelist match (proxy to HTML pages without resources).</li> </ul> <p><b>Note</b> In general, we would expect differences between IPHK and PBHK, because PBHK recalculates the location for every page request (not required for IPHK). However, in our tests there was no significant difference between IPHK and PBHK, because each request came from a different IP whereas in a production environment the same IP would be used for several requests.</p>
Location-based whitelist from HTTP 1.0 proxy client <ul style="list-style-type: none"> <li>SESM server working with SSG on a 7200.</li> <li>Location match with no whitelist matches—proxy to NWSP Login Page containing 50 resources (NWSP using Jetty web server).</li> </ul>	100 requests per second (2 page requests per second).	200 requests per second (4 page requests per second).

**Table D-9 Results for Captive Portal Performance Testing (continued)**

Scenario	Solaris	Linux
Location-based whitelist from HTTP 1.1 non-proxy client. <ul style="list-style-type: none"> <li>• SESM server working with SSG on a 7200.</li> <li>• Location match and whitelist match—proxy to NWSP Login Page containing 50 resources (NWSP using Jetty web server).</li> </ul>	150 requests per second (3 page requests per second).  In this scenario, the following configuration was used: <ul style="list-style-type: none"> <li>• Max threads—1500</li> <li>• Min threads—400</li> <li>• Heap—512 MB</li> </ul>	400 requests per second (8 page requests per second).  In this scenario, the following configuration was used: <ul style="list-style-type: none"> <li>• Max threads—1500</li> <li>• Min threads—400</li> </ul>

## Web Proxy Performance

This section provides the performance test results for Web Proxy.

The setup used for these performance tests is described in [Table D-10](#).

**Table D-10 Setup for Web Proxy Performance Testing**

	Solaris	Linux
SESM server	Sun Fire V210, Dual CPU, 1002 MHz SUNW UltraSPARC-IIIi 2 GB RAM	Linux ES 2.1 HP DL-360, Dual CPU, 2.8 GHz 2 GB RAM
Heap size	256 MB	256 MB
Threads	<ul style="list-style-type: none"> <li>• Max threads—1700</li> <li>• Min threads—400</li> <li>• Web Proxy thread consumes 21 KB memory</li> </ul>	<ul style="list-style-type: none"> <li>• Max threads—1700</li> <li>• Min threads—400</li> </ul>
Ulimit in start.sh	4096	4096

Table D-11 shows the results for these performance tests.

**Table D-11 Results for Web Proxy Performance Testing**

Scenario	Solaris	Linux
Web Proxy proxying web proxy client using HTTP 1.0 to a web page (28 KB) containing four resources (62 KB, 7 KB, 2.3 KB, 0.5 KB)—100 KB total content.	200 requests per second (40 page requests per second).	200 requests per second (40 page requests per second).

## RDP Performance

This section provides the performance test results for RADIUS Data Proxy (RDP):

The setup used for these performance tests is described in Table D-12.

**Table D-12 Setup for RDP Performance Testing**

	Solaris	Linux
SESM server	Sun Fire V210, Dual CPU, 1002 MHz SUNW UltraSPARC-IIIi 2 GB RAM	Linux ES 3.0 HP DL-360, Single CPU, 2.8 GHz, Intel Xeon 1 GB RAM
Heap size	64 MB	64 MB

Table D-13 shows the results for these performance tests.

**Table D-13 Results for RDP Performance Testing**

Scenario	Solaris	Linux
Using the Authentication handler. <ul style="list-style-type: none"> <li>10000 users in LDAP server Sun ONE 5.2. (Sun Fire V210, Single CPU, 1002 MHz, SUNW UltraSPARC-IIIi, 1 GB memory)</li> <li>5 services per user profile.</li> </ul>	Average throughput—200 authentication requests per second.	Average throughput—350 authentication requests per second.

**Table D-13 Results for RDP Performance Testing**

Scenario	Solaris	Linux
Using the iPass Authentication handler. <ul style="list-style-type: none"> <li>SESM Bundled RADIUS Server used as iPass AAA simulator.</li> </ul> <p><b>Note</b> The iPass RADIUS server determines the performance, because the rate at which RDP passes requests to the iPass RADIUS server is faster.</p>	Average throughput—500 authentication requests per second.	Average throughput—600 authentication requests per second.

## DNS Proxy Performance

This section provides the performance test results for DNS Proxy. The setup used for these performance tests is described in [Table D-14](#).

