



## **Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide**

SESM Release 3.1(3) and SPE Version 1.01  
April 2002

### **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

Text Part Number: OL-2147-01

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.

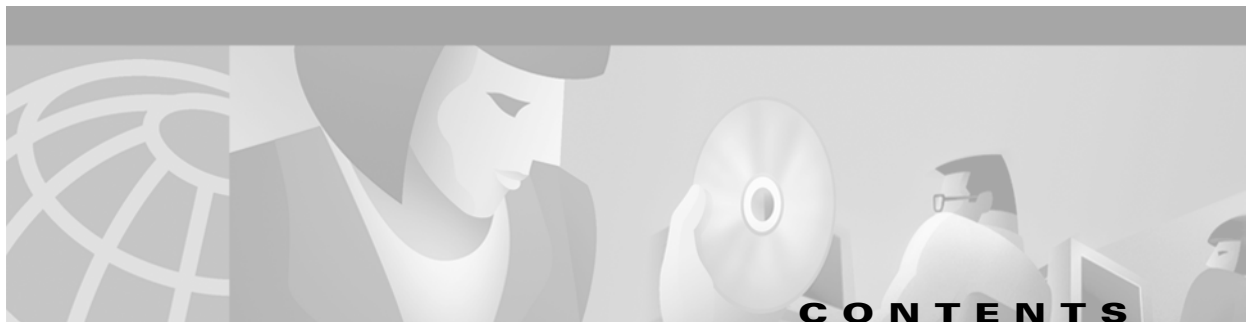
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0203R)

*Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*  
Copyright ©2002, Cisco Systems, Inc.  
All rights reserved.



## CONTENTS

### About This Guide **xiii**

- Document Objectives **xiii**
- Audience **xiii**
- Document Organization **xiv**
- Document Conventions **xv**
- Related Documentation **xv**
- Obtaining Documentation **xvi**
  - World Wide Web **xvi**
  - Documentation Feedback **xvi**
- Obtaining Technical Assistance **xvi**
  - Cisco.com **xvi**
  - Technical Assistance Center **xvii**
    - Cisco TAC Web Site **xvii**
    - Cisco TAC Escalation Center **xviii**

---

## CHAPTER 1

### Product Introduction **1-1**

- Introduction to Cisco SESM **1-1**
- Introduction to Cisco SPE **1-3**
- SESM Deployment Modes **1-4**
  - RADIUS Mode—SESM Using an External RADIUS Server **1-5**
  - LDAP Mode—SESM Integrated with SPE **1-5**
  - Demo Mode **1-5**
- SESM Applications **1-6**
  - Web Development Kit **1-6**
  - Sample Web Portal Applications **1-6**
  - Sample Captive Portal Solution **1-7**
  - RDP Server **1-7**
  - CDAT Application **1-8**
- Software Bundled with SESM **1-8**
  - SPE for LDAP Mode **1-8**
  - J2EE Components **1-9**
- Required Network Components **1-10**
  - Cisco Service Selection Gateway **1-10**
  - Port-Bundle Host Key Feature on SSG **1-10**

- Cisco Access Registrar or Third-Party RADIUS Server [1-11](#)
- LDAP Directory [1-11](#)
- Supported Hardware Platforms [1-12](#)
  - SSG Devices [1-12](#)
  - SESM Application Server Devices [1-12](#)
  - Subscriber Browser Devices [1-13](#)

**CHAPTER 2**

**Deployment Overview [2-1](#)**

- System Description and Network Diagram [2-1](#)
  - Connection Examples [2-3](#)
- SESM in RADIUS Mode [2-4](#)
  - Component Diagram for RADIUS Mode [2-4](#)
  - Processing a Subscriber Request in RADIUS Mode [2-5](#)
  - Installation and Configuration Requirements for RADIUS Mode [2-6](#)
- SESM in LDAP Mode [2-6](#)
  - Component Diagram for LDAP Mode [2-7](#)
  - Processing a Subscriber Request in LDAP Mode [2-8](#)
  - Installation and Configuration Requirements for LDAP Mode [2-9](#)

**CHAPTER 3**

**Feature Descriptions [3-1](#)**

- Web Portal for Subscribers [3-1](#)
  - Subscriber Features [3-1](#)
  - Customized and Branded Web Portal [3-2](#)
  - Personalized Subscriber Experiences [3-2](#)
- Authentication Options [3-2](#)
  - 2-Key Authentication [3-3](#)
  - 3-Key Authentication [3-3](#)
  - Single Sign-on for PPP Clients [3-4](#)
  - Single Sign-on for non-PPP Clients [3-4](#)
- Service Selection and Connection [3-4](#)
  - Service Selection [3-4](#)
  - Service Authentication and Authorization [3-4](#)
  - Automatic Connections [3-5](#)
  - Service Status [3-5](#)
  - Mutually Exclusive Service Selection [3-5](#)
  - Service Selection by Bandwidth [3-6](#)
  - Supported Service Types [3-6](#)
- Features in SESM-SPE [3-7](#)
  - Subscriber Account Self-Management [3-7](#)

Subscriber Service Self-Subscription	3-7
Subscriber Subaccount Creation and Management	3-7
Extended Subscriber Profile Data	3-7
Role Based Access Control	3-8
Captive Portal Features	3-8
Unauthenticated User Captivation	3-8
Unconnected Service Captivation	3-9
Initial Logon Captivation	3-9
Advertisement Captivation	3-9
Enhanced Session Management with Port-Bundle Host Key	3-9
Location Awareness	3-10
Brand Awareness	3-10
Web Development Features	3-11
Localization and Internationalization	3-11
Java Server Pages	3-11
SESM User Shape Mechanism	3-11
Locale and Device Awareness	3-11
Library Resources	3-12
Scaling, Redundancy, and Resiliency Features	3-12
Accounting and Billing Interfaces	3-12
RADIUS Accounting	3-13
Prepaid Services	3-13
Enhancing Prepaid Services Using SESM Captive Portal	3-13

**CHAPTER 4****Demo Quick Start 4-1**

Introduction	4-1
Installing in Demo Mode	4-1
Switching to Demo Mode at Run Time	4-2
Installation Instructions for Demo Mode	4-2
Browsers	4-4
Running the SESM Demo	4-5
Starting the Demo	4-5
Stopping the SESM Demo	4-5
Demo Data File	4-6
Demo Data Filename and Location	4-6
File Contents and Format	4-6
Logon Names and Passwords for a Demo	4-6
Special Demo Profile Attributes for Demonstrating LDAP Features	4-7

**CHAPTER 5**

**Installing Components 5-1**

- Installation Requirements 5-1
  - Installation Platform Requirements 5-1
  - RAM and Disk Space Requirements 5-2
  - Java Software Considerations 5-2
    - Solaris Patch Requirements 5-3
    - Installing the Bundled JRE 5-3
    - Specifying an Existing JRE or JDK 5-3
    - Specifying the JRE or JDK in the Startup Scripts 5-3
    - Obtaining a JDK for SESM Web Development 5-4
  - SSG and RADIUS Considerations 5-4
  - LDAP Directory Configuration Requirements 5-4
    - Advantages to Running an LDAP Directory During SESM Installation 5-5
    - NDS Installation and Configuration Requirements 5-5
    - iPlanet Installation and Configuration Requirements 5-7
  - Dependencies among SESM Components 5-9
  - Uninstalling a Previous Installation 5-10
- Obtaining the SESM Installation File and License Number 5-10
  - Obtaining a License Number 5-11
  - Downloading from the Cisco Web Site 5-11
  - Uncompressing the Image 5-11
- Installation Privileges 5-12
- Installation Modes 5-12
  - Turning On the Installation Logging Feature 5-13
  - Installing Using GUI Mode 5-13
  - Installing Using Console Mode 5-13
  - Installing Using Silent Mode 5-14
- Installation and Configuration Parameters 5-14
- Installation Results 5-30
- Post-Installation Procedures 5-30

**CHAPTER 6**

**Configuring Components after Installation 6-1**

- Configuration Overview 6-1
  - Changing Configuration Information 6-1
  - Configuration Technology 6-2
  - Configuration File Summary 6-3
    - J2EE Configuration Files 6-3
    - MBean Configuration Files 6-4

MBean Configuration File Format	6-5
Java System Properties in the MBean Configuration Files	6-6
Configuring the J2EE Jetty Container	6-7
Containers and Applications	6-7
J2EE Container Configuration Attributes	6-8
Configuring an SESM Portal Application	6-14
SESM Application Attributes	6-14
Associating SSGs and Subscriber Requests	6-25
Using Port-bundle Host Key with Identical SSG Configurations	6-25
Using Port-bundle Host Key with Varying SSG Configurations	6-27
Specifically Mapping SSGs to Subscriber Subnets	6-27
Global and Subnet Attribute Elements	6-28
Configuring RDP	6-30
RDP Modes	6-30
RDP Attributes	6-30
Configuring CDAT	6-36
Cookies Required	6-36
CDAT Attributes	6-36
Configuring SPE	6-37
SPE Attributes	6-37
Extending the Directory Schema and Loading Initial RBAC Objects	6-40
Using an SESM Custom Installation to Update the Schema and Load RBAC Objects	6-40
Using LDIF Commands to Update the Directory Schema	6-41
Loading Sample Data and Logging into CDAT for the First Time	6-41
Configuring Specific Features	6-41
Automatic Connections	6-42
Configuring Automatic Connections	6-42
Subscriber Experiences with Automatic Connections	6-43
Configuration-based Location and Brand Awareness	6-44
Configuring a Customized SESM Application	6-44
SESM Application Definition	6-44
SESM Application Names	6-45
Creating Configuration Files and Startup Scripts	6-45

**CHAPTER 7****Running SESM Components 7-1**

Starting Applications	7-1
Starting the SESM Portals	7-1
Starting RDP	7-2
Starting CDAT	7-3

- Startup Script Explanation [7-3](#)
  - Application-Specific Startup Scripts [7-3](#)
  - Generic Startup Script [7-4](#)
  - Java System Properties in Startup Scripts [7-4](#)
- Logging On [7-6](#)
- Stopping Applications [7-6](#)
  - Stopping SESM Applications on Solaris and Linux [7-7](#)
  - Stopping SESM Applications on Windows NT [7-7](#)
- Adding and Removing Services on Windows NT [7-7](#)
- Memory Requirements and CPU Utilization [7-8](#)
  - SESM Portal Application Memory Requirements [7-8](#)
  - SESM Portal Application CPU Utilization [7-9](#)
  - RDP Memory Requirements [7-10](#)

**CHAPTER 8**

**Deploying a Captive Portal Solution [8-1](#)**

- Introduction [8-1](#)
- SSG and SESM Release Requirements [8-2](#)
- Solution Description [8-2](#)
  - Solution Diagram [8-2](#)
  - SSG TCP Redirect Feature [8-3](#)
  - SESM Captive Portal Application [8-5](#)
  - Content Applications [8-6](#)
    - NWSP Application [8-6](#)
    - Message Portal Application [8-6](#)
  - Alternative Configuration Options for a Captive Portal Solution [8-7](#)
- Installing, Configuring, and Running the Sample Solution [8-8](#)
  - Installing and Configuring the Sample Solution [8-8](#)
  - Installation Results [8-9](#)
  - Additional Configuration Steps [8-9](#)
    - Configuring the SSG to Match the Installed Captive Portal Solution [8-9](#)
    - Loading Sample Profiles for Captive Portal Demonstration [8-10](#)
    - Configuring Unique Service Logon Pages for Service Redirections [8-10](#)
  - Starting the Sample Solution [8-11](#)
  - Demonstrating Captive Portal Features [8-12](#)
- Configuration Details [8-13](#)
  - Configuration File Summary [8-14](#)
  - captiveportal.xml Configuration File [8-15](#)
  - messageportal.xml Configuration File [8-17](#)
  - nwsp.xml Configuration File [8-20](#)



Message Duration Parameters	8-21
Configuring the SSG TCP Redirect Features	8-22
Configuring SSG and Port-Bundle Host Key to Work with the Captive Portal Application	8-22
Defining Captive Portal Groups and Port Lists	8-22
Configuring Unauthenticated User Redirection	8-23
Configuring Unauthorized Service Redirection	8-24
Configuring Initial Logon Redirection	8-25
Configuring Advertising Redirection	8-26
Troubleshooting Captive Portal Configurations	8-26
Some TCP Redirection Types Not Operational	8-27
Redirection Type Turned Off in captiveportal.xml	8-27
Two Redirection Types Assigned to the Same Port in captiveportal.xml	8-27
Redirection Type Not Configured on the SSG	8-27
Redirections Continuously Occur	8-27
Redirected Networks Must Match Service Routes	8-28
Using HTTP1.1 with a Non-SESM Captive Portal Application	8-28
User Name Not Passed in Unauthenticated User Redirections	8-28

**CHAPTER 9****Summary of SESM Communication Attributes 9-1**

Communication Attributes for Interaction Between SESM and SSG	9-1
Communication Attributes for RADIUS Mode	9-3
Communication Attributes for LDAP Mode	9-6
Communication Attributes for LDAP Mode with RDP in Proxy Mode	9-10

**CHAPTER 10****Troubleshooting SESM Installation and Configuration 10-1**

Diagnosing Problems	10-1
Procedures for Troubleshooting an SESM Web Application	10-1
Procedures for Troubleshooting RDP	10-3
Troubleshooting Aids	10-4
Logging and Debugging Mechanisms	10-4
Log File Locations	10-4
Logging and Debugging in SESM Web Applications	10-4
Switching Debugging On and Off at Run Time	10-5
Logging and Debugging in RDP	10-5
Logging and Debugging in CDAT	10-6
Java Command Line Options	10-6
SESM Management Console	10-6
Management Console User Name and Password	10-7
Obtaining License and Version Information	10-7

- Troubleshooting Tips [10-7](#)
  - JRE and JDK Troubleshooting [10-7](#)
    - Warning and Error Messages after JRE Installation [10-7](#)
    - Searching for an Existing JDK or JRE [10-8](#)
    - Using a Pre-installed JRE or JDK [10-9](#)
    - Recompiling a Customized JSP [10-9](#)
  - Installation Troubleshooting [10-10](#)
    - No X Server for a Solaris Installation [10-10](#)
    - Incorrect Permissions [10-10](#)
    - Files Not Found [10-10](#)
    - Incomplete Installation or Files Installed in Incorrect Directory [10-10](#)
  - Configuration File Location Troubleshooting [10-11](#)
  - SESM Configuration Troubleshooting [10-11](#)
    - Communication with SSG [10-11](#)
    - Communication with RADIUS Server [10-11](#)
    - Out of Memory Exceptions [10-11](#)
    - Web Server Unavailable [10-11](#)
  - RADIUS Configuration Troubleshooting [10-12](#)
  - SSG Configuration Troubleshooting [10-12](#)

---

**APPENDIX A**

**SESM Security [A-1](#)**

- Java Platform Security Description [A-1](#)
- HTTP Security Description [A-1](#)
- HTTPS Description [A-2](#)
- Keytool and Keystore [A-2](#)

---

**APPENDIX B**

**Configuring the SSG [B-1](#)**

- Basic SSG Configuration [B-1](#)
- Configuring the Host Key Port Bundle Feature on SSG [B-2](#)
- Sample SSG Configuration [B-3](#)

---

**APPENDIX C**

**DTD for MBean Configuration Files [C-1](#)**

- xmlconfig.dtd [C-1](#)

---

**APPENDIX D**

**Configuring RADIUS [D-1](#)**

- Configuring SSG to Communicate with the RADIUS Server [D-1](#)
- Configuring RADIUS Clients [D-2](#)
- Adding Cisco SSG Vendor-Specific Attributes to the Attribute Dictionary [D-3](#)

Configuring Service Profiles	D-3
Example Service Profiles	D-7
Configuring Service Group Profiles	D-7
Example Service Group Profiles	D-8
Configuring Subscriber Profiles	D-8
Example Subscriber Profiles	D-11
Configuring Next Hop Gateway Profiles	D-11
Configuring the RADIUS Accounting Feature	D-11
Configuring Cisco Access Registrar for SESM Deployments	D-12
Configuring the RADIUS Ports	D-12
Cisco SSG VSAs in Cisco Access Registrar Dictionary	D-12
Configuring NAS Clients in Cisco Access Registrar	D-12
Configuring Attribute Profiles in Cisco Access Registrar	D-13
Configuring Cisco Access Registrar Userlists and Authentication and Authorization Services	D-13
Configuring Accounting on Cisco Access Registrar	D-14
Saving the Configuration and Reloading the Server	D-14

**APPENDIX E****RDP Packet Handlers E-1**

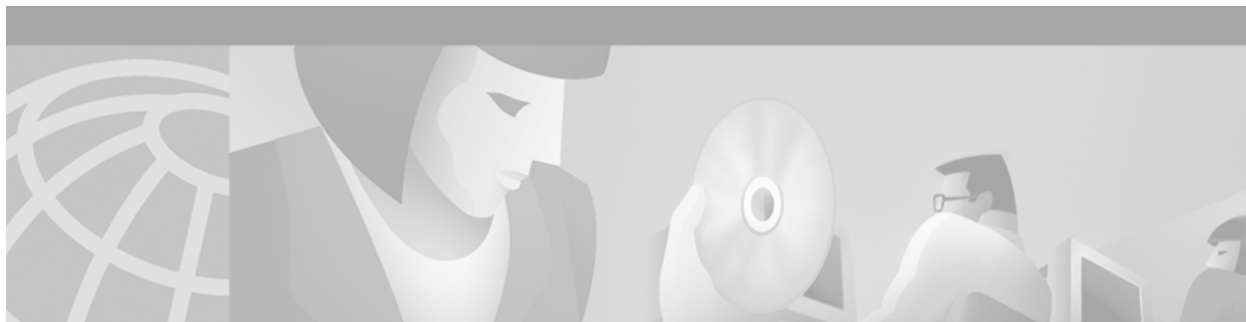
Packet Handlers	E-1
Overview	E-1
Configuring the Packet Handlers	E-2
Adding Additional Packet Handlers	E-2
RDPPacket Class Description	E-2
Processing Requests in Proxy Mode	E-5

**APPENDIX F****Sample MBean Configuration Files F-1**

Sample Container MBean Configuration File	F-1
Sample Application MBean Configuration File	F-3
RADIUS Mode Deployment	F-3
LDAP Mode Deployment	F-8
Sample RDP MBean Configuration File	F-13
Sample CDAT MBean Configuration File	F-16
Sample SPE MBean Configuration File	F-18
Sample Captive Portal Configuration File	F-19
Sample Message Portal Configuration File	F-24

**INDEX**





## About This Guide

---

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

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

## Document Objectives

This guide explains how to install and configure Cisco Subscriber Edge Services Manager (Cisco SESM) applications and related 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 services.

## Audience

This guide is intended for administrators and others responsible for:

- Installing and running the SESM sample applications in Demo mode, which simulates communication with other network components
- Installing, configuring, and running the SESM sample applications in RADIUS or DESS mode, both of which require communication with other network components
- Deploying a customized SESM application

# Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	<a href="#">Product Introduction</a>	Introduces the Cisco SESM product and its components. The chapter includes a list of hardware requirements.
Chapter 2	<a href="#">Deployment Overview</a>	Describes the Cisco SESM deployment options.
Chapter 3	<a href="#">Feature Descriptions</a>	Describes the Cisco SESM features.
Chapter 4	<a href="#">Demo Quick Start</a>	Describes procedures for installing, configuring, running, and using the sample portal applications in Demo mode.
Chapter 5	<a href="#">Installing Components</a>	Describes how to install the Cisco SESM software.
Chapter 6	<a href="#">Configuring Components after Installation</a>	Describes all of the configurable attributes in the SESM software components. Use this chapter to change or fine tune attributes after installation. It also discusses configuration requirements for a customized SESM application.
Chapter 7	<a href="#">Running SESM Components</a>	Describes how to start and stop the SESM software components.
Chapter 8	<a href="#">Deploying a Captive Portal Solution</a>	Describes the features and configuration procedures for the SESM captive portal solution and corresponding SSG TCP redirect features.
Chapter 9	<a href="#">Summary of SESM Communication Attributes</a>	Describes the attributes that control communication between components in an SESM deployment and how to ensure that the values match on both sides of the communication.
Chapter 10	<a href="#">Troubleshooting SESM Installation and Configuration</a>	Includes some troubleshooting procedures and information.
Appendix A	<a href="#">SESM Security</a>	Describes the security features in an SESM web portal.
Appendix B	<a href="#">Configuring the SSG</a>	Describes how to configure SSG to communicate with an SESM web application.
Appendix C	<a href="#">DTD for MBean Configuration Files</a>	Shows the XML document type definition (DTD) for the MBean configuration files used to configure the SESM software components.
Appendix D	<a href="#">Configuring RADIUS</a>	Describes how to configure a RADIUS server to communicate with: <ul style="list-style-type: none"> <li>• SSG and SESM web portals running in RADIUS mode.</li> <li>• SSG for accounting purposes, which is appropriate for SESM deployments in both RADIUS and DESS modes.</li> </ul>

Chapter	Title	Description
Appendix E	<a href="#">RDP Packet Handlers</a>	Describes how the RDP processes requests.
Appendix F	<a href="#">Sample MBean Configuration Files</a>	Contains sample configuration files.
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 the Cisco SESM includes:

- *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(3)*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Distributed Administration Tool Guide*
- *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide* (this guide)

The Cisco SESM documentation 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/ios122/122newft/122limit/122b/122b\\_4/122b4\\_sg/](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/)

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

- *Cisco IOS Security Configuration Guide, Release 12.2*
- *Cisco IOS Security Command Reference, Release 12.2*

If you are including the Cisco Access Registrar (a RADIUS server) in your SESM deployment, see the following documents:

- *Cisco Access Registrar 1.6 Release Notes*
- *Cisco Access Registrar User Guide*

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

### Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.



Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, have available your service agreement number and your product serial number.



# Product Introduction

---

This chapter introduces the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(3) and Cisco Subscriber Policy Engine (Cisco SPE) Version 1.01. The chapter includes the following topics:

- [Introduction to Cisco SESM, page 1-1](#)
- [Introduction to Cisco SPE, page 1-3](#)
- [SESM Deployment Modes, page 1-4](#)
- [SESM Applications, page 1-6](#)
- [Software Bundled with SESM, page 1-8](#)
- [Required Network Components, page 1-10](#)
- [Supported Hardware Platforms, page 1-12](#)

## Introduction to Cisco SESM

The Cisco Subscriber Edge Services Manager (SESM) works in conjunction with other network components to provide extremely robust, highly scalable connection management to services in the broadband and mobile wireless markets.

Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their subscribers with a web interface, or portal, for accessing multiple Internet and other services. ISPs and NAPs can customize and brand the content of the SESM portal web pages and thereby control the user experience for different categories of subscribers.

SESM applications provide support for any platform that supports the Java Runtime Environment (JRE). Platforms tested in our labs include Sun Solaris, Windows NT, Windows 2000, Red Hat Linux, and SuSE Linux.

An SESM solution is deployed with the Cisco Service Selection Gateway (SSG), a feature set embedded in the Cisco IOS software broadband release train. Some of the devices on which SSG can run include the Cisco 7200 Series high-performance multifunction router, the Cisco 7400 Series router, and the Cisco 6400 Universal Access Concentrator (UAC).

The SESM applications run in a default network assessable to the SSG. Together, SESM and SSG provide subscriber authentication, service selection, and service connection capabilities to subscribers in the broadband and mobile wireless environments.

Subscribers interact with an SESM web portal using a standard Internet browser. They do not need to download any software or plug-ins to use the SESM web portal. After a subscriber successfully authenticates, the SESM web portal presents a list of services that the subscriber is currently authorized

to use. The subscriber can gain access to one or more of those services by selecting them from the web portal. Alternatively, an automatic connection feature can automatically connect subscribers to services after authentication.

For service subscribers, the SESM solution offers flexibility and convenience, including the ability to access multiple services simultaneously.

For service providers, the SESM solution provides a way to control the subscriber experience and promote customer loyalty. Service providers can change the look and feel of their SESM web application, brand the application, and control the content of the pages displayed to their subscribers.

**Note**


---

The SESM product was previously called the Cisco Service Selection Dashboard (Cisco SSD).

---

**SESM Deployment Options**

Two SESM deployment options are available:

- **SESM-RADIUS**—In a RADIUS mode deployment, SESM uses subscriber and service information provided by a RADIUS server.
- **SESM-SPE**—When SESM is deployed in LDAP mode, it incorporates an additional component, the Cisco Subscriber Policy Engine (SPE) Version 1.01. The SPE allows subscribers to perform account maintenance and self-care activities, such as subscribing to new services, creating subaccounts (for other members of a family, for example), and changing basic account information, such as address, phone number, and e-mail. In LDAP mode, SESM uses subscriber and service information in an LDAP directory.

**SESM Application Suite**

The SESM product is an extensible Java2 Enterprise Edition (J2EE) compliant suite of applications and components for developing and deploying customized and branded web portal applications. This section describes the applications that are installed with SESM.

SESM includes the following sample portal applications that can be installed and configured for demonstration purposes or used as a starting point for customizations:

- **New World Service Provider (NWSP) portal**—A comprehensive example of most features offered by the SESM web development kit.
- **Wireless Access Protocol (WAP) portal**—Designed specifically for deployment in the mobile wireless industry.
- **Personal Digital Assistant (PDA) portal**—Shows web pages formatted for a PDA device.

You can optionally install the following applications to configure an SESM captive portal solution:


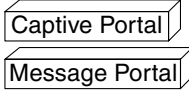



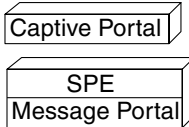
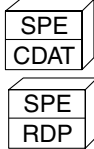

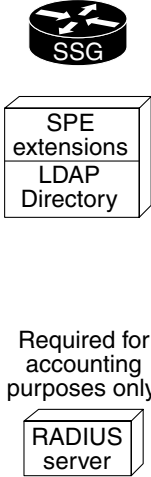
- **Captive Portal application**—A gateway application between the SSG and other applications in a captive portal solution. The default configuration for this application redirects subscriber browsers to either the Message Portal application or the NWSP application.
- **Message Portal application**—Produces sample greetings and advertising pages to demonstrate SESM captive portal features.

SESM-SPE includes two additional supporting applications:

- **Cisco Distributed Administration Tool (CDAT)**—Web-based interface for administrators that manages data in the SPE extensions to the LDAP directory.
- **RADIUS/DESS Proxy (RDP) server**—A RADIUS server that can proxy profile requests or use the SPE components to query the LDAP directory for profile information.

Figure 1-1 shows all of the applications included in SESM Release 3.1(3).

Figure 1-1 SESM Release 3.1(3) Suite of Applications

	SESM Applications Suite	Software Bundled with SESM	Required Network Components
SESM-RADIUS	* SESM portals  Captive Portal Solution 	 Management components	
SESM-SPE	* SESM portals  Captive Portal Solution  Supporting Applications 	 Management components	 Required for accounting purposes only.

69695

\* Includes SESM web development kit

## Introduction to Cisco SPE

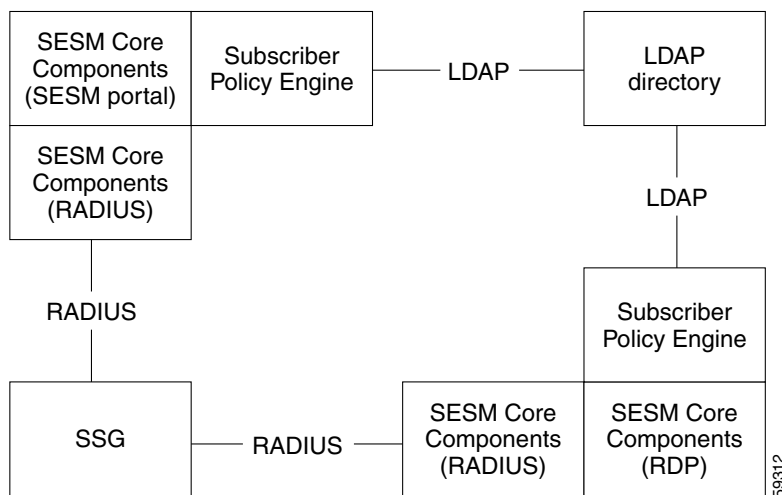
The Cisco Subscriber Policy Engine (SPE) Version 1.01 is a policy server specifically customized to provide granular subscriber service policy. SPE combines role-based access control (RBAC) functionality with an open policy server. Service providers can create differentiated subscriber groups. Service and content providers can use the SPE to provide value added and differentiated services to the subscriber population.

SPE is installed when SESM Release 3.1(3) is deployed in LDAP mode to provide the following enhanced features and capabilities:

- Use of an LDAP directory to manage subscriber, service profile, and policy information
- Subscriber account self-care
- Subscriber sub-account management
- Subscriber self-subscription to services
- Bulk administration of large subscriber populations
- Delegated administration
- Allow service publishers and business partners access to service creation and management
- Allow service providers and business partners to publish services to targeted subscribers

Figure 1-2 shows the relationship between the SESM and SPE products.

**Figure 1-2** *SESM Components in LDAP Mode*



## SESM Deployment Modes

You can deploy SESM portal applications in these modes:

- RADIUS mode—This mode obtains subscriber and service profile information from a RADIUS server. The RADIUS server must support Cisco vendor-specific attributes.
- LDAP mode—The LDAP mode integrates the Cisco Subscriber Policy Engine (SPE) Version 1.01 product with the SESM product to provide access to an LDAP compliant directory for subscriber and service profile information. SPE also provides enhanced functionality for SESM web applications and use of the role-based access control (RBAC) model to manage subscriber access.
- Demo mode—This mode demonstrates the capabilities of both RADIUS and LDAP modes without requiring additional external components, such as SSG, a RADIUS server, or an LDAP directory server.

The same SESM application programming interface (API) is used to develop and customize applications intended for either the RADIUS or the LDAP modes. Applications intended for LDAP mode deployment can include additional features provided by SPE. The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes how to create applications for both RADIUS and LDAP mode deployments.

## RADIUS Mode—SESM Using an External RADIUS Server

In a RADIUS deployment, a RADIUS server stores subscriber and service profiles. RADIUS refers to the Remote Dial-In User Service (RADIUS) database and server that performs authentication, authorization, and accounting (AAA) services for network connections. An SESM deployment works with any RADIUS server that accepts vendor-specific attributes (VSAs).

See the “[SESM in RADIUS Mode](#)” section on page 2-4 for more information about the components and data flow in a RADIUS mode deployment.

## LDAP Mode—SESM Integrated with SPE

An LDAP deployment stores subscriber and service profile information in a Lightweight Directory Access Protocol (LDAP)-compliant directory. An LDAP deployment requires the Cisco Subscriber Policy Engine (SPE) Version 1.01, which is available from the SESM installation package if your SESM purchase license allows it.

See the “[SESM in LDAP Mode](#)” section on page 2-6 for more information about the components and data flow in an LDAP mode deployment.

## Demo Mode

Demo mode is an SESM deployment mode that allows an SESM portal application to run in a simulated network. The application runs in Demo mode without access to other solution components, such as SSG, a RADIUS server, or an LDAP directory. Standalone Demo mode is *only* intended for demonstration purposes. Demo mode is not in any way representative of Cisco SESM performance in an end-to-end solution with actual network components.



### Note

---

If you install SESM in Demo mode, and then later want to perform some development on a customized portal application, we recommend that you perform another SESM installation. Otherwise, you will need to perform extensive edits to the MBean configuration files.

---

Demo mode simulates the actions of an SESM deployment in both RADIUS and LDAP modes. It uses a local copy of a Merit RADIUS file to obtain profile information. See [Chapter 4, “Demo Quick Start,”](#) for information about installing and using SESM in Demo mode.

### Sample Applications versus Demo Mode

Do not confuse the term sample application with Demo mode. The SESM sample applications are fully functioning web applications that were built using the SESM development library. These applications use the services of the Jetty web server and the JMX management server.

Demo mode is an SESM deployment mode for SESM portal applications. You can install and run the sample portal applications (NWSP, WAP, and PDA) in any of the SESM deployment modes: RADIUS, LDAP, or Demo.

Although you can install the captive portal solution in Demo mode, you cannot demonstrate the solution without an SSG redirecting traffic to the Captive Portal application.

## SESM Applications

This section describes the SESM web development kit and suite of applications:

- [Web Development Kit, page 1-6](#)
- [Sample Web Portal Applications, page 1-6](#)
- [Sample Captive Portal Solution, page 1-7](#)
- [RDP Server, page 1-7](#)
- [CDAT Application, page 1-8](#)

## Web Development Kit

When you install the SESM sample portal applications, the SESM libraries and other components required to build your own customized portal application are also installed. The installation provides the following items:

- SESM core component class libraries
- API documentation for the SESM libraries
- Code for each of the sample portal applications
- Images and JSPs for each of the sample portal applications
- Configuration and startup files for each of the sample portal applications
- Sample data files containing profiles appropriate for each of the sample portal applications. The sample data can be used to run the sample application in Demo mode.

See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about developing a customized SESM portal application. Use the configuration information in [Chapter 6, “Configuring Components after Installation,”](#) to deploy and configure the customized applications.

## Sample Web Portal Applications

The first step toward developing a customized SESM web portal is to install and configure the sample web portals in a development environment. You can create the desired look and branded aspects of a customized SESM portal by altering one of these sample applications or writing your own application using one of the samples as an example.

All of these sample portal applications can be deployed in RADIUS mode, LDAP mode, or demonstration (Demo) mode.

- The New World Service Provider (NWSP) portal is a comprehensive example of SESM features and capabilities. It serves as the main reference and example for all of the programming options offered by SESM web development components.
- The Wireless Access Protocol (WAP) portal is designed specifically for deployment in the mobile wireless industry. It has much of the same look and feel and subscriber options as the NWSP application, but it returns pages only in WML format designed for WAP devices. It illustrates service selection with account and service logon and off.



Deployers can customize this application to detect the type and make of various WAP devices used by their subscribers, and tailor the pages to the features of each device.

- The Personal Digital Assistant (PDA) portal illustrates web pages formatted for a PDA device. The application is designed for a business model in which services are always on. That is, all services are automatically connected when the subscriber logs on. Service self-subscription features (usable only in LDAP mode) are included.

Deployers can customize this application to detect the type and make of various PDA devices used by their subscribers, and tailor the pages to the features of each device.

The *Cisco Subscriber Edge Services Manager Web Developer Guide* provides detailed information about each of these sample portal applications.

## Sample Captive Portal Solution

The SESM captive portal feature works in conjunction with the SSG TCP redirect feature to provide enhanced user experiences in the case of unauthenticated network access or unauthenticated or unauthorized service access. Rather than simply being rejected, the subscriber sees a portal page with opportunities for logging on or gaining service authorization. The captive portal features also provide a way to present messages and advertisements to subscribers at initial logon and at timed intervals.

A sample captive portal solution is included with SESM that illustrates all supported types of redirection. The sample solution includes the following applications:

- Captive Portal application—This application handles all TCP redirections from SSG and determines, based on configuration parameters, which other application should handle the request. The Captive Portal application does not provide content to subscribers; rather it issues HTTP redirections to other appropriate portal applications.
- Message Portal application—This application is a sample messaging application. It illustrates an initial greetings page to which the browser is redirected after the subscriber successfully authenticates. The Message Portal application also illustrates timed advertisements. This application is an SESM web portal application, developed using the SESM development components.
- NWSP—The captive portal solution uses pages within the NWSP portal application to illustrate unauthenticated user and unconnected service redirections.

Most deployers will use the captive portal application as installed but provide their own content applications for the HTTP redirections. The content applications can be any web application. When they are SESM web portals, they can use all of the features in the SESM web development kit, including the device and locale awareness features.

See [Chapter 8, “Deploying a Captive Portal Solution,”](#) for more information about captive portal features and how to install and configure the captive portal solution.

## RDP Server

The RADIUS/DESS Proxy (RDP) server is a RADIUS server that can proxy profile requests or use the SPE APIs to query the directory for profiles. RDP acts as the mediator between SSG and the LDAP directory schema extensions. RDP is a required component in the deployment of SESM in LDAP mode.

You can configure the RDP to run in two modes:

- Default mode—In this mode, RDP queries the directory to obtain user authentication and service authorization.

- Proxy mode—In this mode, RDP sends user authentication requests to a specified RADIUS server, rather than to the LDAP directory. This option allows service providers with large RADIUS authentication and accounting services already deployed to continue to use the existing RADIUS database for authenticating users.

This mode does not affect service authorizations. Regardless of the mode, RDP obtains all service authorizations from information in the LDAP directory.

RDP is a Java2 application that uses the services of a JMX server for configuration. It is not a web application and therefore does not run in a J2EE container.

This guide describes how to install and configure RDP. RDP is intended to be used as installed but it is extensible for special purpose deployments. For information, see [Appendix E, “RDP Packet Handlers.”](#)

## CDAT Application

The Cisco Distributed Administration Tool (CDAT) is an administrator’s web-based interface for managing data in the SPE extensions to the LDAP directory. CDAT provides the means for creating and maintaining users, services, user groups, service groups, roles, and policy rules for the RBAC model.

CDAT is a J2EE web application. It runs in a J2EE container and uses the services of a JMX server for configuration.

This guide describes how to install and configure CDAT. For information about using CDAT, creating profiles in the RBAC model, and the SPE directory extensions, see the *Cisco Distributed Administration Tool Guide*.

## Software Bundled with SESM

The SESM installation package provides the following software components in addition to the applications described in the previous section:

- [SPE for LDAP Mode, page 1-8](#)
- [J2EE Components, page 1-9](#)

## SPE for LDAP Mode

When you install the SPE component from the SESM installation package, the 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.

See the *Cisco Distributed Administration Tool Guide* 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.

## J2EE Components

You can install the following items from the SESM installation package:

- Jetty web server—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.com/>

- JSP engine—Jetty includes a Java Server Pages (JSP) package, which is currently the Jasper JSP engine from Apache Software Foundation.
- 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 web server 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. However, SESM is designed to allow the use of any J2EE web server and any JMX-compliant server.



### Note

---

See the [“Port-Bundle Host Key Feature on SSG” section on page 1-10](#) before deploying a J2EE server other than the Jetty server. For SESM Release 3.1(3), the host key feature works only with a Jetty server.

---

### J2EE Server

The SESM portal applications and CDAT are J2EE applications. They require an HTTP listener and must run in a J2EE-compliant server container.

During SESM installation, the sample portal applications and CDAT and their corresponding configuration files and startup scripts are set up to use the Jetty server components from Mort Bay Consulting. If desired, web developers at your site can deploy a J2EE-compliant server other than the Jetty server.

### JMX Server

All of the SESM applications (portals, RDP, and CDAT) require the services of a Java Management Extensions (JMX) server.

The installed sample applications, the configuration files, and the startup scripts are set up to use the Sun example JMX server from Sun Microsystems. The SESM installation program installs the JMX server along with the Jetty server. If desired, web developers at your site can deploy a JMX-compliant server other than the Sun example server.

# Required Network Components

This section describes the network components that are required in an SESM deployment but are not provided by the SESM installation package:

- [Cisco Service Selection Gateway, page 1-10](#)
- [Cisco Access Registrar or Third-Party RADIUS Server, page 1-11](#)
- [LDAP Directory, page 1-11](#)

## Cisco Service Selection Gateway

The Cisco Service Selection Gateway (SSG) is a software feature module embedded in the Cisco IOS broadband release train. The SSG feature can operate in standalone mode to provide Layer 2 service connection support, or it can be configured to work with SESM, which offers enhanced service-related features to subscribers. The SSG runs on a Cisco router or other Cisco device. For a list of Cisco devices currently verified to work with SESM, see the [“SSG Devices” section on page 1-12](#).

An SESM deployment requires the services of SSG. SESM is deployed in an SSG default network. SSG performs authentication and service connection tasks on behalf of an SESM portal application.

### Required Cisco IOS Release

Features in SESM Release 3.1(3) require the SSG embedded in the Cisco IOS Release 12.2(4)B or later. SESM Release 3.1(3) is backward compatible and is verified to work with previously released versions of the Cisco IOS broadband release train containing the SSG feature. For example, an SESM Release 3.1(3) web portal can be deployed with the SSG in Cisco IOS Release 12.1(3)DC running on the Cisco 6400 UAC.

For information about SSG in the Cisco IOS Release 12.2(4)B, see the following documents:

- *SSG Features in Release 12.2(4)B*—The [“Related Documentation” section on page xv](#) provides the URL to the online location of this document.
- Product documentation for the device on which SSG is running.

### Communication Protocol

Regardless of the SESM deployment mode (RADIUS or LDAP), SSG and an SESM web portal application communicate using the RADIUS protocol.

## Port-Bundle Host Key Feature on SSG

The port-bundle host key is an important feature on the SSG that is used for communication between SSG and the SESM portal application. The port-bundle host key feature uses a software token (or key) that *uniquely* identifies each subscriber on the host SSG that is currently logged on to an SESM portal, 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.

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

- 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 port-bundle host key is enabled on the SSG, the SSG preserves the port number of the incoming HTTP request. This remote port number becomes the key that uniquely identifies each subscriber. The key is included in the request that is forwarded to the SESM web application.

The SSG makes the port number available, but the J2EE server must access this information and pass it along to the SESM web application. The Jetty server has been extended to allow access to the request handling part of the server API and thus get the remote port number. It does this with its `PortBundleHandler`. Therefore, the Jetty server is currently the only J2EE-compliant server that can support the port-bundle host key feature.

## Cisco Access Registrar or Third-Party RADIUS Server

The following scenarios require a RADIUS server:

- An SESM portal application deployed in RADIUS mode—This deployment requires user and service profile information in a RADIUS database.
- An SESM portal application deployed in LDAP mode with an RDP running in Proxy Mode—This deployment requires user profiles in a RADIUS database. In Proxy mode, the RDP proxies authentication requests to a RADIUS database. RDP obtains service authorizations through SPE, based on the information in the directory.
- An SESM portal application deployed in either RADIUS or LDAP mode when you want to use the SSG accounting features—For any SESM deployment, you can configure the SSG to generate accounting records and send them to a RADIUS server. The RADIUS accounting features are implemented independently from the RADIUS authentication and authorization features.

SESM works with any RADIUS server that accepts vendor-specific attributes (VSAs). The VSAs define the subscriber and service profile information required in the SESM deployment. The Cisco Access Registrar is a carrier class RADIUS platform that is fully tested with SESM. See the [“Configuring Cisco Access Registrar for SESM Deployments”](#) section on page D-12 for more information about using Cisco Access Registrar in SESM deployments.

Also see the following references for more information about configuring a RADIUS server in an SESM deployment:

- [Appendix D, “Configuring RADIUS”](#)—Describes the Cisco VSAs required in an SESM deployment. It also describes how to configure a RADIUS server for an SESM deployment.
- `demo.txt` file—Contains examples of subscriber and service profiles. This file is a MERIT flat file used by the SESM sample portal applications when they run in Demo mode. The `demo.txt` file is included in your installation directory even if you do not specify demo mode at installation time. You can find `demo.txt` in the `config` directory under each portal directory (for example, `nwsp/config/demo.txt`).

## LDAP Directory

An SESM portal application deployed in LDAP mode requires access to an LDAP-compliant directory. SESM is verified and officially supported to work with the Network Directory Service (NDS) eDirectory Version 8.5 from Novell, Inc. Although initial testing with the iPlanet Directory Server Version 5.0 indicates excellent results, Cisco has not fully verified it in an SESM deployment.

An LDAP directory allows interactive updates, a feature that is not readily supported by a RADIUS server. The LDAP mode uses this update capability to offer SESM features that the RADIUS mode cannot provide, such as:

- Subscriber account self care features—Subscribers can change their account information and see those changes take effect immediately.
- Subscriber self subscription—Subscribers can subscribe to new services and have immediate access to the newly subscribed services.
- Sub-account creation—Subscribers can create sub-accounts to their main account and use the sub-accounts immediately.

## Supported Hardware Platforms

An SESM deployment includes the following hardware platforms:

- [SSG Devices, page 1-12](#)
- [SESM Application Server Devices, page 1-12](#)
- [Subscriber Browser Devices, page 1-13](#)

## SSG Devices

The following devices, when running the Cisco IOS Release 12.2.(4)B or later, with SSG enabled, are verified to work with SESM Release 3.1(3):

- Cisco 6400 Universal Access Concentrator (UAC). Each node route processor (NRP) on the Cisco 6400 UAC runs its own Cisco IOS Software and can be an SSG host device.
- Cisco 7200 Series high-performance multifunction routers
- Cisco 7400 Series Internet routers

## SESM Application Server Devices

This section describes the supported platforms for the SESM applications, which include the web portal applications, the Captive Portal application, RDP, and CDAT.

SESM provides support for applications on any platform that supports the Java Runtime Environment (JRE). Platforms tested in our labs are listed below.

### Solaris

- Sun Ultra10 or Sun E250 (or later version)
- Solaris Version 2.6 (or later version) operating system

### Windows NT

- Pentium III (or equivalent) processor
- Windows NT Version 4.0, Service Pack 5 (or later version)

### Windows 2000

- Pentium III (or equivalent) processor

**Linux**

- Red Hat Linux Version 7.1
- SuSE Linux

## Subscriber Browser Devices

Subscribers can use any type of web browser to access an SESM portal application. However, each web browser and access device has its own limitations, such as differences in display capabilities. Developers of SESM portals must consider the end users of the deployed application and design the application to accommodate the media and browser versions that their subscribers commonly use.

Table 1-1 lists the browsers and devices for which the SESM sample portal applications were designed. The *Cisco Subscriber Edge Services Manager Web Developer Guide* includes information about obtaining and configuring simulators.

**Note**

These browser limitations apply only to the sample applications and are listed to ensure predictable results during demonstrations.

**Table 1-1 Browsers for the SESM Sample Portal Applications**

SESM Portal Application	Device	Other Requirements
NWSP Message Portal	<ul style="list-style-type: none"> <li>• Desktop browsers               <ul style="list-style-type: none"> <li>– Netscape Release 4.x and later</li> <li>– Internet Explorer Release 5.x and later</li> </ul> </li> <li>• WAP devices and simulators</li> <li>• PDA devices and simulators</li> </ul>	<ul style="list-style-type: none"> <li>• Java script enabled</li> </ul>
WAP	WAP devices and simulators	
PDA	PDA devices and simulators	







## Deployment Overview

---

This chapter describes SESM deployment options. It includes the following topics:

- [System Description and Network Diagram, page 2-1](#)
- [SESM in RADIUS Mode, page 2-4](#)
- [SESM in LDAP Mode, page 2-6](#)

## System Description and Network Diagram

This section provides an overview of an SESM deployment and how it fits into a network access provider (NAP) or Internet service provider (ISP) communication network.

### Access Technologies

Subscribers can access the Cisco SESM portal over any access technology, including wireless LAN, fixed wireless, leased line, DSL, and GPRS, with any Web browser on a variety of devices, including Wireless Access Protocol (WAP) phones, personal digital assistants (PDAs), and desktops.

### Default Networks

A *default network* is an IP address or subnet that TCP packets can access without authentication. The SESM web applications and their associated J2EE web servers run in the default network. The default network is configured on the Service Selection Gateway (SSG).