**Table D-14 Setup for DNS Proxy Performance Testing**

	Solaris	Linux
SESM server	Sun Fire V210, Dual CPU, 1002 MHz SUNW UltraSPARC-IIIi 2 GB RAM	Linux ES 3.0 HP DL-360, Single CPU, 2.8 GHz, Intel Xeon 1 GB RAM
Heap size	64 MB	64 MB
Configuration	Default configuration chain with 10000 entries	Default configuration chain with 10000 entries
Types of requests tested	Resolved requests, spoof handler requests, substitute handler requests	Resolved requests, spoof handler requests, substitute handler requests
DNS server timeout	10 seconds	10 seconds
Client side timeout	25 seconds	25 seconds

[Table D-15](#) shows the results for these performance tests.

**Table D-15 Results for DNS Proxy Performance Testing**

Scenario	Solaris	Linux
	Average throughput for all tests—Approximately 4000 requests per second.	Average throughput for all tests—Approximately 6000 requests per second.



---

## A

advertising redirection [5-18](#)  
    configuring [3-11](#)  
API, SESM [5-21](#)  
API, SPE [5-21](#)  
apidoc [5-21](#)  
Application Manager [1-5, 5-8, 5-20](#)  
attributes  
    installation prompts [5-6](#)  
authentication  
    NDS [4-4](#)  
AUTH library [1-4, 5-21](#)

---

## B

browsers [B-7](#)  
bundled components [1-2](#)  
Bundled Proxy server [5-21](#)  
Bundled RADIUS server [5-21](#)

---

## C

captive portal solution [5-16](#)  
CDAT [1-5, 5-8, 5-19](#)  
    creating users and services [B-6](#)  
certificate, for SESM license [2-8, 5-5](#)  
Cisco Distributed Administration Tool (CDAT)  
    logging in [B-7](#)  
Cisco IOS, required releases [3-4](#)  
clients  
    RADIUS server [1-5](#)  
    RDP [5-14, 5-15](#)

SSG subnets [5-10](#)  
Client subnet attribute [5-10](#)  
client subnet attribute [2-6](#)  
cn [5-12](#)  
common name [5-12](#)  
configuration  
    changes in SESM 3.3(1) [C-1](#)  
console  
    installation mode [5-2](#)  
    iPlanet [4-6](#)  
    management [5-9](#)  
    NDS (ConsoleOne) [4-4](#)  
containers, directory [2-7, 5-12](#)  
core model [1-5, 5-8](#)  
custom installations [5-8](#)  
customizing applications [5-21, 5-23](#)

---

## D

default network [3-4](#)  
Demo mode [1-6, 5-8](#)  
deployment modes, switching [1-6, 5-8](#)  
DESS library [1-4](#)  
DESSusecasedata.ldf file [4-7](#)  
directory  
    configuring [2-5](#)  
    configuring for SESM [4-1](#)  
    connection information [5-12](#)  
    container [2-7, 5-12](#)  
    extending schema [1-4, 5-20](#)  
    installation results [5-20](#)  
    IP address [2-7, 5-12](#)  
    meta schema [5-12](#)

organization [2-7, 5-12](#)  
 password [2-7, 5-12](#)  
 ports [2-7, 5-12](#)  
 running during SESM install [5-20](#)  
 sample data [4-7](#)  
 user ID [2-7, 5-12](#)

dn [5-12](#)

downloading SESM [2-7](#)

duration, in redirections [5-18](#)

duration, of messages  
 parameters [3-10, 3-11](#)

## E

error redirections [5-17](#)

evaluation without licenses [2-8, 5-5, 5-7](#)

extending directory schema [1-4, 5-20](#)

## F

files

.iss [5-2](#)

.properties [5-2](#)

DESSusecasedata.ldf [4-7](#)

installation logs [5-3](#)

installation results [5-20](#)

licensenum.txt [5-7](#)

README.SESM.LDIF.html [5-21](#)

ssgconfig.txt [3-5](#)

web.xml [5-21](#)

web-jetty.xml [5-21](#)

frequency, in advertisement redirections [3-11](#)

## G

groups, captive portal [3-5](#)

GUI installation mode [5-1](#)

## H

hardware platforms [2-1](#)

HTTP [5-9, 5-16](#)

redirections [5-17](#)

## I

inetorgPerson attribute [5-12](#)

initial logon redirection [5-18](#)

configuring [3-10](#)

installation

custom [5-8](#)

license [5-7, A-4](#)

logging during [5-3](#)

results [5-20](#)

typical [5-8](#)

installation image

obtaining [2-7](#)

uncompressing [2-7](#)

installation modes [5-1](#)

console [5-2](#)

GUI [5-1](#)

silent [5-2](#)

installing

captive portal solution [5-16](#)

CDAT [5-8, 5-19](#)

Demo mode [1-6, 5-8](#)

directory [5-7](#)

individual components [5-8](#)

JDK [2-4](#)

Message Portal application [5-16](#)

NWSP [5-9](#)

PDA [5-9](#)

portal applications [5-8](#)

RDP [5-8, 5-13](#)

SPE [5-8](#)

WAP [5-9](#)

WSG [1-5, 5-8](#)

Install RBAC option [B-7](#)

IP addresses

- Captive Portal application [5-16](#)
- directory [2-7, 5-12](#)
- RADIUS server [2-6, 5-11, 5-15](#)
- RDP [5-13](#)
- RDP clients [5-15](#)
- SSG [2-6, 3-4, 5-10](#)

iPlanet

- Console [4-6](#)
- installing [4-2](#)
- password [5-12](#)
- uid [5-12, 5-13](#)

iss file [5-2](#)

## J

J2EE [1-2](#)

Jasper JSP framework [5-21](#)

javadoc [5-21](#)

Java Management Extensions

- See JMX

Java Naming and Directory Interface [1-2](#)

Java requirements for SESM [1-2, 2-4](#)

Java server pages

- See JSPs

JAXP XML parser [5-21](#)

JDK

- installing [2-4](#)

Jetty server [1-2, 1-5, 5-8, 5-21](#)

JMX [1-2](#)

- installing framework [5-21](#)
- path [5-21](#)

JNDI [1-2](#)

JRE

- requirements [1-2, 2-4](#)

JSPs

- customizing [5-24](#)
- engine [1-2](#)

- installing framework [5-21](#)
- precompiling [5-21](#)
- recompiling [2-4](#)

JVM [5-20](#)

## L

LDAP

- directory [1-6](#)

LDAP directory [4-1](#)

- See directory

libraries

- SESM [5-21](#)
- SPE [5-21](#)

libraries, SPE [1-4](#)

license

- obtaining number [2-8, 5-5, 5-7](#)
- types, for installation [5-7](#)

licensenum.txt file [5-7, 5-21](#)

licenses

- obtaining number [A-4](#)
- types, for installation [A-4](#)

logging on

- to NWSP [A-5, B-8](#)
- to portal applications [A-5](#)

logs, installation [5-3](#)

## M

management console [5-9](#)

masks [2-6, 5-10](#)

Message Portal application [5-16, 5-21](#)

meta schema, directory [5-12](#)

modes

- See deployment modes; installation modes

## N

naming attribute [5-12](#)

NAS [1-5](#)

NDS

authenticating [4-4](#)

container cn [5-13](#)

directory cn [5-12](#)

directory password [5-12](#)

next hop password [5-14](#)

NWSP

application [A-4](#)

logging on to [A-5, B-8](#)

NWSP application [1-5, 5-8, 5-9](#)

## O

organization, LDAP directory [2-7, 5-12](#)

## P

passwords

directory [2-7, 5-12](#)

directory container [5-13](#)

next hop [5-14](#)

service [2-7, 5-11, 5-14](#)

service group [2-7, 5-11, 5-14](#)

PDA application [1-5, 5-8, 5-9](#)

permissions

LDAP directory [2-7, 5-12, 5-13](#)

platforms, hardware [2-1](#)

portals

logging on [A-5](#)

port-bundle host key [3-4, 3-6, 5-10, 5-23, A-4](#)

port-map [3-4](#)

port-map command [3-6](#)

ports

advertising redirection [5-18](#)

Captive Portal application [5-16](#)

CDAT [5-19](#)

directory [2-7, 5-12](#)

initial logon redirection [5-18](#)

management console [5-9](#)

Message Portal application [5-16](#)

portal applications [5-9, A-4](#)

RADIUS server [2-6, 5-11, 5-15](#)

RDP [5-13](#)

service redirection [5-19](#)

SSG [2-6, 5-10, A-4](#)

SSL [5-9](#)

unauthenticated user redirection [5-17](#)

PPP connections [3-8](#)

precompiling JSPs [5-21](#)

prepaid redirection [3-12](#)

profile caching [3-6](#)

profiles [5-23](#)

properties files [5-2](#)

proxy

RADIUS server [5-21](#)

RDP mode [5-14](#)

web [1-5, 5-8, 5-21](#)

## R

RADIUS

clients [1-5](#)

example SESM installation [A-1](#)

introduction [A-1](#)

password [3-2](#)

server [1-3, 1-5](#)

shared secret

with SSG [2-6, A-4](#)

RADIUS evaluation installation [5-7](#)

RADIUS server [4-1](#)

configuring [2-5](#)

installing bundled [1-5, 5-8](#)

portal communication [5-11, 5-15](#)

primary [2-6, 5-11, 5-15](#)