### Service Selection Gateway

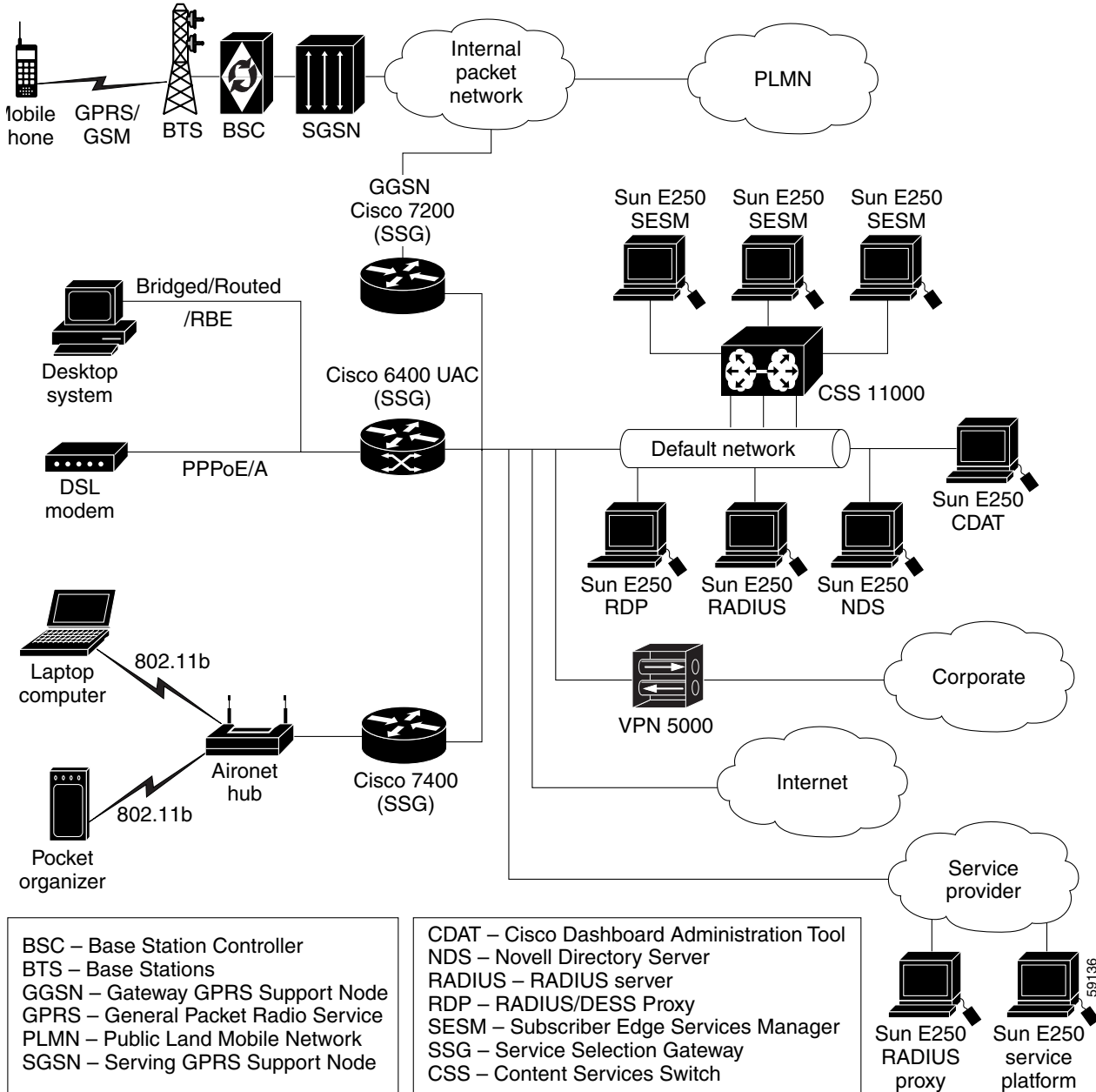
An SESM solution works with the Cisco Service Selection Gateway (SSG), a feature set embedded in the Cisco IOS broadband release train. Some of the devices on which the SSG can run include the Cisco 7200 Series high-performance multifunction router, the Cisco 7400 Series router, and the Cisco 6400 Universal Access Concentrator.

### Network Diagram

[Figure 2-1](#) is a general network diagram showing SESM components, SSGs, and a default network.

Although the figure shows all of the access technologies and three different SSG devices all using the same default network, such a deployment would not be typical. A more typical deployment might consist of several routers of the same type, each one with its own default network. SESM would be deployed on each of the default networks.

Figure 2-1 Network Diagram



### Processing TCP Packets

Regardless of the type of modem or connection layer protocol a subscriber uses, all TCP packets are routed by the SSG when the SSG is enabled. Physically, the TCP traffic passes through the SSG on its way to SESM. Logically the HTTP traffic flows directly to an SESM portal application running on a default network.

J2EE web servers listen for HTTP requests for the SESM portal application. The portal application works with an SSG to establish a session for the user. SESM determines the IP address of the SSG that should handle the session as follows:

- If the host key feature is enabled on the SSG, the SSG's IP address is inserted in the packet.

- If the host key feature is *not* enabled, configuration parameters map client subnets to specific SSGs.

### Scaling and Load Balancing

An SESM web portal application is highly scalable. You can start and stop instances of SESM portal applications without affecting subscribers. This is because an SESM portal application is completely stateless. It does not store any subscriber session information. Rather, the portal application queries SSG for session state information.

Production deployments might include multiple instances of J2EE web servers and associated SESM portals on the default network. For production deployments, we recommend using enterprise-class server systems with hot-swappable components and load-balancing across the multiple servers. The Domain Name System (DNS) resolves host names for any of the SESM portal applications to the IP address of the load balancer. The Cisco Content Services Switch 11000 (CSS 11000) is preferred for load balancing.

## Connection Examples

This section provides some examples of how a subscriber gains access to an SESM portal application.

### Point-to-Point Protocol Example

This example describes the connection sequence for Point-to-Point Protocol (PPP) access to SESM. For example, consider a DSL subscriber using a PPP client configured on a laptop computer.

1. The subscriber launches the PPP client.
2. The TCP packet travels to a Cisco router device which has SSG enabled.
3. The SSG authenticates the PPP user.
4. The subscriber launches a web browser and sends an HTTP message.
  - If the SSG TCP unauthenticated user redirect feature is configured, the subscriber can use any URL and will be automatically redirected to the SESM portal application. If the SESM captive portal feature is configured, the subscriber could be redirected back to the original URL after being authenticated.
  - If the SSG TCP unauthenticated user redirect is not configured, the subscriber must use the URL for the SESM portal application.
5. The TCP packet containing the first HTTP request travels through the SSG to the SSG's default network, and then to the J2EE web server and the SESM portal application.
6. If the SESM single sign-on feature for PPP subscribers is enabled, the user is already authenticated and SESM does not request an additional authentication. Rather, SESM queries the SSG for the subscriber's cached profile. A session is established, and SESM returns the subscriber's home page with a list of authorized services.
7. If the SESM single sign-on feature is disabled, SESM returns the SESM logon page. When this request reaches an SESM web application, the application requests authentication services from the SSG. After the subscriber is authenticated, an SESM session is established.

**Routed Example**

This example describes the connection sequence for routed access to SESM. For example, consider a subscriber using a WAP-enabled phone configured for access through a WLAN access point.

1. The subscriber launches a web browser and sends an HTTP message.
  - If the SSG TCP unauthenticated user redirect feature is configured, the subscriber can use any URL and will be automatically redirected to the SESM portal application. If the SESM captive portal feature is also configured, the subscriber could be redirected back to the original URL after being authenticated.
  - If the SSG TCP unauthenticated user redirect feature is not configured, the subscriber must use the URL for the SESM portal application.
2. The TCP packet containing the first HTTP request travels through the SSG, to the SSG's default network, and then to the J2EE web server and the SESM portal application.
3. The SESM portal application returns the SESM logon page.
4. When the SESM portal application receives the subscriber's logon information, it requests authentication services from the SSG. After the subscriber is authenticated, an SESM session is established.

## SESM in RADIUS Mode

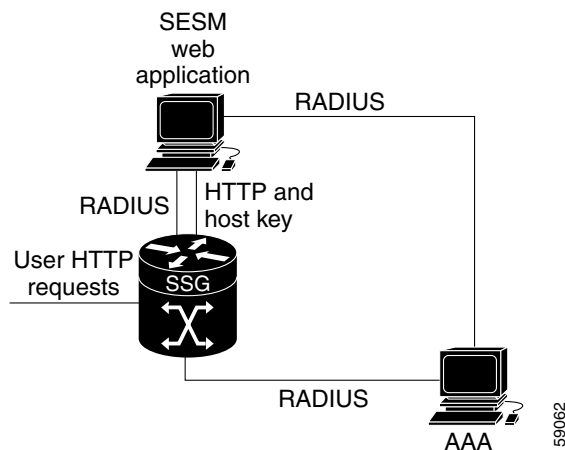
This section describes an SESM deployment in RADIUS mode. It includes the following topics:

- [Component Diagram for RADIUS Mode, page 2-4](#)
- [Processing a Subscriber Request in RADIUS Mode, page 2-5](#)
- [Installation and Configuration Requirements for RADIUS Mode, page 2-6](#)

## Component Diagram for RADIUS Mode

Figure 2-2 shows a simplified view of the SESM deployed in RADIUS mode and the communication mechanisms used between the various software components.

**Figure 2-2** *SESM Deployed in RADIUS Mode*



SSG and the SESM portal application work together to process subscriber requests.

1. SSG authenticates a subscriber based on a subscriber profile stored in the AAA server.
2. The SESM portal application obtains the list of authorized services for a subscriber from the subscriber profile in the AAA server.
3. After the subscriber selects a service, SSG makes the connection to the service based on information in service profiles stored in the AAA server.
4. If the subscriber profile indicates automatic connections for some services, SSG makes the connection to those services immediately after authentication, rather than waiting for the subscriber to select the service from the SESM portal.

## Processing a Subscriber Request in RADIUS Mode

Table 2-1 describes the roles of an SESM portal application and SSG in processing typical subscriber actions in a RADIUS deployment.

**Table 2-1 Role of Components in a RADIUS Deployment**

Subscriber Action	Software Activity	Components Involved
Subscriber logs on	Authenticate the subscriber in the system.	The SESM portal initiates authentication by sending a message to SSG, using the RADIUS protocol. SSG forwards the RADIUS message to the RADIUS server. The RADIUS server authenticates the subscriber and returns a message containing information from the subscriber profile.  SSG creates an internal host object that represents the subscriber in the current session and forwards the message to the SESM portal.
	Display web interface containing customized content appropriate for the logged on subscriber.	The RADIUS message contains the subscriber profile as stored in the RADIUS database. The SESM portal can analyze the subscriber profile and send appropriate content accordingly.
	Display the list of services that the subscriber is currently authorized to access.	The RADIUS message contains the list of services from the subscriber profile. Authorization is implied for all services in the list.  The SESM portal obtains a service profile directly from the RADIUS server for each service in the list.
Subscriber selects a service	Access the service.	The SESM portal sends a connection request to SSG.  SSG creates a connection object, connecting the host object to the service. When the service is connected, SSG creates a service object. SSG then switches traffic from that subscriber to the requested service.
Subscriber selects a second service	Access a second service, without reauthentication.	The SESM portal sends the request to the SSG.  SSG creates a second connection object and service object. Both services are concurrently accessed.
Subscriber deselects a service	Stop access to the service.	The SESM portal sends the request to the SSG.  SSG destroys the appropriate connection object.

## Installation and Configuration Requirements for RADIUS Mode

Table 2-2 summarizes the steps required to deploy the SESM in RADIUS mode.

**Table 2-2 Configuration Requirements for SESM in RADIUS Mode**

Deployment Step	References
1. Install and configure a RADIUS AAA server.	<a href="#">Appendix D, “Configuring RADIUS”</a> and documentation from the RADIUS server vendor
2. Ensure that the SSG host device is running an appropriate Cisco IOS software release. For SESM Release 3.1(3), this is Cisco IOS Release 12.2(4)B or later.	SSG documentation <sup>1</sup>
3. Configure SSG. Use Cisco IOS commands on the SSG host device to: <ul style="list-style-type: none"> <li>– Configure SSG to listen for SESM requests.</li> <li>– Enable or disable the host key mechanism.</li> <li>– Set up SSG-to-RADIUS communication.</li> <li>– Configure security, routing, and other services provided by SSG.</li> <li>– Configure SSG TCP redirect features (optional)</li> </ul>	<a href="#">Appendix B, “Configuring the SSG”</a> SSG documentation <sup>1</sup>
4. Install and configure the SESM portal application and J2EE-compliant web server.	<a href="#">Chapter 5, “Installing Components”</a>
5. Create user and service profiles in the RADIUS database.	<a href="#">Appendix D, “Configuring RADIUS”</a> and documentation from the RADIUS server vendor

1. See the “[Related Documentation](#)” section on page xv for a link to the online version of SSG documentation.

## SESM in LDAP Mode

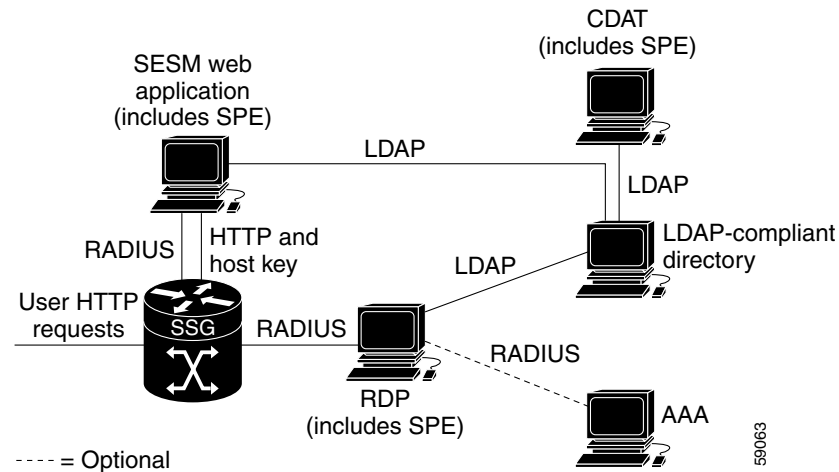
This section describes an SESM deployment in LDAP mode. It includes the following sections:

- [Component Diagram for LDAP Mode, page 2-7](#)
- [Processing a Subscriber Request in LDAP Mode, page 2-8](#)
- [Installation and Configuration Requirements for LDAP Mode, page 2-9](#)

## Component Diagram for LDAP Mode

Figure 2-3 shows a simplified view of the SESM deployed in LDAP mode and the communication mechanisms used between the various software components.

Figure 2-3 SESM Deployed in LDAP Mode



The optional AAA server might provide the following services:

- Accounting services
- User authentication services when RDP is configured in Proxy mode

In an LDAP mode deployment, the Cisco Subscriber Policy Engine (SPE) Version 1.01 provides services to the SESM portal application, CDAT, and RDP. To install SPE services, install the LDAP component from the SESM installation package. This guide describes how to install and configure SPE to work with SESM components.

For more information about SPE, including its logical relationship to SESM components, see the [“Introduction to Cisco SPE”](#) section on page 1-3.

## Processing a Subscriber Request in LDAP Mode

Table 2-3 describes the role of the SESM applications and SSG in processing typical subscriber actions in an LDAP deployment.

**Table 2-3** Role of Components in an LDAP Deployment

Subscriber Action	Software Activity	Components Involved
Subscriber logs on	Authenticate the user in the system.	<p>The SESM portal application initiates authentication by sending a RADIUS message to SSG. SSG forwards the RADIUS message to the RDP. The RDP can authenticate using RADIUS or the LDAP directory, depending on how the RDP is configured:</p> <ul style="list-style-type: none"> <li>• If RDP is configured in proxy mode, it forwards the message to a RADIUS server.</li> <li>• Otherwise, RDP uses the SPE application programming interface (API) to forward the authentication request to the LDAP directory.</li> </ul> <p>The response is returned to the SESM portal application following the same path as described above.</p> <p>SSG creates an internal host object that represents the subscriber in the current session.</p>
	Display appropriate web pages to user.	After the subscriber is authenticated, the SESM portal application uses the SPE API to retrieve a subscriber profile from the LDAP directory. The SESM portal can analyze the profile and display appropriate web pages.
	Display the list of services in the subscriber's profile.	The SESM portal application uses the SPE API to retrieve service profiles from the LDAP directory for each service in the list.
Subscriber selects a service	Access the service.	<p>SSG sends an authorization request to RDP. Regardless of the RDP mode, RDP always uses the SPE API to send service authorization requests to the LDAP directory.</p> <p>If the service is authorized, SSG creates an internal connection object, connecting the host object to the service. When the service is connected, SSG creates a service object. SSG then switches traffic from that subscriber to the requested service.</p>
Subscriber selects a second service	Access a second service without reauthentication.	<p>SSG sends another authorization request to RDP. Regardless of its mode, RDP always uses the SPE API to send service authorization requests to the LDAP directory.</p> <p>If the service is authorized, SSG creates a second connection object and service object. Both services are concurrently accessed.</p>
Subscriber updates an e-mail address	Update the LDAP directory.	The SESM portal application sends the update to the directory using the SPE API.
Subscriber creates a subaccount	Update the LDAP directory.	The SESM portal application sends the update to the directory using the SPE API.
Subscriber deselects a service	Terminate access to the service.	The SESM portal application sends the request to the SSG. SSG destroys the appropriate connection object.



## Installation and Configuration Requirements for LDAP Mode

Table 2-4 summarizes the installation and configuration activities for SESM in LDAP mode.

**Table 2-4 Configuration Requirements for SESM in LDAP Mode**

Activity	Reference
<ol style="list-style-type: none"> <li>1. (Optional) Install and configure a RADIUS server if:               <ul style="list-style-type: none"> <li>– You want to run RDP in Proxy mode so that it can authenticate subscribers using profiles in a RADIUS server, rather than in the directory. This option allows you to use existing RADIUS subscriber profiles, rather than creating the information on the LDAP directory. (Service authorizations still occur using information in the directory.)</li> <li>– You want to use SSG accounting features.</li> </ul> </li> </ol>	<p><a href="#">Appendix D, “Configuring RADIUS”</a> and documentation from the RADIUS server vendor</p>
<ol style="list-style-type: none"> <li>2. Ensure that the SSG host device is running an appropriate Cisco IOS software release. For SESM Release 3.1(3), this is Cisco IOS Release 12.2(4)B or later.</li> </ol>	<p>SSG documentation<sup>1</sup></p>
<ol style="list-style-type: none"> <li>3. Configure SSG. Use Cisco IOS commands on the SSG host device to:               <ul style="list-style-type: none"> <li>– Configure SSG to listen for SESM requests.</li> <li>– Set up SSG to RADIUS communication.</li> <li>– Enable the host key mechanism.</li> <li>– Configure security, routing, and other services provided by SSG.</li> <li>– Configure SSG TCP redirect features (optional).</li> </ul> </li> </ol>	<p><a href="#">Appendix B, “Configuring the SSG.”</a> SSG documentation<sup>1</sup></p>
<ol style="list-style-type: none"> <li>4. Install and configure an LDAP directory.</li> </ol>	<p><a href="#">LDAP Directory Configuration Requirements, page 5-4</a> Documentation from the directory vendor</p>
<ol style="list-style-type: none"> <li>5. Install and configure the SESM software components, which include: the SESM portal application, a J2EE-compliant web server, RDP, SPE, and CDAT.</li> </ol>	<p><a href="#">Chapter 5, “Installing Components”</a></p>
<ol style="list-style-type: none"> <li>6. Load sample data and create roles, groups, and user and service profiles in the LDAP directory.</li> </ol>	<p><i>Cisco Distributed Administration Tool Guide</i></p>

1. See the “[Related Documentation](#)” section on [page xv](#) for a link to the online version of SSG documents.





## Feature Descriptions

---

This chapter describes the features in the Cisco Subscriber Edge Services Manager (SESM). The topics in this chapter are:

- [Web Portal for Subscribers, page 3-1](#)
- [Authentication Options, page 3-2](#)
- [Service Selection and Connection, page 3-4](#)
- [Features in SESM-SPE, page 3-7](#)
- [Captive Portal Features, page 3-8](#)
- [Enhanced Session Management with Port-Bundle Host Key, page 3-9](#)
- [Location Awareness, page 3-10](#)
- [Brand Awareness, page 3-10](#)
- [Web Development Features, page 3-11](#)
- [Scaling, Redundancy, and Resiliency Features, page 3-12](#)
- [Accounting and Billing Interfaces, page 3-12](#)

## Web Portal for Subscribers

This section describes the key features that are visible to subscribers who access an SESM web portal.

### Subscriber Features

An SESM web portal provides the web interface from which subscribers can:

- **Authenticate**—The SESM portal provides a logon window for subscribers.
- **Select one or more services for connection**—The SESM portal presents a list of subscribed services based on the subscriber profile. The subscriber connects to services by selecting them from the list. If appropriate, SESM can display a service logon page.
- **Disconnect from services**—Subscribers can disconnect from a single service, or by logging off of SESM, disconnect from all services.
- **View session status information**—Subscribers can see which services are active in their current session and view other session status information.

When SESM is deployed in LDAP mode, the following additional capabilities can be offered to subscribers:

- Change account information
- Self-subscribe to services
- Create subaccounts on a main account

## Customized and Branded Web Portal

A web designer can customize the look and feel of the SESM web portal to conform to the brand identity required by the deployer. Customization includes the ability to have a different appearance for separate user groups, locations, access devices, services, and other subscriber connection attributes.

## Personalized Subscriber Experiences

An SESM web portal can be personalized such that each subscriber sees pages appropriate to his or her usage, access type, and preferences. Some of the features that provide for a personalized subscriber experience are:

- **Subscribed Services**—The service selection feature presents a personalized list of subscribed services for each subscriber. This information is obtained from the subscriber profile.
- **Device, Locale, and Brand awareness**—The awareness features choose the appropriate resources to use in shaping the pages that are returned to the subscriber's browser.
- **Self-management features**—The self-management features available in LDAP mode allow the subscriber to control account information.
- **Advertisements**—The captive portal feature can deliver advertisement content that is directed at subscriber interests identified in the profile (LDAP mode only) or based on currently subscribed services.
- **Personal options**—Some options within a subscriber profile offer further personalization. For example, you can specify a home URL for Internet connections. Another option allows automatic connections to specified services on a per subscriber basis.

## Authentication Options

Subscribers must authenticate by logging on to the SESM portal before they can select and connect to services. (The exception is open garden services that might be configured on the SSG.)

SESM passes the credentials to the SSG in a RADIUS protocol format. A RADIUS server performs the verification procedures. In LDAP mode, the RADIUS server is the SESM RDP server. The RADIUS server verifies against attribute values stored in the subscriber profile.

SESM supports the following authentication schemes:

- [2-Key Authentication, page 3-3](#)
- [3-Key Authentication, page 3-3](#)
- [Single Sign-on for PPP Clients, page 3-4](#)
- [Single Sign-on for non-PPP Clients, page 3-4](#)

## 2-Key Authentication

The 2-key authentication method bases authentication against the following attributes stored in the subscriber profile:

- User name
- Password

The sample SESM portal applications display a logon page that prompts for the two values listed above. SESM passes these values to SSG as standard RADIUS protocol attributes.

## 3-Key Authentication

Deployments in wireless environments might require authentication based on attributes in addition to user name and password. For example, authentication could be based on the following attributes:

- User name
- Password
- A third attribute, such as:
  - Access point name (APN)—This is RADIUS attribute 30, CALLED\_STATION\_ID. This might be a GGSN.
  - MSISDN—This is RADIUS attribute 31, CALLING\_STATION\_ID. This might be the subscriber's MSISDN or telephone number.
  - Subscriber's telephone number—SESM supports authentication against a telephone number by putting the phone number in the RADIUS attribute 31, CALLING\_STATION\_ID field.
  - Network access server (NAS) identifier—This is attribute 32, NAS\_IDENTIFIER. In SESM deployments, the SSG is the NAS.

A web developer can customize an SESM web portal to use a logon page that prompts for telephone number in addition to user name and password. A sample 3-key logon page is included in the SESM web developer kit. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information. SESM passes the telephone number to SSG as standard RADIUS attribute 31, CALLING\_STATION\_ID. If no value is supplied on the login page, SESM inserts the user name in this field.

The SESM web developer kit does not offer a way to collect an APN or NAS identifier and send it to SSG. SSG includes this support. See the SSG documentation for details.

To implement 3-key authentication:

- If SESM is deployed in RADIUS mode, business logic to verify against three keys must exist in the RADIUS server you are using. See the RADIUS server vendor.
- If SESM is deployed in LDAP mode, you can configure the RDP Server to perform 3-key authentication using any number and any combination of standard RADIUS attributes.

In an LDAP directory, administrators can enter the APN and NAS identifier attributes as group values. See the *Cisco Distributed Administration Tool Guide* for more information.

## Single Sign-on for PPP Clients

The single sign-on feature removes the requirement for point-to-point protocol (PPP) clients to enter authentication details twice. When single sign-on is enabled, the SESM portal does not ask a PPP subscriber to authenticate (log on). Instead, the SESM portal uses the PPP authenticated identity from SSG.

## Single Sign-on for non-PPP Clients

The single sign-on feature also has meaning for non-PPP subscribers. With single sign-on, if any subscriber authenticates using the SESM web portal, that subscriber does not need to sign on again for the duration of the session. The session exists as long as SSG still has a host object for it. This feature has advantages for subscribers in the following situations:

- The subscriber can stop the browser or navigate away from the SESM portal pages, and then return to the SESM pages later and not be required to reauthenticate.
- The subscriber does not need to reauthenticate if SESM automatic memory management clears sessions from the SESM portal.

## Service Selection and Connection

The SESM portal application presents a service list from which the subscriber can select one or more services for connection. The connection features are implemented by SSG and controlled by attributes stored in the subscriber or service profiles.

### Service Selection

After a subscriber authenticates, the SESM portal application displays subscribed services obtained from the subscriber profile. From the list of displayed services, the subscriber selects one or more services for connection. The portal can also display service groups, as defined in service group profiles. The web developer controls the format of the service list and how to portray service groups.

### Service Authentication and Authorization

A preliminary level of service authorization is implied by the service selection list presented to a subscriber. The SESM portal presents for selection only those services to which a subscriber is subscribed, according to the subscriber profile. In LDAP mode, when a subscriber self-subscribes to a new service, that service is added to the subscriber profile and immediate access to that service is possible.

The SESM web portal can present a service authentication page for services that require it. Service authentication can be based on user name and password. For proxy services, an option in the service profile specifies whether the CHAP or PAP protocol is used to authenticate for the service.

## Automatic Connections

With automatic connection, the subscriber gains access to a service immediately after authenticating, without manually selecting the service from the SESM portal. Depending on configuration options, either SSG or SESM performs the connection immediately after the subscriber authenticates.

A service is marked as an autoconnect service in the subscriber profile. By default, an autoconnect service is hidden from the service list on the service selection page, but another option in the subscriber profile can specify that it be included in the list. In LDAP mode, the SESM portal application can offer the subscriber the means to self-select or change the services that should be automatically connected.

Providers can use the automatic connection option as a way to provide always-on services or as a way to bypass the service selection feature. For example, a provider might choose to offer three always-on services to all subscribers, and mark those services as autoconnected in all subscriber profiles. If these are the only services offered by the provider, and the profiles indicate that they are hidden from the service selection list, the web portal could be customized to omit the service selection page.

## Service Status

Information about services that were connected during the current session can be displayed in an SESM web portal. The web developer controls the types of information that are displayed on the status page and how it is presented. See the *Subscriber Edge Services Manager Web Developer Guide* for more information.

You can see a sample status page in the NWSP application. The sample page shows the following information about all connected services (including automatically connected services) during the current session:

- Currently connected services
- Services that were connected during the session but are currently not connected
- Connection length of time (for both current and previously connected services)
- Transmitted and received byte count on a per service basis

The SESM web developer kit provides a way to link images to a service status for display on the portal pages. For example, the NWSP uses the following images:

- No light—Indicates that the service is not selected for connection
- Red light—Indicates an unconnected service
- Green light—Indicates a connected service

## Mutually Exclusive Service Selection

Mutually exclusive service selection restricts a subscriber to accessing only one service at a time in a specified group of services. One use of this feature is described in the [“Service Selection by Bandwidth” section on page 3-6](#).

A service group is a collection of services defined in a service group profile. A subscription to a service group implies subscription to all of the services in the group. It also implies the ability to select all of the services in the group. When a group is defined as mutually exclusive, SESM limits service selection to one service at a time within the group.

An SESM configuration option controls the SESM action when a subscriber is already logged into one service and then selects another service in the group:

- SESM can automatically request SSG to disconnect the first service and connect the new service.
- SESM can prompt the subscriber to log off the first service. After the subscriber logs off, SESM requests the connection to the other service.

**Note**


---

SESM waits for the first service to be disconnected before requesting connection to the new service. If the connection to the new service fails, the subscriber is not connected to either service.

---

A mutually exclusive service group is defined in a service group profile. For RADIUS mode deployments, see [Appendix D, “Configuring RADIUS,”](#) for more information. For LDAP mode deployments, see the *Cisco Distributed Administration Tool Guide*.

## Service Selection by Bandwidth

An SESM web portal can support the SSG hierarchical policing feature in Cisco IOS Release 12.2(4)B by allowing subscribers to choose a different bandwidth from their regularly subscribed bandwidth for a particular service. For example, a subscriber might be subscribed to an Internet or video service with a 128-Kbps bandwidth, but have the option to select 512 Kbps or 1 Mbps service on demand.

To implement this feature, define the bandwidth options for each service as separate and mutually exclusive services within a service group. This restriction is important to prevent subscribers from simultaneously connecting to (and being billed for) the same service over two different bandwidths.

## Supported Service Types

The service type is one of the attributes in a service profile. Service type is known as service class in service profiles on an LDAP directory.

SESM can support a wide range of service types. In general, SESM supports the service types that are supported by the other elements in the network, such as the SSG.

In Cisco IOS Release 12.2(4)B, the SSG supports the following types of service:

- Passthrough—The SSG can forward traffic through any interface using normal routing or a next-hop table. Passthrough service is ideal for standard Internet access.
- Proxy—When a subscriber selects a proxy service, the SESM portal prompts for another user name and password. After authentication, the service is accessible until the user logs out from the service, logs out from the SESM portal, or is timed out.
- Tunnel—When a subscriber selects a tunnel service, SESM determines if the SSG single host logon feature is configured and if the subscription has the credentials for the service connection. If both conditions are true, SESM sends a connection request. Otherwise, SESM displays an authentication page to obtain service connection credentials from the subscriber.



## Features in SESM-SPE

These features are implemented by the SPE component and are therefore available only when SESM is deployed in LDAP mode. To implement these features, you must install and configure SESM in LDAP mode, and populate the LDAP directory with valid subscriber information.

For more information about these features, see the following:

- The *Cisco Distributed Administration Tool Guide* describes how to provision a subscriber with the appropriate permission to perform these tasks.
- The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes how to implement these features in an SESM web portal.

## Subscriber Account Self-Management

Subscriber account self management allows subscribers to change their own account details, such as address information, phone numbers, passwords for account authentication, and credentials for proxy and tunnel service authentications. (Passwords are encrypted.) This subscriber updating capability relieves the service provider from time-consuming maintenance tasks.

## Subscriber Service Self-Subscription

Self-subscription allows subscribers to sign up for new services and have immediate access to those services. This feature relieves the service provider from time-consuming service enrollment tasks. It also benefits the subscriber because there is no delay in receiving access to a new service. Subscribers can also unsubscribe from a service.

## Subscriber Subaccount Creation and Management

Subscriber subaccount creation and management allows a subscriber with a main account to create subaccounts, with different services and access information in each subaccount. For example, a family might have subaccounts for each family member, with a different set of authorized services within each subaccount. The main account can create and delete subaccounts and subscribe to services for the subaccounts, and control whether the subaccounts can subscribe to services themselves.

The service provider can impose limits on the number of subaccounts in a main account. This feature allows providers to sell accounts of differing sizes. It also prevents pranksters from creating an endless number of subaccounts.

## Extended Subscriber Profile Data

SESM in LDAP mode supports many of the fields in the X.500 standard user schema developed for use with LDAP. Some of the fields supported include date of birth, various address and telephone number fields, e-mail, gender, and hobbies. These additional user data fields can optionally be included in a subscriber profile. The information can be maintained by the deployer using CDAT or by the subscriber using the self-management features in the SESM portal.

## Role Based Access Control

Role based access control (RBAC) is an access model that defines access privileges for roles, rather than for individuals, and then assigns individuals to a role. The Cisco implementation extends the model, allowing administrators to manage groups of subscribers, rather than individuals. Using this group-based 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.

The RBAC model applies to data stored in an LDAP directory using the SPE extensions that are delivered as part of the SESM LDAP mode installation. Administrators use the Cisco Distributed Administration Tool (CDAT) to enter and manage the RBAC data in the directory.

See the *Cisco Distributed Administration Tool Guide* for more information about RBAC.

## Captive Portal Features

The SESM captive portal solution works with the TCP redirect features on the SSG to provide several types of subscriber captivation. With captivation, a subscriber's request is captured and handled in an appropriate manner.

The SSG TCP redirect feature redirects incoming TCP packets to a specified SESM captive portal application. The captive portal application issues an HTTP redirection to the subscriber's browser, directing it to another application that returns content to the subscriber. These content applications can be SESM web portals that enforce account authentication and service authorizations or present advertising and message pages.

The following sections briefly describe the types of TCP redirection and captivation supported by the SSG in Cisco IOS Release 12.2(4)B and SESM Release 3.1(3). For more information about captive portal features, configuration details, and corresponding SSG TCP redirect requirements, see [Chapter 8, "Deploying a Captive Portal Solution."](#)

## Unauthenticated User Captivation

Unauthenticated subscribers are those who have submitted an HTTP request when there is no host object on the SSG. A host object exists only after successful authentication. This situation occurs when the subscriber opens a browser and issues a request (or has a home page setting) to a location other than an SESM logon page. Unauthenticated subscriber captivation in a wireless LAN allows unauthenticated access to the LAN but then requires the subscriber to authenticate before accessing the Internet or other services.

The SSG TCP redirect feature redirects unauthenticated packets to the captive portal application. The SESM captive portal solution can redirect the browser to the login page of an SESM web portal. The captive portal solution can also preserve the originally requested service location and redirect again to connect the subscriber to it.

One effect of deploying unauthenticated subscriber redirections is that subscribers do not need to know the URL to the SESM logon page because they are sent there automatically when they start a browser session. Also, after authenticating, they can be redirected to a home page URL or a service address.

## Unconnected Service Captivation

Service redirection handles requests to service domains to which the subscriber has not yet connected. Rather than rejecting these requests, the SSG TCP redirect feature can redirect them to an SESM captive portal application, which can then handle the request in an appropriate way to gain connection or present some explanation to the subscriber.

Some examples of how an SESM captive portal solution can support service captivations are:

- When a subscriber is not authenticated for a service, the captive portal solution can present a service logon page or perform the authentication on behalf of the subscriber.
- When the subscriber is not subscribed to a service, the captive portal solution can present a subscription page.
- When service connection is refused because of lack of funds, the captive portal solution can present an explanation. See the [“Prepaid Services” section on page 3-13](#) for more information.

## Initial Logon Captivation

Initial logon captivation presents all subscribers with a message or greetings page. The TCP redirect feature redirects all authenticated subscribers to the captive portal application. The captive portal solution can present any type of message for a specified length of time, after which the browser is redirected again to the originally requested service, or to an SESM service selection page, or to an automatically connected service.

## Advertisement Captivation

Advertisement captivation presents advertisements at specified intervals for specified durations. The TCP redirect feature handles the interval timer and redirects the next TCP packet originating from the subscriber to the captive portal application. The captive portal solution presents the advertisement content. The captive portal solution can also present service-specific advertisements by identifying the service name or service URL that is being requested, and presenting advertisements appropriate to users of the service.

## Enhanced Session Management with Port-Bundle Host Key

The port-bundle host key feature on the SSG ensures that each currently logged-on subscriber is uniquely identified, regardless of the IP address being used. This is an optional feature, but when enabled, it allows SESM portals to support the following types of subscribers:

- Overlapping IP addresses in PPP and bridged environments—SESM can differentiate between various subscribers using the same IP address.
- Nonroutable subscriber IP addresses—SESM can support subscribers at sites using private IP addressing schemes, including subscribers of ISPs using private addressing schemes.

The SSG port-bundle host key feature also enhances configuration of large SESM deployments. With port-bundle host key, you do not need to map client subnets to SSGs.

# Location Awareness

An SESM portal can derive the location of the subscriber and present different retail pages or different elements within a page based on location. SESM offers several ways to determine location.

## Location Awareness Based on Configuration

In the portal MBean configuration file, you can add entries that associate a location with known configuration attributes, such as:

- SSG IP address—This method assumes that all requests to a particular range of SSG IP addresses are located in the same area.
- Client subnet—This method assumes that all requests from a particular range of client addresses are located in the same area.



**Note** The port-bundle host key feature obscures the client subnet. When the SSGs are configured to use port-bundle host key, infer location from the SSG IP address rather than the client subnet.

## Location Awareness Based on Attributes in the HTTP Request

You can customize an SESM portal to derive the location from attributes in the subscriber's original HTTP request. The SESM web development kit includes a location attribute.

# Brand Awareness

An SESM portal can derive the brand of the subscriber and present different retail pages or different elements within a page based on brand. SESM offers several ways to determine brand.

## Brand Awareness Based on Subscriber Groups

You can use subscriber groups to represent brands. The group is an attribute of a subscriber profile. The SESM portal detects the branding for a subscriber based on the group in which that subscriber is assigned and returns pages appropriate to the brand of that group.



**Note** Subscriber groups are known as user groups in CDAT and the RADIUS profiles.

An SESM portal can implement differences among branded groups in many ways, including:

- Each brand could have different subscriber privileges.
- Each brand could have different subscribed and available services.
- Each brand could have different looks to the browser pages, such as different colors or different menu options.

The sample data installed with SESM defines three subscriber groups for branding purposes: bronze, silver, and gold groups. The sample data also defines one user for each of these groups: bronzeuser, silveruser, and golduser. To illustrate branding possibilities, PDA uses a different look and different colors for each brand. NWSP uses different menu options.

### Brand Awareness Based on Configuration

You can add entries to the portal's MBean configuration file that associate a brand with the SSG IP address or client subnet, as described in the [“Location Awareness Based on Configuration”](#) section above.

## Web Development Features

The SESM web development kit includes technologies and development features for customizing an SESM web portal. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for detailed descriptions of the following and additional web development features.

### Localization and Internationalization

Web developers can use the following techniques to localize and internationalize an SESM web portal.

- An SESM web portal can use conventional Java techniques for internationalization and localization.
- SESM includes additional development components that improve upon the standard Java locale-related classes and help reduce the complexity of localizing an SESM web application. Some localization subjects addressed by the SESM components are: time zone, language, and preferred formats for currency, numbers, dates, and times.
- Resource bundles contain locale-specific data that varies depending on the user's language and region, such as translatable text for status and error messages and for labels on GUI elements. The developer can add additional resource bundles to a web application to accommodate new locales.

### Java Server Pages

JSPs provide a standard way to integrate Java code with HTML, XML, and WML. The SESM portal and captive portal applications use JSPs to present interactive, dynamically updated, personalized, and branded web pages to subscribers.

The JSP pages contain the elements that the developer modifies for the specific requirements of the provider. No servlet programming is required.

### SESM User Shape Mechanism

The SESM user shape mechanism is a method for combining any number of subscriber attributes to determine which resources to use in the JSP returned to a subscriber. This mechanism eases the task of adding more attributes to the decision.

### Locale and Device Awareness

The SESM portal detects information about a subscriber from the header of the initial HTTP request. For example:

- The subscriber's preferred language setting in the browser sets the locale.
- Information about the access device, browser type, and the connection location is available from the header.

The portal developer can use one or all of these attributes in the user shape to determine the look and feel of the JSP returned to the subscriber's browser. For example:

- If the subscriber's browser language is French and the receiving device is a desktop PC, the response can be rendered in French using HTML.
- If another subscriber's browser language is Spanish and the receiving device is a WAP cell phone, the response can be rendered in Spanish using Wireless Markup Language (WML).

## Library Resources

The SESM development components include Dreamweaver templates and library items.

Dreamweaver templates can be very useful for customizing or maintaining a web application's JSP pages when many pages have the same layout. By modifying a template and then updating the JSP pages that use the template, you can change the look and feel of an entire set of pages very quickly.

Dreamweaver library items contain Body elements such as images, text, and other objects that are reused throughout the JSP pages. Each sample SESM web application includes a complete set of customizable images, buttons, and a navigation bar.

## Scaling, Redundancy, and Resiliency Features

An SESM web portal offers the following scaling, redundancy, and resiliency features:

- You can deploy multiple instances of the same SESM web portal and balance the load as you would with any web server application. The Cisco Content Services Switch 11000 is recommended for load balancing.
- The SSG port-bundle host key feature simplifies large deployments because it eliminates manual mapping of subscriber subnets to SSGs.
- SESM applications are highly resilient because they are completely stateless regarding subscriber sessions. SESM applications obtain session status information from the SSG. Therefore, the SESM applications can be started and stopped without affecting a subscriber.

For more information about scaling and redundancy in an SESM deployment, see the following:

- Vendor documentation for the load balancing tool.
- The [“Memory Requirements and CPU Utilization”](#) section on page 7-8 shows memory usage requirements for an SESM web portal application.
- *SSG Features in Release 12.2(4)B* describes how to configure the port-bundle host key feature on the SSG.

## Accounting and Billing Interfaces

The accounting and billing solutions that work with an SSG/SESM deployment are based on actual services used and the duration of use. These interfaces are implemented and configured on the SSG.

## RADIUS Accounting

SSG can be configured to send accounting requests to a RADIUS server. The RADIUS server generates the accounting records. See the [“Configuring the RADIUS Accounting Feature”](#) section on page D-11 for a summary of how to configure this solution.

## Prepaid Services

The SSG Prepaid feature in Cisco IOS Release 12.2(4)B and later supports an interface to a third-party billing server. The third-party server performs billing and accounting functions, which can include prepaid services features. See *SSG Features in Release 12.2(4)B* for more information about the SSG Prepaid feature.

### Enhancing Prepaid Services Using SESM Captive Portal

The SESM captive portal features can be used in conjunction with the SSG prepaid feature to enhance the subscriber’s experience in a prepaid business model. When service connection is refused or a current session is disconnected because of lack of funds, the SESM captive portal solution can display a message page to the subscriber explaining the reasons for the service refusal.

In a prepaid services business model, service connection is denied (unauthorized) if there are no funds in the subscriber’s account. The SSG Prepaid feature allows SSG to check a subscriber’s available credit to determine whether to connect the subscriber to a service and how long the connection can last. The SSG Prepaid feature also supports reauthorizations after connection is granted. If funds are depleted for the account, SSG logs the subscriber off the service.







## Demo Quick Start

---

This chapter describes procedures for installing and running the New World Service Provider (NWSP) application in Demo mode. The chapter includes the following topics:

- [Introduction, page 4-1](#)
- [Installation Instructions for Demo Mode, page 4-2](#)
- [Browsers, page 4-4](#)
- [Running the SESM Demo, page 4-5](#)
- [Demo Data File, page 4-6](#)

## Introduction

SESM Demo mode has two purposes:

- It lets you demonstrate the capabilities of SESM when other required network components, such as SSG, are not available.
- It is a valuable tool for developers of SESM web applications. Using Demo mode, developers can quickly test the customizations they make to an SESM application. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about using Demo mode during application development.

To prepare for using the Demo mode, you can either:

- Install SESM in Demo mode
- Install SESM in LDAP or RADIUS mode and switch to Demo mode at run time

The following sections describe the differences between these two approaches.

## Installing in Demo Mode

The Demo mode installation is quick. It requires the entry of only a few parameters. In Demo mode, you can demonstrate the features of both RADIUS and LDAP deployments.

If you install in Demo mode, you should not expect to switch to LDAP or RADIUS modes at run time for the following reasons:

- The MBean configuration files are not set up properly to support the switch to those other modes. Several manual changes are required in the files.
- The Demo installation might not install all of the components required by the other modes. For example, a Demo installation does not install the SPE component, which is required to run in LDAP mode.

## Switching to Demo Mode at Run Time

You can install and configure SESM to run in LDAP or RADIUS mode, and then easily switch to run the application in Demo mode at run time. The switch from the other modes to Demo mode is supported as follows:

- When you install SESM in LDAP or RADIUS mode, the demo data file that supports Demo mode is included in your installation directory.
- The MBean configuration files are set up to point to the demo data file when the application is run in Demo mode.
- The mode attribute in the nwsp.xml file is a Java system property, so that it can be changed at run time.
- The NWSP startup scripts accept a run time argument to change the mode.

To switch to Demo mode at run time, use the following command:

Platform	Command
Solaris and Linux	jetty/bin/startNWSP.sh -mode Demo
Windows NT	jetty\bin\startNWSP.cmd Demo

## Installation Instructions for Demo Mode

To install SESM in Demo mode, follow these procedures:

- 
- Step 1** Log on as a privileged user:
- On Solaris—Run the installation program as root.
  - On Windows NT—Run the installation program as a member of the Administrators group.
- Make sure you have write privileges to the directory in which you intend to load the demo.
- Step 2** Obtain the installation image from the product CD-ROM or from the Cisco web site. The installation image is a tar or zip file, depending on the platform on which you want to install the demo. See the [“Obtaining the SESM Installation File and License Number”](#) section on page 5-10 for more information.

- Step 3** Uncompress the tar or zip file to a temporary directory. The result includes an executable .bin or .exe file. [Table 4-1](#) shows the names of the compressed and executable files.

**Table 4-1** Installation Image Filenames

Platform	Compressed Filename	Executable Installation Filename
Solaris	sesm-3.1.3-pkg-sol.tar	sesm_sol.bin
Linux	sesm-3.1.3-pkg-linux.tar	sesm_linux.bin
Windows NT	sesm-3.1.3-pkg-win32.zip	sesm_win.exe

- Step 4** Execute the installation image as follows:
- On Solaris, change directories to the location of the installation image, and enter the image name. For example:  

```
solaris>sesm_sol.bin
```
  - On Windows NT, you can double-click the file's icon. Otherwise, open a command prompt window, change directories to the location of the image, and enter the image name. For example:  

```
C:\>sesm_win.exe
```
- Step 5** Follow the instructions on the installation windows to install the demo. [Table 4-2](#) describes the parameters that you use to install the demo.
-

Table 4-2 Demo Installation and Configuration Parameters

Component	Input Summary	Explanation	Value
General installation parameters	License type	Click the <b>Evaluation</b> button. You do not need a license number.	
	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>You can accept the displayed default installation directory, click <b>Browse</b> to find a location, or type the directory name in the box. The default installation directories are:</p> <ul style="list-style-type: none"> <li>On Solaris and Linux: /opt/cisco/sesm_3.1.3</li> <li>On Windows NT: C:\Program Files\cisco\sesm_3.1.3</li> </ul> <p>You must have write privileges to the installation directory.</p>	
	Setup type	<p>Click the <b>Demo</b> button.</p> <p>The difference between a demo installation and a typical installation is the values that the installation program inserts in the configuration files and the components that are installed. For example, a demo mode installation does not install the SPE component.</p>	
NWSP web application configuration	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. 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>	

## Browsers

You can use the following browsers to demonstrate the NWSP application:

- Netscape Release 4.x and later
- Internet Explorer Release 5.x and later

These browser limitations apply to the NWSP sample application and are mentioned to ensure predictable results during demonstrations. When you develop an SESM application for deployment, you should consider the end users of your deployed application, and design the application to accommodate the media that they commonly use.