- secondary [2-6, 5-11, 5-15](#)
- See also ports
- See also ports; Bundled RADIUS server
- RADIUS shared secret
  - with portals [2-6, 5-11](#)
  - with RDP [5-15](#)
  - with SSG [5-10](#)
- RBAC [1-4, 5-20, 5-21](#)
- RDP [1-5, 5-8](#)
  - adding clients [5-14](#)
  - client IP addresses [5-15](#)
  - configuring [5-23](#)
  - installing [1-5, 5-8, 5-13](#)
  - IP address [5-13](#)
  - next hop password [5-14](#)
  - port [5-13](#)
  - proxy mode [5-14, 5-15](#)
  - RADIUS communication [5-15](#)
  - restricted client feature [5-13, 5-14, 5-23](#)
  - service password [5-14](#)
  - shared secret [5-13, 5-15](#)
  - SSG communication [5-13](#)
- README.SESM.LDIF.html file [5-21](#)
- recompiling JSPs [2-4](#)
- restricted client feature [5-13, 5-14, 5-23](#)
- roles, loading [5-20](#)
- running applications [5-23](#)

## S

- sample data, RBAC [1-4, 5-21](#)
- sample LDAP data [4-7](#)
- schema, extending [1-4, 5-20](#)
- secure socket listener
  - See SSL
- service groups, password [2-7, 5-11, 5-14](#)
- service names [5-19](#)
- serviceNotGivenURI attribute [5-19](#)
- serviceportal.host system property [5-17](#)
- serviceportal.port [5-17](#)
- service profiles [3-10](#)
- service redirection [5-17, 5-19](#)
- services
  - creating in CDAT [B-6](#)
- SESM
  - downloading [2-7](#)
  - example RADIUS installation [A-1](#)
  - example SPE installation [B-1](#)
  - information on [A-6, B-9](#)
  - installation image
    - obtaining [2-7](#)
  - LDAP directory [1-6](#)
  - overview [1-1](#)
  - RADIUS server [1-3, 1-5](#)
- SESM Installation
  - information required [2-6](#)
- setup type [5-8](#)
- shared address spaces [3-10](#)
- shared secret
  - RADIUS and portals [2-6, 5-11](#)
  - RADIUS and SSG [2-6, 3-3, 5-10, A-4](#)
  - RDP and RADIUS [5-15](#)
  - RDP and SSG [5-13, 5-15](#)
- silent installation mode [5-2](#)
- single sign-on [3-6](#)
- Solaris
  - patches [2-5](#)
- source ip command [3-4](#)
- SPE [1-5, 4-1, 5-8, 5-21](#)
  - example SESM installation [B-1](#)
- SPE evaluation installation [5-7](#)
- SSG
  - clients to RDP [5-15](#)
  - configuring [2-5, 5-10, 5-23, A-4](#)
  - IP address [2-6, 3-4, 5-10](#)
  - mapping subnets [2-6, 5-10](#)
  - portal communication [5-10, A-4](#)
  - port-bundle host key [3-6](#)

port-map [3-4](#)  
 prepaid redirection [3-12](#)  
 RADIUS server ports [2-6, 5-10, A-4](#)  
 RDP communication [5-13](#)  
 releases [3-4](#)  
 shared secret [2-6, 3-2, 5-10, 5-13, A-4](#)  
 See also TCP redirections; port-bundle host key

ssgconfig.txt [3-5](#)  
 SSG simulator [5-21](#)  
 SSL [5-9](#)  
 starting applications [5-23](#)  
 subnet attributes, SSG [2-6, 5-10](#)  
 Sun ONE  
   installing [4-2](#)  
   password [5-12](#)  
   uid [5-12, 5-13](#)  
 support, technical [5-7](#)

---

## T

TCP redirections  
   configuring [3-5](#)  
 technical support [5-7](#)  
 Telnet interface [3-4](#)  
 temporary disk space [2-2](#)  
 tools directory [5-21](#)  
 typical installation [5-8](#)

---

## U

uid [5-12](#)  
 unauthenticated user redirection [5-17](#)  
   configuring [3-7](#)  
 unconnected service redirection  
   configuring [3-8](#)  
   shared address space [3-10](#)  
 uninstalling SESM [5-20, 5-22, 6-4](#)  
 unique identifier [5-12](#)

user ID, for directory [2-7, 5-12](#)  
 user ID, for directory container [5-13](#)  
 user ID for directory [2-7](#)  
 users  
   creating in CDAT [B-6](#)  
   names for logging into CDAT [B-7](#)

---

## W

WAP application [1-5, 5-8, 5-9](#)  
 warning, during installation [5-13](#)  
 web.xml [5-21](#)  
 webapp directory [5-21](#)  
 WEB-INF directory [5-21](#)  
 web-jetty.xml file [5-21](#)  
 web portal applications [5-9, A-4](#)  
 web portal applications, ports [A-4](#)  
 web portals  
   customizing [5-23](#)  
   ports [5-9](#)  
   running [5-23](#)  
 web proxy [1-5, 5-8, 5-21](#)  
 Web Services Gateway  
   See WSG  
 WSG [1-5, 5-8, 5-21](#)