## Running the SESM Demo

This section includes the following topics:

- [Starting the Demo, page 4-5](#)
- [Stopping the SESM Demo, page 4-5](#)

## Starting the Demo

To start the demo, follow these procedures:

**Step 1** Start the NWSP web application in Demo mode.

Platform	SESM Installed Mode	Demo Startup Command
Solaris and Linux	Demo mode	jetty/bin/startNWSP.sh
	RADIUS or LDAP mode	jetty/bin/startNWSP.sh -mode Demo
Windows NT	Demo mode	jetty\bin\startNWSP.cmd
	RADIUS or LDAP mode	jetty\bin\startNWSP.cmd Demo

**Step 2** Open a web browser.

**Step 3** Go to the NWSP URL, which is:

`http://host:port`

Where:

*host* is the IP address or host name of the computer on which you installed the NWSP application. You can enter the value `localhost`, or the IP address `127.0.0.1`, to indicate the local computer.

*port* is the NWSP port number that you specified during the installation.

For example:

`http://localhost:8080`

The NWSP logon page appears.

**Step 4** Log on using a user ID and password defined in the demo data file. [Table 4-3](#) shows the user IDs and passwords in the installed demo data file.

**Step 5** The NWSP home page appears. The service selection list shows subscribed services for the user ID you used on the logon page. Select a service to demonstrate service connection.

## Stopping the SESM Demo

To stop the demo, follow the procedures described in the [“Stopping Applications” section on page 7-6](#).

# Demo Data File

This section describes the demo data file. It includes the following topics:

- [Demo Data Filename and Location, page 4-6](#)
- [File Contents and Format, page 4-6](#)
- [Logon Names and Passwords for a Demo, page 4-6](#)
- [Special Demo Profile Attributes for Demonstrating LDAP Features, page 4-7](#)

You might want to examine the demo data file to:

- See the services and features associated with each demo user ID.
- See examples of the vendor specific attributes (VSAs) that SESM and SSG require in a RADIUS database.
- Add new profiles or change existing ones to enhance your demonstration

## Demo Data Filename and Location

The subscriber and service profile data that supports the NWSP application running in Demo mode is stored in a RADIUS Merit flat file. The file is located in:

```
nwsp
  config
    demo.txt
```

If you change the name or location of the demo.txt file, you must reflect this change in the demoDataFile attribute in the SESMDemoMode MBean in the nwsp.xml file.

## File Contents and Format

The demo.txt file contains example subscriber profiles, service profiles, and service group profiles that support the SESM sample applications in Demo mode. The file is in Merit RADIUS flat file format and includes profiles that use the following types of attributes:

- RADIUS standard attributes
- Cisco vendor-specific attributes described in [Appendix D, “Configuring RADIUS”](#)
- SESM demonstration attributes described in the following section

You can use the profiles in the demo.txt file as test data for an SESM deployment in RADIUS mode.

## Logon Names and Passwords for a Demo

[Table 4-3](#) shows the user IDs and passwords in the profiles in the installed demo data file.

**Table 4-3 Logon Names and Passwords for a Demo**

Demo Purpose	User IDs	Passwords
To demonstrate RADIUS mode features	radiususer <b>Note</b> Other valid users are user1, user2, and so on, up to user44.	For all of the demo users, the password is: cisco
To demonstrate LDAP mode features	golduser subgolduser <b>Note</b> subgolduser is a subaccount to golduser.	

## Special Demo Profile Attributes for Demonstrating LDAP Features

[Table 4-4](#) describes the subscriber profile attributes for demonstrating features that are available in LDAP mode but not in RADIUS mode. See [Appendix D, “Configuring RADIUS”](#) for a description of all other attributes in the demo data file. The attributes in [Table 4-4](#) are for use in Demo mode only.



### Note

The attributes in [Table 4-4](#) are recognized only by an SESM portal running in Demo mode. They are not valid VSAs and they should not be added to the RADIUS dictionary. These attributes are not recognized by SSG.





Table 4-4 Special Attributes for Demonstrating LDAP Features in Demo Mode

Attribute	Description
Account-Info	<p>Subattributes that can be specified in the demo data file to demonstrate LDAP mode features are:</p> <ul style="list-style-type: none"> <li>• <b>Epermission</b>—Sets permissions to perform a task. The value for <i>permission</i> must be one of the following strings: <ul style="list-style-type: none"> <li>– Service Selection—The permission to perform service selection is implied and does not have to be explicitly coded in the profile.</li> <li>– Self Manage—Use this string to demonstrate the LDAP mode feature that allows a subscriber to update their own X.500 user schema information, such as name, address, e-mail, and hobbies.</li> <li>– Subaccount Manage—Use this string to demonstrate the LDAP mode feature that allows a subscriber to create a subaccount. The Demo mode does not create an actual subaccount; the supporting subaccount profile must be defined in the demo.txt file. Define the subaccount profile and use the <b>F</b> attribute.</li> <li>– Service Subscription—Use this string to demonstrate the LDAP mode feature that allows a subscriber to subscribe to a new service and have immediate access to that service. If you use this string, you must also add a <b>C</b> or <b>L</b> attribute.</li> </ul> </li> <li>• <b>Vname;type;value</b>—Use this attribute to specify the initial values that will appear in the fields on the My Account page in the NWSP application running in Demo mode. The Demo allows you to change these values. Use a separate attribute line for each field. The format for each line consists of: <ul style="list-style-type: none"> <li>– <i>name</i>—Name of the field on the My Account page in the NWSP application. These are X.500 fields. You can add more fields to the demo if you alter the NWSP application to display more fields, as described in the <i>Cisco Subscriber Edge Services Manager Web Developer Guide</i>. See the <i>Cisco Distributed Administrator Tool Guide</i> for a list of the X.500 names.</li> <li>– <i>type</i>—Identifies the format of <i>value</i>, as follows: <ul style="list-style-type: none"> <li>S or s—Indicates that <i>value</i> is a string.</li> <li>V or v—Indicates that <i>value</i> is a vector of strings in the following format, including the parentheses: <pre>{string1;string2;string3}</pre> </li> </ul> </li> <li>– <i>value</i>—Indicates the value to be displayed in the field on the web page display.</li> </ul> <p>For example:</p> <pre>Account-Info = "Vhobbies;V;{science;news;travel}"</pre> </li> <li>• <b>CserviceName</b>—Use this attribute to demonstrate the LDAP mode self-subscription feature. This feature allows a subscriber to subscribe to a new service and have immediate access to that service. The <i>serviceName</i> value must match a service profile name defined elsewhere in the demo flat file (demo.txt).</li> <li>• <b>LgroupName</b>—Use this attribute to demonstrate the LDAP mode self-subscription feature, subscribing to a predefined group of services. The <i>groupName</i> value must match a service group profile name defined elsewhere in the demo.txt file.</li> <li>• <b>FparentAccountName</b>—Use this attribute to indicate that this subscriber profile is a subaccount profile. The <i>parentAccountName</i> must match another subscriber profile name defined elsewhere in the demo flat file. (In the installed demo.txt file, subgolduser is defined as a subaccount to golduser.)</li> <li>• <b>RusergroupName</b>—Use this attribute to indicate that this subscriber is a member of a user group. The PDA application running in Demo mode demonstrates brand awareness by displaying different branded pages based on the user group values of bronze, silver, and gold. See the pdademo.txt file.</li> </ul>





## Installing Components

---

This chapter describes how to install the Cisco Subscriber Edge Services Manager (SESM) software and bundled components, including SPE. It includes the following topics:

- [Installation Requirements, page 5-1](#)
- [Obtaining the SESM Installation File and License Number, page 5-10](#)
- [Installation Privileges, page 5-12](#)
- [Installation Modes, page 5-12](#)
- [Installation and Configuration Parameters, page 5-14](#)
- [Installation Results, page 5-30](#)
- [Post-Installation Procedures, page 5-30](#)

## Installation Requirements

This section describes prerequisites to installing SESM. It includes the following topics:

- [Installation Platform Requirements, page 5-1](#)
- [RAM and Disk Space Requirements, page 5-2](#)
- [Java Software Considerations, page 5-2](#)
- [SSG and RADIUS Considerations, page 5-4](#)
- [LDAP Directory Configuration Requirements, page 5-4](#)
- [Dependencies among SESM Components, page 5-9](#)
- [Uninstalling a Previous Installation, page 5-10](#)

## Installation Platform Requirements

You can install SESM components on Sun Solaris, Linux, and Microsoft Windows platforms. See the [“Supported Hardware Platforms”](#) section on [page 1-12](#) for more information.

## RAM and Disk Space Requirements

Table 5-1 shows RAM and disk space requirements for a single instance of each component in SESM. These requirements are approximately the same on the Sun Solaris and the Windows NT platforms.

**Table 5-1 RAM and Disk Space Requirements**

Component Name	Disk Space (MB)	RAM
Jetty server	1.5	The Jetty server provides the J2EE application environment in which the SESM portal applications and CDAT execute. The application memory needs specified for NWSP and CDAT, below, include Jetty server usage.
SESM portal applications (NWSP, WAP, and PDA)	18.9	RAM requirements increase relative to the number of subscribers logged in. The following numbers are approximations: <ul style="list-style-type: none"> <li>• In RADIUS mode, 64MB of JVM can service a maximum of 12,800 users.</li> <li>• In LDAP mode, the DESS cache adds to the memory requirements. A JVM memory size of 64MB can service a maximum of 1800 users. See the <a href="#">“SPE Attributes” section on page 6-37</a> for cache size information.</li> </ul> See the <a href="#">“Memory Requirements and CPU Utilization” section on page 7-8</a> for memory utilization equations.
Captive Portal	2.0	The Captive Portal installation includes the Captive Portal and Message Portal applications.
RDP	4.2	The RDP uses the DESS cache. Memory requirements are roughly proportional to the login rate. See the <a href="#">“RDP Memory Requirements” section on page 7-10</a> for more information.
SPE components	1.9	N/A
CDAT	5.6	RAM requirements increase proportionally to the number of objects stored in the directory. For most directory sizes, the 64 MB requirements of the operating system (OS) and other system software should be sufficient for heavily populated directories.

## Java Software Considerations

A JRE Version 1.2.2 is bundled in the installation image. The installation process installs this bundled version if it cannot find a suitable version on the installation platform.

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

- [Solaris Patch Requirements, page 5-3](#)
- [Installing the Bundled JRE, page 5-3](#)
- [Specifying an Existing JRE or JDK, page 5-3](#)
- [Specifying the JRE or JDK in the Startup Scripts, page 5-3](#)

- [Obtaining a JDK for SESM Web Development, page 5-4](#)

## Solaris Patch Requirements

On older Solaris platforms, you might need to apply Solaris operating system upgrades (patches). To determine if the machine requires patches, go to the Sun Microsystems Java site and start the process of downloading the JRE Version 1.2.2. After you log in, a list of download options appears, including the necessary patches for your operating system version. You should also download the README file, which contains instructions on how to apply the patches.

## Installing the Bundled JRE

The installation program determines for itself whether or not to install the bundled JRE Version 1.2.2 by doing the following:

1. It searches for a JDK Version 1.2.2 that is already installed.
2. Failing that, it searches for a JRE Version 1.2.2 or later that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.2.2.

To search for an existing JDK or JRE, the installation program looks in the following locations:

- On Windows NT, it looks in the NT Registry for a referenced location.
- On Solaris, it looks in well-known locations. See the [“Searching for an Existing JDK or JRE” section on page 10-8](#) for a list of these locations.
- On Linux, it looks in well-known locations. See the [“Searching for an Existing JDK or JRE” section on page 10-8](#) for a list of these locations.

## Specifying an Existing JRE or JDK

On Windows NT, Solaris, and Linux, you can explicitly specify the location of a pre-installed JDK or JRE by starting the installation process on a command line and specifying the javahome parameter, as follows:

```
installImageName -is:javahome location
```

Where:

*installImageName* is the name of the downloaded SESM image.

*location* is the path name for the JRE or JDK directory. For example, /usr/java1.2.

## Specifying the JRE or JDK in the Startup Scripts

The installation process sets the location of the JDK or JRE in the startup files for the SESM portal applications, CDAT, and RDP.

If you change the location of the JDK or JRE after installation, make the corresponding change in the following two startup files:

- Generic startup script—This common script is executed by the startup scripts for the SESM portal applications and CDAT. It can also be used by the startup scripts for customized SESM portal applications.
- RDP startup script

Table 5-2 shows the path names of the startup scripts that you must change.

**Table 5-2 Startup Script Names**

Platform	Generic Startup Script	RDP Startup Script
Solaris and Linux	jetty/bin/start.sh	rdp/bin/runrdp.sh
Windows	jetty\bin\start.cmd	rdp\bin\runrdp.cmd

## Obtaining a JDK for SESM Web Development

A Java Development Kit (JDK) Version 1.2.2 or later must be installed on any system that will be used by web developers to create or modify the Java Server Pages (JSPs) for a customized SESM application. You can obtain JDK Version 1.2.2 or later from the Sun Java web page:

<http://java.sun.com/products/j2se>

On systems that will be used to customize an SESM application, we recommend that you install the JDK before you install SESM. In that way, the SESM installation program uses the JDK in the application startup scripts, rather than a JRE. The JDK is necessary for recompiling the changed JSPs. See the “[Recompiling a Customized JSP](#)” section on page 10-9 for more information.

If you install the JDK after installing SESM, then you must:

- Edit the SESM application start script to use the JDK.
- Ensure that the JDK\_HOME environment variable points to the directory into which you installed the JDK.

## SSG and RADIUS Considerations

The SESM installation program does not attempt to communicate with SSGs or RADIUS servers. Therefore, SSGs and RADIUS servers do not need to be configured and running for you to install SESM components.

However, you should be prepared to provide correct communication information about those network components during the installation. Otherwise, you must manually edit the configuration files at a later time for the SESM application to work correctly.

The installation program updates configuration files with information that you provide about the SSGs and RADIUS servers. [Table 5-5 on page 5-15](#) describes the configuration information that the installation program prompts you for.

## LDAP Directory Configuration Requirements

If you are installing SESM in LDAP mode, the installation program establishes communication with your LDAP directory, if possible. This section includes the following topics:

- [Advantages to Running an LDAP Directory During SESM Installation, page 5-5](#)
- [NDS Installation and Configuration Requirements, page 5-5](#)
- [iPlanet Installation and Configuration Requirements, page 5-7](#)

## Advantages to Running an LDAP Directory During SESM Installation

The LDAP directory does not need to be configured and running on the network for you to complete the Cisco SESM installation. However, it is advantageous if the directory is configured and running. If the installation program can communicate with the LDAP directory using the communication parameters that you provide, it 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 before running an SESM web application or CDAT, as described in the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 6-40.

## NDS Installation and Configuration Requirements

This section describes how to install and configure Novell eDirectory Version 8.5 to work with SESM. On completion of these instructions, your NDS directory is configured as follows:

- Access to the NDS server is granted with the following distinguished name (dn):  
cn=admin.ou=sesm.o=cisco
- The following SESM container exists in the NDS directory:  
Tree name: sesm  
Server context: ou=sesm.o=cisco
- The following administrative user has all required permissions to update the NDS directory schema and also to create and modify objects in the SESM container.  
name: admin  
password: value you specified during the NDS installation
- The Allow Clear Text Passwords option is set to true (required).

To install and configure NDS 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 super user.
- Step 2** Create an NDS directory on the Solaris machine. A typical location is /usr/nds.
- Step 3** If you have an NDS tar file, place it into the directory you just created and expand it.
- Step 4** Run the installation file, which is located in:  
`/usr/nds/NDS8.5/Solaris/setup/nds-install`
- Step 5** The installation program prompts you to read and accept the License agreement.
- Step 6** The installation program prompts you to choose the components to install, as follows:  
1)NDS Server  
2)Administration Utilities  
3)Management Console for NDS (ConsoleOne)

In most cases, you should install all three components. To do so, enter:

1 2 3

**Step 7** The installation program prompts you for the location of the license files. Enter:

```
/usr/nds/NDS8.5/licensefiles
```



**Note** Refer to the NDS documentation if you do not have the license files.

**Step 8** The installation program installs the requested packages. Then it asks whether or not you want to install the Java Runtime Environment (JRE). The JRE is required for ConsoleOne, the NDS management console. If you do not already have a suitable JRE installed on the machine, enter:

```
yes
```

**Step 9** The installation program opens the NDS server configuration file (/etc/ndscfg.inp) in a text editor. Use the editor to enter the following required information. Use the values shown below to ensure compatibility with SESM installation and sample data defaults:

```
Admin Name and Context: cn=admin.ou=sesm.o=cisco
Tree Name: sesm
Create NDS Tree: YES
Server Context: ou=sesm.o=cisco
```

Two additional fields (server IP address and Database Files directory) are optional. You do not need to enter values for them.

**Step 10** Save the configuration file and quit the editor.

**Step 11** The installation program prompts you for a password for the admin user. Enter any password.



**Note** The SESM installation program prompts you for the administrator name (admin) and this password when you install the SPE component.

**Step 12** The installation program concludes by prompting you to manually edit two environment variables:

```
PATH=$PATH:/usr/ldaptools/bin
MANPATH=$MANPATH:/usr/ldaptools/man
```



**Note** The following instructions describe how to set the Allow Clear Text Passwords attribute. For SESM to work with NDS, this attribute must be enabled. This attribute allows transmission of bind requests that include passwords over nonencrypted connections. By default, only passwords exchanged over SSL connections are encrypted. The allow clear text password attribute is a property of the LDAP Group object of a server.

**Step 13** Start ConsoleOne. Run the following file:

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

**Step 14** Authenticate to the NDS Directory as follows:

- In the tree, click the **NDS** icon.
- From the menu, choose **File** → **Authenticate**.
- In the Login window, type the password you entered for the admin user during installation. Accept the defaults displayed in the other fields in the login window. Click **Enter**.

Upon successful authentication, the .SESM. icon appears in the right panel.



**Step 15** Set the Allow Clear Text Passwords to **true**, as follows:

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

```
NDS
 .SESM.
 cisco
 sesm
```

- In the left panel, click **SESM** to select it.
- In the right panel, right-click the **LDAP Group object**.
- Choose **Properties** from the pop-up menu.
- In the **General** tab, in the middle of the window, check the **Allow Clear Text Passwords** option.
- Click **Apply**. Then click **Close**.

**Step 16** Exit ConsoleOne and proceed to the SESM installation.

---

## iPlanet Installation and Configuration Requirements

This section describes how to install and configure iPlanet to work with SESM. On completion of these instructions, your iPlanet directory is configured as follows:

- Access to the server is granted with the following distinguished name (dn):  
uid=admin.ou=sesm.o=cisco
- The following SESM container exists in the directory:  
Tree name: sesm  
Server context: ou=sesm.o=cisco
- The following administrative user has all required permissions to update the directory schema:  
name: Directory Manager  
password: value you specify during the iPlanet installation
- The following administrative user has all required permissions to create and modify objects in the SESM container.  
name: admin  
password: value you specify during the iPlanet installation

To install and configure iPlanet to work with SESM, perform the following steps. These instructions assume that you are installing iPlanet Version 5.0 on a Solaris machine.

---

**Step 1** Log on as superuser.

**Step 2** If you have a tar file, expand it.

**Step 3** Execute the setup file. Follow the instructions in the setup program.

**Step 4** When the program displays the following prompt, select the **iPlanet Servers** option.

- ```
1. iPlanet Servers
   Installs iPlanet Servers with the integrated iPlanet Console onto your computer.
2. iPlanet Console
   Installs iPlanet Console as a stand-alone Java application on your computer.
```

- Step 5** In response to subsequent prompts to install components, select **all components**.
- Step 6** When the program displays the following prompt, we recommend that you enter the standard port **389**, rather than accepting the random default port. You must know this port number later in this procedure and also during SESM installation.
- ```
Directory server network port [nnnnn]: 389
```
- Step 7** At the following prompt, accept the default value of **admin**.
- ```
iPlanet configuration directory server
administrator ID [admin]:
Password:
Password (again):
```
- Enter the password of your choice. This user name and password has privileges to update the directory schema. You must enter this admin ID and password later in this procedure and also during SESM installation.
- Step 8** When the program displays the following prompt, enter the value **o=cisco**.
- ```
Suffix [dc=]:o=cisco
```
- Step 9** When the program displays 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 user name and password has privileges to add objects to the cisco container you created in the previous step. You must enter this Directory Manager DN and password later in this procedure and also during SESM installation.
- Step 10** When the program displays the following prompt, enter any port number. The configuration examples later in this procedure use the value 390.
- ```
Administration port [15197]:390
```
- Step 11** When the program displays the following prompt, enter a user name or accept the default value (root).
- ```
Run Administration Server as [root]:
```
- The installation process is complete. After successful installation, the iPlanet servers start automatically.
- Step 12** Change the directory to:
- ```
/usr/iplanet/servers
```
- Step 13** Execute the following program:
- ```
startconsol
```
- A logon window appears.
- Step 14** Log on as follows:
- ```
User ID:cn=Directory Manager
Password:
AdminURL:http://hostname:390
```
- The iPlanet Console window appears.
- Step 15** Expand the folders in the iPlanet Console window until the Directory Server object appears. Select **Directory Server** and click **Open** at the top right corner of the window.
- An iPlanet Directory Server window appears.

- Step 16** Right-click the **cisco** folder. Choose **New** → **Org Unit** from the pop-up menu.
- Step 17** In the Name field, enter **sesm** and click **OK**.  
Name: sesm
- Step 18** Right-click the **sesm** object. Choose **New** → **User** from the pop-up menu. A Create New User window appears.
- Step 19** Enter appropriate values. In the UserID field, enter **admin**. Click **OK**.  
First Name:  
Last Name:  
Common Name:  
UserID: admin  
Password:
- Step 20** Right-click the **sesm** object. Choose **Set Access Permissions** from the pop-up menu. The Manage Access Control window for ou=sesm,o=cisco appears.
- Step 21** Click **New**. The Edit ACI window for ou=sesm,o=cisco appears.
- Step 22** Enter any value for ACIName and click **Add**.  
ACI Name :aciAdmin  
  
The Add User & Group window appears.
- Step 23** Enter the following value in the search field and click **Search**:  
admin  
  
The admin user appears in the top window.
- Step 24** Select **admin** and click **Add**. The admin user appears in the bottom window. Click **OK**.
- Step 25** Click **Targets**. Click **This Entry**. Click **OK**.
- Step 26** Click **OK** in the Manage Access Control window.
- Step 27** Exit iPlanet and proceed to the SESM installation.
- 

## Dependencies among SESM Components

You can install all SESM components together on the same machine (a typical installation), or you can install some components separately in a distributed manner (a custom installation). [Table 5-3](#) describes components that must be installed together on the same machine. The installation program detects these dependencies and enforces the correct installation.

**Table 5-3 Component Dependencies in a Distributed Installation**

SESM Mode	Component Dependencies
RADIUS mode	<ul style="list-style-type: none"> <li>An SESM portal application requires a J2EE server (for example, jetty) on the same machine.</li> </ul>
LDAP mode	<ul style="list-style-type: none"> <li>An SESM portal application requires a J2EE server (for example, jetty) and the SPE component on the same machine.</li> <li>CDAT requires a J2EE server (for example, jetty) and the SPE component on the same machine.</li> <li>RDP requires the SPE component on the same machine.</li> </ul>

## Uninstalling a Previous Installation

Use the uninstall utility provided with the SESM product to remove a previous installation. 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.

After running the uninstall utility, you can safely reinstall one or more SESM components into the same directory.



### Note

Do not uninstall SESM by manually deleting the contents of the installation directory. If you do so, and then attempt a reinstall into the same directory, the installation might not be complete. If the installation is incomplete, see the [“Incomplete Installation or Files Installed in Incorrect Directory”](#) section on page 10-10 for information.

## Obtaining the SESM Installation File and License Number

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

- [Obtaining a License Number, page 5-11](#)
- [Downloading from the Cisco Web Site, page 5-11](#)
- [Uncompressing the Image, page 5-11](#)

## Obtaining a License Number

The SESM installation program installs evaluation and licensed versions of SESM:

- **Evaluation**—The evaluation options do not require a license number and do not have an expiration period. An evaluation installation provides full software functionality. You can install a RADIUS mode evaluation or an LDAP mode evaluation.
- **Licensed**— You must install a licensed version using a license number before deploying SESM in a production environment.

The license number is available on the License Certificate that is shipped with a purchased product. If you have 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.

## Downloading from the Cisco Web Site

If you purchased a contract that allows you to obtain the SESM software from the Cisco web site, follow these procedures:

- 
- Step 1** Open a web browser and go to:  
`http://www.cisco.com`
  - Step 2** Click the **Login** button. Enter your Cisco **user ID** and **password**.  
To access the Cisco images from the CCO Software Center, you must have a valid Cisco user ID and password. See your Cisco account representative if you need help.
  - Step 3** Under Service and Support, click **Software Center**.
  - Step 4** Click **Web Software**.
  - Step 5** Click **Cisco Subscriber Edge Services Manager**.
  - Step 6** Download the appropriate image based on the platform you intend to use for hosting the SESM web application.
- 

## Uncompressing the Image

Copy and uncompress the tar or zip file to a temporary directory. When you uncompress the file, the results are:

- The installation executable file—A `.bin` or `.exe` file, depending on the platform you are using.
- Files used for a silent mode installation—These are `.iss` and `.properties` files. See the [“Installing Using Silent Mode”](#) section on page 5-14 for information about silent mode.

Table 5-4 shows the names of the compressed and executable files.

**Table 5-4 Installation Image Filenames**

Platform	Compressed Filename	Executable Installation Filename
Solaris	sesm-3.1.3-pkg-sol.tar	sesm_sol.bin
Linux	sesm-3.1.3-pkg-linux.tar	sesm_linux.bin
Windows NT	sesm-3.1.3-pkg-win32.zip	sesm_win.exe

## Installation Privileges

You must log on as a privileged user to perform the installation. In addition, you must have write privileges to the directory in which you intend to load the solution components.

The installation program writes to parts of the file system or Windows registry that are only accessible to a privileged user. The outcome of the installation is unpredictable if you are not privileged.

Log on as a privileged user as follows:

- On Solaris and Linux—Run the installation program as root.
- On Windows NT—Run the installation program as a member of the Administrators group.

## Installation Modes

You can install SESM using the following installation modes:

- **Installing Using GUI Mode**—An interactive installation method that communicates with you by displaying interactive windows. You use the mouse and the keyboard to provide input during the installation.  
To run the installation in GUI mode, execute the installation image. No special arguments are required.
- **Installing Using Console Mode**—A text-only, question and answer interactive installation method.  
To run the installation in console mode, use the `-console` argument on the command line when you execute the installation image.
- **Installing Using Silent Mode**—A text-only noninteractive method. This mode, also known as batch mode, is useful for multiple installs. Before you start the installation process, you prepare files that contain your installation and configuration information. The installation program obtains all input from the response file.  
To run the installation in silent mode, use the `-option fileName` argument on the command line when you execute the installation image.

The following sections provide more details about performing installations in these modes.

## Turning On the Installation Logging Feature

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

- On Solaris:

```
solaris> sesm_sol.bin -log location @ALL
```

Where:

*location* can be `#` to send logging messages to the console or a filename.

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

- On Windows NT:

```
C:\> sesm_win.exe -options -log location @ALL
```

Where:

*location* can be `#` to send logging messages to the console or a filename.

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

## Installing Using GUI Mode

GUI mode is the default installation mode. To run in this mode, execute the installation image. No options are required.

- On Solaris, change directories to the location of the installation image, and enter the image name. For example:

```
solaris> sesm_sol.bin
```

- On Windows NT, double-click the installation image filename. Alternatively, open a command prompt window, change directories to the location of the image, and enter the image name. For example:

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

## Installing Using Console Mode

To run in console mode, use the `-console` option on the command line.

- On Solaris, change directories to the location of the installation image, and enter the following command:

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

- On Windows NT, open a command prompt window, change directories to the location of the image, and enter the following command:

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

## Installing Using Silent Mode

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 process. It includes the name of the .properties file. This file is specified as an argument on the command line when you start the installation process.
- 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. You must modify both files to match your requirements before you start the installation.

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 5-5 on page 5-15](#) 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 in silent mode, use the `-options` option on the command line, as follows:

```
imageName -options issFileName
```

Where:

*imageName* is the name of the downloaded installation image.

*issFileName* is the name of the install shield properties file you prepared.

For example:

- On Solaris, change directories to the location of the installation image, and enter the following command:
 

```
solaris> sesm_sol.bin -options myseesm.iss
```
- On Windows NT, open a command prompt window, change directories to the location of the image, and enter the following command:
 

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

## Installation and Configuration Parameters

[Table 5-5](#) describes the installation and configuration parameters to enter during the installation process. Use the Value column in the table to record your planned input values.



You can change the value of any configuration parameter later by editing configuration files, as described in Chapter 4. You cannot change the values of the general installation parameters identified in the first part of the table.

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

Category	Input Summary	Explanation	Value
General installation parameters	Installation type and license number	<p>Choose the type of installation:</p> <ul style="list-style-type: none"> <li>• <b>RADIUS Evaluation</b>—Choose 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 mode.</li> <li>• <b>LDAP Evaluation</b>—Choose this option to evaluate SESM in an LDAP 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 mode.</li> <li>• <b>Licensed</b>—If you purchased an SESM license, choose this option and enter the license number provided by Cisco.</li> </ul> <p>The installation program interprets the license number you enter and proceeds to install either RADIUS or LDAP mode components, whichever matches the license you purchased. A RADIUS mode license will not allow you to install the LDAP-specific components, such as CDAT and 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, choose one of the Evaluation modes.</p> <p>The licensenum.txt file in your root installation directory records your license number and the software version number you installed. This information is important when you access Cisco technical support for this product.</p>	
	License agreement	<p>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.</p>	
	Installation directory	<p><b>Note</b> You must have write privileges to the installation directory.</p> <p>To specify the installation directory, you can 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 directories are:</p> <ul style="list-style-type: none"> <li>• On Solaris and Linux: /opt/cisco/sesm_3.1.3</li> <li>• On Windows NT: C:\Program Files\cisco\sesm_3.1.3</li> </ul>	

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

Category	Input Summary	Explanation	Value
General installation parameters (continued)	Setup type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Typical</b>—If you are installing a RADIUS evaluation or a RADIUS license, the Typical installation includes the following components: <ul style="list-style-type: none"> <li>– Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model.</li> <li>– Jetty—Includes the Jetty web server, the JMX server, and JNDI.</li> </ul> </li> </ul> <p>If you are installing an LDAP evaluation or LDAP license, the Typical installation includes the following components:</p> <ul style="list-style-type: none"> <li>– Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model.</li> <li>– Jetty</li> <li>– SPE</li> <li>– RDP</li> <li>– CDAT</li> </ul> <ul style="list-style-type: none"> <li>• <b>Custom</b>—Allows you to choose the components to install and configure from a checklist. Choose this option to: <ul style="list-style-type: none"> <li>– Include the SESM captive portal solution in your installation.</li> <li>– Reinstall one of the components.</li> <li>– Distribute the SESM components among different workstations.</li> </ul> </li> <li>• <b>Demo</b>—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. Choose this option when those components are not available.</li> </ul> <p>The difference between a demo installation and a typical installation is the contents of the configuration files. In addition, a demo installation does not install the SPE component.</p>	

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

Category	Input Summary	Explanation	Value
Web server configuration	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. 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>When the application port is 8080, the SSL port is:  <math display="block">8080 - 80 + 443 = 8443</math></p> </li> <li>A management console port is derived as follows:  <math display="block">\text{application port} + 100</math> <p>When the application port is 8080, the management port is:  <math display="block">8080 + 100 = 8180</math></p> </li> </ul>	

**Note** If you are installing SESM in Demo mode, you are finished with the installation.

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

Category	Input Summary	Explanation	Value
SESM to SSG communication  <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 an SESM application. This value must match the value that was configured on the SSG host with the following command:  <code>ssg radius-helper authenticationPort</code>  The default value is 1812.	
	SSG shared secret	Specify the shared secret used for communication between SSG and an SESM application. This value must match the value that was configured on the SSG host with the following command:  <code>ssg radius-helper key secret</code>  The default value is <code>cisco</code> .	
	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:  <code>ssg port-map length</code>  We recommend using the value 4.  A value of 0 indicates that the SSG is not using the port-bundle host key mechanism.  <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.  The default value is 0.	

When the port bundle size is 0, you must map SSGs to client subnets. The following category of parameters lets you map one client subnet for one SSG. You must manually edit the configuration file to:

- Map additional non-host key SSGs,
- Add more client subnets to this SSG, or
- Override the global values you specified in the previous category.

See the [“Associating SSGs and Subscriber Requests” section on page 6-25](#) for more information.

One non-host key SSG	SSG address	Enter the host name 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.	

**Note** If you are installing SESM in LDAP mode, skip the following two categories and continue with the “Directory server information” category later in this table.

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

Category	Input Summary	Explanation	Value
SESM to RADIUS server communication	Primary AAA server IP	Enter the IP address or the host name of the primary RADIUS server.	
	Primary AAA server port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on. The default is 1812.	
	Secondary AAA server IP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	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 same 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. The default value is <code>cisco</code> .	
Passwords	Service password	Enter the password that the SESM application uses to request service profiles from RADIUS. It must match the service password values used in the service profiles in the RADIUS database.  This password must also match the value that was configured on the SSG host with the following command:  <code>ssg service-password password</code>  The service-password value must be the same on all of your SSGs.  The default value is <code>servicecisco</code> .	
	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.  The default value is <code>groupcisco</code> .	

**Note** If you are installing SESM in RADIUS mode, you are finished with the installation.

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

Category	Input Summary	Explanation	Value
Directory server information	Directory address	Enter the IP address or the host name of the system on which the directory server is running.	
	Directory port	Enter the port on which the directory server listens.	
	Directory admin user	Enter a user ID that has permissions to extend the directory schema. Use cn or uid as appropriate. For example: <ul style="list-style-type: none"> <li>For NDS, enter: cn=admin, ou=sesm, o=cisco</li> <li>For iPlanet, enter: uid=Directory Manager, ou=sesm, o=cisco</li> </ul>	
	Directory admin password	Enter the password for the directory administrator. This is the password you entered during directory installation and configuration. For example: <ul style="list-style-type: none"> <li>For NDS, enter the password you specified for the admin user during installation.</li> <li>For iPlanet, enter the password you entered for the Directory Manager user during installation.</li> </ul>	
	Meta Schema	Choose the component in distinguished name (dn) that your LDAP directory uses to allow access to the directory. <ul style="list-style-type: none"> <li>common name (cn)—NDS, for example, uses cn.</li> <li>unique identifier (uid)—iPlanet, for example, uses uid.</li> </ul> <p><b>Note</b> The SESM sample data uses cn. If you choose uid, you must edit the sample data before loading it into the directory. See the <a href="#">“Loading Sample Data and Logging into CDAT for the First Time”</a> section on page 6-41.</p>	

**Note** The installation program attempts to access the directory server, using the information you provided. If access 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. If the directory is not running, you can continue the installation of SPE components by clicking the **Ignore** button on the warning window. However, if you click **Ignore**, the installation program cannot update the directory for SESM use. You must perform the updates at a later time before you run SESM web applications or CDAT. See the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 6-40 for instructions.

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

Category	Input Summary	Explanation	Value
Directory container information	Directory container	<p>Enter the organization and organizational unit that will hold the SESM service, subscriber, and policy information. Use the following format:</p> <pre>ou=orgUnit,o=org</pre> <p>For example, the installation program's default values are:</p> <pre>ou=sesm,o=cisco</pre> <p>The above defaults are the values used in the sample data file that is shipped with CDAT.</p>	
	Directory user ID	<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: <pre>cn=admin,ou=sesm,o=cisco</pre> </li> <li>For iPlanet, the container administrator is not the same. You created this directory administrator after installation. <pre>uid=yourAdmin,ou=sesm,o=cisco</pre> </li> </ul>	
	Directory password	Enter the password associated with the directory user ID.	
<p><b>Note</b> The installation program attempts to access the container using the information you provided. If it is unsuccessful, a warning message appears, as described in the previous note.</p>			
CDAT	CDAT port number	<p>Enter the port number on which the CDAT web server will listen.</p> <p>The default is 8081.</p>	

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


Category	Input Summary	Explanation	Value
RDP Configures RDP to SSG communication	IP address	Enter the IP address or host name of the RDP.   <b>Caution</b> This value must be a real IP address to which the SSG host device can route. You cannot use the values localhost or 127.0.0.1.	
	Port number	Enter the port on which the RDP will listen. The default is 1812.	
	Shared secret	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:  <code>radius-server key SharedSecret</code>  When the restricted client feature is turned off, the shared secret must be the same on all SSGs.  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 the RDP MBean description in <a href="#">Table 6-6 on page 6-32</a> for more information.  The next set of prompts from the installation program lets you choose whether to turn the restricted client feature on or off.  The default shared secret value is <code>cisco</code> .	
	Service password	Enter the password that RDP uses to request service profiles from the directory. This value must match two other configured values:  <ol style="list-style-type: none"><li>1. This password must match the value that was configured on the SSG host with the following command:  <code>ssg service-password password</code>  The service-password value must be the same on all the SSGs that communicate with this RDP server.</li><li>2. This value must also match the service password value you entered for the SESM portal. See the SESM “<a href="#">Passwords</a>” section on <a href="#">page 5-19</a>.</li></ol> The default value is <code>servicecisco</code> .	
Group password	Enter the password that RDP uses to request service group profiles from the directory.  This password must match the group password value you entered for the SESM portal. See the SESM “ <a href="#">Passwords</a> ” section on <a href="#">page 5-19</a> .  The default value is <code>groupcisco</code> .		



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

Category	Input Summary	Explanation	Value
	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:</p> <pre>ssg next-hop download nextHopTableName password</pre> <p>The service-password value must be the same on all of the SSGs that communicate with this RDP server.</p> <p>The default is <code>nexthopcisco</code>.</p>	
RDP Options	Proxy mode	<p>Choose 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>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 services	<p>Choose this option if you want the SSG to perform automatic connections to services when a subscriber's profile includes the autoconnect attribute. When you choose this option, RDP includes the subscriber's service list and related information in replies to SSG. The service information consumes memory on the SSG device.</p> <p>Do not choose this option if space is a consideration on the SSG device. Instead, you can configure the SESM application to initiate automatic connections. See the <a href="#">“autoConnect” section on page 6-20</a> for more information.</p>	
	Add client	<p>Choose 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 must manually edit the <code>rdp.xml</code> file to add more clients.</p> <p>If you do not check this option, the RDP accepts requests from any client (any SSG).</p>	

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

Category	Input Summary	Explanation	Value
If you choose the Add client option, the installation program prompts you for the following information about one RDP client. To add more clients, manually edit the rdp.xml file			
RDP Client	Client name	Identifies the SSG. This value is used in logs and traces and does not have to match any other configured value.	
	Client IP address	The IP address of the SSG.	
	Shared Secret	The shared secret used for SSG to RDP communication. This value must match the value configured on the SSG devices, using the following command:  <code>radius-server key SharedSecret</code>	
If you are doing a Custom installation and you checked the Captive Portal item, the installation program prompts you for the following information.			
<b>Note</b> Captive portal installation 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 during SESM captive portal installation. Then configure the SSG based on the example captiveportal/config/ssgconfig.txt file. See <a href="#">Chapter 8, “Deploying a Captive Portal Solution,”</a> for more information.			
Captive Portal Server Configuration	Captive portal address	Enter the IP address of the hardware platform on which you are installing the captive portal solution.	
	Captive portal port number	Enter the port number on which the first listener in the captive portal web server will listen.  This installation program sets up the captiveportal.jetty.xml file to create 7 listeners in the web server, as follows: <ul style="list-style-type: none"> <li>• 1 Subscriber redirection listener</li> <li>• 1 Initial logon redirection listener</li> <li>• 1 Advertising redirection listener</li> <li>• 1 Default service redirection listener</li> <li>• 3 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.  <b>Note</b> If you use the same port number for more than one listener, some redirections will not work.  Default: 8090	
	Install Message Portal	Choose 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.	

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

Category	Input Summary	Explanation	Value
If you choose 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. Default: 8085	
	Redirect after message page	Choose 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 choose this option, the subscriber must enter an URL to leave the message page. Default: true	
Portal for service and error redirections	Host	Enter the host name or IP address of the web server for the NWSP or other application that will respond to: <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 has been used which is not configured for redirection).</li> </ul> This value becomes the default value for the serviceportal.host system property in the captiveportal.xml file.	
	Port	Enter the port number on which the web server named above will listen. This value becomes the default value for the serviceportal.port system property in the captiveportal.xml file. Default: 8080	

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

Category	Input Summary	Explanation	Value
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 URL Out: Port URL Out: URI	<p>These fields define the URL to which browsers are redirected for unauthenticated user redirections. The default values reference 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.</li> <li>• Port—Enter the listener port number for this content application. The default is the port number you entered for the NWSP application.</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>	
Initial Captivation	Enable	Check this box to configure initial logon redirections.	
	Port In	<p>Enter the port that the Captive Portal web server will listen on for initial logon redirections.</p> <p><b>Note</b> You must configure the SSG TCP redirect feature to send initial logon redirections to this port.</p> <p>Default: 8091</p>	
	URL Out: Host URL Out: Port URL Out: URI	<p>These fields define the URL to which browsers are redirected for initial logon redirections. The default values reference the Message Portal 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 initial logon redirections.</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.</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	<p>The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL.</p> <p>Default: 15</p>	

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

Category	Input Summary	Explanation	Value
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.  <b>Note</b> You must configure the SSG TCP feature to send advertising redirections to this port.  Default: 8092	
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for advertising redirections. The default values reference the Message Portal application. <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.</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.</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.  Default: 15	

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

Category	Input Summary	Explanation	Value
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  <b>Note</b> You must configure the SSG TCP feature to send default service redirections to this port.  Default: 8093	
	First Service Redirect Port In Second Service Redirect Port In 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.  <b>Note</b> You must configure the SSG TCP feature to send redirections to these ports.  Defaults: 8094, 8095, 8096	
	URL Out	Enter the URL to which browsers are redirected for any type of service redirection. The default value references 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.	
Details for Service Redirection	Pass Service Names	Choose 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.  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.	

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

Category	Input Summary	Explanation	Value
If you choose Proxy mode for RDP, then the installation process prompts you for the following RADIUS server information.			
RDP to RADIUS communication	Primary AAA server IP	Enter the IP address or the host name of the primary RADIUS AAA server that you want RDP to communicate with.	
	Primary AAA server port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on.	
	Secondary AAA server IP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	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 same value used for the primary server.	
	Shared secret	Enter the shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers.  The default is <code>cisco</code> .	

The installation program installs the components on your system. When it is finished installing the files, it displays an additional window about modifications to the LDAP directory.

LDAP directory modifications	Extend schema	<p>Choose this option if you want the installation program to apply the SPE schema extensions to the LDAP directory. These extensions include the <code>dess</code> and <code>auth</code> classes and attributes. For more information about the extensions, see the <i>Cisco Distributed Administration Tool Guide</i>.</p> <p>If you do not choose this option, you must extend the directory schema later, before running the SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “<a href="#">Extending the Directory Schema and Loading Initial RBAC Objects</a>” section on page 6-40 for more information.</p> <p><b>Note</b> If you are installing the SPE components in multiple locations, you only need to extend the schema one time.</p>	
	Install RBAC	<p>Choose this option if you want the installation program to load the top-level RBAC objects.</p> <p>If you do not choose this option, you must install RBAC objects later, before running an SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “<a href="#">Extending the Directory Schema and Loading Initial RBAC Objects</a>” section on page 6-40 for more information.</p> <p><b>Note</b> If you are installing the SPE components in multiple locations, you only need to install the RBAC objects one time.</p>	

# Installation Results

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

- `_uninst`—This subdirectory contains the utility to uninstall the components you just installed. To uninstall components, run the executable file in this directory.
- `jetty`—This directory contains the following subdirectories:
  - `bin`—Contains start scripts for Jetty server applications
  - `config`—Contains configuration files that control Jetty servlets
  - `lib`—Contains the Jetty server class libraries.
- `lib`—This directory contains the SESM libraries and the `docs` subdirectory, which contains the Java application documentation.
- `licensenum.txt`—This file contains the license number that you used during installation and the version number of the SESM software that you installed.
- `nwsp`, `pda`, and `wap`—These directories contain the following subdirectories:
  - `config`—Contains configuration files for the portal application and `demo.txt` files.
  - `docroot`—Contains the Web application, including libraries, JSPs, images, and a J2EE configuration file.
- `nwsp311`—Contains the NWSP application from SESM Release 3.1(1). This earlier application is included as a migration tool.
- `redist`—This directory contains libraries from other 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.
- `captiveportal` and `messageportal`—These directories are included only if you installed the Captive Portal solution using a Custom installation.

When you install SESM in LDAP mode, the installation directory contains the following additional directories:

- `rdp`—This directory contains startup scripts, configuration files, and libraries for the RADIUS/DESS Proxy Server.
- `cdat`—This directory contains configuration files and libraries for CDAT.
- `dess-auth`—This directory contains the SPE DESS and AUTH libraries, SPE DESS schema, and sample data.

## Post-Installation Procedures

This section outlines the steps to take after you successfully complete an installation.

- 
- Step 1** Perform all configuration activities listed in [Table 2-2 on page 2-6](#) (RADIUS mode) or [Table 2-4 on page 2-9](#) (LDAP mode).
- Step 2** Add configuration information for additional SSGs, if the SSG port bundle host key feature is not used on the SSGs.



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 SSG to client subnet mapping. See the [“Associating SSGs and Subscriber Requests”](#) section on page 6-25 for instructions.

- Step 3** (Optional) If you installed the captive portal solution, see the [“Additional Configuration Steps”](#) section on page 8-9 for instructions on configuring an SSG to work with the installed captive portal features.
- Step 4** (Optional) 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. You must edit the rdp.xml file to add additional clients. See the useClientList attribute in [Table 6-6](#) on page 6-32.
- Step 5** Start an SESM portal application, start a web browser, and logon as described in [Chapter 7, “Running SESM Components.”](#)
- 

See the [“Configuring a Customized SESM Application”](#) section on page 6-44 for information about configuring a customized SESM portal applications.





# Configuring Components after Installation

---

This chapter describes all of the configurable attributes in the Subscriber Edge Services Manager (SESM) software components. Use this chapter to change or fine-tune attributes after installation.

This chapter includes the following topics:

- [Configuration Overview, page 6-1](#)
- [Configuring the J2EE Jetty Container, page 6-7](#)
- [Configuring an SESM Portal Application, page 6-14](#)
- [Configuring RDP, page 6-30](#)
- [Configuring CDAT, page 6-36](#)
- [Configuring SPE, page 6-37](#)
- [Configuring Specific Features, page 6-41](#)
- [Configuring a Customized SESM Application, page 6-44](#)

## Configuration Overview

This section provides an overview of the configuration technology used by SESM. It includes the following topics:

- [Changing Configuration Information, page 6-1](#)
- [Configuration Technology, page 6-2](#)
- [Configuration File Summary, page 6-3](#)

## Changing Configuration Information

The installation program assigns initial values to all of the key attributes in the MBean configuration files, using a combination of default values and values you provide during the install. To change these initial values, administrators can manually edit the configuration files.

If you change configuration information, you must stop and restart the SESM web application and the Jetty server. If you deployed SESM in LDAP mode, you also must stop and restart RDP. See [Chapter 7, “Running SESM Components,”](#) for instructions.

## Configuration Technology

SESM configuration is based on the Java Management Extensions (JMX) specification and its related JMX MBean standards. For descriptions of these standards, go to:

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

The configuration elements involved in SESM are:

- **MBeans**—MBeans are Java classes that follow a model described in the MBean standards. An MBean represents the management interface for a resource. The management interface is the set of all necessary information and controls that a management application needs to operate on the resource.

SESM uses MBeans to configure components and the communications connections between those components. For example, an SESM MBean configures the SESM mode; an SSG MBean configures communication between SSG and the SESM web application, an AAA MBean configures communication between RADIUS servers and the SESM web application, and so on.

Container-specific parameters are also defined as MBeans. For example, Cisco created a logging MBean for the Jetty server.

- **JMX server**—The JMX server, sometimes known as the MBean server, is a registry for objects which are exposed to management operations by an agent. Any object that is registered with the JMX server becomes visible to the agent. (For SESM, the agent is the Cisco ConfigAgent.) MBeans are registered by the ConfigAgent or by other MBeans.

The Jetty component in the SESM installation package includes a JMX server. You can substitute any JMX-compliant server.

- **Cisco ConfigAgent**—The Cisco ConfigAgent is a JMX-compliant agent provided by Cisco. ConfigAgent configures MBeans by reading and implementing values from MBean configuration files. ConfigAgent is an MBean, started by the SESM web application.
- **MBean Configuration Files**—The MBean configuration files are XML files in a format defined in `xmlconfig.dtd`, a Cisco DTD. These files set configurable attributes in SESM. The SESM installation program assigns values for all of the key attributes in these files, using a combination of default values and values you provide during the install. You can change the value of any attribute by editing the appropriate MBean configuration file.

### Cisco ConfigAgent

Cisco ConfigAgent performs the following management functions for MBeans.

- **Constructs and initializes an MBean**—The `<Instantiate>` tag causes ConfigAgent to construct and initialize an MBean. Most MBeans are initialized by other objects (for example, other MBeans) and not by ConfigAgent.

After initialization, an MBean registers itself with the JMX server.

- **Configures an MBean**—The `<Configure>` tag causes ConfigAgent to configure an MBean.

When the ConfigAgent detects a newly registered MBean, ConfigAgent configures that MBean if there is a matching entry in the XML files for that MBean.

The `<Set>` tag sets attribute values for the MBean.

- **Starts an MBean**—The `<Call>` tag causes ConfigAgent to start an MBean.

The contents of the MBean configuration files control ConfigAgent activity.

## Configuration File Summary

This section includes the following topics:

- [J2EE Configuration Files, page 6-3](#)
- [MBean Configuration Files, page 6-4](#)
- [MBean Configuration File Format, page 6-5](#)
- [Java System Properties in the MBean Configuration Files, page 6-6](#)

### J2EE Configuration Files

The J2EE configuration files, such as `web.xml` and `webdefaults.xml`, define how the applications run in the J2EE environment. These files conform to Java specifications, as described in the Java Servlet Version 2.3 specifications from Sun Microsystems.

The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes application-specific parameters in the J2EE configuration files. For information about other parameters, see the Java Servlet Version 2.3 specifications. To download these specifications, go to:

<http://java.sun.com/aboutJava/communityprocess/first/jsr053>

[Table 6-1](#) shows the J2EE configuration files used to configure SESM web portals.

**Table 6-1 Summary of J2EE Configuration Files**

Component	File Path and Name	Description
Container (Jetty)	jetty config webdefault.xml	This file sets attributes for the Jetty server's handling of HTTP requests and how they map to servlets and JSPs.
SESM web application	applicationName docroot WEB-INF web.xml	This file defines J2EE application parameters, including parameters related to Java Server Pages (JSPs).  There is a separate <code>web.xml</code> file for each web application.

## MBean Configuration Files

Table 6-2 lists all of the MBean configuration files in an SESM deployment.

**Table 6-2 Summary of MBean Configuration Files**

Component	File Path and Name	Description
Container (Jetty)	jetty config nwsp.jetty.xml wap.jetty.xml pda.jetty.xml cdat.jetty.xml captiveportal.jetty.xml messageportal.jetty.xml yourapp.jetty.xml	These files configure the Jetty server instance associated with each application. These files configure: <ul style="list-style-type: none"> <li>• Logging and debugging for the Jetty server. This log filename is <i>nnn.jetty.log</i>.</li> <li>• HTTP listener, which configures: <ul style="list-style-type: none"> <li>– The application that is running in the container and the application port.</li> <li>– The web server’s standard HTTP request log. This log filename is <i>nnn.request.log</i>.</li> </ul> </li> </ul>
SESM web portals	nwsp config nwsp.xml wap config wap.xml pda config pda.xml captiveportal config captiveportal.xml messageportal config messageportal.xml	This file configures: <ul style="list-style-type: none"> <li>• SESM deployment options</li> <li>• Communication between an SESM web application and SSG</li> <li>• Communication between an SESM web application and RADIUS servers</li> <li>• Logging and debugging for the SESM web application. The log filename is <i>nnn.application.log</i>.</li> <li>• Captive portal options and behavior. See <a href="#">Chapter 8, “Deploying a Captive Portal Solution,”</a> for more information.</li> </ul>
RDP	rdp config rdp.xml	This file configures: <ul style="list-style-type: none"> <li>• RDP options, including 3-key authentication and packet handlers</li> <li>• RDP communication with SSG</li> <li>• Optionally, RDP communication with a RADIUS server</li> <li>• Logging and debugging for RDP</li> </ul>
CDAT	cdat config cdat.xml	This file configures: <ul style="list-style-type: none"> <li>• System resource usage for the CDAT application</li> <li>• Logging and debugging for the CDAT application</li> </ul>
SPE	dess-auth config config.xml	This file configures attributes used by the executing classes in the SPE application programming interfaces (APIs). The SPE APIs provide the underlying support for communication between an LDAP directory and the RDP, CDAT, and SESM portal applications. If these applications are installed on the same machine, the same config.xml file applies to all of the applications.  This file configures LDAP directory security and connection attributes, SPE caching, and SPE logging.

## MBean Configuration File Format

This section summarizes the MBean file format defined in `xmlconfig.dtd`. The purpose of this summary is to provide enough information for you to easily edit the MBean files. For the full text of the DTD, including extensive comments, see [Appendix C, “DTD for MBean Configuration Files.”](#)

Use the following example as a reference while reading the format guidelines that follow. The example configures the debugging MBean for an SESM application.

```
<Instantiate order="1"
  class="com.cisco.aggbu.jmx.LoggerMBean"
  jmxname="com.cisco.aggbu:name=Logger"/>

</Instantiate>

<!-- ===== -->
<Configure jmxname="com.cisco.aggbu:name=Logger">
  <Set name="debug" type="boolean"><SystemProperty name="nwsp.debug"
    default="false"/></Set>
  <Set name="debugPatterns"></Set>
  <Set name="debugThreads"></Set>
  <Set name="debugVerbosity">LOW</Set>
  <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS</Set>
  <Set name="logFile"><SystemProperty name="application.log"
    default="./logs"/>/>yyyy_mm_dd.application.log</Set>
  <Set name="logFrame" type="boolean">false</Set>
  <Set name="logStack" type="boolean">false</Set>
  <Set name="logThread" type="boolean">true</Set>
  <Set name="logToErr" type="boolean"><SystemProperty name="nwsp.logToErr"
    default="false"/></Set>
  <Set name="trace" type="boolean">true</Set>
  <Set name="warning" type="boolean">true</Set>
</Configure>
```

The following guidelines explain the basic format of the MBean configuration files.

- The MBean configuration file contains a single `<XmlConfig>` element containing one or more `<Configure>` elements.
- Each `<Configure>` element describes the configuration for either:
  - A single MBean, identified with the `name` attribute
  - A class of MBeans, identified with the `class` attribute

Each `<Configure>` element must contain one of the above attributes, or both. `ConfigAgent` matches a registered MBean by both class and name, so that two `<Configure>` elements might be applied to an MBean.

The `<Instantiate order = x>` tag causes the `ConfigAgent` to construct and initialize the named MBean or class of MBeans.

The value assigned to the `order` attribute controls the order in which objects are initialized by the `ConfigAgent`. The lowest value is initialized first and the highest value is initialized last. For example, in the `nwsp.xml` file, the logger MBean uses the value 1, to ensure that it is initialized first.

After being initialized, an MBean registers itself with the MBean server. When `ConfigAgent` detects the newly registered object, it then configures the object.

- The `<Set>` tag identifies an MBean attribute. The format for the `<Set>` tag is:

```
<set name="parmName" [type="dataType"]>value</set>
```

Where:

*parmName* is the MBean parameter name whose value is being set. Do not change any *parmName*.  
*dataType* is the required data type of the value you specify. If *dataType* is not explicitly identified, the default *dataType* is string. It is best not to change any *dataType*.

*value* is the parameter value. You can edit the value, making sure that the value you provide conforms to the data type specified.

- The <Call> tag calls a method defined within the class or the object's class. If the method expects arguments, they are specified within the call tag as well.
- The <Arg> tag inside a call tag can be set to any of the following:
  - Literal values.
  - Objects that are created by a New element or returned by a Call element. Call and New elements might contain Set, Put, and Call elements after any Arg elements. These nested elements are applied to the created or returned object.
- A <SystemProperty> tag might appear inside a <Set> or <Call> tag. See the next section (“[Java System Properties in the MBean Configuration Files](#)”) for more information.

## Java System Properties in the MBean Configuration Files

The MBean configuration files use Java system properties as the value for some attributes. The value of a Java system property is set as follows:

1. You can specify a value on the command line at run time. The command line value overrides all other values. The -D argument to the JAVA command defines the value of a system property.
2. You can specify a value in the startup script. For example, the following lines from the installed start scripts (START.sh or START.cmd) set some system properties.

```
$JAVA -Xmx64m -Xmx64m \
  -classpath $CLASSPATH \
  -Djetty.home=$JETTYDIR \
  -Dapplication.home=$APPDIR \
  -Dapplication.log=$LOGDIR \
  -Dapplication.portno=$PORTNO \
```

For a description of how the start script derives values for the environment variables used in the assignments, see [Table 7-1 on page 7-5](#).

3. If a value is not specified by either of the above methods at run time, the application uses a default value specified in the MBean configuration file.

In the MBean configuration files, the <SystemProperty> tag might appear inside a <Set> or <Call> tag. The format is:

```
<SystemProperty name="propertyName" default="value"/>
```

Where:

*propertyName* is the Java system property name.

*value* is the default value used if no value is assigned at run time.



### Note

If a system property is defined in the startup script, the default values in the MBean configuration files are not used, unless you delete the setting in the startup script.



# Configuring the J2EE Jetty Container

This section includes the following topics:

- [Containers and Applications, page 6-7](#)
- [J2EE Container Configuration Attributes, page 6-8](#)

## Containers and Applications

This section defines containers and applications, and describes the relationship between them.

SESM applications and CDAT are J2EE web applications. The J2EE web server is the *container* for the applications that run in it. For example, the Jetty server is the container for the installed NWSP application.

### One-to-One Relationship

The SESM core model, the NWSP sample application, and CDAT are designed and configured with the assumption that there is a one-to-one relationship between the web server container and each web application. That is, each application runs in its own web server container. If you are running two instances of the same application, or two different applications, you are running two web servers.

This one-to-one relationship means that you can configure the J2EE server differently for each application. For example, you can turn on logging for one application and turn it off for another.

### Configuration File Locations

Each SESM web application (and also CDAT) has two MBean configuration files associated with it. The two files are:

- Application MBean configuration file—Configures the application. For example:

```
nwsp
  config
    nwsp.xml

cdat
  config
    cdat.xml
```

- Container MBean configuration file—Configures the J2EE server for the application. The container's config directory holds an MBean configuration file for *each* application. For example:

```
jetty
  config
    nwsp.jetty.xml
    cdat.jetty.xml
    newapplication.jetty.xml
```

This modular approach has the following advantages:

- Easy to switch containers. If you change the J2EE container, you must make changes to the container MBeans, such as changing class or object names, or adding more MBeans.
- Defines the process that each MBean is configuring. For example, both the container and the application have logging and debugging MBeans.

The RDP and SPE components are not web applications. Therefore, the jetty directory does not contain an MBean configuration file for those components.

## J2EE Container Configuration Attributes

This section describes the attributes in the J2EE container MBean configuration files. These files are located in the container's config directory. For example:

```
jetty
  config
    nwsp.jetty.xml
    cdat.jetty.xml
```

The container MBean configuration files configure the following MBeans:

- Log—Enables the Jetty server logging mechanism and configures the information to appear in the jetty log files.
- DebugMBean—Enables or disables the Jetty server debugging mechanism.
- Jetty—Configures the following:
  - The port that the Jetty server listens on for HTTP requests from subscribers and the listener thread pools. Two listeners are used, a main listener and a listener for requests on the Secure Sockets Layer (SSL). Each listener has one pool.
  - The web application to which the requests should be sent. The installed sample files identify two sample applications: the NWSP application and the captive portal application.
  - A request log, which records all HTTP requests.

[Table 6-3](#) describes the attributes in the container MBean configuration files. For an example file, see the [“Sample Container MBean Configuration File”](#) section on page F-1.

Table 6-3 Attributes in the Container MBean Configuration Files

Object Name	Attribute Name	Explanation
Log	append	Indicates if messages overwrite existing contents (false) or are appended to the existing file (true). Installed default: true
	filename	Specifies the log filename and path, as follows: <i>application.log/yyyy_mm_dd.jetty.log</i> Where: <ul style="list-style-type: none"> <li><i>application.log</i>—Is a Java system property. The same system property is used for all log files, so that they are all created in the same directory. <a href="#">Table 7-1 on page 7-5</a> describes how the start script sets <i>application.log</i>.</li> <li><i>yyyy_mm_dd</i>—Is the year, month, and day that the file was created.</li> <li><i>.jetty.log</i>—Is a constant identifying the Jetty log files.</li> </ul>
	logTimezone	Installed default: empty
	logDateFormat	Controls the format of the date stamp in the log messages. Installed default: yyyyMMdd:HHmmss.SSS
	logLabels	Controls whether or not logging messages include frame details. Installed default: false
	logOneLine	Installed default: false
	logStackSize	Controls whether or not logging messages include an indication of stack depth. Installed default: false
	logStackTrace	Controls whether or not logging messages include trace information. Installed default: false
	logTags	Installed default: false
	logTimeStamps	Installed default: false
retainDays	Indicates the number of days to keep an old log file before deleting it. Installed default: 31	

**Table 6-3** Attributes in the Container MBean Configuration Files (continued)

Object Name	Attribute Name	Explanation
DebugMBean	debug	Controls whether or not debugging messages are produced. Installed default: false
	debugPatterns	By specifying one or more patterns, you turn on a filtering mechanism that excludes any message that does not match the pattern. The patterns are file, class, or method names. Pattern matching is based on substring matches. For example, if you specify the pattern RADIUS, the software focuses on RADIUS messages. To specify multiple patterns, separate the patterns using a comma. Installed default: empty
	debugTriggers	Installed default: empty
	verbose	Specifies the level of detail reported in debugging messages. The range of allowed values is 0 (no details) to 255 (all details). Installed default: 0
	suppressStack	Controls whether or not stack information is included in debug messages. Installed default: false
	suppressWarnings	Controls whether or not warning messages are included in debug messages. Installed default: false

Table 6-3 Attributes in the Container MBean Configuration Files (continued)

Object Name	Attribute Name	Explanation
Jetty addListener for http.SocketListener	port	<p>Sets the port number that the web server listens on. The installed value is a Java system property named:</p> <pre>application.portno</pre> <p><b>Note</b> The startup script sets this system property. Unless you alter the startup script, the default value in the MBean configuration file is ignored during application startup.</p> <p>To change the value of <code>application.portno</code>, edit the application-specific startup script.</p> <p>Installed value: The SESM installation program sets the <code>application.portno</code> in the startup script to the NWSP port that you provided during the installation process.</p>
	minThreads	<p>Sets the minimum number of threads that this listener will maintain during periods of low load. This listener will always have system resources allocated for this number of threads.</p> <p>Installed default: 5</p>
	maxThreads	<p>Sets the maximum number of threads that this listener can allocate resources for, even during peak loads. This listener can have up to this number of threads.</p> <p>Installed default: 255</p>
	maxIdleTimeMs	<p>Specifies how long a thread can be idle (not used) before the listener deallocates it. The unit is milliseconds.</p> <p>Installed default: 60000</p>
	maxReadTimeMs	<p>Specifies the time that a read on a request can block. This is how long the web server waits for a request to come from a client after the client opens a socket connection. When <code>maxReadTimeMs</code> is exceeded, the web server closes the socket connection.</p> <p>Installed default: 60000</p>

Table 6-3 Attributes in the Container MBean Configuration Files (continued)


Object Name	Attribute Name	Explanation
Jetty AddListener for http.SunJsseListener	port	<p>Sets the port that the secure socket layer (SSL) listener uses. The installed value is a Java system property named:</p> <pre>application.ssl.portno</pre> <p><b>Note</b> The startup script sets this system property. Unless you alter the startup script, the default value in the MBean configuration file is ignored during application startup.</p> <p>The generic startup script derives a value for <code>application.ssl.portno</code> based on the value of <code>application.portno</code>, as follows:</p> <pre>application.ssl.portno = application.portno - 80 + 443</pre> <p>To change the value of <code>application.ssl.portno</code>, edit the generic startup script.</p>
	MinThreads	<p>Sets the minimum number of threads that this listener will maintain during periods of low load. This listener will always have system resources allocated for this number of threads.</p> <p>Installed default: 5</p>
	MaxThreads	<p>Sets the maximum number of threads that this listener can allocate resources for, even during peak loads. The listener can allocate up to this number of threads.</p> <p>Installed default: 255</p>
	MaxIdleTimeMs	<p>Specifies the length of time a thread can be idle (not used) before the listener deallocates it. The unit is milliseconds.</p> <p>Installed default: 50000</p>
	Keystore	<p>Sets the path name of the SSL keystore file. The keystore file is a binary file created by keytool. A sample keystore file is included in the installation. The name and location of the sample is:</p> <pre>jetty.home/config/nwspkeystore</pre> <p>Where:</p> <p><i>jetty.home</i>—Is a Java system property. The NWSP start script derives the value of <i>jetty.home</i> from an expected (installed) directory structure. To change the value of <i>jetty.home</i>, edit the start script. Unless you alter the start script, the default value for <i>jetty.home</i> specified in this MBean configuration file is ignored at run time.</p> <p> <b>Caution</b> A keystore file is required for deployments that use HTTPS. HTTPS does not function without a valid keystore file. The nwspkeystore file included with the SESM installation works, but you should replace it with a keystore valid for your specific deployment. See the “<a href="#">HTTPS Description</a>” section on page A-2 for more information</p>
	Password	Must match the value in the keystore file referenced above.
KeyPassword	Must match the value in the keystore file referenced above.	

Table 6-3 Attributes in the Container MBean Configuration Files (continued)

Object Name	Attribute Name	Explanation
Jetty logSink  Configures a log file that records the incoming HTTP requests.	This is a positional argument.	The logSink class has one argument, which specifies the name and location of the request log. The installed value is:  <i>application.log/yyyy_mm_dd.request.log</i>  Where: <ul style="list-style-type: none"> <li><i>application.log</i>—Is a Java system property, whose value is set in the generic startup script. The same system property is used for all log files, so that they are all created in the same directory. See <a href="#">Table 7-1 on page 7-5</a> for a description of how the start script sets <i>application.log</i>.</li> <li><i>yyyy_mm_dd</i>—Is the year, month, and day that the file was created. The installation program uses the appropriate path name delimiter for the installation platform.</li> <li><i>.request.log</i>—Is a constant identifying an HTTP request file.</li> </ul>
	retainDays	Indicates the number of days to keep an old log file before deleting it. Installed default: 90
	append	Indicates whether or not to append messages to an existing file or to create a new file for each application instance. Installed default: true

Table 6-3 Attributes in the Container MBean Configuration Files (continued)

Object Name	Attribute Name	Explanation
Jetty— <Call AddWebApplication>  This call adds the NWSP application to run on the web server.	These are positional arguments.	AddWebApplication has five positional arguments: <ol style="list-style-type: none"> <li>1. The first positional argument specifies the virtual host name for the web server application.</li> <li>2. The second positional argument specifies the context path for locating the web server application. For example, / or /pathname/*.</li> <li>3. The third positional argument identifies the location of the application. The value is: <i>application.home/docroot</i> Where: <i>application.home</i> is a Java system property.</li> <li>4. The fourth positional argument identifies the location of the webdefault.xml file for this application. The value is: <i>jetty.home/config/webdefault.xml</i> Where: <i>jetty.home</i> is a Java system property</li> <li>5. The fifth positional argument specifies whether or not web archive (WAR) files are used. Valid values are TRUE and FALSE. Set this value to FALSE, because NWSP and CDAT are not WAR files.</li> </ol> The first three arguments define the location of the web server application. <i>host/context/application</i>  The NWSP start script derives the values for <i>application.home</i> and <i>jetty.home</i> from an expected (installed) directory structure. To change the value of <i>application.home</i> or <i>jetty.home</i> , edit the start script.

## Configuring an SESM Portal Application

This section describes how to configure an SESM portal application, using the NWSP application as an example. The section includes the following topics:

- [SESM Application Attributes, page 6-14](#)
- [Associating SSGs and Subscriber Requests, page 6-25](#)

## SESM Application Attributes

This section describes the SESM application MBean configuration file. This file is located in the application's config directory. For example:

```
nwsp
  config
    nwsp.xml
```



The application MBean configuration file configures the following MBeans:

- **Logger**—The `com.cisco.aggbu.jmx.LoggerMBean` configures both logging and debugging tools. The logging tool traces business events in the SESM portal. The debugging mechanism produces messages useful to developers in debugging applications.
- **ManagementConsole**—This MBean configures a management console port for development and testing purposes. On this port, you can see the currently set values for all attributes in all of the MBean configuration files.
- **SESM**—This MBean configures SESM features and options, including the SESM mode.
- **SESMDemoMode**—This MBean configures SESM in demo mode.
- **DESSMode**—This MBean configures SPE attributes used by the SESM application.
- **SSG**—The SSG MBean configures communication between SESM web application and SSG. These components communicate using the RADIUS protocol, so this MBean includes RADIUS protocol attributes. The MBean also includes attributes that determine which SSG should handle a subscriber request.
- **AAA**—The AAA MBean configures communication between SESM web application and the RADIUS servers.
- **WebApp**—The WebApp MBean configures options of the SESM portal application, including:
  - Attributes that control the behavior of the application
  - Attributes that control captive portal service redirections handled by NWSP
  - Context parameters, which are used by an application for any arbitrary reason. The `nwsp.xml` file contains an example of using context parameters to control web page content based on location.

[Table 6-4](#) explains the configurable attributes in the MBeans listed above. For an example file, see the [“Sample Application MBean Configuration File”](#) section on page F-3.

Table 6-4 Attributes in the Application MBean Configuration File

Object	Attribute Name	Explanation
Logger	debug	<p>Turns debugging on or off. Note that logging is on regardless of this value.</p> <ul style="list-style-type: none"> <li>False—The application produces trace messages but not debug messages. The trace messages record business activity performed by the SESM portal. This setting is the normal, recommended setting for production environments. The trace messages provide important information for diagnosing configuration problems.</li> <li>True—The application produces trace and debug messages. This setting is intended for development environments to debug portal code behavior. The logging of debug messages can affect performance; hence, this setting is not recommended for production environments.</li> </ul> <p>The following parameters control the contents of debug messages that the application generates: logFrame, logStack, logThread, debugPatterns, and debugThreads.</p> <p>The following parameters control the types of logging messages produced: trace and warning.</p> <p>Installed default: false</p>
	debugPatterns	<p>By specifying one or more patterns, you turn on a filtering mechanism that excludes any message that does not match the pattern. The patterns are file, class, or method names. Pattern matching is based on substring matches. For example, if you specify the pattern RADIUS, the software focuses on RADIUS messages. To specify multiple patterns, separate the patterns using a comma.</p> <p>Installed default: empty, which means that you receive all messages.</p>
	debugThreads	<p>Specifies a specific thread name for which to show debugging messages. You can specify multiple thread names, separating them using a comma. By default, no thread name is specified.</p> <p>Because each user interaction with the SESM web application takes place in a thread named for that user, this parameter can be used to focus the logging trace on a specific user activity. (This feature is not implemented in SESM Release 3.1(1).)</p> <p>Installed default: empty</p>
	debugVerbosity	<p>Specifies the level of detail in debugging messages. When the debug attribute is set to false, this attribute is ignored. Values are:</p> <ul style="list-style-type: none"> <li>MAX</li> <li>MED</li> <li>LOW</li> </ul> <p>Installed default: LOW</p>
	logDateFormat	<p>Specifies format of dates in the log file.</p> <p>Installed default: yyyyMMdd:HHmmss.SSS</p>

**Table 6-4** Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
Logger (continued)	logFile	Specifies the filename and location for the logging (tracing) of business events performed by the SESM application. The installed default is:  <i>application.log/yyyy_mm_dd.application.log</i>  Where: <ul style="list-style-type: none"> <li><i>application.log</i>—Is a Java system property. The same system property is used for all log files, so that they are all created in the same directory. See <a href="#">Table 7-1 on page 7-5</a> for a description of how the start script sets <i>application.log</i>.</li> <li><i>yyyy_mm_dd</i> —Is the year, month, and day that the file was created.</li> <li><i>application.log</i>—Is a constant identifying the application log files.</li> </ul>
	logFrame	Controls whether or not to log the calling member function. Installed default: false
	logStack	Controls whether or not to log stack traces. Installed default: false
	logThread	Controls whether or not to log thread IDs. Installed default: true
	logToErr	Controls whether or not to route log messages to stderr, in addition to the log file. This parameter is useful for monitoring the SESM web application at the command line. Displaying output to stderr is not recommended for production deployments. Installed default: true
	trace	Controls whether or not to log trace messages. These messages indicate entry and exit to code points. Installed default: true
	warning	Controls whether or not to log warning messages (nonfatal exceptions). Installed default: true

Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
ManagementConsole	Port	<p>Specifies a port for a management console.</p> <p>The management console displays the current settings of all attributes in all of the MBean configuration files. The console is useful in development and testing environments.</p> <p><b>Note</b> The ManagementConsole is the HTML adaptor server included with the Sun example JMX server. However, the HTML adaptor server is not production quality. For example, configuration changes that you make using the management console are not persistent. You should remove the HTML adaptor server from your configuration before transitioning the SESM deployment to public use.</p> <p>To remove the JMX HTML adaptor server, comment out the following lines in the configuration files:</p> <pre>&lt;Configure jmxname="com.cisco.aggbu:name=ManagementConsole"&gt; &lt;Call name="start"/&gt; &lt;/Configure&gt;</pre> <p>The port value is a Java system property named:</p> <pre>management.portno</pre> <p>All of the installed startup scripts set this Java system property to the following value:</p> <pre>application.portno + 100</pre> <p>For example, if the application.portno is 8080, the management.portno is 8180.</p> <p>This runtime setting overrides any value you enter in the configuration file. To change the value of this attribute, edit the start script.</p>
	AuthInfo	<p>AuthInfo provides a level of access control on the Management Console. When a user attempts to access the management console port from a web browser, a logon window appears first. The user must enter a user ID and password that matches the values specified here.</p> <p>AuthInfo requires two positional arguments:</p> <ol style="list-style-type: none"> <li>1. User ID—Enter a user ID that will be required to access the management console. The default value in all of the MBean configuration files is <code>MgmtUser</code>.</li> <li>2. Password—Enter a password that will be required to access the management console. The default value in all of the MBean configuration files is <code>MgmtPassword</code>.</li> </ol>

Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
SESM	mode	<p>An SESM portal runs in one of the following modes.</p> <ul style="list-style-type: none"> <li>• RADIUS—In this mode, the SESM web application communicates with SSG and a RADIUS server.</li> <li>• LDAP—In this mode, the SESM web application communicates with SSG and an LDAP directory.</li> <li>• Demo—In this mode, the SESM web application does not communicate with other components. Rather, it simulates communication by reading data from a Merit flat file. This mode is intended for demonstrations only, when network components such as SSG, RADIUS, or an LDAP directory are not available.</li> </ul> <p>The value for mode is a Java system property named:</p> <pre>sesm.mode</pre> <p>This system property is different from most of the other system properties used in the MBean configuration files, in that, by default, the startup script does <i>not</i> set this system property. Therefore, the application runs in the mode specified in the MBean configuration file unless you explicitly override that value at run time. The installation program sets the default value to match the type of installation you perform (RADIUS, LDAP, or Demo.)</p> <p>To change the mode, you can:</p> <ul style="list-style-type: none"> <li>• Reinstall the software.</li> <li>• Edit the MBean configuration files, changing the mode and other attributes, as appropriate.</li> <li>• Use the mode option on the SESM application startup script command line. This command line option provides a way to quickly switch between modes for testing purposes. You might need to alter the start script to access a different set of MBean configuration files for each mode, or use some other method to ensure that the attributes match the mode you are using. The syntax is: <ul style="list-style-type: none"> <li>– On Solaris: <code>jetty/bin/startNWSP.sh -mode {Demo   RADIUS   LDAP}</code></li> <li>– On Windows: <code>jetty\bin\startNWSP.cmd {Demo   RADIUS   LDAP}</code></li> </ul> </li> </ul> <p><b>Note</b> The best way to change the SESM mode is to reinstall the software. Several other configuration attributes must be aligned with the mode for SESM to run properly in the selected mode. Also, you might not have all of the appropriate components to run in a mode other than the one you installed. For example, a demo installation does not install the SPE component.</p>

Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
SESM (continued)	singleSignOn	<p>Enables or disables the single sign-on feature.</p> <ul style="list-style-type: none"> <li>• True—Subscribers only need to authenticate during a session. Single sign-on offers the following advantages: <ul style="list-style-type: none"> <li>– Subscribers can stop the browser or navigate away from the SESM portal pages, and then return to the SESM pages later and not be required to reauthenticate.</li> <li>– Subscribers do not need to reauthenticate if SESM automatic memory management clears sessions from the SESM portal.</li> <li>– Point-to-point protocol (PPP) clients do not need to authenticate to the SESM portal. Instead, the SESM portal uses the PPP authenticated identity from SSG.</li> </ul> </li> <li>• False—Subscribers are required to reauthenticate for all of the cases described above.</li> </ul> <p>Installed default: true</p>
	autoConnect	<p>Specifies if SESM should send connection requests to SSG for the services marked for auto connection in the subscriber's profile. Values are:</p> <ul style="list-style-type: none"> <li>• False—SESM does not send connection requests to SSG</li> <li>• True—SESM sends connection requests to SSG</li> </ul> <p>In RADIUS mode, set this attribute to false, because SSG automatically makes the connections immediately after authentication. You do not need SESM to request those connections.</p> <p>In LDAP mode, the SSG performs automatic connections if it obtains a service list from the RDP. If SSG does not obtain the service list from RDP, you should set this attribute to true.</p> <p>The Add Services option, which is set during RDP installation, controls whether or not the RDP returns a service list to SSG. The Add Services option configures RDP to either:</p> <ul style="list-style-type: none"> <li>• Return a service list to SSG—SSG performs automatic connections for services marked as auto connect in a subscriber's profile. In this configuration, set the autoConnect attribute to false.</li> <li>• Not return a service list to SSG—SSG cannot perform automatic connections. The advantage to this configuration is that it saves memory on the SSG device. In this configuration, set the autoConnect attribute to true.</li> </ul>
	profileCachePeriod	<p>Specifies the time in seconds that a service or group object must be idle in the cache before its resources are deallocated from memory.</p> <p>Installed default: 600</p>
	sessionCachePeriod	<p>The minimum time in seconds that an SESM session can be in memory without being accessed.</p> <p>Installed default: 1200</p>

Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
SESM (continued)	confirmMutex Disconnect	<p>Controls the action of the SESM portal if a subscriber is currently connected to a service in a mutually exclusive service group and then selects another service in that group.</p> <ul style="list-style-type: none"> <li>• True—The SESM portal displays an error message to the subscriber stating that the current service must be disconnected before selecting the newly selected service.</li> <li>• False—The SESM portal sends a request to SSG to disconnect the current service before sending the request to connect to the newly selected service.</li> </ul> <p>Installed default: false</p>
SESMDemoMode	demoDataFile	<p>Specifies the file that contains data for demo mode. The installed value is:</p> <p><i>application.home/config/demo.txt</i></p> <p>Where:</p> <p><i>application.home</i> is a Java system property</p> <p>The NWSP start script derives the value for <i>application.home</i> from an expected (installed) directory structure. To change the value of <i>application.home</i>, edit the start script.</p>
DESSMode	tokenCheckInterval	<p>The time in seconds between checking the authorization tokens.</p> <p>Default: 300 seconds</p>
	tokenMaxAge	<p>The length of time in seconds a token can remain in cache without being used before it is deleted.</p> <p>Default: 600 seconds</p>

Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
SSG Global attributes The global attributes apply to all SSGs that the SESM web application might communicate with. To determine how an SSG was configured, use the <b>show run</b> command on the SSG host.	throttle	<p>The global value for the maximum number of simultaneous requests that SESM portals can send to an SSG. The RADIUS protocol queues additional requests and issues them as the SSG returns responses or timeout messages for previous requests.</p> <p>If set correctly, this throttle attribute prevents the situation in which the SSG receives requests at a faster rate than it can handle, causing the SESM application to time out waiting for responses. Set the throttle value according to the ability of the SSG device to process access requests from a client. Try adjusting this value lower if the SESM portal is timing out while waiting for responses from the SSG.</p> <p>You cannot override the global value. (The same throttle value applies to all SSGs.)</p> <p>Installed default: 20</p>
	PORT	<p>The global value for RADIUS ports on the SSG hosts. This value must match the value that was configured on the SSG device using the following command:</p> <pre>ssg radius-helper authenticationPort</pre> <p>You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.</p>
	TIMEOUTSECS	<p>The number of seconds the SESM web application waits before timing out RADIUS packets that it sends to SSG. You cannot override this global value.</p> <p>Installed default: 5</p>
	RETRIES	<p>The number of times the SESM web application resends a RADIUS packet to SSG if no response is received. You cannot override this global value.</p> <p>Installed default: 3</p>
	SECRET	<p>The global value for the RADIUS protocol shared secret used for communication between the SESM web application and the SSGs. This value must match the value entered on the SSG device using the <b>ssg radius-helper key</b> command.</p> <p>You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.</p>
	MASK	<p>The global value for the mask that the SESM web application applies to incoming subscriber IP addresses to derive an IP address for the SSG.</p> <p>You can create subnet entries in the MBean configuration file to override this global value for specific subnets.</p>
	BUNDLE_LENGTH	<p>The global value for the port bundle length that SSGs use when the port-bundle host key feature is enabled.</p> <p>The port bundle length is the number of bits that SSG uses to indicate bundled slots. For example, a value of 4 indicates 16 bundled slots. This value must match the value used in the following command on the SSG host:</p> <pre>ssg port-map length</pre> <p>Default: You set this value during installation.</p>



Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
SSG global attributes (continued)	PORT_BUNDLE_ HOST_KEY_ SWITCH	<p>The global value indicating whether or not the port-bundle host key feature is enabled on the SSGs. If BUNDLE_LENGTH is zero, then the value of this switch is important.</p> <ul style="list-style-type: none"> <li>• True—The SSGs have port-bundle host key enabled with a 0 bundle length.</li> <li>• False—The SSGs do not have port-bundle host key enabled.</li> </ul> <p><b>Note</b> If BUNDLE_LENGTH is non-zero, this switch is ignored, because a nonzero value implies the use of the host key feature.</p>
SSG Subnet entries  Use subnet entries to override the global values or to map client subnets to specific SSGs when the port-bundle host key feature is not being used.	Subnet entries use positional arguments.	<p>The call to setSubnetAttribute has four positional arguments:</p> <ol style="list-style-type: none"> <li>1. <i>subnetAddress</i> is the subnet for which you are explicitly setting a value, overriding the globally set value.</li> <li>2. <i>subnetMask</i> is the mask that can be applied to the subscriber's IP address to derive the subnet.</li> <li>3. <i>argumentName</i> is the argument that you are explicitly setting.</li> <li>4. <i>argumentValue</i> is the value for <i>argumentName</i>.</li> </ol> <p>See the <a href="#">“Associating SSGs and Subscriber Requests”</a> section on page 6-25 for more information.</p>

Table 6-4 Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
AAA  This MBean defines communication between the SESM web application and the RADIUS server, which occurs only when the SESM application is running in RADIUS mode.	Connection	The Configure element in the AAA MBean includes a connection attribute that identifies the type of request. Values are: <ul style="list-style-type: none"> <li>ServiceProfile—The MBean for this connection type includes the servicePassword attribute.</li> <li>ServiceGroupProfile—The MBean for this connection type includes the serviceGroupPassword attribute.</li> </ul>
	throttle	The maximum number of simultaneous requests that SESM web applications can send to a RADIUS server. This is a RADIUS protocol attribute. The RADIUS protocol queues additional requests and issues them as the server returns responses or timeout messages for previous requests.  Installed default: 256
	timeOut	The number of seconds the SESM web application waits before timing out RADIUS packets that it sends to the AAA server.  Installed default: 4
	retryCount	The number of times the SESM web application resends packets to the AAA server if no response is received.  Installed default: 3
	primaryIP	The IP address or the host name of the primary AAA server.
	primaryPort	The port number that the primary RADIUS server listens on.  Default: 1812
	secret	The shared secret used between the RADIUS server and the SESM web application. The shared secret must be the same for the primary and secondary servers. It must match the secret specified when you configured SESM as a NAS client on the RADIUS server.  Default: <code>cisco</code> .
	secondaryIP	The IP address or host name of the secondary AAA server. If you are not using a secondary RADIUS server, reenter the primary server.
	secondaryPort	The port number that the secondary RADIUS server listens on. If you are not using a secondary server, reenter the primary server.  Default: 1812
	servicePassword	The password that the SESM web application uses to request service profiles from the RADIUS server. It must match the service password values used in the service profiles in the RADIUS database. It must also match the value that was configured on the SSG host with the following command:  <code>ssg service-password password</code>  The service-password value must be the same on all of your SSGs.  Default: <code>servicecisco</code>
serviceGroup Password	The password that the SESM web application uses to request group profiles from the RADIUS server. It must match the service group password values used in the service group profiles in the RADIUS database.  Default: <code>groupcisco</code>	

**Table 6-4** Attributes in the Application MBean Configuration File (continued)

Object	Attribute Name	Explanation
WebApp	confirmAtService Logon	Controls whether or not the application prompts the user for confirmation before it acts on a request to start a service. Default: FALSE
	confirmAtService Logoff	Controls whether or not the application prompts the user for confirmation before it acts on a request to log off. Default: TRUE
	confirmAtAccount Logoff	Controls whether or not the application prompts the user for confirmation before it acts on a request to log off of the SESM application. Default: TRUE
	sessionTimeOut	The number of seconds of inactivity allowed before the application closes a session. This value overrides the timeout value in the nwsp.jetty.xml file. Default: 7200
	credentialMax Length	Controls the maximum length of user names and passwords. Default: 30
	serviceNotGivenURI defaultURI serviceSubscriptioURI serviceStartURI serviceLogonURI	These attributes are related to the captive portal solution. See <a href="#">Table 8-6 on page 8-20</a> for explanations of these attributes.
	Call addDimension	The addDimension call adds any arbitrary property to an incoming request. See the “ <a href="#">Configuration-based Location and Brand Awareness</a> ” section on <a href="#">page 6-44</a> for more information.

## Associating SSGs and Subscriber Requests

A typical SESM deployment consists of multiple SSGs. An SESM web application must know which SSG is handling each subscriber request. This section describes how to configure the associations between a subscriber request and its SSG. It includes the following topics:

- [Using Port-bundle Host Key with Identical SSG Configurations, page 6-25](#)
- [Using Port-bundle Host Key with Varying SSG Configurations, page 6-27](#)
- [Specifically Mapping SSGs to Subscriber Subnets, page 6-27](#)
- [Global and Subnet Attribute Elements, page 6-28](#)

### Using Port-bundle Host Key with Identical SSG Configurations

The easiest way to associate the correct SSG with each subscriber request is to use the port-bundle host key feature on all SSGs, and configure certain attributes identically on all of the SSG hosts. We recommend using port-bundle host key unless you need backward compatibility with SSD Release 2.5(1).

**Note**

To use the port-bundle host key feature, the SSG device must be running Cisco IOS Release 12.2(2)B or later and the SSG port-bundle host key feature must be configured appropriately.

When the port-bundle host key feature is enabled on an SSG, the SSG replaces the subscriber IP address in the request with a software token (or key) when it forwards the request to SESM. The SESM application uses this key in its responses to SSG, and the SSG does an internal translation to an actual host object.

The key is a unique combination of an SSG IP address from a range of IP addresses and a port number from a range of port numbers, as follows:

*IP\_address:port*

The IP address and port ranges are configured on each SSG. The key uniquely identifies each subscriber currently logged on to SESM, even when multiple subscribers are using the same IP address.

To use the port-bundle host key feature to associate SSGs, follow these procedures:

1. Enable and configure the port-bundle host key feature on all of the SSGs, as described in the [“Configuring the Host Key Port Bundle Feature on SSG” section on page B-2](#).
2. Configure the same values on all of the SSG hosts for the following attributes:
  - Port—The SSG port on the SSG host. Specify the port that SSG uses to listen for RADIUS requests from an SESM application. Configure this value on the SSG device with the following command:
 

```
ssg radius-helper authenticationPort
```
  - Shared secret—The shared secret used for communication between SSG and an SESM application. Configure this value on the SSG device with the following command:
 

```
ssg radius-helper key
```
  - Port bundle length—The number of bits that SSG uses for port bundling when the port-bundle host key feature is enabled. This value must be 0 or 4. Configure this value on the SSG device with the following command:
 

```
ssg port-map length
```
3. Enter these globally configured values when the SESM installation program prompts you for them. These values are reflected in global elements in the <Configure name="SSG"> section of the application MBean configuration file, as the following example illustrates.

**Example Using Port-Bundle Host Key**

When the port-bundle host key feature is enabled and configured, you can set all parameters globally.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
</Configure>
```

In this example, all SSGs are configured to use a port of 1812 and a shared RADIUS secret of `cisco`. The `BUNDLE_LENGTH` of 4 indicates that port-bundle host key is configured on all SSGs.

The MASK attribute specifies the mask that SESM applies to the client (source) IP address in a received message to determine the client's subnet, and, from that, the SSG IP address. However, when a host key is used, the client (source) IP address is the SSG IP address. The SESM installation program provides the default mask of 255.255.255.255.

## Using Port-bundle Host Key with Varying SSG Configurations

If port-bundle host key is enabled on all SSGs, but some are configured differently, you can configure the global case and then specifically configure the exceptions. For example, if all but one SSG is assigned the same shared secret, you can configure the shared secret attribute globally, and then add one subnet entry to configure the different secret for the one SSG.

The installation program lets you provide one set of SSG global attribute values and one subnet entry. It records these attribute values in the <Configure name="SSG"> section of the application MBean configuration file, as illustrated in the following example.

### Example Using Port-bundle Host Key with One Noncomplying SSG

In this example, port-bundle host key is enabled on all SSGs. In addition, all SSGs are using the same port, secret, and client IP address mask, except that one SSG uses a different port. In this case, you can set all parameters globally, and then use one subnet entry to define:

- The client subnet being serviced by the SSG that uses the nonconforming port.
- The port value that overrides the globally-set port value.

In the following example, the SSG that services subnet 10.1.1.0 uses port 1245.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>PORT
</Arg><Arg>1245</Arg></Call>
</Configure>
```

## Specifically Mapping SSGs to Subscriber Subnets

Each request arriving at an SESM web application contains a source, or client, IP address. SESM uses this client IP address to determine which SSG should handle each request.

- If the configuration file explicitly provides an SSG IP address for a subnet or a specific client IP address, SESM uses that SSG. You code an explicit IP address in a <subnet> element. The MASK value in the subnet element specifies whether the element applies to a subnet or to a specific subscriber IP address. The <IP> parameter in the subnet element specifies the SSG IP address.

For example, the following subnet entry explicitly sets the SSG IP address to 10.6.7.1 for subnet 10.2.0.0:

```
<Call name="setSubnetAttribute">
<Arg>10.2.0.0</Arg><Arg>255.255.0.0</Arg><Arg>IP</Arg><Arg>10.6.7.1</Arg></Call>
```

- If an explicit IP address for the SSG is not provided, SESM masks the subscriber's IP address to determine the SSG that should handle the request. Use masking as follows:
  - If port-bundle host key is enabled—The port-bundle host key feature replaces the original client IP address with the IP address of the SSG. (The port bundle key appended to the address preserves a unique identity for each subscriber). Since the client IP address is the SSG IP address, a global setting for MASK of 255.255.255.255 correctly results in the client IP address being used as the SSG IP address.
  - If the SSG uses the first IP address in a particular set of client subnets—Specify the mask that SESM web application can apply to the client IP address to derive the SSG IP address. For example, if, for all 10.x.0.0 client subnets, the SSG IP address is 10.x.0.1, you would specify a subnet of 10.0.0.0 and a mask of 255.0.0.0.
  - If the SSG IP is the first IP in all client subnets—You can set a global value for mask. For example, for all subscriber addresses x.y.z.n, if the SSG always has an IP address of x.y.0.1, then use a global mask of 255.255.0.0.

**Note**

Set the widest global or subnet mask possible. Each SSG IP address consumes some resources on the machine where the SESM application is running. (Each one uses an open file descriptor.) For example, even when the SSG is using port-bundle host key, a mask of 255.255.255.0 is desirable so that the SESM uses a single SSG IP address rather than 254 different SSG IP addresses. A mask of 255.255.255.255 is the least efficient, but it is the default setup.

**Example Mapping Client Subnets to SSGs**

In this example, port-bundle host key is not being used. In this case, you must explicitly define the mapping from subscriber subnet to the SSG IP address.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1645</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.1.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.2.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.2.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.3.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.3.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.4.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.4.2</Arg></Call>
</Configure>
```

**Global and Subnet Attribute Elements**

You can set the attributes that associate an SSG with subscriber requests globally, by client subnet, or for a specific client IP address, as follows:

- Global attribute elements—A global setting applies to all SSGs. For example, a global shared secret setting means that all SSGs are configured using the same secret. The global attributes are: PORT, SECRET, MASK, and BUNDLE\_LENGTH.
- Subnet attribute elements—The subnet attributes apply to a specific subnet and override the global attribute value. The subnet attributes are optional; if any of them are not specifically coded, the global attribute value is used. Subnet attributes that you can supply are: PORT, SECRET, MASK, BUNDLE\_LENGTH, and IP. The IP attribute is the IP address of the SSG for a specified subnet.

You can also specify some optional session information in a subnet entry, using context parameter values. See [Table 6-5 on page 6-29](#).

- A specific client IP address is specified in a subnet element.

The format for the global attribute entries is illustrated in the following examples:

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1645</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.0</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>
</Configure>
```

The format for subnet entries is:

```
<Call name="setSubnetAttribute">
<Arg>subnetAddress</Arg>
<Arg>subnetMask</Arg>
<Arg>argumentName</Arg>
<Arg>argumentValue</Arg>
</Call>
```

Where:

*subnetAddress* is the subnet for which you are explicitly setting a value, overriding the globally set value.

*subnetMask* is the mask that can be applied to the subscriber's IP address to derive the subnet.

*argumentName* is the argument that you are explicitly setting ([Table 6-5](#)).

*argumentValue* is the value for *argumentName* ([Table 6-5](#)).

**Table 6-5 Argument Names and Values for Subnet Entries**

<i>argumentName</i> Value	<i>argumentValue</i> Explanation
PORT	The SSG port for the specified subnet. Overrides the globally-set SSG port.
MASK	The mask used on the subscriber's IP address to derive the subnet. Overrides the globally-set mask.
SECRET	The shared secret used between SESM and SSG. Overrides the globally-set shared secret.
BUNDLE_LENGTH	<p>The host key bundle length used on the SSG. Overrides the globally-set bundle length.</p> <p>Bundle length is the number of bits that SSG uses for the port bundle feature. For example, a value of 4 indicates 16 bundled slots. A value of 0 indicates that the SSG is not using the port-bundle host key mechanism.</p> <p>This value must match the value used in the following command on the SSG host:</p> <pre>ssg port-map length</pre> <p>To determine how SSG has configured the port bundle length, use the <b>show run</b> command on the SSG host.</p>
IP	Explicitly sets the IP address for the SSG that services the specified <i>subnetAddress</i> .

**Table 6-5** Argument Names and Values for Subnet Entries (continued)

<i>argumentName</i> Value	<i>argumentValue</i> Explanation
SESSION_LOCATION	The location associated with the specified subnet. Valid values are defined as arbitrary properties in the WebApp MBean. See the <a href="#">“Configuration-based Location and Brand Awareness”</a> section on page 6-44 for more information.
SESSION_BRAND	The brand of service associated with the specified subnet. Valid values are defined as arbitrary properties in the WebApp MBean. See the <a href="#">“Configuration-based Location and Brand Awareness”</a> section on page 6-44 for more information.

## Configuring RDP

This section describes how to configure the RDP application. The section includes the following topics:

- [RDP Modes, page 6-30](#)
- [RDP Attributes, page 6-30](#)

## RDP Modes

RDP can run in two modes:

- **Non-proxy mode**—In this mode, RDP uses the SPE API to obtain authentication and authorization information from the LDAP directory.
- **Proxy mode**—In this mode, RDP sends authentication requests to a RADIUS server. It uses the SPE API to obtain authorization information from the LDAP directory.

You choose the mode during RDP installation. The content of the `rdp.xml` file is significantly different depending on the mode. Therefore, to change the mode, we recommend reinstalling the RDP component. (Choose a Custom installation to reinstall a single component.)

## RDP Attributes

The MBean configuration file for RDP is located in:

```
rdp
  config
    rdp.xml
```

The `rdp.xml` file configures the following MBeans:

- **Logger**—The `com.cisco.aggbu.jmx.LoggerMBean` configures both logging and debugging features. The logging feature logs RDP application activity. The debugging mechanism produces messages useful to developers in debugging applications. See the *Cisco Subscriber Edge Services Web Developer Guide* for more information about debugging an application.
- **ManagementConsole**—This MBean configures a management console port. Administrators can go to this console port on a web browser and see the currently set values for all attributes in all of the MBean configuration files.



- **RDPPacketFactory**—This MBean creates RDP packets that analyze and process requests from SSG. Each request becomes a series of packets. Each type of packet is handled by a different packet handler.
- **RDP MBean**—The RDP MBean configures the listener for requests sent through SSG. It configures the SESM 3-key authentication feature.
- **AAA**—This MBean applies only when RDP is running in Proxy mode. In that mode, RDP is a RADIUS proxy server. The RDP AAA MBean defines the proxy server attributes.

[Table 6-6](#) explains the configurable attributes in these MBeans. For an example file, see the [“Sample RDP MBean Configuration File”](#) section on page F-13.

Table 6-6 Attributes in the RDP MBean Configuration File

MBean	Attribute Name	Explanation
Logger		See the Logger object in <a href="#">Table 6-4 on page 6-16</a> .
ManagementConsole		See the ManagementConsole object in <a href="#">Table 6-4 on page 6-16</a> .
RDPPacketFactory	<b>Note</b>	<p>RDP uses password values, described below, to identify the type of request it receives and determine how to handle the request. Each of the three password values <i>must</i> be unique.</p> <p>The only attributes in this MBean that administrators must change are the password attributes associated with service profile requests. These password attributes are used to identify a service request as one of the following: a single service request, a service group request, or a next hop table request. SSG sets the password in the request; RDP interprets the password. You must configure the values on both sides, as follows:</p> <ul style="list-style-type: none"> <li>• On SSG, you set the values for these three passwords using IOS commands.</li> <li>• On RDP, you set the values for the three passwords as described here.</li> </ul> <p>If the password in a request from SSG does not match one of the three values you set on the RDP side, the request is discarded.</p> <p>To find the password attributes in this MBean, search the file for the following string:</p> <pre>&lt;arg&gt;PASSWORD:</pre> <p>No security implications exist for these attributes. It might be helpful to view the attributes as identifying keys, rather than passwords.</p> <p>The three password attributes are:</p> <ul style="list-style-type: none"> <li>• <b>ServiceRequest</b>—Requests containing this password are handled by the ServiceRequest packet handler. The ServiceRequest packet handler uses the SPE API to obtain a list of authorized services for a subscriber. This password must match:</li> <li>• <b>GroupRequest</b>—Requests containing this password are handled by the GroupRequest packet handler. The GroupRequest packet handler forwards requests to a RADIUS server to obtain a list of authorized services for the group of which the subscriber is a member. Group requests are relevant only when RDP is configured in proxy mode.</li> <li>• <b>NextHopRequest</b>—Requests containing this password are handled by the ProxyNextHop packet handler. The Proxy NextHop packet handler passes authentication requests to the AAAMBean when the RDP is configured in proxy mode, or through SPE to the directory when the RDP is not in proxy mode. On the SSG side, set this password using the following command:</li> </ul> <pre>ssg next-hop download nextHopTableName password</pre> <p>See one of the following sections for more information about matching these password values to values configured elsewhere in an SESM deployment:</p> <ul style="list-style-type: none"> <li>• <a href="#">Communication Attributes for LDAP Mode, page 9-6</a></li> <li>• <a href="#">Communication Attributes for LDAP Mode with RDP in Proxy Mode, page 9-10</a></li> </ul> <p>See <a href="#">Appendix E, “RDP Packet Handlers,”</a> for more information about how RDP processes requests from SSG.</p>

Table 6-6 Attributes in the RDP MBean Configuration File (continued)

MBean	Attribute Name	Explanation
RDP MBean	secret	<p>The useClientList attribute, which appears later in this MBean, affects how the secret attribute is used.</p> <ul style="list-style-type: none"> <li>If the useClientList attribute is false, the secret is the shared secret for communication between all of the SSGs and RDP. This value must match the value configured on the SSG devices, using the following command:  <pre>radius-server key SharedSecret</pre> <p>The same shared secret value must be configured on all of the SSGs.</p> </li> <li>When the useClientList attribute is true, this secret attribute is ignored. Instead, you configure a specific shared secret for each client (each SSG).</li> </ul> <p>The installation program's displayed default is <code>cisco</code>.</p>
	localIPAddress	<p>Enter the IP address or host name of the RDP.</p> <p><b>Note</b> This value cannot be localhost (127.0.0.1)</p>
	localPort	<p>Enter the port on which the RDP will listen. The installed value is a Java system property:  <pre>application.portno</pre> <p>The installation program sets the value of <code>application.portno</code> in the RDP startup script to whatever you specified during installation. To change the value of <code>application.portno</code>, edit the start script.</p> <p>The installation program's displayed default is 1812.</p> </p>
	minThreads	<p>Sets the minimum number of threads that RDP will maintain during periods of low load. RDP will always have system resources allocated for this number of threads.</p> <p>Installed default: 10</p>
	maxThreads	<p>The total number of simultaneous requests that the RDP can handle. If the RDP is receiving more requests than the current setting, and the RDP host machine is not processor-bound, then you can increase this number for a potential performance improvement.</p> <p>Installed default: 256</p>
	maxIdleTimeMs	<p>The number of milliseconds that a thread can remain idle before the system deallocates its resources.</p> <p>Installed default: 10000</p>
	threeKeyAuth	<p>Specifies whether to use the 2-key or 3-key method to authenticate a subscriber.</p> <ul style="list-style-type: none"> <li>True—Turns on 3-key authentication, which authenticates a subscriber using the user name and password, plus one additional attribute as specified in the <code>authAttribute</code> attribute.</li> <li>False—Turns off 3-key authentication. RDP authenticates using a user name and password.</li> </ul> <p>Installed default: false</p>

Table 6-6 Attributes in the RDP MBean Configuration File (continued)

MBean	Attribute Name	Explanation
RDP (continued)	authAttribute	Specifies the RADIUS attribute number to use for the additional key when 3-key authentication is turned on. Any standard RADIUS attribute can be used. Typical values are: <ul style="list-style-type: none"> <li>• 30—CALLED_STATION_ID (APN)</li> <li>• 31—CALLING_STATION_ID (MSISDN)</li> <li>• 32—NAS_IDENTIFIER</li> </ul>
	useClientList	Turns the RDP restricted client feature on or off. Values are: <ul style="list-style-type: none"> <li>• True—The RDP accepts requests only from the clients specified in an addClient call later in this MBean. RDP clients are SSGs.</li> <li>• False—The RDP accepts requests from any client (any SSG).</li> </ul> You set the initial value of this attribute during RDP installation.
addClient	These are positional arguments.	The addClient call adds a client to the client list when the useClientList attribute is true. RDP clients are SSGs. You can add more clients by adding more addClient elements to the rdp.xml file. The addClient call has three positional arguments: <ol style="list-style-type: none"> <li>1. The first positional argument specifies a client name. This value is used in logs and traces and does not have to match any other configured value.</li> <li>2. The second positional argument specifies the client IP address.</li> <li>3. The third positional argument specifies the shared secret for communication between RDP and this client. It must match the shared secret configured on the SSG device using the following command: <pre>radius-server key SharedSecret</pre> </li> </ol>

Table 6-6 Attributes in the RDP MBean Configuration File (continued)

MBean	Attribute Name	Explanation
AAA This MBean applies only when RDP is configured in Proxy mode.	Connection	The Configure tag for the AAA MBean includes a connection attribute whose value is either: <ul style="list-style-type: none"> <li>• NextHop</li> <li>• Proxy</li> </ul> The RDP proxy handlers use the connection name to identify the AAA server to proxy the request to.
	throttle	The maximum number of simultaneous requests that RDP can send to a RADIUS server. This is a RADIUS protocol attribute. The RADIUS protocol queues additional requests and issues them as the RADIUS server returns responses or timeout messages for previous requests. Installed default: 256
	timeOut	The number of seconds RDP waits before timing out RADIUS packets that it sends to the AAA server. Installed default: 4
	retryCount	The number of times RDP resends packets to the AAA server if no response is received. Installed default: 1
	primaryIP	Enter the IP address or the host name of the primary RADIUS AAA server that you want RDP to communicate with.
	primaryPort	Enter the port number on the primary RADIUS server host that the RADIUS server listens on.
	AAASecret	Enter the RADIUS client shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers. The installation program's displayed default value is <code>cisco</code> .
	secondaryIP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.
	secondaryPort	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 same value used for the primary server.

# Configuring CDAT

This section describes how to configure the CDAT application. The section includes the following topics:

- [Cookies Required, page 6-36](#)
- [CDAT Attributes, page 6-36](#)

## Cookies Required

Make sure that the cookies feature is enabled on the browser where you are running CDAT. If the CDAT application seems to log itself off unexpectedly, check your cookies setting.

## CDAT Attributes

The CDAT MBean configuration file is located in:

```
cdat
  config
    cdat.xml
```

The cdat.xml file configures the following MBeans:

- **Logger**—The Logger MBean configures both logging and debugging tools. The logging tool logs CDAT application activity. The debugging mechanism produces messages useful for debugging.
- **ManagementConsole**—This MBean configures a management console port. Administrators can go to this console port on a web browser and see the currently set values for all attributes in all of the MBean configuration files.
- **CDAT**—The CDAT MBean configures resource attributes for the CDAT application.

[Table 6-7](#) explains the configurable attributes in this MBean. For an example file, see the [“Sample CDAT MBean Configuration File”](#) section on page F-16.

**Table 6-7** Attributes in the CDAT MBean Configuration File

MBean Name	Attribute Name	Explanation
Logger		See the Logger object in <a href="#">Table 6-4 on page 6-16</a> .
ManagementConsole		See the ManagementConsole object in <a href="#">Table 6-4 on page 6-16</a> .
CDAT	sessionTimeout	The maximum period of inactivity allowed during a CDAT login, after which the user will be logged out. Values are in seconds. A negative value will prevent the user from ever being logged out. Changes will only take effect for subsequent logins.  Default: 600
	maxVariables	The maximum number of page/page instance variables allowed for each CDAT session. This number affects how many pages can be visited before their state is lost, though it is not a one-to-one mapping. If you see many StateTimedOut errors, you should increase this number.  Default: 40
	queryMaxResults	The maximum number of results to return from any one directory query. Changes will take immediate effect. A value of zero will remove any limits.  Default: 500
	queryTimeout	The timeout (in milliseconds) for directory queries. Changes will take immediate effect. A value of zero will cause an infinite timeout.  Default: 0

## Configuring SPE

This section describes how to configure the SPE component. The section includes the following topics:

- [SPE Attributes, page 6-37](#)
- [Extending the Directory Schema and Loading Initial RBAC Objects, page 6-40](#)

Also see the “[LDAP Directory Configuration Requirements](#)” section on [page 5-4](#), which describes basic configuration requirements for the LDAP directory that must be met before you install the SPE component.

## SPE Attributes

The MBean configuration file for SPE is located in:

```
dess-auth
  config
    config.xml
```

This file applies to SESM applications that incorporate the SPE APIs, which are:

- Any SESM portal deployed in LDAP mode
- RDP
- CDAT

If these applications are installed on the same machine, the same config.xml file applies to all of them. If the applications are installed on different machines, the SPE component will be installed with each of them, and each config.xml file can contain different attribute values.

The config.xml file for SPE contains the following MBean:

- Directory—The Directory MBean configures security, location, logging, and caching attributes for executing classes in the Dess and Auth APIs.

Table 6-8 explains the configurable attributes in this MBean. For a sample file, see the “[Sample SPE MBean Configuration File](#)” section on page F-18.

**Table 6-8 Attributes in the Dess-Auth MBean Configuration File**

Object Name	Attribute Name	Explanation
Directory MBean	poolSize	Number of active connections allowed to the LDAP server.
	URL	URL of the LDAP server.
	principal	Name used when connecting to the LDAP server.
	credentials	Credentials (such as password) used for connecting to the LDAP server.
	context	Default LDAP context. This is the organization and organizational unit that was created to hold the SESM data.
	DESSPrincipal	Name used to connect to the SESM organization and organization unit. This user must have permission to create objects in the SESM context.
	alwaysGetAllAttributes	If set to true, all the attributes of an LDAP entry are returned for every query.
	traceFileName	Name of the directory log file.
	traceLevel	Should be one of: NONE, ERROR, BRIEF, VERBOSE, or DEBUG.
	printTraceToConsole	If set to true, the application sends trace messages to the console and writes them into the log file.
	stackTrace	If set to true, the application prints a stack trace with each trace message.
	cacheMaxObjects	Specifies the maximum number of software objects to hold in the cache. Objects represent subscribers, services, privileges, roles, and so on. When the cache contains cacheMaxObjects, old objects are deleted from cache, regardless of available cache space. Set this value high to allow the available cache space to be the determining factor for cache management. Installed default: 50000



Table 6-8 Attributes in the Dess-Auth MBean Configuration File (continued)

Object Name	Attribute Name	Explanation
Directory MBean	cacheMinFreeMem	<p>Specifies the percentage of Java virtual memory that must remain available (that is, not used by the cache) after the application is loaded into memory. You can calculate the specific amount of memory available for the cache as follows:</p> $cacheSize = (JavaVM - applCodeSize) * (100\% - cacheMinFreeMem)$ <p>Where:</p> <p><i>JavaVM</i> is the maximum virtual memory size specified at application startup time with the <i>jvm</i> argument. The installed startup scripts use the following values:</p> <ul style="list-style-type: none"> <li>• The startNWSP script uses 64 MB</li> <li>• The runrdp script uses 20 MB</li> </ul> <p><i>applCodeSize</i> is the application size. The NWSP is approximately 18 MB.</p> <p><i>cacheMinFreeMem</i> specifies the percentage of Java virtual memory that must remain available after the application is loaded into memory. The installed default value is 10. If NWSP and RDP applications are installed on the same machine, the same <i>cacheMinFreeMem</i> attribute value applies to both applications.</p> <p>For example, using all of the installed default values, the <i>cacheSize</i> for the NWSP application is 90% of 14 MB, or 12.6 MB:</p> $cacheSize = (32 MB - 18 MB) * (100\% - 10\%)$ <p>Installed default: 10</p>
	cacheSessionTimeout	<p>Specifies the timeout of inactive client sessions in seconds.</p> <p>Installed default: 600</p>
	cacheExpireInterval	<p>Specifies the interval in seconds after which the cache attempts to expire objects.</p> <p><b>Note</b> Do not set this attribute to 0. A value of 0 causes <i>every</i> request to go to the directory, bypassing caching and any memory storage from a recent request for the same object. A value of 0 degrades performance substantially.</p> <p>Installed default: 600</p>
	cacheObjectTimeout	<p>Specifies the number of seconds before objects time out.</p> <p>Installed default: 600</p>

## Extending the Directory Schema and Loading Initial RBAC Objects

An SESM deployment running in LDAP mode requires the following update activities on the LDAP directory:

- Extend the directory schema. These extensions include the `dess` and `auth` classes and attributes that will hold the SESM data. For more information about the extensions, see the *Cisco Distributed Administration Tool Guide*.
- Install initial RBAC objects. Some initial top-level rules and roles must be created in the directory before an administrator can log into CDAT and create additional objects.

The SPE installation process optionally performs these two update activities. If you did not choose these options during the installation, you must do them before running CDAT or an SESM application running in LDAP mode.



### Note

If the SESM components are distributed among different servers, which means that SPE might be installed in more than one location, you only need to perform these update activities one time against the LDAP directory.

To perform these updates after the initial SPE installation, use either of the following procedures:

- Use the SESM installation process to perform the updates by running a custom installation of the SPE component.
- Perform the updates manually using native administration tools and commands.

## Using an SESM Custom Installation to Update the Schema and Load RBAC Objects

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

- 
- 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 allows you to update the directory schema
    - A user ID and password that allows you to update the container (organization and organizational unit) that you created for SESM data
  - Step 3** Execute the SESM installation program on a server that has network access to the LDAP directory.
  - Step 4** When the installation program prompts for setup type, choose **Custom**.
  - Step 5** When the installation program prompts for the components to install, choose **SPE**.
  - Step 6** 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 7** When the installation program displays the options, click the **Update schema** and **Install RBAC** check boxes.
-

## Using LDIF Commands to Update the Directory Schema

To use LDIF commands to manually update the directory, follow these procedures:

- 
- Step 1** Make sure the LDAP directory server is running.
  - Step 2** Make sure you have a user ID and password for the directory that allows you to update the schema.
  - Step 3** Obtain the required updates from the following location under your installation directory. Choose NDS or Netscape, depending on the LDAP directory you are using:

```
dess-auth
  schema
    NDS
    Netscape
```

Apply the contents of all of the ldf files found under the NDS or Netscape directories:

```
authattr.ldf
authclas.ldf
dessattr.ldf
dessclas.ldf
Policy15.ldf
```

- Step 4** Use the **ldapmodify** command to apply all of the preceding files to your directory. On successful completion, you have applied all of the required updates.
- 

## Loading Sample Data and Logging into CDAT for the First Time

Before any administrator can log into CDAT to create objects, some initial RBAC rules and roles must be loaded into the directory. Load these top level objects by loading the sample RBAC data files that are installed with SPE. You can also use your own data generating tool.

See the *Cisco Distributed Administration Tool Guide* for information about the initial RBAC objects, loading sample data, and logging into CDAT.

The sample data is located in the following directory:

```
dess-auth
  schema
```



### Note

The sample data uses common name (cn) as a component of distinguished name (dn). If your LDAP directory uses unique identifier (uid) rather than common name to allow access to the directory, you must edit the sample data files before loading them. Edit the `DESSusecasedata.ldf` and `DESSadmin.ldf` files, replacing all occurrences of cn with uid.

---

## Configuring Specific Features

This section describes how to configure the following features:

- [Automatic Connections, page 6-42](#)
- [Configuration-based Location and Brand Awareness, page 6-44](#)

## Automatic Connections

An automatically connected service is one that is connected immediately after the subscriber authenticates, without requiring the subscriber to explicitly select the service. This section describes two topics related to automatic connections:

- [Configuring Automatic Connections, page 6-42](#)
- [Subscriber Experiences with Automatic Connections, page 6-43](#)

## Configuring Automatic Connections

In general, if a service is marked as an auto connect service, the SSG performs the automatic connection after the subscriber authenticates. There is a special case with SESM in LDAP mode in which SESM is involved with automatic connection.

### Configuring a Service for Automatic Connection

A subscriber profile specifies services for automatic connection. The subscriber profile also controls whether or not the service is hidden or not. If an auto connect service is hidden, it does not appear in the service list displayed on a service connection page.

In RADIUS mode, to configure a service for automatic connection, use the Account-Info A attribute in the subscriber profile. See [Table D-5 on page D-9](#) for more information.

In LDAP mode, to configure a service for automatic connection:

- Subscribers can use the web portal's self-management features to select and deselect the auto connect feature for a service.
- Administrators can use CDAT to maintain subscriber profiles. See the *Cisco Distributed Administration Tool Guide* for information.

### Configuring SESM to Request Automatic Connections in LDAP Mode

In LDAP mode, the SSG performs automatic connections if it has the service list. If SSG does not have the service list, the SESM application can perform the automatic connections. During RDP installation, the Add Services option configures RDP to either:

- Return a service list to SSG—In this case, RDP includes the subscriber's service list and related information in replies to SSG, and SSG performs automatic connections for services marked for auto connection in the subscriber's profile.

The service information consumes memory on the SSG host.

- Not return a service list to SSG—In this case, SSG cannot perform automatic connections. The advantage to this configuration is that it saves memory on the SSG host.

In this case, you can configure the SESM application to perform automatic connections. The following line in the application MBean configuration file (for example, nwsp/config/nwsp.xml) controls whether the SESM web application performs automatic connections:

```
<Set name="autoConnect" type="boolean">false</Set>
```

Change the value to `true` to enable automatic connections by the SESM web application.

To change the setting of the RDP service list option, either reinstall RDP or edit the configuration files to enable the correct set of packet handlers. See [Appendix E, "RDP Packet Handlers,"](#) for information about the packet handlers that are used in the various configurations.

## Subscriber Experiences with Automatic Connections

This section describes the behavior of the SESM portal application regarding automatically connected services.

### Connection Status for Auto Connect Services

The status page in an SESM portal shows the status for all services, including automatically connected services. In NWSP, the selection page includes service status indicators for each service listed. Hidden services are not listed. See the [“Configuring a Service for Automatic Connection”](#) section on page 6-42 for an explanation of a hidden service.

Immediately after logging in, the service status for auto connect services might display as not connected. This happens if the service indicators display before the connection is completed. Proxy and tunnel services, for example, can take a while to connect. If the subscriber refreshes the window or selects the status window, the automatically connected services display with a connected status.

### Pop-Up Window for Auto Connect Services

If the subscriber has a home URL set to an auto connect service, the pop-up window for the service might appear before the connection completes. If this occurs, the following message appears in the pop-up window:

```
Page cannot be displayed.
```

The URL is the correct one. If the subscriber waits a short time and resubmits the request using the URL already displayed in the window, the service pages appear.

### Changing the Auto Connect Property for a Service

In LDAP mode, a subscriber can use the SESM self-management features to select or deselect the auto connect property. These changes are recorded immediately in the LDAP directory, but the change is not effective immediately. Changes are not visible in SESM until the cache timeout period in RDP elapses.

For example, a subscriber might select the auto connect property for a service, log out of SESM, log back in, and notice that the service was not automatically connected. Caching in the RDP causes this delay.

Caching in RDP improves system performance. The deployer can turn off caching or reduce the cache period, but those actions impact performance.

### Disconnecting Auto Connect Services

A subscriber can disconnect an auto connected service at any time. The disconnected status persists as long as the subscriber remains authenticated. The SESM single sign-on option affects whether a subscriber remains authenticated across SESM sessions. If the subscriber has to reauthenticate after an SESM session expires, the SSG reconnects all auto connect services.

An SESM session might expire, for example, because the subscriber closed the browser or navigated away from the SESM pages. When an SESM session expires:

- With single sign-on, subscribers are not required to reauthenticate.
- Without single sign-on, subscribers are required to reauthenticate when they navigate back to the SESM portal application. As a result of the reauthentication, SSG reconnects the auto connect services.

We recommend running SESM portal applications with single sign-on turned on.

## Configuration-based Location and Brand Awareness

You can use various ways to determine a subscriber's location and brand. This section describes how to implement the configuration-based methods. See the “[Location Awareness](#)” section on page 3-10 and “[Brand Awareness](#)” section on page 3-10 sections for a summary of other ways to determine location and brand.

You can implement location and brand awareness by adding the following elements in the SESM portal application's configuration file.

- In the SSG MBean, an SSG subnet entry can have the following attributes:
  - SESSION\_LOCATION
  - SESSION\_BRAND

The subnet entry associates an SSG IP address or client subnet address with a specific location or brand value. See the “[Global and Subnet Attribute Elements](#)” section on page 6-28 for information about subnet entries.

- In the WebApp MBean, the addDimension call defines the SESSION\_LOCATION or SESSION\_BRAND values.
- In the WebApp MBean, the addDimension call can create and assign arbitrary properties to the location or brand values. The SESM portal can use these properties.

For the session or brand determination to be meaningful, a web developer must change the SESM portal application to use the values. For new arbitrary properties to be meaningful, the portal must be changed to take an action with them.

The nwsp.xml file includes a configuration example that:

- Uses the SESSION\_LOCATION attribute in an SSG subnet entry to associate a location to an SSG IP address.
- Uses the addDimension call to associate a different URL to specific locations.



### Note

The example is only a configuration example; the NWSP application does not use the derived location or the associated URL.

## Configuring a Customized SESM Application

The Cisco SESM is a collection of components for creating specialized Java 2 Platform, Enterprise Edition (J2EE) web server applications. J2EE provides a framework for using various Java-based components to develop multi-tiered applications. The multi-tiered application (as opposed to the 2-tiered client server application) provides many opportunities for isolating and controlling functional pieces of a large application. For more information about the J2EE development platform, see:

<http://java.sun.com/j2ee/>

## SESM Application Definition

A Cisco SESM application consists of the following:

- SESM servlets and classes—The SESM API defines the SESM classes, including the configurable MBeans, used to implement the application functionality.

- **ConfigAgent**—The ConfigAgent is a Cisco developed MBean that configures other MBeans. It configures MBeans that are registered with the JMX server by applying parameter values from .xml files. Because .xml files are easily maintained and changed by system administrators, applications that use ConfigAgent are highly configurable without recompiling. Chapter 4 in this guide explains all of the configurable parameters in all of the MBeans.
- **Java Server Pages (JSPs)**—JSPs offer a way to deliver dynamic content in web pages. Web developers at the deployment site can control their subscriber's SESM experience through the JSPs. The *Cisco Subscriber Edge Services Manager Web Developer Guide* provides instructions for defining and compiling JSPs.
- **Images**—Images are used by the JSPs and control the look and feel and branding aspects of an SESM application. The *Cisco Subscriber Edge Services Manager Web Developer Guide* provides instructions for changing images and incorporating them into the JSPs.

## SESM Application Names

The SESM application name that you use for a customized application is arbitrary, but it must match in all of the following locations:

- The name of the application-specific subdirectory under the installation directory. For example, the directory that holds all application specific information for the NWSP application is:

```
<installDir>nwsp
```

- Application parameter inside the application startup script. In the installed scripts, the application name is hardcoded on the line that calls the generic start script. For example, for the NWSP application on Windows NT, the call line is:

```
call "%SCRIPTDIR%start.cmd" nwsp %PORTNO%
```

- Name of the application's configuration file in the `jetty` subdirectory. For example, for the NWSP application, the configuration filename is:

```
nwsp.jetty.xml
```

An application name in the startup script tells the ConfigAgent which configuration file to open. The application name is passed to ConfigAgent by the application startup scripts. The application name might also be used in other ways. For example, you can configure the parameter that defines the Jetty Server log filename to incorporate the application name in the log filename.

## Creating Configuration Files and Startup Scripts

Application developers at your site might make changes to the delivered NWSP sample application, producing a customized application. Customized applications require their own set of configuration files, although the files might be very similar to those provided for the sample application.

To create the required configuration files and startup scripts for a customized SESM application that will run in a Jetty server, follow these steps:

- 
- Step 1** Create a configuration file for the new application in the container's config directory. You can copy the `nwsp.jetty.xml` file and appropriately rename it. For example:

```
jetty
  config
    newApplication.jetty.xml
```

**Step 2** Edit the new file, enabling and disabling features as described in the [“Configuring an SESM Portal Application” section on page 6-14](#).

**Step 3** Create a startup script for the new application by copying the `startNWSP` script and appropriately renaming the copy. For example:

```
jetty
  bin
    startNewApplication
```

**Step 4** Edit the new file, changing the application name and the port number parameters. See the [“Startup Script Explanation” section on page 7-3](#) for more information.

**Step 5** Copy the `nwsp` directory structure, and rename the `nwsp` objects appropriately. For example, copy:

```
nwsp
  config
    nwsp.xml
  docroot
  docs
```

**Step 6** See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about customizing the JSPs, images, and other components. That guide also describes how to update the `docroot` folder, recompile affected components, and edit the `web.xml` file.

---





## Running SESM Components

---

This chapter describes how to start and stop Cisco Subscriber Edge Services Manager (SESM) applications. The chapter contains the following topics:

- [Starting Applications, page 7-1](#)
- [Logging On, page 7-6](#)
- [Stopping Applications, page 7-6](#)
- [Adding and Removing Services on Windows NT, page 7-7](#)
- [Memory Requirements and CPU Utilization, page 7-8](#)

### Starting Applications

This section describes the startup scripts for SESM applications. Topics are:

- [Starting the SESM Portals, page 7-1](#)
- [Starting RDP, page 7-2](#)
- [Starting CDAT, page 7-3](#)
- [Startup Script Explanation, page 7-3](#)
- [Java System Properties in Startup Scripts, page 7-4](#)

### Starting the SESM Portals

An SESM portal application is a J2EE web application that runs in a J2EE-compliant web server container. The installed startup scripts for the portal applications start the jetty server that is the container for the portal application. The Jetty server is configured (through MBeans in the container's MBean configuration file) to add the portal application to the container.

#### Startup Script Names

Start the portal applications using the following startup scripts.

Platform	Startup Scripts
Solaris and Linux	<pre>jetty/bin/startNWSP.sh [-mode mode] jetty/bin/startWAP.sh [-mode mode] jetty/bin/startPDA.sh [-mode mode] jetty/bin/startCAPTIVEPORTAL.sh [-mode mode] jetty/bin/startMESSAGEPORTAL.sh [-mode mode]</pre>
Windows NT	<pre>jetty\bin\startNWSP.cmd [mode] jetty\bin\startWAP.cmd [mode] jetty\bin\startPDA.cmd [mode] jetty\bin\startCAPTIVEPORTAL.cmd [mode] jetty\bin\startMESSAGEPORTAL.cmd [mode]</pre>

### Mode Argument

The startup scripts accept an optional command-line argument for specifying the run mode of the portal application. This option provides the capability to switch easily between a fully configured deployment (RADIUS or LDAP mode) and the demonstration deployment (Demo mode).

If the mode argument is included on the command line, it overrides the default mode specified in the SESM MBean in the portal application configuration file. If you switch modes using the command line option, you must make sure that all other configuration attributes are aligned with the mode that you choose.

Valid values for mode are:

- Demo—This mode uses configuration attributes in the SESMDemoMode MBean in the application configuration file.
- RADIUS—This mode uses configuration attributes in the SESM, SSG, and AAA MBeans in the application configuration file.
- LDAP—This mode uses configuration attributes in the SESM and SSG MBeans in the application configuration file, as well as attributes in the RDP and dss-auth configuration files.

## Starting RDP

RDP is a Java 2 application that uses the Cisco ConfigAgent and JMX server. RDP does not use the J2EE HTTP server. Therefore, its startup file is not in the Jetty server's bin directory.

Start RDP with the following script:

Platform	Script
Solaris and Linux	<code>rdp/bin/runrdp.sh</code>
Windows NT	<code>rdp\bin\runrdp.cmd</code>

## Starting CDAT

CDAT is a J2EE application. The startup script for CDAT is in the Jetty server's bin directory. This startup script calls the same generic startup script used by the SESM web applications.

Start CDAT with the following script:

Platform	Script
Solaris and Linux	jetty/bin/startCDAT.sh
Windows NT	jetty\bin\startCDAT.cmd

## Startup Script Explanation

When you start an SESM portal application or CDAT, you are executing two scripts:

- Application-specific startup script—Sets application-specific parameters and calls the generic script
- Generic startup script—Infers additional parameters and starts the Jetty server, which in turn adds the portal application to the container.

All of the scripts are located in:

```
jetty
  bin
```

You should create an application-specific startup script in this same `bin` directory for customized SESM web applications.

## Application-Specific Startup Scripts

The application-specific startup scripts set the following variables:

- application name—Identifies the application name. The generic startup script derives pathnames for configuration files and the docroot subdirectory from the application name. If you create a customized application, provide the name that identifies your application. See the [“SESM Application Names” section on page 6-45](#) for information about using a new application name value.
- port number—Identifies the port that the application's container (the web server) will listen on.

The installation program updates the application startup script with the port number that you provide during the installation time. To change the port number after installation, edit the startup script. The default values displayed by the installation program are 8080 for an SESM portal application and 8081 for CDAT.

The port number must be unique on the server machine. If multiple SESM portal applications are running simultaneously on the same server machine, make sure each one listens on a different port. This caveat applies whether you are running two instances of the same application or two different applications.

## Generic Startup Script

The generic startup script derives two other port numbers from the application port number:

- It derives a management console port number as follows.

```
application port + 100
```

For example, if you are using the default application port of 8080 for NWSP, the management console port for NWSP is:

```
8080 + 100 = 8180
```

- It derives a secure socket listener (SSL) port as follows:

```
application port - 80 + 443
```

Starting with the default application port value of 8080, the default SSL port is:

```
8080 - 80 + 443 = 8443
```

The generic startup script does the following:

- Accepts the variables passed to it from the application startup script
- Sets additional variables, based on the expected (installed) directory structure. For example, it infers the location of the configuration files.
- Starts a Jetty server instance, which uses configuration attributes in the container MBean configuration file to add applications to run in the container.

## Java System Properties in Startup Scripts

[Table 7-1](#) describes the java system properties that are set by the generic startup script and how the assigned values are derived. The table describes the following lines, which are located at the end of the generic startup script:

```
$JAVA -Xmx64m -Xmx64m \
  -classpath $CLASSPATH \
  -Djetty.home=$JETTYDIR \
  -Dapplication.home=$APPDIR \
  -Dapplication.log=$LOGDIR \
  -Dapplication.portno=$PORTNO \
  -Dmanagement.portno=$MGMTPORTNO \
```

Table 7-1 Java System Properties in Startup Scripts

System Property and Variable Name	Explanation	Installed Values in the Start Script
jetty.home=\$JETTYDIR	jetty.home is the container's directory name.  The startup script sets \$JETTYDIR to the value <code>jetty</code> under the installation directory.	<code>installDir</code> <code>jetty</code>
application.home=\$APPDIR	application.home is the application's directory name.  The startup script sets \$APPDIR to <code>applicationName</code> under the installation directory. The <code>applicationName</code> parameter is passed from another script. (startNWSP.sh, for example).	<code>installDir</code> <code>nwsp</code> or <code>installDir</code> <code>rdp</code> or <code>installDir</code> <code>cdat</code>
application.log=\$LOGDIR	application.log is the location of all log files created for this application.	The startup script sets \$LOGDIR differently according to the platform: <ul style="list-style-type: none"> <li>On Solaris and Linux, \$LOGDIR is the logs directory under the application directory in the install directory. For example: <code>installDir/nwsp/logs</code></li> <li>On Windows NT, \$LOGDIR is <code>userTemp\application\logs</code> where <code>userTemp</code> is the administrator's temporary directory. For example: <code>temp\nwsp\logs</code></li> </ul>
application.portno=\$PORTNO	application.portno is the port that the web server listens on for HTTP requests from subscribers.  The startup script sets \$PORTNO to the <code>portNo</code> parameter passed from another script (startNWSP.sh, for example).	Specified during installation. The default is 8080 for the SESM portal applications and 8081 for CDAT.
management.portno=\$MGMTPORTNO	management.portno is the console port that displays the current values for all attributes in all of the MBean configuration files.	The startup script sets \$MGMTPORTNO to <code>\$PORTNO + 100</code> .

# Logging On

To access an SESM portal application, such as the NWSP application, follow these procedures:

- 
- Step 1** Start the SESM portal application using its startup script.
- Step 2** Start a web browser on a device (such as a desktop computer, a WAP phone, or a PDA) that has network access to the server on which the SESM portal application is running.
- Step 3** Go to the URL of the SESM portal application:

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

The URL consists of the host and port number that you specified during the SESM portal application installation, or whatever is currently specified in the portal application's startup script. An example portal application URL is:

```
http://server1:80
```

Default values used during an SESM installation are:

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




---

**Note** If the captive portal unauthenticated user redirect feature is implemented and correctly configured and the corresponding TCP redirect features are correctly configured on the SSG, subscribers are redirected to the captive portal application without entering an URL.

---

- Step 4** When the SESM portal application's logon page appears, log in using a valid user ID and password. A valid user ID and password is defined in user profiles as follows:
- In RADIUS mode, the user profile must exist in the RADIUS server database. See [Appendix D, "Configuring RADIUS,"](#) for more information.
  - In LDAP mode:
    - If RDP is configured in Proxy mode, the user profile must exist in the RADIUS server database that the RDP is proxying to.
    - If RDP is configured in normal (non-Proxy) mode, the user profile must exist in the LDAP directory in the SPE-specified format. See the *Cisco Distributed Administration Toolkit Guide* for more information.




---

**Note** See [Chapter 4, "Demo Quick Start,"](#) for instructions on logging on and demonstrating the NWSP application running in Demo mode.

---

# Stopping Applications

This section describes how to stop SESM applications. It includes the following topics:

- [Stopping SESM Applications on Solaris and Linux, page 7-7](#)
- [Stopping SESM Applications on Windows NT, page 7-7](#)

## Stopping SESM Applications on Solaris and Linux

To stop SESM applications on Solaris and Linux, execute the stop scripts listed in [Table 7-2](#). None of the scripts take arguments.

**Table 7-2** *SESM Stop Scripts on the Solaris and Linux Platforms*

Application	Stop Script Location and Name on Solaris and Linux Platforms
SESM portals and Jetty	jetty/bin/stopNWSP.sh jetty/bin/stopWAP.sh jetty/bin/stopPDA.sh jetty/bin/stopcaptiveportal.sh jetty/bin/stopmessageportal.sh
CDAT and Jetty	jetty/bin/stopCDAT.sh
RDP	rdp/bin/stoprdp.sh

## Stopping SESM Applications on Windows NT

To stop SESM applications and their J2EE containers on Windows NT platforms, you can:

- Open the Task Manager window, select the appropriate task, and click the **End Task** button. If you are prompted again, click the **End Now** button.
- If you added the application as an NT service, you can use the Services window to stop the service. Open **Control Panel > Services** or **Control Panel > Administrative Tools > Services** and select the service you want to stop. Use the menu commands on the Services window to stop the selected service.

## Adding and Removing Services on Windows NT

On a Windows NT platform, you can add your applications to the list of Windows NT services. When the application is a service, it appears in the **Services** window accessed from **Control Panel > Services** or **Control Panel > Administrative Tools > Services**. You can start and stop any service from this window. Also, you can optionally configure a service to start automatically when the system reboots.

The SESM installation program provides services scripts with the NWSP, CDAT, and RDP applications. The command syntax is the same for all of the services scripts:

- `scriptName -i` installs the application as a service so that it can be managed from the Services window
- `scriptName -h` displays the command usage
- `scriptName -r` removes the application from the Services window

Table 7-3 lists the names and locations of the scripts that add and remove services.

**Table 7-3 Scripts for Adding and Removing Services on Windows NT**

SESM Application	Services Script Location and Name	Default Service Name
RDP	rdp\bin\rdpsvc.cmd	RDP Application
CDAT	jetty\bin\cdatsvc.cmd	CDAT Web Application
SESM portals	jetty\bin\nwspsvc.cmd jetty\bin\wapsvc.cmd jetty\bin\pdasvc.cmd jetty\bin\captiveportalsvc.cmd jetty\bin\messageportalsvc.cmd	NWSP Web Application WAP Web Application PDA Web Application Captive Portal Web Application Message Portal Web Application

## Memory Requirements and CPU Utilization

This section includes the following topics:

- [SESM Portal Application Memory Requirements, page 7-8](#)
- [SESM Portal Application CPU Utilization, page 7-9](#)
- [RDP Memory Requirements, page 7-10](#)

## SESM Portal Application Memory Requirements

The total java virtual memory requirements for an SESM portal application depends on several factors:

- Number of subscribers concurrently logged in
- Number of subscribed services
- Rate of new logons—The login rate affects transitory memory use.

The most important of these factors is the number of subscribers concurrently logged on. Use the following formula to determine memory requirements for your installation:

$$\text{requiredJVM} = \text{reservedMem} + (\text{maxConcurrentUsers} * \text{KBPerUser})$$

Where:

- *requiredJVM* is the amount of Java Virtual Memory (JVM) to reserve for use by the SESM portal application. The generic startup script (jetty/bin/start.sh) sets the JVM. The JVM is an argument to the java command, which is located at the end of the start script, as follows:

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

The first -X argument is the initial JVM to reserve. The second -X argument is the maximum JVM. We recommend using the same value for both.

- *reservedMem* is 10.4 MB, a constant value that represents the initial memory requirement for the application before subscribers begin logging on.
- *maxConcurrentUsers* is the maximum number of concurrently logged on subscribers that you wish to support.



- *KBPerUser* is the estimated amount of memory required to service one subscriber. This number will vary depending on factors such as how many services the typical subscriber is subscribed to. Suggested values are:
  - For RADIUS mode: 4.18 KB per subscriber.
  - For LDAP mode: 29 KB per subscriber.

See [Table 7-4](#) for additional guidelines in determining an appropriate *kbytePerUser* figure.

### Symptoms of Insufficient Memory

The installed start script sets the java virtual memory to 64 MB. Consider increasing this default value if you notice these symptoms of insufficient memory:

- Out of memory exceptions
- Messages stating that the web server is unavailable

### Verified Memory Requirements

[Table 7-4](#) shows verified memory requirements for the NWSP portal application. We verified these memory requirements using one SESM application instance. It is possible, given more memory, to support larger numbers of users.

**Table 7-4** SESM Portal Memory Requirements

SESM Mode	JVM Heap Size (MB) Specified in start script <sup>1</sup>	Maximum Users <sup>2</sup>	KB per user
RADIUS mode	32	4550	4.73
	64	12800	4.18
	96	20500	4.17
	128	29100	4.04
LDAP mode	64	1800	29.73
	96	3000	28.50
	128	5000	23.50
	256	11000	22.32

1. Includes 10.4 MB reserved memory

2. In the verification tests, all users were subscribed to three services: one passthrough, one proxy, and one tunnel

## SESM Portal Application CPU Utilization

CPU utilization by an SESM portal application increases as the rate of new logons increases. [Table 7-5](#) shows CPU utilization at specified logon rates for the NWSP portal. These rates are verified using consistent login rates, with all users subscribed to three services. The logon rates indicate successful logon and authentication of all users.

**Table 7-5** *SESM Portal CPU Utilization*

<b>SESM Mode</b>	<b>Logon Rate Sustained until Maximum Users Reached<sup>1</sup></b>	<b>Maximum Users</b>	<b>CPU Utilization on Sun Sparc U5-10 400-MHz server</b>
RADIUS mode	20 logons per second	12,800	20%
	40 logons per second		40%
	60 logons per second		60%
	80 logons per second		80%
	100 logons per second		100%
LDAP mode	10 logons per second	11,000	60%

1. All users are subscribed to three services: one passthrough, one proxy, and one tunnel.

## RDP Memory Requirements

The amount of memory RDP uses is roughly proportional to the number of users that are logged in within a fixed period of time. If you find that RDP is running out of memory, increase the amount of memory allocated to the program by editing the startup script.

As a rough guide, RDP requires 64 MB of memory when 5000 users are logged in within any 20 minute period. If the logon rate is likely to exceed this rate, you should increase the RDP memory allocation.



## Deploying a Captive Portal Solution

---

This chapter describes the Cisco SESM captive portal solution and how to configure it. The chapter contains the following topics:

- [Introduction, page 8-1](#)
- [SSG and SESM Release Requirements, page 8-2](#)
- [Solution Description, page 8-2](#)
- [Installing, Configuring, and Running the Sample Solution, page 8-8](#)
- [Configuration Details, page 8-13](#)
- [Configuring the SSG TCP Redirect Features, page 8-22](#)
- [Troubleshooting Captive Portal Configurations, page 8-26](#)

### Introduction

The SESM captive portal features, combined with the TCP redirect features on the Service Selection Gateway (SSG), can provide the following benefits for subscribers and deployers:

- Direct subscribers to an SESM web portal application even if they do not know the URL to the web server.
- Force subscribers to authenticate before accessing the network or specific services.
- Ensure that subscribers are only allowed to access the services that the service provider wants them to access.
- Ensure that subscribers are shown a specific message for a defined period while attempting to access services.
- Display advertising messages at specified intervals during an SESM session.
- Display advertising messages based on specific subscriber characteristics, such as hobbies.

All of the above mentioned uses of captive portal are demonstrated in the sample captive portal solution that comes with the SESM package. With some customized programming and development, the following additional types of activities could be achieved using an SESM captive portal solution:

- Direct all incoming requests destined to a specific network to a specific URL
- Direct all requests destined to a specific port to a specialized advertising page that shows new services

- Direct subscribers to a billing server application that provides account status information or account payment opportunities.

## SSG and SESM Release Requirements

The following table shows the Cisco IOS and Cisco SESM release requirements for implementing captivation features.

Captivation Type	Required Cisco IOS Release Level (SSG)	Required Cisco SESM Release Level
Unauthenticated user redirection	Cisco IOS Release 12.1(5)DC1 or later	SESM Release 3.1(1) or later
Unauthorized service redirection	Cisco IOS Release 12.2(4)B or later	SESM Release 3.1(3) or later
Initial logon redirection		
Advertising redirection		



### Note

The SSG TCP redirect features can redirect to any web server application. There is no requirement to use SESM applications. However, this chapter assumes that you are using SESM applications.

## Solution Description

The SESM installation package includes a sample captive portal solution using SESM portal applications. This section describes the components in the sample solution. Topics in this section are:

- [Solution Diagram, page 8-2](#)
- [SSG TCP Redirect Feature, page 8-3](#)
- [SESM Captive Portal Application, page 8-5](#)
- [Content Applications, page 8-6](#)
  - [NWSP Application, page 8-6](#)
  - [Message Portal Application, page 8-6](#)
- [Alternative Configuration Options for a Captive Portal Solution, page 8-7](#)

## Solution Diagram

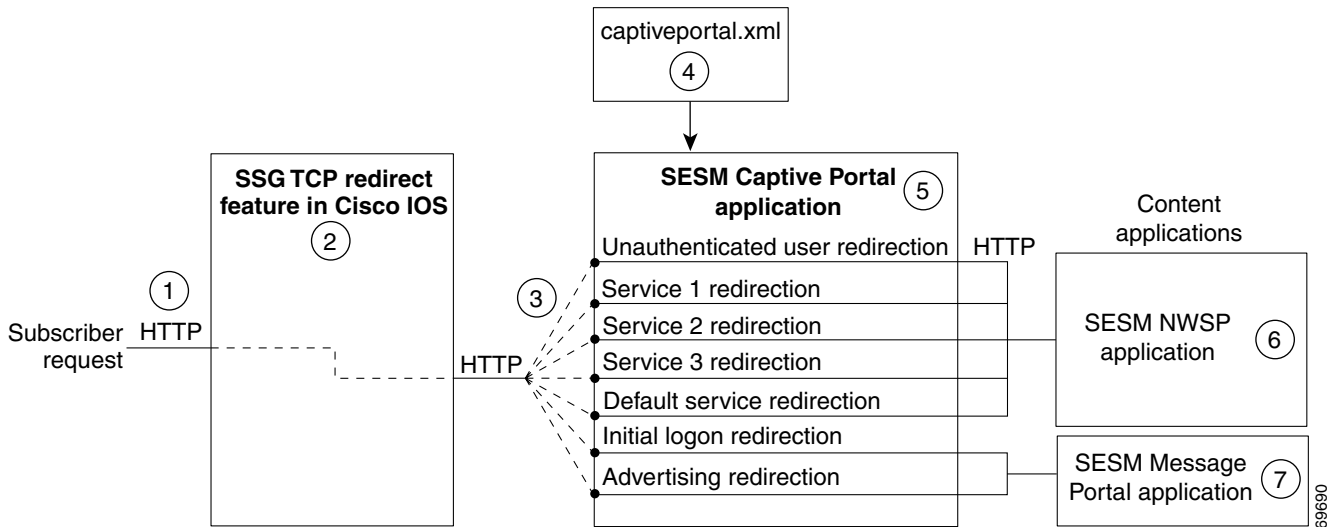
[Figure 8-1](#) illustrates how the components in the SESM captive portal solution work together to provide appropriate content to the subscriber.



### Note

[Figure 8-1](#) shows the sample solution as it would be configured using all of the default values provided by the SESM installation program. There are many possible variations to this default deployment.

Figure 8-1 Sample SESM Captive Portal Solution



1	Incoming HTTP requests from subscribers pass through the SSG.
2	When a packet qualifies for redirection, the SSG changes the destination IP address and port in the TCP packet. Cisco IOS configuration commands issued on the SSG host device define which packets qualify for redirection and the redirected destinations.
3	The sample SESM captive portal solution requires the following configurations for the TCP redirected destinations. <ul style="list-style-type: none"> <li>The IP address must identify a web server running an SESM Captive Portal application. All types of redirection can use the same web server (the same IP address).</li> <li>Each type of redirection must use a different port value. The port number identifies the type of redirection to the SESM Captive Portal application.</li> </ul>
4	The captiveportal.xml file associates an incoming port number to a content application URL. The SESM Captive Portal application uses the services of a JMX server to obtain the attribute values from the XML file.
5	The SESM Captive Portal application acts as a gateway to the content applications. It issues an HTTP redirect that redirects the subscriber's browser to an appropriate content application. The redirect request can include information from the original HTTP request, in the form of query parameters appended to the HTTP redirect URL.
6	The NWSP portal is the content application that services unauthenticated user redirection and service redirections.
7	The Message Portal is the content application that services initial logon and advertising redirections.

## SSG TCP Redirect Feature

The SSG TCP redirect feature intercepts TCP packets and reroutes them to a configured group of captive portal applications, usually SESM captive portal applications. The SSG modifies the IP address and the port in the TCP packet to cause the redirection. The reason for the redirection and the redirected destinations are configured on the SSG using Cisco IOS commands.

Table 8-1 describes the SSG TCP redirection types and how the SESM captive portal solution supports those redirection types.

Table 8-1 Supported Redirection Types

Redirect Type	Role of SSG TCP Redirect Feature	Role of SESM Captive Portal Solution
Unauthenticated user redirection—Handles attempted access to services by subscribers who have not yet authenticated to SSG.	<p>Without TCP redirection, the SSG discards packets from unauthenticated users. That is, the subscriber needs to know the URL of a logon page, such as an SESM logon page, to authenticate with the SSG before accessing any services.</p> <p>With TCP redirection, these packets are allowed some controlled access to particular services within the SSG, such as access to a captive portal application.</p>	<p>Provides a logon page so the subscriber can authenticate.</p> <p>In a point-to-point protocol (PPP) client with single sign-on enabled, performs authentication transparently to the subscriber.</p> <p>After authentication, redirects the browser again to the subscriber's original request.</p>
Unconnected service redirection—Handles unauthorized attempts to access a service.	<p>Without TCP redirection, the SSG discards packets directed at services for which the subscriber is not authorized. With TCP redirections, these packets are allowed controlled access to particular services within the SSG, such as an SESM captive portal solution. There are two types of service redirection:</p> <ul style="list-style-type: none"> <li>• Specific service redirection—Redirects access to specific networks.</li> <li>• Default service redirection—Redirects unauthorized access to networks not handled by the specific service redirections.</li> </ul>	<p>For specific service redirections, presents a logon page specific to the service being requested.</p> <p>For default service redirections, displays a default service selection page. In an LDAP deployment, displays a self-subscription page if the subscriber is not already subscribed to the service.</p>
Initial logon redirection—Gives providers a way to deliver messages to subscribers when they first log in.	<p>Redirects all TCP packets destined to a configured list of ports when the host object is first created.</p> <p>Activates a timing mechanism for a specified duration, during which the subscriber is truly captivated and cannot redirect the browser. The configured Captive Portal application (as opposed to SSG) controls what occurs after the duration time elapses.</p>	<p>Provides message content.</p> <p>After the message duration time elapses, optionally redirects the browser to the original request with no further action required from the subscriber.</p>
Advertising redirection—Gives providers a way to deliver advertising or other messages at timed intervals during an active session.	<p>Redirects all TCP packets destined to a configured list of ports at specified intervals.</p> <p>Activates a session timing mechanism to keep track of the time since the last advertisement. When the configured interval elapses, SSG performs an advertising redirection the next time the subscriber initiates a TCP packet.</p> <p>Activates a message duration timing mechanism as described above for the initial logon redirection.</p>	<p>Provides advertising content.</p> <p>After the advertising duration time elapses, optionally redirects the browser to the previous URL with no further action required from the subscriber.</p>
SMTP redirection—Forwards SMTP traffic.	Handles all aspects of Simple Mail Transfer Protocol (SMTP) redirection.	This type of redirection does not require a captive portal application.

## SESM Captive Portal Application

The SESM Captive Portal application acts as a gateway for all of the different redirections coming from the SSG. This application does not provide any content to subscribers. Its main purpose is to preserve and pass along information from the original subscriber request to the content applications.

The SESM Captive Portal application performs the following functions:

- Preserves information from the subscriber's original HTTP request.
- Issues an HTTP redirection that redirects the subscriber's browser to a content application that can handle the request appropriately and provide content to the subscriber. The HTTP redirect includes the preserved information from the original subscriber, in the form of parameters appended to the redirection URL.
- Determines which content application should handle the request based on configuration attributes that associate incoming port numbers to content application URLs. These URLs can point to different pages within the same application, or to different applications.

Table 8-2 shows the parameters that the Captive Portal application captures and forwards to content applications. The names of these parameters are configurable in the captiveportal.xml file.

See Table 8-4 on page 8-15 for a description of the configuration attributes in the captiveportal.xml file.

**Table 8-2 Parameters Appended to URLs in HTTP Redirections**

Type of SSG TCP Redirection	Parameter Name in SESM Captive Portal HTTP Redirect	Explanation and Usage by the Content Applications
Unauthenticated user redirection	CPURL	The URL in the subscriber's original request. The NWSP application uses this value to redirect the browser to this original request after successful authentication.
Service redirection	service	The service name that was requested in the original request. The NWSP application uses this value to log on to the service.
	username	The user name that the subscriber used for SESM authentication. NWSP does not use this value, but it is available for use in customizations.
	serviceURL	The URL to the service that was requested in the original request. The NWPS uses this value to display a pop-up window after service connection. It overrides the URL that NWSP would normally use after service connection, which is the URL in the service profile.
Initial logon and advertising redirections	CPURL	The URL in the subscriber's original request. The Message Portal application optionally redirects to this URL after the message duration time elapses. If the redirect feature is turned off in the messageportal.xml file, the message portal application ignores this parameter.
	CPDURATION	The message duration obtained from the captiveportal.xml file. The Message Portal application waits this amount of time before attempting to redirect to the CPURL.  There are duration attributes on both the SSG side and the SESM side. See the <a href="#">"Message Duration Parameters" section on page 8-21</a> .
	CPSUBSCRIBER	The subscriber name as obtained from the subscriber profile.

## Content Applications

Content applications provide the SESM browser pages that the subscriber sees. Content applications can be SESM web portal applications or compatible third-party web applications. This guide assumes that you use SESM web portal applications.

### NWSP Application

The NWSP application is the content application for unauthenticated user redirections and unauthorized service redirections.

- For unauthenticated user redirections—NWSP presents the SESM login page so the subscriber can authenticate.
- For unauthorized access to specific services:
  - NWSP presents a service logon page for the service and coordinates with the SSG to authenticate to the service and then connect to the service.
  - You can configure various contingency pages to handle situations when connection is not possible. For example, suppose the service does not exist or the subscriber is not subscribed to the service. Attributes in the nwsp.xml file configure these situations.
  - In LDAP mode, when a subscriber is not subscribed to a service, the default configuration directs the subscriber to a self-subscription page.
- For the default service redirections (unauthorized access to services other than the specifically configured ones):
  - If the Captive Portal application is configured so that it does not pass a service name in the query string for this type of redirection, NWSP uses the serviceNotGivenURI attribute to determine a redirection destination.
  - The default configuration of the sample solution references the NWSP status page.

See [Table 8-1 on page 8-4](#) for a description of the parameters that the Captive Portal application forwards to the NWSP application.

See [Table 8-6 on page 8-20](#) for a description of the configuration attributes in the nwsp.xml file related to captive portal.

### Message Portal Application

The SESM Message Portal application provides the message pages for initial and advertisement captivation. It provides the following content pages:

- Greetings page for initial captivation
- Advertising page for advertising captivation
- In LDAP mode, the Message Portal application displays an advertisement that matches the first subscriber interest in the subscriber profile.

This application also provides a timing mechanism to control the duration of the displays. Timing starts when the page is displayed and ends when the duration time elapses. When the duration time elapses, the message portal application can optionally redirect to the URL in the subscriber's original HTTP request. Otherwise, the message remains displayed until the subscriber enters another URL.



See [Table 8-1 on page 8-4](#) for a description of the parameters that the Captive Portal application forwards to the Message Portal application. See [Table 8-5 on page 8-17](#) for a description of the configuration attributes in the `messageportal.xml` file.

## Alternative Configuration Options for a Captive Portal Solution

The sample SESM captive portal solution offers one way to implement captivation features. This section describes some alternative deployment options.

### Eliminating Redirection Types

You do not need to deploy all of the redirection types. Each type of TCP redirection is independent of the others. To eliminate a redirection type from the captive portal solution, you can do any of the following:

- Turn off the redirection type in the `captiveportal.xml` file.
  - During captive portal installation, you can uncheck the enable box for any redirection type.
  - After installation, you can set to false the appropriate attribute by editing the `captiveportal.xml` file.
- Do not configure that redirection type on the SSG.

### Eliminating J2EE Listeners

The web server container in which the captive portal application is running is configured with a separate listener for each TCP redirect port you configured. That is, there is a separate listener for user redirections, each service redirection, a default service redirection, initial logon redirections, and advertising redirections. If you do not implement all of the redirection types, you might want to edit the `captiveportal.jetty.xml` file to disable the unnecessary listeners. This is optional.

### Using Different Content Applications

You can deploy one or many content applications. You might have a single content application that handles all types of redirection, or you might have a different application for each type of redirection, including a different application for each configured service redirection. The content applications do not need to be SESM applications. The SESM Captive Portal application can redirect to any web application.

### Using a Different Captive Portal Application

The SSG TCP redirect feature can accept any type of web application in the SSG captive portal groups. There is no requirement to use the SESM Captive Portal application. In addition, there is no requirement to use the 2-tiered approach used by the SESM solution. However, using the 2-tiered approach with the SESM Captive Portal application has certain advantages:

- It is an efficient, small footprint, application.
- By acting as a gateway to any number of other applications with varying functions, it isolates common functionality into a single application.
- It simplifies configuration when you want to add or change content applications to your solution. In those cases, you add or change configuration parameters in the Captive Portal application configuration file (an XML file) to point to the new content applications. This is much easier than changing the captive portal group configuration on the SSG, which would require Cisco IOS commands on each SSG host device.

You can configure the TCP redirect feature to redirect directly to an application that provides content to the subscriber. For example:

- You could configure captive portal groups for unauthenticated user redirections as instances of NWSP (or some other appropriate web application), bypassing the SESM Captive Portal application. However, if you want to retain the feature that preserves the originally requested URL from the user, you must customize the NWSP application by adding some code that is currently in the SESM Captive Portal application.
- Similarly, you could configure captive portal groups for initial logon and advertising redirections as instances of a content application similar to the SESM Message Portal application, bypassing the SESM Captive Portal application.

**Note**

If you redirect directly to the delivered SESM Message Portal (bypassing the Captive Portal application), the originally requested URL is not available and no pages based on subscriber profile are presented.

## Installing, Configuring, and Running the Sample Solution

This section describes how to install and configure the sample solution in the quickest possible configuration. To alter the default configuration after installation, see the [“Configuration Details” section on page 8-13](#).

This section includes the following topics:

- [Installing and Configuring the Sample Solution, page 8-8](#)
- [Installation Results, page 8-9](#)
- [Additional Configuration Steps, page 8-9](#)
- [Starting the Sample Solution, page 8-11](#)
- [Demonstrating Captive Portal Features, page 8-12](#)

## Installing and Configuring the Sample Solution

Install the sample captive portal solution from the SESM installation package. Detailed installation procedures for captive portal are included with the installation procedures for other SESM components. The captive portal installation starts in the [“Captive Portal Server Configuration” section on page 5-24](#).

The following information concerning captive portal installation is important:

- You must choose Custom Install to install the captive portal solution. Captive portal is not included in a typical installation.
- Many of the captive portal installation 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 during SESM captive portal installation.
  - Use the `ssgconfig.txt` file to configure the SSG. The configuration values in `ssgconfig.txt` match the default values used in the SESM installation program. See the [“Configuring the SSG to Match the Installed Captive Portal Solution” section on page 8-9](#) for instructions on using `ssgconfig.txt`.

## Installation Results

The captive portal installation procedure adds two directories under your SESM installation directory:

```
captiveportal
  config
    captiveportal.xml
    ssgconfig.txt
  docroot
  docs
messageportal
  config
    messageportal.xml
  docroot
  docs
```

The installation procedure also adds startup scripts and container configuration files for Captive Portal and Message Portal to the jetty directory under your SESM installation directory:

```
jetty
  bin
    startCAPTIVEPORTAL
    startMESSAGEPORTAL
  config
    captiveportal.jetty.xml
    messageportal.jetty.xml
```

## Additional Configuration Steps

This section describes configuration that you must perform before you can see the captive portal solution in operation. These tasks are in addition to the configuration performed by the installation program.

- [Configuring the SSG to Match the Installed Captive Portal Solution, page 8-9](#)
- [Loading Sample Profiles for Captive Portal Demonstration, page 8-10](#)
- (Optional) [Configuring Unique Service Logon Pages for Service Redirections, page 8-10](#)

## Configuring the SSG to Match the Installed Captive Portal Solution

To demonstrate the complete capabilities of the captive portal solution, you need to 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, follow these procedures:

- 
- Step 1** Make sure the SSG device is running the appropriate Cisco IOS release, as described in the [“SSG and SESM Release Requirements” section on page 8-2](#). If not, upgrade the Cisco IOS release before proceeding.
- Step 2** Make sure that basic SSG functionality is enabled and configured, as described in [Appendix B, “Configuring the SSG.”](#)
- Step 3** 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 commands required to configure the four types of TCP redirection that the sample captive portal solution can demonstrate. The commands in this file will configure SSG to match the default values presented during the captive portal installation. The file includes placeholder IP addresses.



**Note** The installation program displays default inputs for captive portal group names and port numbers. The default inputs 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 4** Edit `ssgconfig.txt` as follows:
- You *must* edit the placeholder IP addresses, changing 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 5** On the SSG host device, enter the contents of `ssgconfig.txt` to update the Cisco IOS running-config file.
- Step 6** Save running-config.

## Loading Sample Profiles for Captive Portal Demonstration

To demonstrate the features in the captive portal solution, you must load some appropriate sample profiles into the RADIUS database or LDAP directory. To fully demonstrate all of the features of the solution, the profiles should include:

- Service profiles should have service names that match the service names used in the `captiveportal.xml` file. Matching service names are required to demonstrate service redirections that pass a service name to NWSP for connection.
- Service profiles must have service routes that match exactly the destination networks of the service redirections configured in the SSG TCP redirect commands. See the [“Redirected Networks Must Match Service Routes”](#) section on page 8-28.
- Subscriber profiles must include subscriptions to the above services.
- For LDAP mode, subscriber profiles should include hobbies. Hobbies are required to illustrate the Message Portal’s capability to display messages tailored to the first hobby listed in the subscriber profile.

In LDAP mode, create some basic subscriber profiles using CDAT. You can then use the NWSP account management feature to modify interests (hobbies) or add subscriptions.

## Configuring Unique Service Logon Pages for Service Redirections

The SESM installation program configures three specific service redirections and a default service redirection. However, the installation program asks for only one destination URL for services. It configures all of the service redirections to use this URL. The default value provided by the installation program is the service logon page in NWSP.

You might want to change the configuration so that each service redirection is assigned a unique redirection destination.

To change a destination URL for service redirections, follow these procedures:

**Step 1** Open the captiveportal.xml file in a text editor. The location is:

```
captiveportal
  config
    captiveportal.xml
```

**Step 2** Locate the service redirect definition. For example:

```
<Call name="defineServiceRedirect">
  <Arg><SystemProperty name="serviceRedirect1.port" default="8094"/></Arg>
  <Arg><SystemProperty name="serviceRedirect1.URL" default=""/></Arg>
  <Arg><SystemProperty name="serviceRedirect1.service" default="service1"/></Arg>
</Call>
```

**Step 3** Change the URL in the second argument in the service redirection definition to the desired service URL.



**Note** When the second argument is empty (or its system property default is empty), the value in the serviceRedirectDefaultURL attribute is used. By using a default page in serviceRedirectDefaultURL attribute, you do not have to enter the same URL for all the service redirections.

The default value provided by the installation program for the serviceRedirectDefaultURL attribute is the NWSP /serviceRedirect page.

## Starting the Sample Solution

The following table shows the startup script names for the applications in the sample captive portal solution.

Platform	Startup Scripts
Solaris and Linux	jetty/bin/startCAPTIVEPORTAL.sh jetty/bin/startMESSAGEPORTAL.sh jetty/bin/startNWSP.sh
Windows NT	jetty\bin\startCAPTIVEPORTAL.cmd jetty\bin\startMESSAGEPORTAL.cmd jetty\bin\startNWSP.cmd

For information about the contents of these startup scripts, see [Chapter 7, “Running SESM Components.”](#) The optional mode argument described in that chapter can be used with these startup scripts. However, the run mode for the Captive Portal and Message Portal applications must agree with the run mode of the main portal application (NWSP).

## Demonstrating Captive Portal Features

To demonstrate captive portal features:

**Step 1** Make sure the SSG is configured as described in the [“Configuring the SSG to Match the Installed Captive Portal Solution” section on page 8-9](#).

**Step 2** Start all of the applications in the captive portal solution by executing their startup scripts:

```
jetty
  bin
    startNWSP
    startCAPTIVEPORTAL
    startMESSAGEPORTAL
```

**Step 3** Open a web browser from a network configured as an incoming network on the SSG. Attempt to go to a popular Internet page, such as [www.yahoo.com](http://www.yahoo.com), or allow the browser to attempt to display a home page setting.

Unauthenticated user redirection causes the NWSP logon page to display.

**Step 4** Sign on using a user ID and password from the subscriber profiles you loaded. After successful authentication, the following occurs:

1. The NWSP home page appears in the main window.
2. A pop-up window appears, intended for the [www.yahoo.com](http://www.yahoo.com) URL.
3. Initial logon redirection causes the greetings page from the Message Portal application to display in the pop-up window.
4. After the length of time specified by the duration parameter, one of the following occurs:
  - If the `redirectOn` configuration parameter for Message Portal is set to true, the Message Portal application redirects the browser to the originally requested URL ([www.yahoo.com](http://www.yahoo.com)). The service is subjected to service redirections (see the next item).
  - If the `redirectOn` configuration parameter for Message Portal is set to false, the greetings page continues to display until you enter another URL.
5. In response to a service redirection, NWSP displays one of the following in the main window:
  - If the service requires credentials, NWSP displays a service logon page.
  - If the subscriber is not subscribed to the service, NWSP displays the subscription page.
  - If it does not find the service, NWSP displays the home page.
  - Otherwise, NWSP attempts to start the service and brings the service pop-up window to the foreground.

If the service redirection did not work, check the following configurations. To demonstrate service redirection for a service named yahoo, all of the following configurations must be set:

- A service profile must exist whose service name is yahoo and the service URL is [www.yahoo.com](http://www.yahoo.com).
- A specific service redirection must be configured. The service name yahoo must be specified in the service definition in `captiveportal.xml`.
- The subscriber name that you used during login must be subscribed to the service named yahoo. Check the subscriber profile.

**Step 5** To demonstrate a default service redirection, from the NWSP service selection list, select a service with an IP address outside the destination networks of all the specific service redirections. It does not matter if the subscriber is subscribed to the service or not.

Default service redirection is usually configured so that a service name is not passed to NWSP, which causes NWSP to display the page specified in the `serviceNotGivenURI` attribute in `nwsp.xml`. In the default configuration suggested during installation, the `serviceNotGivenURI` attribute points to the NWSP session status page. You could change this value to point to a different pages, such as the NWSP subscription page or home page.

**Step 6** To demonstrate an advertising redirection:

1. Wait until the configured TCP advertising interval time has elapsed. (The default time interval used during installation is 60 seconds.)
2. Perform some action on the SESM web page, such as selecting another service or requesting the status page. The SSG intercepts the request with an advertising redirection. An advertisement page from the Message Portal application appears.

**Step 7** To demonstrate the captivation feature, enter another URL before the TCP advertising duration elapses. (The default duration time configured in the sample `ssgconfig.txt` file is 10 seconds.) The newly entered URL is not honored, and the advertisement page from the Message Portal application redispays.

---

## Configuration Details

This section describes the configuration details for the SESM captive portal solution. Use this section if you want to change configuration after installation. This section includes the following topics:

- [Configuration File Summary, page 8-14](#)
- [captiveportal.xml Configuration File, page 8-15](#)
- [messageportal.xml Configuration File, page 8-17](#)
- [nwsp.xml Configuration File, page 8-20](#)
- [Message Duration Parameters, page 8-21](#)

## Configuration File Summary

Table 8-3 lists all of the configuration files that affect the sample SESM captive portal solution.

**Table 8-3 Configuration Files in the SESM Captive Portal Solution**

Component	File Path and Name	For More Information
J2EE configuration files	jetty config webdefault.xml	See the “ <a href="#">J2EE Configuration Files</a> ” section on page 6-3 for a summary of these files.
	applicationName docroot WEB-INF web.xml	See the <i>Cisco Subscriber Edge Services Manager Web Developer Guide</i> for SESM-specific information in these files.
Jetty container MBean configuration file	jetty2 config captiveportal.jetty.xml nwsp.jetty.xml messageportal.jetty.xml	These files configure the jetty containers for each of the applications. For more information, see the following sections: <ul style="list-style-type: none"> <li>• <a href="#">Configuring the J2EE Jetty Container, page 6-7</a></li> <li>• <a href="#">Eliminating J2EE Listeners, page 8-7</a></li> </ul>
Application MBean configuration files	captiveportal config captiveportal.xml messageportal config messageportal.xml nwsp config nwsp.xml	The Captive Portal and Message Portal applications use an MBean to retrieve configuration attributes from an xml file in the same way that any SESM portal application retrieves configuration attributes.  The following sections describe attributes related to captive portal configuration: <ul style="list-style-type: none"> <li>• <a href="#">captiveportal.xml Configuration File, page 8-15</a></li> <li>• <a href="#">messageportal.xml Configuration File, page 8-17</a></li> <li>• <a href="#">nwsp.xml Configuration File, page 8-20</a></li> </ul>



## captiveportal.xml Configuration File

Table 8-4 explains the configurable attributes used by the Captive Portal application.

**Table 8-4** Attributes in the Captive Portal MBean Configuration File

Object Name	Attribute Name	Explanation
Logger		See the Logger object in Table 6-4 on page 6-16.
ManagementConsole		See the ManagementConsole object in Table 6-4 on page 6-16.
captiveportal	userRedirectOn initialCaptiveOn advertisingCaptiveOn serviceRedirectOn	<p>These attributes provide a convenient way to switch on and off one or more of the TCP redirection types. Changing these attributes is much easier than reconfiguring the SSG. Valid values are:</p> <ul style="list-style-type: none"> <li>• True—The captive portal application performs an HTTP redirect to an appropriate content application.</li> <li>• False—The captive portal application does not respond to that particular type of TCP redirection. The subscriber experience is the same as if this type of TCP redirection were not configured.</li> </ul>
	host	Identifies the captive portal host. The value can be a comma-separated list of aliases and/or addresses. The application uses this attribute to detect loops. If the request host and this host value match, as well as the request port and the listener port, the captive portal application redirects the browser to the URL in errorURL.
The following attributes have values that are Java system properties. You can change the default value of a system property in the XML file, or you can override the default value at run time on the startup script command line.		
captiveportal	userRedirectURL initialCaptiveURL advertisingCaptiveURL	<p>The URL that you want the subscriber's browser to be redirected to after each type of redirection. Each URL is constructed as:</p> <p><code>http://host:portURI</code></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>host</i> is the IP address or host name of the web server for the content application that will handle the redirection type. The host is defined as one of the following java system properties: <ul style="list-style-type: none"> <li>– serviceportal.host (usually the NWSP IP address)</li> <li>– messageportal.host (usually the Message Portal IP address)</li> </ul> </li> <li>• <i>port</i> is the port that the web server is listening on. The port is defined as one of the following java system properties: <ul style="list-style-type: none"> <li>– serviceportal.port</li> <li>– messageportal.port</li> </ul> </li> <li>• <i>URI</i> is the absolute path for the page within the content application that you want the subscriber's browser to be redirected to. The default values used during installation are: <ul style="list-style-type: none"> <li>– For user redirections: /home, which is the NWSP logon page.</li> </ul> </li> </ul>

Table 8-4 Attributes in the Captive Portal MBean Configuration File (continued)

Object Name	Attribute Name	Explanation
captiveportal (continued)		<ul style="list-style-type: none"> <li>– For initial logon redirections: /initial, which is the Message Portal greetings page.</li> <li>– For advertising redirections: /advertising, which is the Message Portal advertising page.</li> </ul> <p>The default values for the system properties and the URIs were set during installation in the “URL Out” fields.</p>
	userRedirectPort initialCaptivePort advertisingCaptivePort	<p>The port that the web server for the Captive Portal application will listen on for each redirection type coming from the SSG. These attributes are set to the following java system properties:</p> <ul style="list-style-type: none"> <li>• userRedirect.port</li> <li>• initialCaptive.port</li> <li>• advertisingCaptive.port</li> </ul> <p>The default values for the system properties are the values you provided during installation in the “Port In” fields.</p> <p>If you change a port value, you must also change the SSG configuration to send redirections to the same port.</p>
	initialCaptiveDuration advertisingCaptiveDuration	<p>This value is passed to the Message Portal application in the CPDURATION parameter. It specifies the length of time that the Message Portal application waits before attempting to perform a redirection to the subscriber’s originally requested URL.</p> <p><b>Note</b> The SSG TCP redirect commands also accept a duration attribute. See the “<a href="#">Message Duration Parameters</a>” section on page 8-21 for more information.</p>
	serviceRedirectDefaultURL	<p>The URL that the subscriber’s browser is redirected to for any service redirection that does not have a service-specific URL defined in the defineServiceRedirect call, described next.</p>
	defineServiceRedirect	<p>defineServiceRedirect is a system call that passes 3 arguments. There is a call for each specific service redirection and one for the default service redirection.</p> <ol style="list-style-type: none"> <li>1. Port—The port that the web server for the Captive Portal application will listen on for the service redirections coming from the SSG. Its value is a Java system property whose default value was set during installation in the “Port In” fields.</li> </ol> <p>If you change a port value, also change the SSG configuration to send the service redirection to the same port value.</p> <ol style="list-style-type: none"> <li>2. URL (Optional)—The complete URL to the page you want the browser to be redirected to after the service redirection. If blank, the serviceRedirectDefaultURL is used.</li> </ol> <p><b>Note</b> The installation program does not prompt for or set these URLs, which means that all service redirections are redirected to the serviceRedirectDefaultURL above. If you want to set service-specific URLs for each service redirection, provide the URLs here.</p>

**Table 8-4** Attributes in the Captive Portal MBean Configuration File (continued)

Object Name	Attribute Name	Explanation
captiveportal (continued)		3. service name (Optional)—If provided, the captive portal application includes the service name in the query parameters appended to the URL that it forwards to the configured content application (for example, NWSP). The NWSP application uses the service name to attempt to connect to the service.
	errorURL	The URL that the Captive Portal application redirects to if it does not find a URL to redirect to for the given port that the request came in on. The default value set at installation time redirect to the NWSP /home page.
	parameter names: <ul style="list-style-type: none"> <li>• userRedirectURLParam</li> <li>• serviceRedirectURLParam</li> <li>• serviceRedirectServiceParam</li> <li>• serviceRedirectSubscriberParam</li> <li>• messageRedirectURLParam</li> <li>• messageRedirectSubscriberParam</li> <li>• messageRedirectDurationParam</li> </ul>	<p>These attributes define the parameter names used in the HTTP redirect requests. For example, the parameter name used to identify the subscriber's originally requested URL is CPSUBSCRIBER. You can change this to some other name by changing the value of userRedirectURLParam or MessageRedirectURLParam.</p> <p>These parameter names are visible to the subscriber in the browser's URL field. They appear in the query string appended to the URL.</p>

## messageportal.xml Configuration File

Table 8-5 explains the configuration attributes used by the Message Portal application.

**Table 8-5** Attributes in the Message Portal MBean Configuration File

Object Name	Attribute Name	Explanation
Logger		See the Logger object in <a href="#">Table 6-4 on page 6-16</a> .
ManagementConsole		See the ManagementConsole object in <a href="#">Table 6-4 on page 6-16</a> .
SESMBean		<p>See the description for <a href="#">SESM, page 6-19</a>.</p> <p>The mode attribute for the Message Portal application must be one of the following:</p> <ul style="list-style-type: none"> <li>• LDAP, if the mode for the Captive Portal application is LDAP.</li> <li>• Demo, if the mode for the Captive Portal application is RADIUS. (The Message Portal application does not obtain any subscriber profile information from a RADIUS database; therefore RADIUS mode is not implemented in this sample application. Demo mode provides all of the required SESM functionality.)</li> </ul>

Table 8-5 Attributes in the Message Portal MBean Configuration File (continued)

Object Name	Attribute Name	Explanation
SESMDemoMode		See the description for <a href="#">SESMDemoMode</a> , page 6-21. If you run Message Portal in Demo mode, it obtains subscriber profiles from the file identified in this MBean. You can add interests (hobbies) to the demo data file as described in <a href="#">Table 4-4 on page 4-9</a> , “ <a href="#">Special Attributes for Demonstrating LDAP Features in Demo Mode</a> ” earlier in this guide.
DESSMode		See the description for <a href="#">DESSMode</a> , page 6-21.
messageportal	defaultPage	For advertisement redirections, specifies the default page to redirect to if: <ul style="list-style-type: none"> <li>• The subscriber profile does not contain any interests</li> <li>• The ignoreProfile attribute is set to true</li> <li>• The interestPages attribute indicates that the default page should be used for a specific interest.</li> </ul>
	defaultURL	For initial logon and advertisement redirections, specifies a default URL to redirect to after the captivation duration has elapsed, if a CPURL parameter was not included in the query string of the HTTP request from the Captive Portal application. The CPURL parameter specifies the originally requested URL from the subscriber (before redirection).
	defaultDuration	Optional. This value is used if the Captive Portal application does not forward a CPDURATION parameter.  This attribute applies only if the redirectOn attribute is true. For initial logon and advertisement redirections, it specifies the length of time that the Message Portal application waits before attempting to perform the redirection to the subscriber’s originally requested URL.  <b>Note</b> The SSG TCP redirect commands also accept a duration attribute. See the “ <a href="#">Message Duration Parameters</a> ” section on page 8-21 for more information.
	ignoreProfile	For advertisement redirections, indicates whether the interest attribute in the subscriber profile should be used to determine the page to redirect to. Valid values are: <ul style="list-style-type: none"> <li>• True—Ignore the interest field. Redirect to the page specified in the defaultPage attribute.</li> <li>• False—Redirect to a page based on the first interest in the subscriber profile.</li> </ul> <b>Note</b> In RADIUS mode, this attribute must be set to true. The interest attribute is not available with RADIUS profiles.

Table 8-5 Attributes in the Message Portal MBean Configuration File (continued)

Object Name	Attribute Name	Explanation
messageportal (continued)	redirectOn	<p>For initial logon and advertisement redirections, indicates action to take after the captivation duration elapses:</p> <ul style="list-style-type: none"> <li>• True—Issue another redirection to the original page requested before the logon or advertisement redirection occurred. This is the URL specified in CPURL parameter in the query string of the HTTP request from the Captive Portal application.</li> <li>• False—Do not issue another redirection. The message or advertisement page remains displayed until the subscriber enters another URL.</li> </ul>
	interests	<p>Specifies the interest values that can appear in a subscriber profile. Separate each interest value with a comma. For example:</p> <pre>cinema, science, internet, news, sports, travel, finance, community</pre> <p>The interest values must match the options that you allow the subscriber to choose (for example, on an account self management page in NWSP) or that the service provider administrators are allowed to enter into an LDAP subscriber profile.</p>
	interestPages	<p>Specifies the advertisement page to display for each interest. (The Message Portal application displays the page appropriate to the first interest listed in a subscriber profile.) Separate each interest page with a comma.</p> <p>To use the default page for an interest, use any single character in the interestPages list.</p> <p>In the following example, subscribers whose profile contains science as the first interest see the default page as an advertisement.</p> <pre>cinema.jsp, ., internet.jsp, news.jsp, sports.jsp, travel.jsp, finance.jsp, community.jsp</pre>

## nwsp.xml Configuration File

The NWSP portal is the content application for unauthenticated user redirection and service redirections.

Table 8-6 explains configuration attributes in nwsp.xml that are directly related to the captive portal solution.

**Table 8-6** Captive Portal Attributes in nwsp.xml

Object Name	Attribute Name	Explanation
WebAppMBean	serviceNotGivenURI	For service redirections, tells NWSP which page to redirect to if the HTTP request from the Captive Portal application does not include a service parameter.  The default value that exists after installation is the NWSP status page.
	defaultURI	For service redirections, tells NWSP which page to redirect to if: <ul style="list-style-type: none"> <li>• The service specified in the HTTP request from the Captive Portal application is not available.</li> <li>• The service exists, the subscriber is not subscribed to it, and the subscriber does not have permission to visit the subscription page.</li> <li>• Any other unexpected conditions</li> </ul> The default value that exists after installation is the NWSP home page.
	serviceSubscriptionURI	For service redirections, tells NWSP which page to redirect to if the subscriber is not subscribed to the service that is specified in the HTTP request from the Captive Portal application.  The default value that exists after installation is: <ul style="list-style-type: none"> <li>• In LDAP mode, the NWSP subscriptionManage page.</li> <li>• In RADIUS mode, the NWSP displays the page specified in the defaultURI attribute.</li> </ul>
	serviceStartURI	For service redirections, tells NWSP which page to redirect to when the service in the HTTP request from the Captive Portal application does not require service logon.  The default value that exists after installation is the NWSP serviceStart page.
	serviceLogonURI	For service redirections, tells NWSP which page to redirect to when the service in the HTTP request from the Captive Portal application requires service logon credentials.  The default value that exists after installation is the NWSP serviceLogon page.

## Message Duration Parameters

This section describes how message durations are specified and how the specifications interact. In summary:

- The SSG duration specifies the minimal amount of time that a message is displayed.
- The SESM duration specifies the maximum amount of time that the message is displayed before an automatic redirect occurs to the originally requested page. (The automatic redirect feature can be turned off, in which case the greeting or message page is displayed until the subscriber enters another URL.)

SESM duration must be equal to or longer than the SSG duration. Otherwise, redirections that SESM attempts to perform will be too soon and will not happen.

### Durations on the SSG Side

On the SSG side, the message duration controls how long the SSG holds the browser to the message page before allowing the browser to display any other URL. If the subscriber or any web application (such as the SESM message portal application) attempts to redirect the browser before the SSG duration time has elapsed, the attempt fails. On the SSG side, duration is specified as follows:

- In the SSG TCP redirect commands.
- In the subscriber profile. The duration attributes are optional in a subscriber profile. If provided, they override the values specified in the SSG TCP commands.

### Durations on the SESM Side

On the SESM side, the message duration controls how long the content application waits before attempting to redirect the browser from the message page to the subscriber's originally intended URL or to a default URL. (If the redirect feature is turned off in the messageportal.xml file, then the SESM duration attributes are ignored.) On the SESM side, duration is specified as follows:

- In the captiveportal.xml file.

The duration values in the captiveportal.xml file are forwarded to the content application. One set of attributes applies to all messaging applications. The captive portal application forwards this value to the content application, using the CPDURATION parameter in the query string of the HTTP redirect.

The duration attributes in the captiveportal.xml file are:

- initialCaptiveDuration
  - advertisingCaptiveDuration
- In the messageportal.xml file.

The defaultDuration attribute in the messageportal.xml file is a default value used if the Captive Portal application does not forward a duration attribute.

## Configuring the SSG TCP Redirect Features

This section summarizes how to configure the TCP redirect features on the SSG host device. For additional information, see the SSG documentation listed in the “[Related Documentation](#)” section on [page xv](#).

This section includes the following topics:

- [Configuring SSG and Port-Bundle Host Key to Work with the Captive Portal Application, page 8-22](#)
- [Defining Captive Portal Groups and Port Lists, page 8-22](#)
- [Configuring Unauthenticated User Redirection, page 8-23](#)
- [Configuring Unauthorized Service Redirection, page 8-24](#)
- [Configuring Initial Logon Redirection, page 8-25](#)
- [Configuring Advertising Redirection, page 8-26](#)

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

To allow the Captive Portal application to obtain the subscriber name from profiles, the following 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 feature 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 follow:

```
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 and Port Lists

SSG sends a redirected TCP packet to a 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
```



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 the following sections illustrate how to create port lists and captive portal groups.

## Configuring Unauthenticated User Redirection

### Overview

When a subscriber is authenticated, SSG creates a host object for that subscriber. The absence of a host object relating to the source address of the packet indicates the need to redirect the packet to the portal group that is associated with unauthenticated user redirection. The result is that subscribers cannot access any part of the network beyond the SSG without first authenticating.

If you do not configure a captive portal group to handle TCP packets from unauthenticated users, SSG discards packets from unauthenticated users. To obtain the SESM logon page, subscribers must enter the URL of the SESM web server.

### PPP Connections—A Special Case

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 host object 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 group-name
```

The following commands from `ssgconfig.txt` create a captive portal group named `userRedirect`. The group consists of one web server whose IP address is 10.0.1.4, with a listener on port 8090. (In the sample solution, 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 unauthenticated user redirections in the `captiveportal.xml` file.) The `userRedirect` group is associated with unauthenticated user redirections. A port list cannot be assigned to this type of redirection—user redirection applies to all TCP packets that are not authenticated.

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

## Configuring Unauthorized Service Redirection

If a TCP packet is destined to the SSG default network or Open Gardens, it is not a candidate for service redirection. Also, if it is destined to a service to which the subscriber is already connected, the packet is not examined for redirection.

Otherwise, service redirection redirects a TCP packet if all of 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, not enough funds in the account

### Cisco IOS Configuration Commands

The following IOS commands from `ssgconfig.txt` configure three specific service redirections and a default service redirection. All of the service redirections are applied only to traffic coming into ports 80 and 8080. Each type of service redirection uses a different port on the same web server (the web server at IP address 10.0.1.4, which is the web server in which the SESM Captive Portal application is running).

```

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.

## Configuring Initial Logon Redirection

The initial logon redirection redirects all subscribers when they first log on, which is when SSG first creates the host object for the session. The length of time that the message is displayed 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 the [“Message Duration Parameters”](#) section on page 8-21 for more information.

### Cisco IOS Configuration Commands

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 captivate initial default group group-name duration seconds
```

The following commands from `ssgconfig.txt` create a port list named `ports` and a captive portal group named `initialCaptivate`. The group consists of one web server whose IP address is 10.0.1.4, with a listener on port 8091. (In the sample solution, 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 initial logon redirections in the `captiveportal.xml` file.) The `initialCaptivate` group is associated with initial logon redirections. The message captivation lasts for 10 seconds, unless the subscriber profile overrides the value. Redirections to this group are applied to TCP packets arriving on SSG ports 80 or 8080, as specified in the port list.

```
ssg tcp-redirect
  port-list ports
    port 80
    port 8080
  server-group initialCaptivate
    server 10.0.1.4 8091
  redirect port-list ports to initialCaptivate
  redirect captivate initial default group initialCaptivate duration 10
```

## Configuring Advertising Redirection

The advertising redirection redirects subscribers at timed intervals throughout the current session. 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 the [“Message Duration Parameters”](#) section on page 8-21 for more information.

### Cisco IOS Configuration Commands

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 captivate advertising default group group-name duration seconds
frequency seconds
```

The following commands from ssgconfig.txt create a port list named ports and a captive portal group named advertisingCaptivate. The group consists of one web server whose IP address is 10.0.1.4, with a listener on port 8092. (In the sample solution, 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.) The advertisingCaptivate group is associated with advertising redirections. The captivation lasts for 5seconds and occurs every 60 seconds, unless the subscriber profile overrides those values. Redirections to this group are applied to TCP packets arriving on the SSG at ports 80 or 8080, as specified in the port list.

```
ssg tcp-redirect
  port-list ports
    port 80
    port 8080
  server-group advertisingCaptivate
    server 10.0.1.4 8092
  redirect port-list ports to advertisingCaptivate
  redirect captivate advertising default group advertisingCaptivate duration 5 frequency
  60
```

## Troubleshooting Captive Portal Configurations

This section describes some potential problems with captive portal installation and configuration:

- [Some TCP Redirection Types Not Operational](#), page 8-27
- [Redirections Continuously Occur](#), page 8-27
- [User Name Not Passed in Unauthenticated User Redirections](#), page 8-28

## Some TCP Redirection Types Not Operational

If some TCP redirections do not seem to be occurring, check whether or not any of the following configuration problems exist:

- [Redirection Type Turned Off in captiveportal.xml, page 8-27](#)
- [Two Redirection Types Assigned to the Same Port in captiveportal.xml, page 8-27](#)
- [Redirection Type Not Configured on the SSG, page 8-27](#)

### Redirection Type Turned Off in captiveportal.xml

Check the following parameters in the captiveportal.xml file to make sure that the redirection type is turned on in the captive portal application:

- userRedirectOn
- initialCaptiveOn
- advertisingCaptiveOn
- serviceRedirectOn

### Two Redirection Types Assigned to the Same Port in captiveportal.xml

If you use the same port number for more than one type of redirection in the captiveportal.xml file, only one of the redirections per port is operational. This might happen if, during captive portal installation, you change the default port numbers suggested by the installation program, and erroneously reuse the same port number.

The precedence order that determines which type of redirect is operational on a port is:

1. unauthorized user redirections
2. initial logon redirections
3. advertising redirections
4. service redirections

### Redirection Type Not Configured on the SSG

Check the SSG configuration to make sure that:

- The redirection type is associated with the SESM Captive Portal application (and not the Message Portal application)
- The redirection type is associated with the same port that you specify in the captiveportal.xml file for that redirection type.

## Redirections Continuously Occur

If the browser is continuously redirected to the same page, investigate the following topics:

- [Redirected Networks Must Match Service Routes, page 8-28](#)
- [Using HTTP1.1 with a Non-SESM Captive Portal Application, page 8-28](#)

## Redirected Networks Must Match Service Routes

The service route for a service, which is defined in the service profile, must exactly match the destination network that you configure in a service redirection for that service.

For example, suppose you want to establish service redirections for a service on network 10.1.1.1. If you define the incoming destination network that is eligible for redirections as follows:

```
ssg tcp-redirect
network-list serviceNetwork1
network 10.1.1.0 255.255.255.0
```

then you must define the service route for the service using the same IP address and mask (10.1.1.0 and 255.255.255.0).

If you define the service route differently (for example, you use 10.1.1.1 and 255.255.255.255), then the service redirection will occur repeatedly. After the first and required service redirection, any subsequent requests are subject to the service redirection, even though the service is connected.

The symptom of this misconfiguration is the continuous redisplay of the redirect URL. For example, in the sample SESM solution, the NWSP service logon page appears each time you click the OK button, even though the service is already connected.

## Using HTTP1.1 with a Non-SESM Captive Portal Application

If you deploy a web server other than the SESM Captive Portal application as the redirect server, and the web server uses HTTP1.1, make sure to use the protocol options that explicitly close the connection for each response from the web server.

HTTP1.1 persists connections. The persistent connection causes the SSG to continue redirecting for subsequent requests because it is still handling the same connection. The SSG continues redirecting even after the mapping times out on the SSG. This behavior is particularly noticeable for initial captivation, where one would expect the redirection to occur only one time.

## User Name Not Passed in Unauthenticated User Redirections

If the captive portal application is not passing the subscriber name (CPSUBSCRIBER) in the HTTP redirection for unauthenticated user redirections:

- Ensure that the SSG is configured as described in the [“Defining Captive Portal Groups and Port Lists” section on page 8-22](#).
- Check the following two attributes in captiveportal.xml. If they are empty, the captive portal application does not attempt to retrieve or pass the subscriber name.
  - messageRedirectSubscriberParam
  - serviceRedirectSubscriberParam



**Note** When these two attributes are empty, the user name feature is turned off. This might be desirable, for example, for performance reasons.



## Summary of SESM Communication Attributes

This section describes the attributes that control communication between components in an SESM deployment. In many cases, attributes with matching values must be set on both sides of the communication for the communication to be successful.

This section includes the following topics:

- [Communication Attributes for Interaction Between SESM and SSG, page 9-1](#)
- [Communication Attributes for RADIUS Mode, page 9-3](#)
- [Communication Attributes for LDAP Mode, page 9-6](#)
- [Communication Attributes for LDAP Mode with RDP in Proxy Mode, page 9-10](#)

### Communication Attributes for Interaction Between SESM and SSG

The section applies to all SESM deployments, regardless of the SESM mode.

[Figure 9-1](#) shows the attributes whose values must match for successful communication between an SESM web application and SSG. [Table 9-1](#) describes how to set these attributes on both sides of the communication.

**Figure 9-1** Attributes for SESM to SSG Communication in All Modes

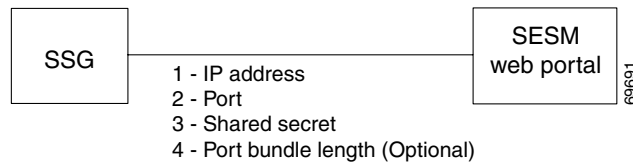


Table 9-1 Setting Attributes for SESM to SSG Communication in All Modes

Configuring Communication Between an SESM Web Application and SSG	
On the SSG side	Set these values using Cisco IOS commands on the SSG host. If the SSG is already configured, use <b>show run</b> to view the settings.
	<p>1. IP Address—Use the following command to specify the network that the SESM web application is running on:</p> <pre>ssg default-network networkIPAddress mask</pre>
	<p>2. Port—Use the following command to specify the port on the SSG host that handles RADIUS protocol communication between the SSG and the SESM web application:</p> <pre>ssg radius-helper auth-port port</pre>
	<p>3. Shared Secret—Use the following command to specify the shared secret used in RADIUS protocol communication between the SSG and the SESM web application:</p> <pre>ssg radius-helper key secret</pre>
	<p>4. (Optional) Host Key Port Bundle Length—When the host key feature is enabled on the SSG, the port bundle length defaults to 4 bits. You can use the following command to specify a different port bundle length:</p> <pre>ssg port-map length bits</pre> <p><b>Note</b> Additional commands are required on SSG to enable and configure the host key feature. For more information, see the <a href="#">“Configuring the Host Key Port Bundle Feature on SSG”</a> section on page B-2.</p>
On the SESM web application side	1. IP Address—Make sure to install SESM web applications and their containers (the J2EE web servers) on the SSG default network.
	Set the following values in the SSG MBean in the application MBean configuration file (nwsp.xml, for example):
	<p>2. Port—Use the following attributes to set the RADIUS protocol ports for communication between the SSGs and SESM. These settings must match the settings on the SSG hosts.</p> <ul style="list-style-type: none"> <li>• PORT global attribute</li> <li>• PORT subnet attribute—Overrides the global setting if all of the SSGs are not configured the same.</li> </ul>
	<p>3. Shared Secret—Use the following attributes to set the RADIUS protocol shared secrets for communication between the SSGs and SESM. These settings must match the settings on the SSG hosts.</p> <ul style="list-style-type: none"> <li>• SECRET global attribute</li> <li>• SECRET subnet attribute—Overrides the global setting if all of the SSGs are not set the same.</li> </ul>
	<p>4. Host Key Port Bundle Length—Use the following attributes to set the port-bundle length to match the settings on the SSG hosts.</p> <ul style="list-style-type: none"> <li>• BUNDLE_LENGTH global attribute</li> <li>• BUNDLE_LENGTH subnet attribute—Overrides the global setting if all of the SSGs are not configured the same.</li> </ul>



### Attribute Definitions

The RADIUS protocol is the communication mechanism used between an SESM web application and SSG. The following attributes are required by the RADIUS protocol:

- IP address and port—In communications between SESM and SSG, SSG acts as the server and SESM is the client. In the RADIUS protocol, the client must know the IP address of the server and the port that the server listens on. SSG uses the concept of a RADIUS helper to define this port. The RADIUS helper port is a different attribute from the RADIUS port used for communication with a RADIUS server. However, the values of these two attributes might be the same. The value 1812 is common for both.
- Shared secrets—Shared secrets are the key for the MD5 encryption algorithm used by the RADIUS protocol. They are required in all RADIUS protocol communications. The shared secret value is known on each side of the communication but is never sent across the network.

The following attribute is used by the SSG port-bundle host key feature:

- Port-bundle length—This attribute controls how many ports are in each bundle in the SSG host key feature, and, indirectly, how many bundles are available within each host key source IP address as configured on the SSG. The length defines the number of bits required to represent the number of ports in each bundle. For example, a length of 4 (bits) means that the number of available ports in each bundle is  $2^4$ , or 16 ports per bundle.



**Note** Cisco strongly recommends using the same port bundle length on all SSGs in the same network. The default value of 4 is recommended, which results in 16 ports per bundle and 4032 bundles per host key source IP address.

## Communication Attributes for RADIUS Mode

This section describes attributes in a RADIUS mode deployment whose values must match each other for successful communication to occur.

Figure 9-2 shows the attributes whose configured values must match. Table 9-2 describes how to set these attributes on each side of the communication.

**Figure 9-2 Communication Attributes in a RADIUS Mode Deployment**

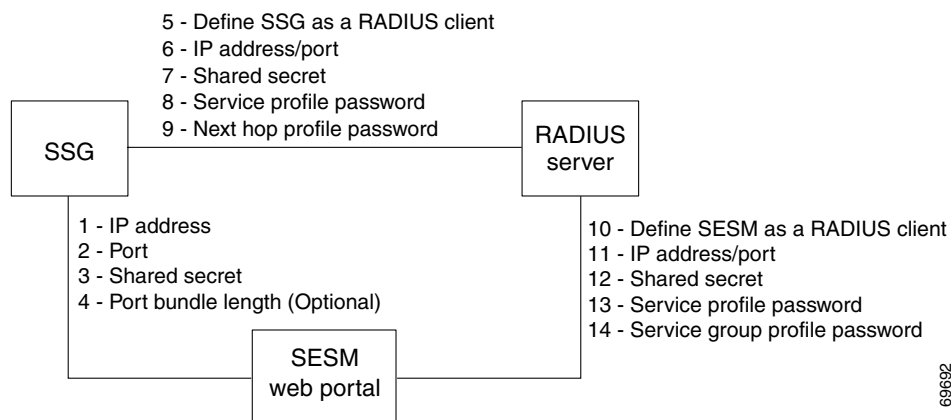


Table 9-2 Setting Communication Attributes in a RADIUS Mode Deployment

Configuring Communication Between an SESM Application and SSG		
On the SESM and SSG sides	<b>1. to 4.</b>	See <a href="#">Table 9-1, “Setting Attributes for SESM to SSG Communication in All Modes”</a>
Configuring Communication Between a RADIUS Server and SSG		
On the RADIUS side	Set these values using the RADIUS product’s native configuration procedures:	
	<b>5.</b>	Define SSG as a RADIUS Client—Define SSG as a NAS client.
	<b>6.</b>	IP address/port—The IP address is the address of the RADIUS server host machine. The port is the port the RADIUS server uses to listen for authentication and authorization requests. If you do not specifically set the authentication port, it usually defaults to port 1812.
	<b>7.</b>	Shared secret—The shared secret value is specified when defining the SSG as a NAS client.
	<b>8.</b>	Service password—The service password is included in the service profiles stored in the RADIUS database. Use the same password value in all service profiles.
	<b>9.</b>	(Optional) Next hop password—The password used in the next hop table profile stored in the RADIUS database. Next hop profiles are an optional feature in an SESM deployment. Use the same password value in all next hop profiles.
On the SSG side	Set these values using Cisco IOS commands on the SSG host:	
	<b>5.</b>	Set up SSG as a RADIUS client—Use the following commands:  <pre>#aaa new-model #aaa authentication ppp default local group radius #aaa authorization network default local group radius</pre> <p><b>Note</b> If the SSG is not supporting PPP connections, you do not need the <b>aaa authentication ppp</b> command.</p>
	<b>6.</b>	IP address/port—Use the following command:  <pre>radius-server host RadiusHostIpAddr auth-port port</pre>
	<b>7.</b>	Shared secret—Use the following command:  <pre>radius-server key RadiusSharedSecret</pre>
	<b>8.</b>	Service Password—Use the following command:  <pre>ssg service-password servicePassword</pre>
	<b>9.</b>	(Optional) Next Hop Password—Use the following command:  <pre>ssg next-hop download nextHopTableName password</pre>

Table 9-2 Setting Communication Attributes in a RADIUS Mode Deployment (continued)

Configuring Communication Between a RADIUS Server and an SESM Application	
On the RADIUS side	Set these values using the RADIUS product's native configuration procedures:
	<b>10.</b> Define a RADIUS client—Define SESM as a NAS client.
	<b>11.</b> IP address/port—You can set the port on the RADIUS server host machine that the RADIUS server uses to listen for authentication requests. The port is usually port 1812, which is the industry's default port for a RADIUS server.
	<b>12.</b> Shared secret—You set the shared secret value when you define the SESM application as a NAS client.  <b>Note</b> If you are configuring primary and secondary RADIUS servers, the shared secret value established for the SESM NAS client must be the same on both RADIUS servers.
	<b>13.</b> Service password—The service password is included in the service profiles stored in the RADIUS database. Use the same password value in all service profiles.
	<b>14.</b> Group password—The service group password is included in the service group profiles stored in the RADIUS database. Use the same password value in all service group profiles.
On the SESM web application side	Set the following value in the SESM MBean in the SESM web application configuration file (nwsp.xml, for example):
	<b>10.</b> Define a RADIUS client—The attribute name is mode. To deploy SESM in RADIUS mode, the value for mode must be RADIUS.  <b>Note</b> You can override the value for mode on the command line when you start the SESM application. For more information, see the <a href="#">“Starting the SESM Portals”</a> section on page 7-1.
	Set the following values in the AAA MBean in the SESM application configuration file (nwsp.xml, for example):
	<b>11.</b> IP Address/Port—The attribute names for identifying IP addresses and authentication ports on primary and secondary RADIUS servers are: <ul style="list-style-type: none"> <li>• primaryIP</li> <li>• primaryPort</li> <li>• (Optional) secondaryIP</li> <li>• (Optional) secondaryPort</li> </ul>
	<b>12.</b> Shared Secret—The attribute name is secret. There is only one secret attribute because the the secret value must be the same on both the primary and secondary servers.
	<b>13.</b> Service Password—The attribute name is servicePassword. Use this attribute to provide SESM with the generic password used in the service profiles.
	<b>14.</b> Group Password—The attribute name is groupPassword. Use this attribute to provide SESM with the generic password used in the service group profiles.

### Attribute Definitions

The RADIUS protocol is the communication mechanism used between all of the components in this deployment. The following attributes are required by the RADIUS protocol:

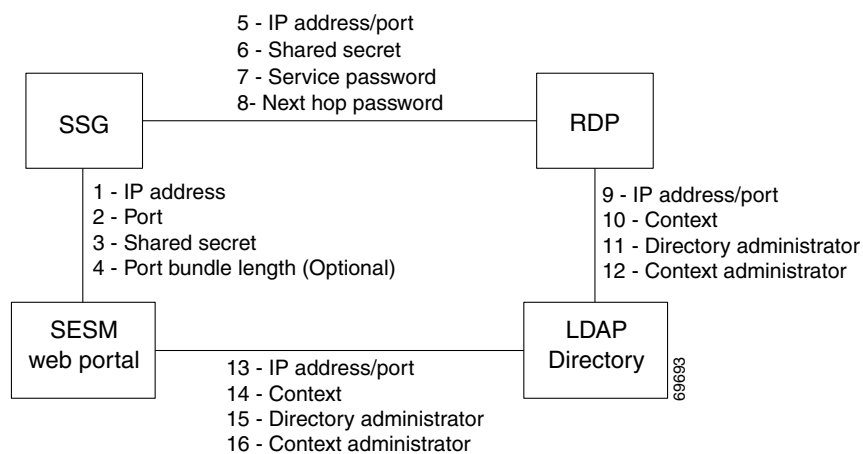
- RADIUS IP address and port—The RADIUS clients must know the IP address of the RADIUS server machine and the port that RADIUS uses for authentication and authorization requests. The port is set when the RADIUS server is configured. It is usually port 1812, which is the industry’s default authentication and authorization port for a RADIUS server.
- Shared secrets—Shared secrets are the key for the MD5 encryption algorithm used by the RADIUS protocol. They are required in all communications between a RADIUS client and a RADIUS server. The shared secret value is known on each side of the communication but is never sent across the network.
- Profile passwords—In a RADIUS database, the service, service group, and next hop profiles include passwords. The RADIUS protocol requires that requests for these profiles include the profile password. In an SESM RADIUS mode deployment, all profiles of the same type must use the same password. For example, all service profiles use the same password; all service group profiles use the same password, and so forth. You provide these generic password values to the RADIUS clients (SSG or SESM) using configuration attributes.

## Communication Attributes for LDAP Mode

This section describes attributes in a LDAP mode deployment whose values must match each other for successful communication to occur.

Figure 9-3 shows the attributes whose configured values must match on each side of the communication to successfully deploy SESM in LDAP mode. Table 9-3 describes how to set these attributes on each side of the communication.

**Figure 9-3** Communication Attributes in an LDAP Mode Deployment



**Table 9-3 Setting Communication Attributes in an LDAP Mode Deployment**

<b>Configuring Communication Between an SESM Web Application and SSG</b>		
On the SESM and SSG sides	<b>1. to 4.</b> See <a href="#">Table 9-1, “Setting Attributes for SESM to SSG Communication in All Modes”</a>	
<b>Configuring Communication Between RDP and SSG</b>		
On the RDP side	Set the following values in the RDP MBean in the rdp.xml file on the RDP host machine.	
	<b>5.</b> IP address/port—The attribute names are: <ul style="list-style-type: none"> <li>localIPAddress—The IP Address or host name of the RDP host machine. (You cannot enter the value localhost or 127.0.0.1.)</li> <li>localPort—The port on which RDP will listen for RADIUS authentication and authorization requests. The value is usually 1812, which is the industry’s default authentication and authorization port.</li> </ul>	
	<b>6.</b> Shared secret—The attribute name is secret. This is the RADIUS protocol shared secret value used for communication between SSG and RDP.	
	Set the following values in the RDPPacketFactory MBean in the rdp.xml file on the RDP host machine. These values are arguments to a programming call, rather than named attributes.	
	<b>7.</b> Service password—Identify the correct argument by searching for: <pre>&lt;Arg&gt;PASSWORD:servicecisco&lt;/Arg&gt; &lt;Arg&gt;ServiceRequest&lt;/ARG&gt;</pre> <p>Replace <code>servicecisco</code> with the service password set on the SSG side.</p>	
	<b>8.</b> (Optional) Next hop password—Identify the correct argument by searching for: <pre>&lt;Arg&gt;PASSWORD:nexthopcisco&lt;/Arg&gt; &lt;Arg&gt;NextHopRequest&lt;/ARG&gt;</pre> <p>Replace <code>nexthopcisco</code> with the next hop password set on the SSG side. Next hop profiles are an optional feature in an SESM deployment.</p>	
	On the SSG side	Set the following values using Cisco IOS commands on the SSG:
	<b>5.</b> IP address/port—Use the following command: <pre>radius-server host <i>RDPHostIpAddr</i> auth-port <i>port</i></pre>	
<b>6.</b> Shared secret—Use the following command: <pre>radius-server key <i>RDPSharedSecret</i></pre>		
<b>7.</b> Service password—Use the following command to set the key that SSG will use to identify service requests: <pre>ssg service-password <i>servicePassword</i></pre>		
<b>8.</b> (Optional) Next hop password—Use the following command to set the key that SSG will use to identify next hop table requests: <pre>ssg next-hop download <i>nextHopTableName</i> <i>password</i></pre>		

Table 9-3 Setting Communication Attributes in an LDAP Mode Deployment (continued)

<b>Configuring Communication Between RDP and an LDAP Directory</b>	
SPE configuration on the RDP side	<p>Set these values in the <code>dess-auth</code> configuration file on the RDP host machine (<code>dess-auth/config/config.xml</code>, for example).</p> <p><b>9.</b> IP Address/Port—The attribute name is <code>URL</code>. Provide the complete URL of the directory server, including the <code>ldap</code> protocol label and a port number. A sample entry is:</p> <pre>ldap://127.0.0.1:389/</pre> <p>You provide the initial value for this attribute during installation. The installation program prompts you for a directory address and directory port, and then it combines your responses, prefaces it with the <code>ldap</code> protocol label, and inserts the resulting string in the <code>URL</code> field in the <code>config.xml</code> file.</p> <p><b>10.</b> Context—The attribute name is <code>context</code>. Provide the organizational unit and organization in the LDAP directory that holds the SESM data. A sample entry is:</p> <pre>ou=sesm,o=cisco</pre> <p>You provide the initial value for this attribute during installation. The installation program prompts you for the directory container.</p> <p><b>11.</b> Directory administrator—The attribute names are:</p> <ul style="list-style-type: none"> <li><b>principal</b>—This must be an administrator ID that exists in the LDAP directory with permissions to extend the LDAP directory schema. A sample entry is:</li> </ul> <pre>cn=admin,ou=sesm,o=cisco</pre> <p>or</p> <pre>uid=Directory Manager, ou=sesm, o=cisco</pre> <ul style="list-style-type: none"> <li><b>credentials</b>—Provide the password that goes with the principal.</li> </ul> <p>You provide the initial values for these attributes during installation. The installation program prompts you for directory server admin information.</p> <p><b>12.</b> Context administrator—The attribute name is <code>DESSPrincipal</code>. This is an administrator ID with permissions to access and create objects in the organization and organizational unit identified by the context attribute described above. An example entry is:</p> <pre>cn=user,ou=sesm,o=cisco</pre> <p>You provide the initial values for this attribute during installation. The installation program prompts you for directory container admin information.</p>
On the LDAP Directory side	<p><b>9. to 12.</b> Use native administration tools for the LDAP directory product to configure the directory for SESM deployment. See the “<a href="#">LDAP Directory Configuration Requirements</a>” section on page 5-4 for guidelines and requirements.</p>

**Table 9-3** Setting Communication Attributes in an LDAP Mode Deployment (continued)

<b>Configuring Communication Between an SESM Application and an LDAP Directory</b>		
SPE configuration on the SESM application side	<b>13. to 16.</b>	If the RDP and SESM applications are installed on the same machine, the same config.xml file applies to both applications. In that case, the values you configured for fields 9 to 12 above are also used for communication between the SESM application and the directory.  If the RDP and SESM web applications are installed on different machines, you must maintain two versions of the dss-auth configuration file. In that case, follow the instructions in fields 9 to 12 above to configure the config.xml file on the SESM web application's host machine.
On the LDAP directory side	<b>13. to 16.</b>	You only need to configure the LDAP directory one time.

**Attribute Definitions**

RDP and SESM web applications use the LDAP protocol to communicate with the LDAP directory. Some of the LDAP attributes required for communication are:

- IP address/port—These attributes identify the location of the LDAP directory.
- Context—This attribute identifies the container within the LDAP directory that was created specifically for the SESM data.
- Directory administrator—This is a top-level administrator who has permissions to create new contexts within the directory and extend the contexts with application-specific definitions.
- Context administrator—This is an administrator of the context that was created for the SESM data. This administrator must have permissions to add objects into the SESM-specific context.

RDP and SESM web applications use the RADIUS protocol to communicate with SSG. Some of the attributes are:

- IP address/port—RDP is a proxy RADIUS server. You configure SSG to communicate with RDP using the same commands that you use to configure SSG to RADIUS server communication.
- Shared secrets—Shared secrets are the key for the MD5 encryption algorithm used by the RADIUS protocol. They are required in all communications between a RADIUS client and a RADIUS server. The shared secret value is known on each side of the communication but is never sent across the network.
- Service and next hop passwords—The service and next hop requests that SSG sends to RDP include a key word, or password. RDP uses this key word to identify the type of request it has just received and to determine how to process the request. You must configure matching password values on both SSG and RDP for this mechanism to work.

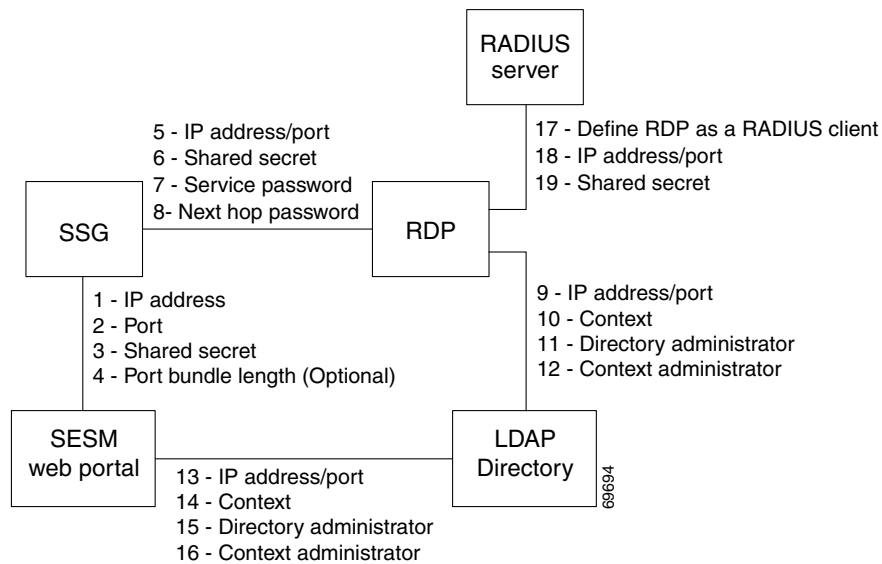
## Communication Attributes for LDAP Mode with RDP in Proxy Mode

This section describes the attributes that must be configured to use a proxy RADIUS server in an LDAP mode configuration.

Figure 9-4 shows the attributes whose configured values must match on each side of the communication between RDP in proxy mode and the RADIUS Server. Table 9-4 describes how to set these attributes on each side of the communication.

All other communication in this deployment are the same as described in the previous section.

**Figure 9-4** Communication Attributes in an LDAP Mode Deployment with RDP in Proxy Mode



### Note

The service group password is not used in this deployment. Service group requests are obtained by the SESM web portal from the LDAP directory, and a password is not required.



Table 9-4 Setting Communication Attributes in an LDAP Mode Deployment with RDP Proxy

Configuring Communication Between Components in LDAP Mode	
See Table 9-3.	<b>1. to 12.</b> See Table 9-3, “Setting Communication Attributes in an LDAP Mode Deployment”
Configuring Communication Between RDP and a RADIUS Server	
On the RDP side	Set the following values in the rdp.xml file on the RDP host machine, in the AAA MBean that contains the connection=Proxy parameter:
	<b>13.</b> Define RDP as a RADIUS client—To configure RDP as a RADIUS client, you need to install RDP in Proxy mode. The content of the rdp.xml file contains different packet handlers depending on the RDP mode. Therefore, to change the RDP mode, we recommend reinstalling the RDP component. (Choose a Custom installation, and then check RDP, to reinstall only the RDP component.)
	<b>14.</b> IP Address/Port—The attribute names for identifying ports on a primary and secondary RADIUS server are: <ul style="list-style-type: none"> <li>• primaryIP</li> <li>• primaryPort</li> <li>• (Optional) secondaryIP</li> <li>• (Optional) secondaryPort</li> </ul>
	<b>15.</b> Shared Secret—The attribute name is AAASecret. The RADIUS shared secret value must be the same on both the primary and secondary servers, so there is only one secret attribute.
	Set the following value in the RDPPacketFactory MBean in the rdp.xml file on the RDP host machine. This value is an argument to a programming call, rather than a named attribute.
	<b>16.</b> Service Group Password—Identify the correct argument by searching for: <pre>&lt;Arg&gt;PASSWORD:groupcisco&lt;/Arg&gt; &lt;Arg&gt;GroupRequest&lt;/ARG&gt;</pre> Replace <code>groupcisco</code> with the password you use in the service group profiles on the RADIUS database.
On the RADIUS side	Set these values using the RADIUS product’s native configuration procedures:
	<b>17.</b> Set up a RADIUS Client—Define RDP as a NAS client.
	<b>18.</b> IP Address/Port—You can set the port on the RADIUS server host machine that the RADIUS server uses to listen for authentication requests. The port is usually port 1812, which is the industry’s default authentication and authorization port for a RADIUS server.
	<b>19.</b> Shared secret—You set the shared secret value when you define the RDP application as a NAS client. <p><b>Note</b> If you are configuring primary and secondary RADIUS servers, the shared secret value must be the same on both RADIUS servers.</p>





# Troubleshooting SESM Installation and Configuration

---

This chapter provides some help with troubleshooting problems in a Cisco Subscriber Edge Services Manager (SESM) deployment. It includes the following topics:

- [Diagnosing Problems, page 10-1](#)
- [Troubleshooting Aids, page 10-4](#)
- [Troubleshooting Tips, page 10-7](#)

## Diagnosing Problems

This section contains procedural charts that show you how to research a problem and identify the general area of the problem before escalating it to the Cisco Technical Assistance Center. The section includes the following procedures:

- [Procedures for Troubleshooting an SESM Web Application, page 10-1](#)
- [Procedures for Troubleshooting RDP, page 10-3](#)

## Procedures for Troubleshooting an SESM Web Application

[Figure 10-1](#) shows a procedure for analyzing problems in an SESM web application. The numbered callouts are keyed to the table that follows the figure.

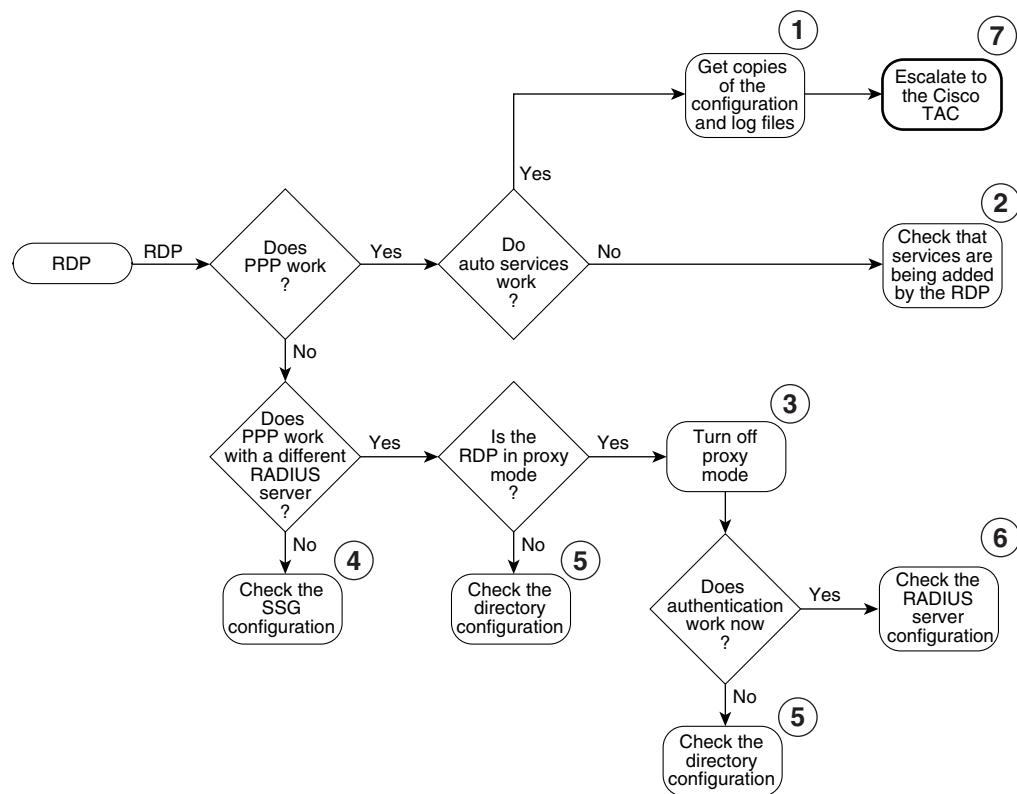


5	Make sure the subscriber is subscribed to services and has the proper privileges to access those services. See the URL for CDAT documentation: <a href="http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_311/toolgd/index.htm">http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_311/toolgd/index.htm</a>
6	See <a href="#">Obtaining Technical Assistance</a> , page xvi.
7	See <a href="#">Procedures for Troubleshooting RDP</a> , page 10-3.

## Procedures for Troubleshooting RDP

Figure 10-2 shows a procedure for analyzing problems in RDP. The numbered callouts are keyed to the table that follows the figure.

Figure 10-2 Procedures for Troubleshooting RDP



59611

1	See <a href="#">Configuration File Summary</a> , page 6-3 and <a href="#">Logging and Debugging Mechanisms</a> , page 10-4.
2	See the RDPPacketFactory object in <a href="#">Table 6-6</a> on page 6-32.
3	See <a href="#">RDP Modes</a> , page 6-30.
4	See <a href="#">Configuring the SSG</a> , page B-1.
5	See <a href="#">Configuring SPE</a> , page 6-37.
6	See the AAA object in <a href="#">Table 6-4</a> on page 6-16.
7	See <a href="#">Obtaining Technical Assistance</a> , page xvi.

# Troubleshooting Aids

This section describes some facilities that might be useful in troubleshooting SESM installation and configuration problems. It includes the following topics:

- [Logging and Debugging Mechanisms, page 10-4](#)
- [Java Command Line Options, page 10-6](#)
- [SESM Management Console, page 10-6](#)
- [Obtaining License and Version Information, page 10-7](#)

## Logging and Debugging Mechanisms

This section describes the logging and debugging options available to help troubleshoot SESM applications and deployment. The logging and debugging mechanisms are MBeans which are configured in the MBean configuration files. By changing the configuration of the logging and debugging mechanisms, you can change the amount of detail reported and specify message filtering. The topics in this section are:

- [Log File Locations, page 10-4](#)
- [Logging and Debugging in SESM Web Applications, page 10-4](#)
- [Switching Debugging On and Off at Run Time, page 10-5](#)
- [Logging and Debugging in RDP, page 10-5](#)
- [Logging and Debugging in CDAT, page 10-6](#)

## Log File Locations

The log files for the SESM web applications, RDP, and CDAT, are located in log directories. All of the configuration files use the `application.log` Java system property to set the location of the log directory. Java system properties are set by the application startup scripts.

See [Table 7-1 on page 7-5, “Java System Properties in Startup Scripts”](#) for information about how the application startup scripts set `application.log`, the default values of `application.log`, and how to change the default.

## Logging and Debugging in SESM Web Applications

You can use the SESM application’s log files to troubleshoot problems. Two of the log files have debugging mechanisms that you can configure along with the logging features.

An SESM web application and its Jetty container write to the following log files:

- Jetty container’s HTTP request log—This log file records all incoming HTTP requests. You can use this log file to analyze volume and traffic patterns for the web server.  
The default name for this file is `date.request.log`. For information on configuring this log, including file name and retention period, see the “Jetty Log Sink” object in [Table 6-3 on page 6-9](#).
- Jetty container’s application log—This log file records logging and debugging messages. The logging messages record the startup of the Jetty server and all ongoing activity, such as errors trapped by the Jetty server and HTTP errors. If the SESM application fails to start, look at this log.

Make sure you monitor this log file for illegal HTTP requests that might indicate attempts to subvert the web server. If you enable debugging, the log file also includes more detailed debugging messages.

The default name for this file is *date.jetty.log*. For information on configuring this log, including file name, retention period, and contents, see:

- The “Log” object in [Table 6-3 on page 6-9](#), to configure the container’s log file
- The “DebugMBean” object in [Table 6-3 on page 6-9](#), to configure the container’s debugging features
- SESM web application log—This log file records logging and debugging messages. The logging tool logs SESM web application activity. The debugging mechanism produces messages useful to developers in debugging applications.

The default name for this file is *date.application.log*. See the “Logger” object in [Table 6-4 on page 6-16](#) for information on configuring this file, including its file name and retention period, whether debugging is turned on or off, and the content of logging and debugging messages.

Configure the container logs in the container MBean configuration file for the application:

```
jetty
  config
    nwsp.jetty.xml
    wap.jetty.xml
```

Configure the application log in the application MBean configuration file:

```
nwsp
  config
    nwsp.xml
```

## Switching Debugging On and Off at Run Time

The debug attribute in the Logger MBean in the application configuration file controls whether debug is on or off. The attribute is a Java system property:

```
nwsp.debug
```

You can switch debugging on or off at the command line to override the default value in the XML file or use the `-D` option on the command line when you start the portal application.

## Logging and Debugging in RDP

The RDP application writes to the RDP application log file, which records logging and debugging messages. The logging feature logs RDP application activity. The debugging mechanism might be useful in debugging packet handling. The default name for this log file is *date.application.log*.

RDP uses the same logging facility that the SESM web applications use. Both use a Logger MBean to configure the logging and debugging features. For RDP, you configure the Logger MBean in the RDP configuration file:

```
rdp
  config
    rdp.xml
```

See the “Logger” object in [Table 6-4 on page 6-16](#) for information about configuring the Logger MBean.

## Logging and Debugging in CDAT

CDAT is a web application running in a J2EE container, similar to the SESM web applications. The CDAT application and its Jetty container write to the same types of log files as the SESM web applications, as described previously in the “[Logging and Debugging in SESM Web Applications](#)” section on page 10-4.

Configure the container logs in the CDAT-specific container MBean configuration file:

```
jetty
  config
    cdat.jetty.xml
```

Configure the application log in the CDAT MBean configuration file:

```
cdat
  config
    cdat.xml
```

## Java Command Line Options

When you execute a startup script that includes the java command, you can specify any Java option on the command line. To specify Java options, use `-jvm` as an option on the command line. For example, you can add the following option to the command line when you execute the SESM application startup script:

```
-jvm -Djava.compiler=NONE
```

## SESM Management Console

The Sun example JMX server, which is the JMX server installed with the Jetty component in the SESM installation package, includes a JMX HTML adaptor. SESM uses the adaptor to produce a management console that shows the current value of all MBean attributes in all of the MBean configuration files.



### Note

This JMX HTML adaptor is not production quality. For example, configuration changes made using this console are not persistent. You should remove it from your configuration files before transitioning the SESM application to public use. See the “ManagementConsole” object in [Table 6-4 on page 6-16](#) for information about configuring and removing this adaptor.

You can access the SESM management console on a web browser at the following URL:

```
http://SESMserver:managementPortNumber/
```

Where:

*SESMserver*—Host name or IP address of the workstation on which SESM is installed.

*managementPortNumber*—The port configured in the `HtmlAdaptorServer` MBean in the application configuration file. The default management port number used by the SESM installation program is:

```
applicationPortNumber + 100
```

For example, for NWSP, the installer uses a default application port number of 8080 and a corresponding management port number of 8180.



## Management Console User Name and Password

Before you gain access to the management console, you must enter a valid user name and password. Enter the values that match the values in the ManagementConsole MBean in the application's configuration file. See the "ManagementConsole" object in [Table 6-4 on page 6-16](#) for more information.

## Obtaining License and Version Information

If you purchased SESM, your license number is available on the License Certificate shipped with the product. If you have not purchased SESM, you can install an evaluation copy of the software without a license number. An evaluation installation provides full software functionality. Although the evaluation options do not have an expiration period, you must obtain a license before deploying SESM in a production environment.

The installation program records the license number and the software version you installed in the licensenum.txt file under the installation directory.

## Troubleshooting Tips

This section contains some hints that might help you identify and fix problems in SESM. The problems are divided into the following topics:

- [JRE and JDK Troubleshooting, page 10-7](#)
- [Installation Troubleshooting, page 10-10](#)
- [Configuration File Location Troubleshooting, page 10-11](#)
- [SESM Configuration Troubleshooting, page 10-11](#)
- [RADIUS Configuration Troubleshooting, page 10-12](#)
- [SSG Configuration Troubleshooting, page 10-12](#)

## JRE and JDK Troubleshooting

If the installer does not find an appropriate JRE, it installs the bundled JRE Version 1.2.2.

This section contains the following topics:

- [Warning and Error Messages after JRE Installation, page 10-7](#)
- [Searching for an Existing JDK or JRE, page 10-8](#)
- [Using a Pre-installed JRE or JDK, page 10-9](#)
- [Recompiling a Customized JSP, page 10-9](#)

## Warning and Error Messages after JRE Installation

The JRE installation might produce warning messages and nonfatal error messages. These messages are expected and normal.

- The warning message states that JSPs will not be compiled. You do not need to recompile JSPs to run the NWSP application.

If you are a Web developer expecting to write new JSPs or change the NWSP JSPs, you must load the Java Development Kit (JDK). To obtain a recent JDK, go to:

<http://java.sun.com/products/j2se>

- The nonfatal JIT relocation error message is the result of a problem within the bundled JVM obtained from Sun Microsystems. It does not affect SESM operation. You can ignore this message and all supporting information.

## Searching for an Existing JDK or JRE

The installer does the following when searching for a valid JDK or JRE:

1. It searches for a JDK Version 1.2.2 that is already installed.
2. Failing that, it searches for a JRE Version 1.2.2 or later that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.2.2.

In some cases, even though a JRE is installed, the installer may not find it or finds a different JRE

On Windows NT, the installer looks in the NT Registry for the location of a JDK or JRE. It uses Java Version 1.2.2 in preference to Version 1.3.

On Solaris, the installer looks in the following well-known locations before installing the bundled JRE:

/usr/jre	/opt/jre	/usr/jre1.3	/opt/jre1.3
/usr/jre1.2.2	/opt/jre1.2.2	/usr/jre1.3.0	/opt/jre1.3.0
/usr/java1.2	/opt/java	/usr/java1.3	/opt/java
/usr/java	/opt/java1.2	/usr/java	/opt/java1.3
/usr/java1.2.2	/opt/java1.2.2	/usr/java1.3.0	/opt/java1.3.0
/usr/jdk	/opt/jdk	/usr/jdk	/opt/jdk
/usr/jdk1.2	/opt/jdk1.2	/usr/jdk1.3	/opt/jdk1.3
/usr/jdk1.2.2	/opt/jdk1.2.2	/usr/jdk1.3.0	/opt/jdk1.3.0

On Linux, the installer looks in the following well-known locations before installing the bundled JRE:

sun.java.1.2.2.jvm:	sun.java.1.3.x.jvm:	blackdownjdk122:
/usr/jre	/usr/jre1.3	/usr/jdk1.2.2
/usr/jre1.2.2	/usr/jre1.3.1	/usr/local/jdk1.2.2
/usr/java1.2	/usr/java1.3	/opt/jdk1.2.2
/usr/java	/usr/java	
/usr/java1.2.2	/usr/java1.3.1	blackdownjdk13.jvm:
/usr/jdk	/usr/jdk	/usr/j2sdk1.3
/usr/jdk1.2	/usr/jdk1.3	/usr/local/j2sdk1.3
/usr/jdk1.2.2	/usr/jdk1.3.1	/opt/j2sdk1.3
/opt/jre	/opt/jre1.3	
/opt/jre1.2.2	/opt/jre1.3.1	ibmjdk13.jvm:
/opt/java	/opt/java	/opt/IBMJava2-13/
/opt/java1.2	/opt/java1.3	/usr/IBMJava2-13/
/opt/java1.2.2	/opt/java1.3.1	/usr/local/IBMJava2-13/
/opt/jdk	/opt/jdk	/opt/jdk13
/opt/jdk1.2	/opt/jdk1.3	/usr/jdk13
/opt/jdk1.2.2	/opt/jdk1.3.1	/usr/local/jdk13

## Using a Pre-installed JRE or JDK

On either platform, you can specify the location of a pre-installed JRE or JDK by starting the installation process on a command line and specifying the `javahome` parameter, as follows:

```
installImageName -is:javahome location
```

Where:

*installImageName* is the name of the SESM downloaded image.

*location* is the path name for the JRE or JDK.

## Recompiling a Customized JSP

If you do not see changes that you make to a JSP, follow these procedures:

- 
- Step 1** Install a JDK (Version 1.2.2 or later).
  - Step 2** Edit the application start script so that it uses the JDK, rather than the JRE (for example, edit `jetty/bin/start.sh`).
  - Step 3** Ensure that `JDK_HOME` points to the directory into which you installed the JDK.
  - Step 4** Stop the SESM application.
  - Step 5** Change directories to the application's WEB-INF directory. For example, enter:

```
cd installDir/nwsp/docroot/WEB-INF
```

- Step 6** In the WEB-INF directory, back up the web.xml file by renaming it. For example, enter:
- ```
cp web.xml web.xml.bak
```
- Step 7** In the WEB-INF directory, copy the web.recompile.xml file over web.xml. For example, enter:
- ```
cp web.recompile.xml web.xml
```
- Step 8** Restart the SESM application.
- 

The installed web.xml file points to precompiled versions of the JSPs. It does *not* reference the JSPs in /nwsp/docroot. Thus, changing the JSPs in docroot has no effect if you use the installed web.xml file.

The web.recompile.xml file references the JSPs in /nwsp/docroot, rather than using the precompiled JSPs.

## Installation Troubleshooting

This section describes some potential problems that you might encounter during installation.

### No X Server for a Solaris Installation

To install SESM on a Solaris server with no X server, use the Silent or Console installation modes.

### Incorrect Permissions

The SESM installation program writes to parts of the file system or Windows registry that are only accessible to a privileged user (that is, root on Solaris, or a member of the Administrators group on Windows NT). An SESM installation must be performed by a privileged user who has access to these resources. Otherwise, the outcome of the installation is unpredictable.

### Files Not Found

If you receive Java error messages indicating missing files in system level directories (for example, /var, on Solaris), you do not have correct permissions to perform the installation. See the preceding [“Incorrect Permissions”](#) section.

### Incomplete Installation or Files Installed in Incorrect Directory

On a Solaris system, if you remove the contents of the SESM installation directory using the **rm** command instead of uninstalling SESM using the uninstall utility, then subsequent installations of SESM into the same directory might be adversely affected.

Uninstall SESM using uninstall.bin. If uninstalling is not possible, before reinstalling SESM, delete the vpd.properties file from the home directory of the person who is performing the installation.



#### Note

If you deploy multiple SESM installations, and you delete the vpd.properties file to recover from removing one of the installations, then you cannot use uninstall.bin to uninstall any of the other installations.

---

## Configuration File Location Troubleshooting

The SESM installation program places the J2EE web server and SESM configuration files in the correct directories as defined in the startup scripts. If the configuration files are moved for any reason, then you must edit the web.xml file to reflect the new locations.

## SESM Configuration Troubleshooting

If the SESM software is installed correctly, and all of the configuration files are in the proper location, but the SESM web application does not function, then examine the configuration values in the SESM application's MBean configuration file (for example, nwsp/config/nwsp.xml).

### Communication with SSG

If the SSG port number or shared secret specified in the SESM application's MBean configuration file does not match actual SSG configuration (as performed on the SSG host), the SSG cannot see the SESM requests or is unable to decrypt the requests because the shared secret does not match. When the shared secret does not match, the SSG returns an Access Reject message.

For more information on SSG configuration, see [Appendix B, "Configuring the SSG."](#)

### Communication with RADIUS Server

If incorrect IP addresses or port numbers are specified in the SESM application's MBean configuration file for the primary and secondary RADIUS servers, the RADIUS servers cannot see the SESM requests.

If the IP addresses and port numbers are correct, the RADIUS server returns an Access Reject when either of the following errors is present:

- The shared secret specified for the RADIUS server in the application's MBean configuration file is not correct.
- The SESM web application is not properly configured as a RADIUS client.

For more information on RADIUS configuration, see [Appendix D, "Configuring RADIUS."](#)

### Out of Memory Exceptions

Out of memory exceptions might indicate that there is not enough Java virtual memory reserved to handle the number of users currently logged on.

The generic startup script sets the Java virtual memory (VM) size to 64 MB. To change this value, stop the application, edit the generic start script (start.sh or start.cmd), and restart the application.

### Web Server Unavailable

Messages stating that the web server is unavailable might indicate that there is not enough Java virtual memory reserved to handle the number of users currently logged on. Follow the instructions in the ["Out of Memory Exceptions" section on page 10-11](#) to increase Java virtual memory.

## RADIUS Configuration Troubleshooting

The RADIUS server must be configured to recognize the following two clients:

- SESM web application
- SSG

If either of these configuration items is incorrect, then the RADIUS server sends Access Reject messages in response to all requests. See the [“Configuring RADIUS Clients”](#) section on page D-2 for information on configuring these RADIUS clients.

For service profile requests, the password for service and service group profiles must match those defined for the SSG and the SESM application. This password is used in Access Request messages for profiles, where the profile name is the service or service group name and the password is as defined in the following two locations:

- The servicePassword attribute in the AAA section of the SESM application’s MBean configuration file
- The service-password parameter for the SSG

## SSG Configuration Troubleshooting

The SSG must have a default network location defined, from which the SESM web application is accessible. Otherwise, client requests never reach the SESM application, and the client browser eventually times out.

The SSG must have the radius-helper parameters configured with the correct port numbers and shared secret so that the SSG can see SESM messages and decrypt them. Because the SSG carries out authentication against the RADIUS server, it must also have the correct values defined for the radius-server parameters.



## SESM Security

---

This appendix describes the security mechanisms used in a Subscriber Edge Services Manager (SESM) application.

The Cisco SESM:

- Is built using Java technology based on the J2EE specification. As such, it inherits the security features both of the Java language platform and the security framework in J2EE.
- Is a web server-based application, and so must be deployed in a web server that enforces HTTP security.
- Plays a role in authentication for the user, so it must also enforce constraints at this level.

## Java Platform Security Description

The following URLs provide a description of Java platform security:

- <http://java.sun.com/security/index.html>
- For specific Java platforms:
  - <http://java.sun.com/products/jdk/1.2/docs/guide/security/>
  - <http://java.sun.com/products/jdk/1.3/docs/guide/security/>
- For training:
  - <http://developer.java.sun.com/developer/onlineTraining/Security/Fundamentals/index.html>
- For miscellaneous articles:
  - <http://developer.java.sun.com/developer/technicalArticles/Security/>

## HTTP Security Description

HTTP security involves two separate issues:

- Encryption of communications using HTTPS
- Basic and digest access authentication in HTTP1.1 (RFC 2617)

## HTTPS Description

HTTPS (Secure Hypertext Transfer Protocol) is HTTP over Secure Sockets Layer (SSL), which are HTTP packets sent as encrypted data. This is the mechanism by which data is securely transmitted over the Internet between a browser client and a server.

SESM implements SSL using the Java Secure Sockets Extension (JSSE). For information about JSSE, go to:

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

The J2EE specifications describe an extension framework for the integration of SSL implementations. For implementations other than JSSE, go to:

[http://www.phaos.com/e\\_security/prod\\_ssl.html](http://www.phaos.com/e_security/prod_ssl.html)

## Keytool and Keystore

The SSL part of HTTPS requires a certificate to generate the encryption key. For the Jetty web server bundled with the Cisco SESM, the certificate is named keystore and is found in the /etc directory. The keystore file is created by the keytool utility. For detailed instructions on the use of keytool, go to the following URL:

<http://java.sun.com/products/jdk/1.2/docs/guide/security/SecurityToolsSummary.html>

The sample keystore functions for nonproduction deployments. However, you must obtain a site-specific certificate for production deployments from VeriSign, Inc. at:

<http://www.verisign.com>

Though certificates are generally the same in concept, they tend to differ in implementation. Therefore, a degree of certificate manipulation is required to obtain a certificate from a given source to work with a given SSL implementation. For JSSE and the Jetty web server, the required steps are described at:

<ftp://jetty.mortbay.com/pub/Jetty-dev/webapps/jetty/JsseSSL.html>

For other implementations, go to:

<http://www.openssl.org>

The keystore file is a certificate used for secure sockets layer (SSL) encryption. The SSL implementation shipped with the Cisco SESM is of commercial quality and can use certificates generated by keytool. Keytool resides in the same directory as the JRE.

**Caution**

---

A keystore is required for deployments that use HTTPS. HTTPS does not function without a valid keystore file. The file included with the installation works, but you should replace it with a keystore valid for your specific deployment.

---





## Configuring the SSG

---

This appendix shows some basic steps for configuring the Cisco Service Selection Gateway (SSG) to work with a Subscriber Edge Services Manager (SESM) web application.

### Basic SSG Configuration

This section shows basic procedures for enabling an SSG and configuring it to communicate with a RADIUS server. When following these procedures, replace the sample IP addresses, port numbers, and passwords with values that are appropriate for your configuration.

- 
- Step 1** Log on to the SSG device.
- Step 2** To access enabled mode, enter:
- ```
en
```
- Step 3** To change the configuration, enter:
- ```
conf t
```
- Step 4** To enable the SSG, enter:
- ```
ssg enable
```
- Step 5** To remove a line, enter:
- ```
no radius-server host 10.3.3.2 auth-port 1647 acctport 1648 0 key cisco
```
- Step 6** To add an entry, enter:
- ```
radius-server host 10.3.3.2 auth-port 1812 acctport 1813 0 key cisco
```
- Step 7** To end editing, enter:
- ```
Ctrl-Z
```
- Step 8** To rebuild the configuration, enter:
- ```
wr t
```
- Step 9** To examine the current configuration, enter:
- ```
show run
```

**Step 10** The relevant configuration entries are as follows:

- a. To identify the network that the SESM web application is running on, enter:

```
ssg default-network 10.3.3.0 255.255.255.0
```

- b. To specify the password to query RADIUS for service profiles, enter:

```
ssg service-password servicecisco
```

- c. To configure the RADIUS protocol communication used between SSG and the SESM web application, specify the port on which the SSG is listening as follows:

```
ssg radius-helper auth-port 1812
```

- d. To specify the shared secret for password encryption between SSG and the SESM web application, enter:

```
ssg radius-helper key cisco
```

- e. To specify the maximum number of concurrent services for a user, enter:

```
ssg maxservice 21
```

- f. To configure communication between SSG and the RADIUS server, specify the authentication port, the accounting port, and the secret as follows:

```
radius-server host 10.3.3.2 auth-port 1812 acct-port 1813 key cisco
```

- g. To specify the number of RADIUS retries for authentication, enter:

```
radius-server retransmit 3
```

- h. To specify the shared secret for password encryption to the RADIUS server, enter:

```
radius-server key cisco
```

## Configuring the Host Key Port Bundle Feature on SSG

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



### Note

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

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 above, because these IP addresses must be recognized as corresponding to a local interface or loopback.

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

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

## Sample SSG Configuration

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

```
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 profile-cache
ssg default-network 192.168.254.16 255.255.255.248
ssg service-password pw
ssg radius-helper auth-port 1812 acct-port 1813
ssg radius-helper key cisco
ssg accounting interval 999999
```

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

```
ssg port-map enable
ssg port-map destination range 8080 to 8080
ssg port-map destination range 8443 to 8443
ssg port-map source ip Loopback0
!
!
ssg bind service passthrough1 FastEthernet4/0
ssg bind service proxy1 FastEthernet4/0
ssg bind service tunnel1 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 1645 acct-port 1646 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#

```



## DTD for MBean Configuration Files

---

This appendix shows the full text of the DTD for the MBean configuration files used by ConfigAgent. This DTD name is `xmlconfig.dtd`.

### `xmlconfig.dtd`

```
<!-- Copyright (c) 2001 by Cisco Systems, Inc. All rights reserved.
This is the document type descriptor for the com.cisco.aggbu.jmx.XmlConfig
class, which was copied with permission from the
com.mortbay.Util.XmlConfiguration class. It allows a MBean object to be
configured by with a sequence of Set, Put and Call elements.
```

The XML file contains a single `<XmlConfig>` element containing one or more `<Configure>` elements describing the configuration for a single object or class of object.

Each object or class to be configured is defined in a `<Configure>` element section. A `Configure` element must have either a `class` or a `jmxname` attribute defined. MBeans to be configured are matched by both `class` and `jmxname`, so that two sets of configuration may be applied to an object. If a `Configure` element has an `init` element and a `class` attribute, then an MBean instance of that class is initialized and registered by the `#newInstances(MBeanServer)` method. If a `jmxname` attribute is also provided, that is used for registration with the MBean server.

`Configure` elements may contain `Set`, `Put` and `Call` elements which are used in order by the `#configure(MBeanServer, ObjectInstance)` method. Examples of these tags and their java equivalents are:

```
<Set name="Test">value</Set>           ~ obj.setTest("value");
<Put name="Test">value</Put>           ~ obj.put("Test","value");
<Call name="test"><Arg>value</Arg></Call> ~ obj.test("value");
<Call name="test">
  <Arg>value</Arg>
  <Call name="other"/>
</Call>                                ~ obj.test("value").other();
```

Values may be literals or objects that are created with the `New` element or returned from a `Call` element:

```
<Set name="Test1">
  <New class="com.acme.MyClass"/>
</Set>

<Set name="Test2">
```

```

    <New class="com.acme.MyClass"/>
      <Arg type="int">42</Arg>
      <Set name="something"/>
    </New>
  </Set>

```

Note that Call and New elements may contain Set, Put and Call elements after any Arg elements. These nested elements are applied to the created or returned object.

Untyped values are matched to arguments on a best effort approach. Primitive types may be specified as element attributes and the value is treated as a String and converted to that type.

```
-->
```

```

<!ENTITY % CONFIG "Set|Put|Call">
<!ENTITY % TYPE "String|char|short|byte|int|long|boolean|float|double|URL">
<!ENTITY % VALUE "#PCDATA|Call|New|SystemProperty|Array">

```

```

<!ENTITY % IDATTR "id ID #IMPLIED" >
<!ENTITY % TYPEATTR "type (%TYPE;) #IMPLIED " >
<!ENTITY % ORDERATTR "order NMTOKEN #REQUIRED" >
<!ENTITY % CLASSATTR "class NMTOKEN #IMPLIED" >
<!ENTITY % NAMEATTR "name NMTOKEN #REQUIRED" >
<!ENTITY % JMXNAMEATTR "jmxname CDATA #IMPLIED" >

```

```
<!--
```

XmlConfig Element.

This is the root element of the configuration file:

```
<XmlConfig> <Configure>...</Configure> ... </XmlConfig>
```

An XmlConfig element can contain Configure elements.

```
-->
```

```

<!ELEMENT XmlConfig ((Instantiate|Configure)*) >
<!ATTLIST XmlConfig %IDATTR; %CLASSATTR;>

```

```
<!--
```

Configure Element.

This is the root element that specifies the class of object that can be configured:

```
<Configure name="domain:n=v"> ... </Configure>
```

A Configure element can contain an optional Init element followed by any number of Set, Put or Call elements.

```
-->
```

```

<!ELEMENT Configure (%CONFIG;)* >
<!ATTLIST Configure %IDATTR; %JMXNAMEATTR; %CLASSATTR;>

```

```
<!--
```

Instantiate Element.

This element specifies a set of arguments to an object constructor and an order attribute specifying when the object is to be constructed wrt all of the other objects scheduled to be created by the ConfigAgent:

```
<Instantiate order="20"> ... </Init>
```

```
-->
```

```

<!ELEMENT Instantiate (Arg*,(%CONFIG;)*>
<!ATTLIST Instantiate %IDATTR; %ORDERATTR; %JMXNAMEATTR; class NMTOKEN #REQUIRED>

```



```

<!--
Set Element.
This element maps to a call to a set method on the current object.
The name and optional type attributes are used to select the set
method.
A Set element can contain value text and/or the value elements Call,
New and SystemProperty. If no value type is specified, then white
space is trimmed out of the value. If it contains multiple value
elements they are added as strings before being converted to any
specified type.
-->
<!ELEMENT Set ( %VALUE; )* >
<!ATTLIST Set %IDATTR; %NAMEATTR; %TYPEATTR; >

<!--
Put Element.
This element maps to a call to a put method on the current object,
which must implement the Map interface. The name attribute is used
as the put key and the optional type attribute can force the type
of the value.

A Put element can contain value text and/or the value elements Call,
New and SystemProperty. If no value type is specified, then white
space is trimmed out of the value. If it contains multiple value
elements they are added as strings before being converted to any
specified type.
-->
<!ELEMENT Put ( %VALUE; )* >
<!ATTLIST Put %IDATTR; %NAMEATTR; %TYPEATTR;>

<!--
Call Element.
This element maps to an arbitrary call to amethod on the current object,
The name attribute and Arg elements are used to select the method.

A Call element can contain a sequence of Arg elements followed by
a sequence of Set, Put and/or Call elements which act on any object
returned by the original call:

  <Call name="test"><Arg>value1</Arg><Set name="Test">Value2</Set></Call>

This is equivalent to:

  Object o2 = o1.test("value1");
  o2.setTest("value2");
-->
<!ELEMENT Call (Arg*, (%CONFIG;)* ) >
<!ATTLIST Call %IDATTR; %NAMEATTR;>

<!--
Arg Element.
This element defines a positional argument for the Call element.
The optional type attribute can force the type of the value.

An Arg element can contain value text and/or the value elements Call,
New and SystemProperty. If no value type is specified, then white
space is trimmed out of the value. If it contains multiple value
elements they are added as strings before being converted to any
specified type.
-->

```

```
<!ELEMENT Arg ( %VALUE; )* >
<!ATTLIST Arg %IDATTR; %TYPEATTR; >
```

```
<!--
New Element.
This element allows the creation of a new object as part of a
value of a Set, Put or Arg element. The class attribute determines
the type of the new object and the contained Arg elements
are used to select the constructor for the new object.
```

A New element can contain a sequence of Arg elements followed by a sequence of Set, Put and/or Call elements which act on the new object:

```
<New class="com.acme.MyClass">
  <Arg>value1</Arg><Set name="Test">Value2</Set>
</New>
```

This is equivalent to:

```
Object o = new com.acme.MyClass("value1");
o.setTest("value2");
```

```
-->
<!ELEMENT New (Arg*, (%CONFIG;)*)>
<!ATTLIST New %IDATTR; %CLASSATTR; >
```

```
<!--
System Property Element.
This element allows JVM System properties to be retrieved as
part of the value of a Set, Put or Arg element.
The name attribute specifies the property name and the optional
default argument provides a default value.
```

```
<SystemProperty name="Test" default="value"/>
```

This is equivalent to:

```
System.getProperty("Test", "value");
```

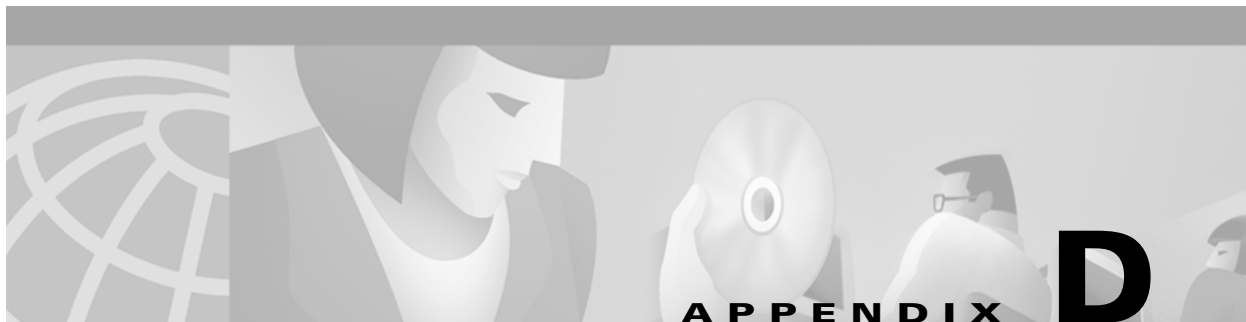
```
-->
<!ELEMENT SystemProperty EMPTY>
<!ATTLIST SystemProperty %IDATTR; %NAMEATTR; default CDATA #IMPLIED>
```

```
<!--
Array element
Can have a class attribute to specify the base type of each object
in the array.
```

```
-->
<!ELEMENT Array (Item)* >
<!ATTLIST Array %IDATTR; %CLASSATTR;>
```

```
<!--
Item element
Only occurs inside Arrays and is identical to Arg in every way except its name
```

```
-->
<!ELEMENT Item ( %VALUE; )* >
<!ATTLIST Item %IDATTR; %TYPEATTR; >
```



## Configuring RADIUS

---

This appendix describes the configuration steps required to include a RADIUS server in a Cisco Subscriber Edge Services Manager (SESM) deployment. This appendix includes the following topics:

- [Configuring SSG to Communicate with the RADIUS Server, page D-1](#)
- [Configuring RADIUS Clients, page D-2](#)
- [Adding Cisco SSG Vendor-Specific Attributes to the Attribute Dictionary, page D-3](#)
- [Configuring Service Profiles, page D-3](#)
- [Configuring Service Group Profiles, page D-7](#)
- [Configuring Subscriber Profiles, page D-8](#)
- [Configuring Next Hop Gateway Profiles, page D-11](#)
- [Configuring the RADIUS Accounting Feature, page D-11](#)
- [Configuring Cisco Access Registrar for SESM Deployments, page D-12](#)

### Configuring SSG to Communicate with the RADIUS Server

You must configure SSG to communicate with the RADIUS server. To do so, use the **radius-server host** Cisco IOS command on the SSG host. Different ports are used for handling authentication and accounting packets. For example:

```
radius-server host 10.3.3.2 auth-port 1812 acct-port 1813 key cisco
```

To use different RADIUS servers for authentication and accounting, use two commands as follows:

```
radius-server host 10.3.3.2 auth-port 1812 acct-port 0 key cisco  
radius-server host 10.3.3.3 auth-port 0 acct-port 1813 key cisco
```

# Configuring RADIUS Clients

The RADIUS protocol is based on a client server model. The RADIUS server is the server. Multiple dial-in Network Access Server (NAS) devices are the clients. Before communication can occur, each client must be configured on the server.

An SESM deployment requires that you configure the following NAS clients on the RADIUS server:

- The SSG host—This is the Cisco device on which SSG is running, such as the Cisco 7200, Cisco 7400, or a node route processor (NRP) on the Cisco 56. The RADIUS server must recognize each SSG host as a client.
- The SESM web portal—This is the NWSP application, or your customized SESM web application. SESM web portals query the RADIUS server directly for service information. The RADIUS server must recognize the SESM web portal as a client.

[Table D-1](#) summarizes the information that might be required to define a NAS client on the RADIUS server. See your RADIUS server vendor documentation for more specific requirements, syntax, and procedures.

**Table D-1** NAS Client Configuration

Property	Description
Name or IP Address	Identifies the client. Use either IP address or host name.
Shared Secret	Must match a shared secret value configured on the client. If the shared secrets do not match, the RADIUS server issues an access-reject message.  A shared secret is a value that is configured on both the client and the server. It is never sent over the network. The shared secret is used for MD5 encryption of the profile password.
Type	For SSG—Cisco:NAS  For SESM—RAD_RFC+ACCT_RFC

The following sample entries show a Merit RADIUS format defining SESM web portals and an SSG host as RADIUS clients. The examples use the value `cisco` as the shared secret on all of the clients.

```
#Entries for SESM-Server clients
10.3.3.2      cisco      type=RAD_RFC+ACCT_RFC
10.3.3.101   cisco      type=RAD_RFC+ACCT_RFC
10.3.3.102   cisco      type=RAD_RFC+ACCT_RFC

#Entries for SSG host
192.168.1.6  cisco      type=Cisco:NAS
```

# Adding Cisco SSG Vendor-Specific Attributes to the Attribute Dictionary

An attribute dictionary defines attributes to the RADIUS server. The attribute dictionary contains:

- Standard RADIUS attributes as defined by RFC 2138.
- Vendor-specific attributes (VSAs) that extend the standard attributes. VSAs add new capabilities, supported by specific vendors, to the RADIUS server. The value of a VSA can be one or more subattributes whose meanings depend on the vendor's definition.

An SESM deployment requires that you add Cisco VSAs to your RADIUS attribute dictionary. See your RADIUS server vendor's documentation for instructions and syntax. The Cisco Access Registrar ships with all of the Cisco SESM VSAs preconfigured.

[Table D-2](#) shows the Cisco VSAs required in an SESM deployment that uses a RADIUS server, which includes:

- SESM running in RADIUS mode. In this deployment, the RADIUS server supports authorization, authentication, and accounting features.
- SESM running in LDAP mode and using SSG accounting features. In this deployment, the RADIUS server supports accounting features.
- SESM running in LDAP mode and using the RDP server in proxy mode. In this deployment, the RADIUS server supports authentication features.

**Table D-2 Cisco SSG VSAs**

RADIUS Attribute	Vendor ID	Subattribute	Name	Type
26	9	1	Cisco-Avpair	String
26	9	250	Account-Info	String
26	9	251	Service-Info	String
26	9	253	Control-Info	String

## Configuring Service Profiles

Service profiles define the services that subscribers can select from an SESM web portal.

In an SESM deployment, you must configure a service profile for each service that will be accessible through the SESM web portal.

[Table D-3](#) briefly describes the attributes in a RADIUS service profile. Use the following references for more information.

- If you are using the Cisco Access Registrar, see the [“Configuring Cisco Access Registrar for SESM Deployments” section on page D-12](#) for service profile examples and syntax. Otherwise, see your RADIUS server vendor documentation for the syntax of a service profile
- For sample SESM service profiles, see the demo.txt file located in the NWSP config directory (for example, nwsp/config/demo.txt). This file is installed whether or not you choose the demo option. It shows service and subscriber profiles in Merit RADIUS format.

- The SSG documentation describes service profile attributes and provides examples of their use. See the “[Related Documentation](#)” section on page xv for a link to online SSG documentation.

**Table D-3 Attributes in Service Profiles**

Attribute	Description
Service profile name	An identifying name for a service profile. Each profile name must be unique. Service profile names are used in the subscriber profiles to indicate that a subscriber is subscribed to the service.
Password	Must match the service password that was configured on the SSG host and in SESM. On the SSG host, configure a service password using the following Cisco IOS command: <pre>ssg service password password</pre> In SESM, configure the service password in the following line from the AAA MBean in the nwsp.xml file: <pre>&lt;Set name="servicePassword"&gt;servicecisco&lt;/Set&gt;</pre>
Service-Type	Standard RADIUS attribute number 6. The value must be “outbound.”
Session-Timeout	Standard RADIUS attribute number 27. Specifies the maximum length of time, in seconds, that this service (the service object on SSG) can remain active in a session at any one time. When the time expires, SSG deletes the service object, which disconnects the subscriber from the service. If the host key feature is enabled on the SSG, the SSG signals the state change to the SESM web portal. <b>Note</b> The NWSP application does not relay this state change to the subscriber. If Session-Timeout is not set, there is no limit on how long the subscriber can use the service. In a dial-up networking or bridged (non-PPP) network environment, a subscriber can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, which can be a problem if the IP address is obtained by another user. You can use the Session-Timeout and the Idle-Timeout attributes to prevent this problem.
Idle-Timeout	Standard RADIUS attribute number 28. Specifies the maximum length of time, in seconds, that a service connection can remain idle before it is disconnected. See the explanation of the Session-Timeout attribute, above, for more information about setting this attribute.

Table D-3 Attributes in Service Profiles (continued)

Attribute	Description
Service-Info	<p>A vendor-specific attribute (attribute number 26), vendor 9, subattribute 251. Valid values for Service-Info attributes are:</p> <ul style="list-style-type: none"> <li>• <b>AauthenType</b>—Specifies whether SSG uses the CHAP or PAP protocol to authenticate users for proxy services.</li> <li>• <b>Idescription</b>—Service description. Optional. Describes the service.</li> <li>• <b>Ttype</b>—Type of service. Optional. Valid values for <i>type</i> are: <ul style="list-style-type: none"> <li>– P—Passthrough. This is the default.</li> <li>– T—Tunnel</li> <li>– X—Proxy. Indicates that the SSG performs proxy service.</li> </ul> </li> <li>• <b>Mmode</b>—Service mode. Optional. Valid values for <i>mode</i> are: <ul style="list-style-type: none"> <li>– S—Sequential mode. Prevents the subscriber from accessing any other services while connected to this service.</li> <li>– C—Concurrent mode. This is the default. Allows the subscriber to simultaneously log onto this service while connected to other services.</li> </ul> </li> <li>• <b>Rip_address;mask</b>—Service route (destination). Required. Specifies the network or the host where the service resides. Multiple instances of this attribute can exist within a single service profile, to specify multiple service destinations. An Internet service is typically specified as "R0.0.0.0;0.0.0.0".</li> <li>• <b>Dip_address_1;ip_address_2</b>—DNS Server Address. Optional. Specifies the IP addresses for the primary and secondary DNS servers to use for the domains that are defined using the O option.</li> <li>• <b>Oname1[name2]...[nameX]</b>—Domain names. Optional.</li> <li>• <b>SRadiusServerAddress;authPort;acctPort;secret</b>—Remote server information. Required when type of service (T) is Proxy (X); not applicable for other service types. Specifies the remote RADIUS server that will perform authentication, authorization, and accounting for this service.</li> <li>• <b>Gkey</b>—Service next hop gateway. Specifies the next hop key for this service. Each SSG uses its own next hop gateway table that associates this key with a valid IP address. See the <a href="#">“Configuring Next Hop Gateway Profiles”</a> section on page D-11 for information about creating a next hop gateway table.</li> <li>• <b>Uurl</b> or <b>Hurl</b>—These attributes specify the URL that is displayed in the HTTP address field when the service opens. If the SESM web portal is designed to use HTML frames, then these options also specify whether the service is displayed in a new browser window or in a frame in the current (SESM) window, as follows: <ul style="list-style-type: none"> <li>– <b>Uurl</b>—URL for a service displayed in its own browser window.</li> <li>– <b>Hurl</b>—URL for a service displayed in a frame in the SESM portal window.</li> </ul> </li> </ul> <p><b>Note</b> In a frameless application, both U and H cause a new browser window to open for the service. The NWSP application is a frameless application.</p> <ul style="list-style-type: none"> <li>• <b>Bsize</b>—The PPP maximum transmission unit (MTU) for SSG as a LAC. By default, the PPP MTU size is 1500 bytes.</li> </ul>

Table D-3 Attributes in Service Profiles (continued)

Attribute	Description
Service-Info (continued)	<ul style="list-style-type: none"> <li>• <b>X</b>—Indicates that the RADIUS authentication and accounting requests use the full user name (for example, user@service).</li> <li>• <b>Vstring</b>—Service-defined cookie. Optional. Specifies any information that you wish to include in RADIUS authentication and accounting requests. SSG does not parse or interpret <i>string</i>. You must configure the proxy RADIUS server to interpret this attribute. SSG supports only one service-defined cookie per service profile. Use this attribute to add fields to accounting records.</li> </ul>
Cisco-AVpair	<p>A vendor-specific attribute (attribute number 26), vendor 9, subattribute 1. Valid values for the Cisco-AVpair attribute in a service profile are:</p> <ul style="list-style-type: none"> <li>• <b>“ip:inacl[#number]={standardACL   extendedACL}”</b>—Upstream access control list (ACL). Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to upstream traffic coming from the subscriber.</li> <li>• <b>“ip:outacl[#number]={standardACL   extendedACL}”</b>—Downstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to downstream traffic going to the subscriber. <ul style="list-style-type: none"> <li>– <i>number</i>—Identifies the access list. If a profile includes multiple <i>inacl</i> or <i>outacl</i> attributes, the attributes are downloaded and executed according to the order implied by <i>number</i>.</li> <li>– <i>standardACL</i>—A Cisco IOS standard ACL.</li> <li>– <i>extendedACL</i>—A Cisco IOS extended ACL.</li> </ul> </li> </ul> <p><b>Note</b> A profile can include multiple instances of <i>inacl</i> attributes and multiple instances of <i>outacl</i> attributes. Use one attribute for each ACL statement. Multiple attributes can be used for the same ACL.</p> <ul style="list-style-type: none"> <li>• <b>“vpdn:ip-addresses=address1[&lt;delimiter&gt;address2][&lt;delimiter&gt;address3]...”</b>—Virtual private dial-up network (VPDN) IP address. Specifies the IP addresses of the home gateways (LNSs) to receive the L2TP connections. <ul style="list-style-type: none"> <li>– <i>address</i>—IP address of the home gateway.</li> <li>– <i>&lt;delimiter&gt;</i>—A comma (,) or a space ( ) indicates that the SSG selects load sharing among IP addresses. A slash (/) indicates that the SSG considers IP addresses on the left side of the slash a higher priority than those on the right side of the slash.</li> </ul> </li> <li>• <b>“vpdn:tunnel-id=name”</b>—VPDN tunnel ID. Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.</li> <li>• <b>“vpdn:tunnel-password=secret”</b>—L2TP tunnel password. Specifies the secret (password) used for L2TP tunnel authentication.</li> <li>• <b>“vpdn:12tp-hello-interval=interval”</b>—L2TP hello interval. Specifies the number of seconds for the hello keepalive interval.</li> </ul>



## Example Service Profiles

The service configuration examples in this section use a Merit RADIUS format.

### Example Service Profile for Passthrough Service

```
internet Password = "servicecisco", Service-Type = Outbound
  Service-Info = "IInternet",
  Service-Info = "R153.153.153.0;255.255.255.0",
  Service-Info = "MC",
  Service-Info = "TP"
```

### Example Service Profile for Proxy Service

```
corporate Password = "servicecisco", Service-Type = Outbound
  Service-Info = "ICorporate Intranet (proxy)",
  Service-Info = "R154.154.154.0;255.255.255.0",
  Service-Info = "S10.3.3.101;1812;1813;cisco",
  Service-Info = "MC",
  Service-Info = "TX"
```

### Example Service Profile Using Timeout Values

```
iptv Password = "servicecisco", Service-Type = Outbound
  Service-Info = "IIP/TV",
  Service-Info = "R160.160.160.0;255.255.255.0",
  Service-Info = "MC",
  Service-Info = "TP"
  Idle-Timeout = 60,
  Session-Timeout = 60
```

## Configuring Service Group Profiles

Service group profiles contain a list of services. [Table D-4](#) briefly describes the attributes in a RADIUS subscriber profile.

**Table D-4** Attributes in Service Group Profiles

Attribute	Description
Password	
Service-Type	Standard RADIUS attribute number 6. The level of service. Must be outbound.
Account-Info	<p>A vendor-specific attribute (attribute number 26), vendor 9, subattribute 250. Valid values for Account-Info attributes are:</p> <ul style="list-style-type: none"> <li>• <b>“Idescription”</b>—Describes the service group. If this field is omitted, the service group profile name is used.</li> <li>• <b>“GName”</b>—Service group name.</li> <li>• <b>“Nname”</b>—Lists the services that belong to the group.</li> <li>• <b>“TE”</b>—Indicates that this is a mutually exclusive service group.</li> </ul>

## Example Service Group Profiles

The service group configuration examples in this section use a Merit RADIUS format.

### Example Service Group Profile

```
SvcGroup1 Password = "servicecisco", Service-Type = Outbound
  Account-Info = "Nvidconf",
  Account-Info = "Ndistlearn",
  Account-Info = "Ncorporate",
  Account-Info = "Nbanking"
```

### Example Service Group Profile for a Mutex Group

```
MutexGrp1 Password = "groupcisco", Service-Type = Outbound
  Account-Info = "IBandwidth-QoS",
  Account-Info = "Nbw-gold",
  Account-Info = "Nbw-silver",
  Account-Info = "Nbw-bronze",
  Account-Info = "TE"
```

## Configuring Subscriber Profiles

Subscriber profiles define SESM logon names and passwords, access control lists associated with each logon, and subscribed services for each logon.

In an SESM RADIUS mode deployment, you must define a subscriber profile for each subscriber that will sign onto an SESM portal from a web browser.

[Table D-5](#) briefly describes the attributes in a RADIUS subscriber profile. Use the following references for more information:

- If you are using the Cisco Access Registrar, see the [“Configuring Cisco Access Registrar for SESM Deployments” section on page D-12](#) for subscriber profile examples and syntax. Otherwise, see your RADIUS server vendor documentation for the syntax of a subscriber profile
- For sample SESM subscriber profiles, see the demo.txt file located in the NWSP config directory (for example, nwsp/config/demo.txt). This file is installed whether or not you choose the demo option. It shows service and subscriber profiles in Merit RADIUS format.
- The SSG documentation describes subscriber profile attributes and provides examples of their use. See the [“Related Documentation” section on page xv](#) for a link to online SSG documentation.

Table D-5 Attributes in Subscriber Profiles

Attribute	Description
User-Name	Standard RADIUS attribute number 1. The subscriber name used for authentication.
User-Password	Standard RADIUS attribute number 2. The subscriber password used for authentication.
Called-Station_Id	Standard RADIUS attribute number 30. The access point name (APN), which can optionally be used for authentication.
Calling-Station_Id	Standard RADIUS attribute number 31. The MSISDN, which can optionally be used for authentication.
NAS-Identifier	Standard RADIUS attribute number 32. The NAS identifier, which can optionally be used for authentication.
Session-Timeout	<p>Standard RADIUS attribute number 27. Specifies the maximum length of time, in seconds, that this subscriber session (the host object on SSG) can remain active at any one time. When the time expires, SSG deletes the host object, which ends the session. If the host key feature is enabled on the SSG, the SSG signals the state change to the SESM web portal.</p> <p><b>Note</b> The NWSP application does not relay this state change to the subscriber.</p> <p>If Session-Timeout is not set, there is no limit on how long the session lasts.</p> <p>In a dial-up networking or bridged (non-PPP) network environment, a subscriber can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, which can be a problem if the IP address is obtained by another user. You can use the Session-Timeout and the Idle-Timeout attributes to prevent this problem.</p>
Idle-Timeout	Standard RADIUS attribute number 28. Specifies the maximum length of time, in seconds, that a subscriber session can remain idle before it is disconnected. See the explanation of the Session-Timeout attribute, above, for more information about setting this attribute.
Account-Info	<p><b>Note</b> In SSG Release 12.2.4(B) or later, if a point-to-point protocol (PPP) subscriber profile does not include any VSAs, the SSG does not create a host object for the subscriber and therefore, the SSG does not apply any control over the subscriber's access. The fact that the PPP link is established and the SSG is not applying any control means that the subscriber has unrestricted access to any downstream connections defined in the subscriber's profile or by the Cisco IOS configuration on the SSG host device. If it is important to avoid this situation, make sure that all PPP clients are subscribed to at least one service or define any other Cisco SSG VSA in the profile, such as a <b>U</b>rl or <b>H</b>url attribute.</p> <p>A vendor-specific attribute (attribute number 26), vendor 9, subattribute 250. Valid values for Account-Info attributes are:</p> <ul style="list-style-type: none"> <li>• “<b>N</b>serviceName”—Service name. Subscribes the subscriber to the specified service and includes the service in the service list obtained by the SESM web portal. The <i>serviceProfileName</i> must be defined in a service profile. There can be multiple instances of this attribute within a subscriber profile.</li> <li>• “<b>G</b>serviceGroupProfileName”—Service group. Creates a folder for the service group on the subscriber's SESM web portal. The <i>serviceGroupProfileName</i> must be defined in a service group profile. There can be multiple instances of this attribute within a subscriber profile.</li> </ul>

Table D-5 Attributes in Subscriber Profiles (continued)

Attribute	Description
Account-Info (continued)	<ul style="list-style-type: none"> <li>• <b>“AautoConnectServiceName”</b>—Automatic connection. Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon.</li> </ul> <p><b>Note</b> The service list displayed by SESM does not include A entries. It only shows N entries. To display an auto connect service on the SESM service list, include both an A and an N entry for the service in the profile. See the <a href="#">“Example Subscriber Profile for Auto Services”</a> section on page D-11 for an example.</p> <ul style="list-style-type: none"> <li>• <b>“Uurl or Hurl”</b>—These attributes specify the URL for the user’s preferred Internet home page. If the SESM web portal is designed to use HTML frames, then these options also specify whether the home page is displayed in a new browser window or in a frame in the current (SESM) window, as follows: <ul style="list-style-type: none"> <li>– <b>Uurl</b>—URL for the home page displayed in its own browser window.</li> <li>– <b>Hurl</b>—URL for the home page displayed in a frame in the SESM browser window.</li> </ul> </li> </ul> <p><b>Note</b> In a frameless application, both U and H cause a new browser window to open for the home page. The NWSP application is a frameless application.</p> <ul style="list-style-type: none"> <li>• <b>“RIgroup;duration[;service]”</b>—Overrides the TCP redirect configuration on the SSG for initial logon redirections. The <i>group</i> is the captive portal group to use for initial logon redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The <i>duration</i> is the duration of the captivation (in seconds). If you specify the optional <i>service</i> field, initial logon redirection occurs only when the subscriber requests connection to the named service.</li> <li>• <b>“RAgroup;duration;frequency[;service]”</b>—Overrides the TCP redirect configuration on the SSG for advertisement redirections. The <i>group</i> is the captive portal group to use for advertisement redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The <i>duration</i> is the duration of the captivation (in seconds). The frequency is the approximate interval between redirections (in seconds). If you specify the optional <i>service</i> field, redirection occurs only when the subscriber requests connection to the named service.</li> </ul> <hr/> <ul style="list-style-type: none"> <li>• <b>“RS”</b>—The subscriber has SMTP forwarding capability.</li> </ul>
Cisco-AVpair	<p>A vendor-specific attribute (attribute number 26), vendor 9, subattribute 1. Valid values for the Cisco-AVpair attribute in a subscriber profile are:</p> <ul style="list-style-type: none"> <li>• <b>“ip:inacl[#number]={standardACL   extendedACL}”</b>—Upstream access control list (ACL). Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to upstream traffic coming from the subscriber.</li> <li>• <b>“ip:outacl[#number]={standardACL   extendedACL}”</b>—Downstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to downstream traffic going to the subscriber. <ul style="list-style-type: none"> <li>– <i>number</i>—Identifies the access list. If a profile includes multiple inacl or outacl attributes, the attributes are downloaded and executed according to the order implied by <i>number</i>.</li> <li>– <i>standardACL</i>—A Cisco IOS standard ACL.</li> <li>– <i>extendedACL</i>—A Cisco IOS extended ACL.</li> </ul> </li> </ul> <p><b>Note</b> A profile can include multiple instances of inacl attributes and multiple instances of outacl attributes. Use one attribute for each ACL statement. Multiple attributes can be used for the same ACL.</p>

## Example Subscriber Profiles

The subscriber profile example in this section is in a Merit RADIUS format.

### Example Subscriber Profile for Auto Services

```
user1 Password = "cisco"
  Service-Type = Framed-User,
  Account-Info = "Ainternet",      (hidden on the subscriber's web page)
  Account-Info = "Ninternet"      (makes it visible)
```



#### Note

The first Account-Info line specifies automatic connection to the service. If you do not include the second line, the auto connection service does not appear on the SESM web portal. To display the service on the SESM web portal, you must include both entries as shown in the example.

## Configuring Next Hop Gateway Profiles

Next Hop Gateway profiles associate next hop gateway keys with IP addresses. Because multiple SSGs might access services from different networks, service profiles can specify next hop keys. (See the service-info G attribute in [Table D-3 on page D-4.](#)) If this is the case, you must configure a next hop gateway pseudo-service profile to resolve the keys to valid IP addresses.

An example next hop gateway pseudo-service profile follows:

```
ssg-next-hop Password = "xssg-key"
  Control-Info = "Gl2tp-net7;192.168.1.101",
  Control-Info = "Gl2tp-net40;192.168.1.102",
  Control-Info = "Gweb-key;192.168.1.101",
  Control-Info = "Gproxy-radius-key;192.168.1.101",
  Control-Info = "Gxint-24;192.168.1.101"
```

## Configuring the RADIUS Accounting Feature

If you configure a RADIUS accounting port, SSG generates accounting records and forwards them to the RADIUS server. To configure a RADIUS server for accounting only, you must perform the following configuration steps.

- Configure the NAS clients as described in the [“Configuring RADIUS Clients”](#) section on page D-2.
- Add the Cisco VSAs to the RADIUS server attribute dictionary, as described in the [“Adding Cisco SSG Vendor-Specific Attributes to the Attribute Dictionary”](#) section on page D-3.
- Configure an accounting port, as described in the [“Configuring SSG to Communicate with the RADIUS Server”](#) section on page D-1.



#### Note

You do not need to provide service and subscriber profiles if you are using the RADIUS server solely for accounting purposes.

The subscriber actions that cause SSG to generate a RADIUS accounting record are:

- Subscriber logs in
- Subscriber logs off

- Subscriber accesses a service
- Subscriber terminates a service

Use the following references for more information:

- SSG documentation—Describes the attributes contained in the accounting records
- RADIUS server vendor documentation—Describes RADIUS accounting capabilities

## Configuring Cisco Access Registrar for SESM Deployments

This section describes how to configure the Cisco Access Registrar (Cisco AR) for an SESM deployment. The section includes profile examples in Cisco AR format.

### Configuring the RADIUS Ports

By default, Cisco Access Registrar listens on ports 1645 and 1646 for any type of RADIUS request. You can configure Cisco Access Registrar to listen on ports 1812 and 1813 instead by entering the following commands:

```
add /Radius/Advanced/Ports/1812
add /Radius/Advanced/Ports/1813
```

These commands cause Cisco Access Registrar to listen on the explicitly defined ports, 1812 and 1813, for all types of RADIUS requests. It no longer listens on the default ports.

### Cisco SSG VSAs in Cisco Access Registrar Dictionary

Cisco Access Registrar is installed with the following Cisco VSAs already defined in its attribute dictionary:

- Cisco-AVPair
- Cisco-SSG-Account-Info
- Cisco-SSG-Service-Info
- Cisco-SSG-Command-Code
- Cisco-SSG-Control-Info

### Configuring NAS Clients in Cisco Access Registrar

Use the following commands to configure the NAS clients required by an SESM deployment:

```
add /Radius/Clients/SESM1 "" 10.3.3.2 cisco
add /Radius/Clients/SESM2 "" 10.3.3.101 cisco
add /Radius/Clients/SESM1 "" 10.3.3.102 cisco
```

## Configuring Attribute Profiles in Cisco Access Registrar

This section shows commands for creating sample profiles in Cisco Access Registrar format.

### Internet Service Profile

```
add /Radius/Profiles/internet-profile
set /Radius/Profiles/internet-profile/Attributes/Cisco-SSG-Service-Info IInternet
R153.153.153.0;255.255.255.0 MC TP
```

### Corporate Service Profile

```
add /Radius/Profiles/corporate-profile
set /Radius/Profiles/corporate-profile/Attributes/Cisco-SSG-Service-Info "ICorporate
Intranet(proxy)" R154.154.154.0;255.255.255.0 S10.3.3.101;1812;1813;cisco MC TX
```

### IPTV Profile

```
add /Radius/Profiles/iptv-profile
set /Radius/Profiles/iptv-profile/Attributes/Cisco-SSG-Service-Info IIP/TV
R160.160.160.0;255.255.255.0 MC TP
set /Radius/Profiles/iptv-profile/Attributes/Idle-Timeout 60
set /Radius/Profiles/iptv-profile/Attributes/Session-Timeout 60
```

### Standard Subscriber Profile

```
add /Radius/Profiles/std-user-profile
set /Radius/Profiles/std-user-profile/Attributes/Service-Type Framed
set /Radius/Profiles/std-user-profile/Attributes/Cisco-SSG-Account-Info Ainternet
Ninternet
```

### Pseudo-service Profile

```
add /Radius/Profiles/pseudo-service-profile
set /Radius/Profiles/pseudo-service-profile/Attributes/Cisco-SSG-Control-Info
G12tp-net7;192.168.1.101 G12tp-net40;192.168.1.102 Gweb-key;192.168.1.101
Gproxy-radius-key;192.168.1.101 Gxint-24;192.168.1.101
```

## Configuring Cisco Access Registrar Userlists and Authentication and Authorization Services

This section describes how to configure userlists and authentication and authorization services on Cisco Access Registrar.

### Configuring Userlist for SESM Services

The following commands configure userlists containing SESM services and corresponding attribute profiles.

```
add /Radius/Userlists/SESMservices
add /Radius/Userlists/SESMservices/internet "" servicecisco TRUE "" internet-profile
add /Radius/Userlists/SESMservices/corporate "" servicecisco TRUE "" corporate-profile
add /Radius/Userlists/SESMservices/iptv "" servicecisco TRUE "" iptv-profile
```

### Configuring Userlist for SESM Users

The following commands configure userlists containing SESM users and corresponding attribute profiles.

```
add /Radius/Userlists/SESMusers
add /Radius/Userlists/SESMusers/user1 "" cisco TRUE "" std-user-profile
```

```
add /Radius/Userlists/SESMusers/ssg-next-hop "" xssg-key TRUE "" pseudo-service-profile
```

### Configuring AA Services

The following commands configure Cisco Access Register AA services. The first command configures services for the SESM services userlist. The second command configures services for SESM users userlist.

```
add /Radius/Services/Outbound "" local "" "" RejectAll "" SESMservices
add /Radius/Services/SESMdefault "" local "" "" RejectAll "" SESMusers
```

### Checking the Service-Type Attribute

The following commands configure Cisco Access Registrar to check the Service-Type attribute in the request. If Service-Type is set to Outbound, then the Outbound AA service is used; otherwise, the SESM default AA service is used.

```
set /Radius/DefaultAuthenticationService ${q|Service-Type}{SESMdefault}
set /Radius/DefaultAuthorizationService ${q|Service-Type}{SESMdefault}
```

## Configuring Accounting on Cisco Access Registrar

To configure accounting services, use the following commands:

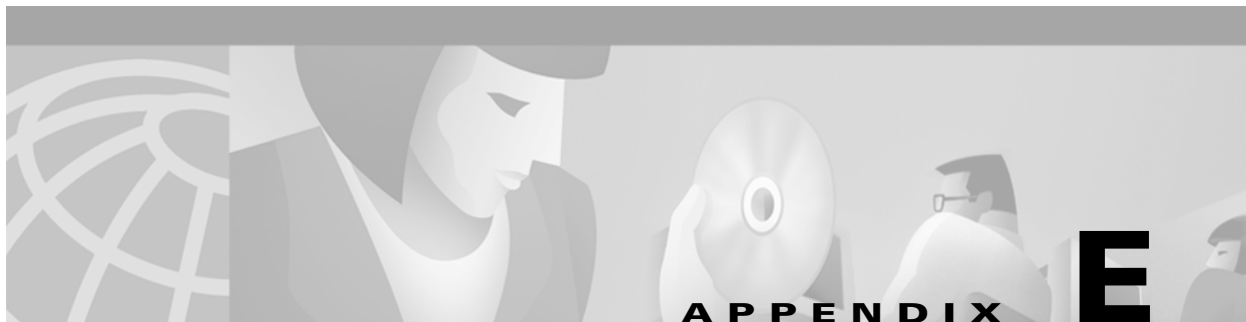
```
add /Radius/Services/SESMaccounting "" file
set /Radius/DefaultAccountingService SESMaccounting
```

## Saving the Configuration and Reloading the Server

To save the configuration and reload the Cisco Access Registrar server, use the following commands:

```
save
reload
```





## RDP Packet Handlers

---

RDP is a flexible and extensible application. This appendix describes the programming methodology in RDP that processes requests received from SSG. It includes the following topics:

- [Packet Handlers, page E-1](#)
- [RDPPacket Class Description, page E-2](#)
- [Processing Requests in Proxy Mode, page E-5](#)

### Packet Handlers

This section describes the RDP packet handler class. It includes the following topics:

- [Overview, page E-1](#)
- [Configuring the Packet Handlers, page E-2](#)
- [Adding Additional Packet Handlers, page E-2](#)

### Overview

The RDP application is very flexible in the way it handles requests that it receives from SSG. This flexibility is implemented with a number of different packet handlers, each handling a request in a different way. Developers at your site can extend the RDP application with additional packet handlers to provide even more flexibility.

RDP cycles a request from SSG through several levels of packet handlers, each one working to narrow down the type of packet, until a response is generated. The request is initially untyped and is processed by the packet handler for untyped packets. As the request gets processed by various packet handlers, it gets typed several times, each time with a more specific type. RDP creates a new packet object to process each newly assigned packet type.

## Configuring the Packet Handlers

The RDPPacketFactoryMBean is the configurable class that specifies the packet handlers to use for each packet type. The rdp.xml file includes the following entries for each packet handler:

```
<Call name="addType">
  <Arg>packetType</Arg>
  <Arg>class</Arg>
</Call>
```

Each <Call name="addType"> element takes two arguments: a packet type and a class that will handle that packet type. The packetType is a string. The class is a string specifying an RDPPacket derived class. Class parameters follow the class and are separated from it by a semicolon.

The RDPPacketFactoryMBean also accepts entries that set attributes. The attribute entries are used as parameters to the ProfileRequestPacket packet handler to narrow down the packet type.

```
<Call name="setAttribute">
  <Arg>PASSWORD:password</Arg>
  <Arg>packetType</Arg>
</Call>
```

Each <Call name="setAttribute"> element takes two arguments: a password and a packetType.

There must be a corresponding <Call name="addType"> element for packetType, to specify the packet handler class for that packet type.

## Adding Additional Packet Handlers

The packet handling mechanism is extensible. Web developers can write customized or additional packet handlers and map them to specific packet types by making changes or additions in the rdp.xml file.

## RDPPacket Class Description

When RDP receives a request, it creates an RDPPacket. The packet handlers in the RDPPacket class have two public methods:

- getType method
- handle method

An RDPPacket derived class either overrides the getType method, in which case it narrows down the type of the packet, or it overrides the handle method, in which case it generates a response. An object calls the handle method first. If the handle method can process the request, it does so, generating the response. Otherwise, the default RDPPacket handle method calls the getType method.

The getType method determines some information about the type of packet. The default handle method uses the returned type to create a new RDPPacket derived packet. The handle method is then called on the new packet, as described in the previous paragraph.

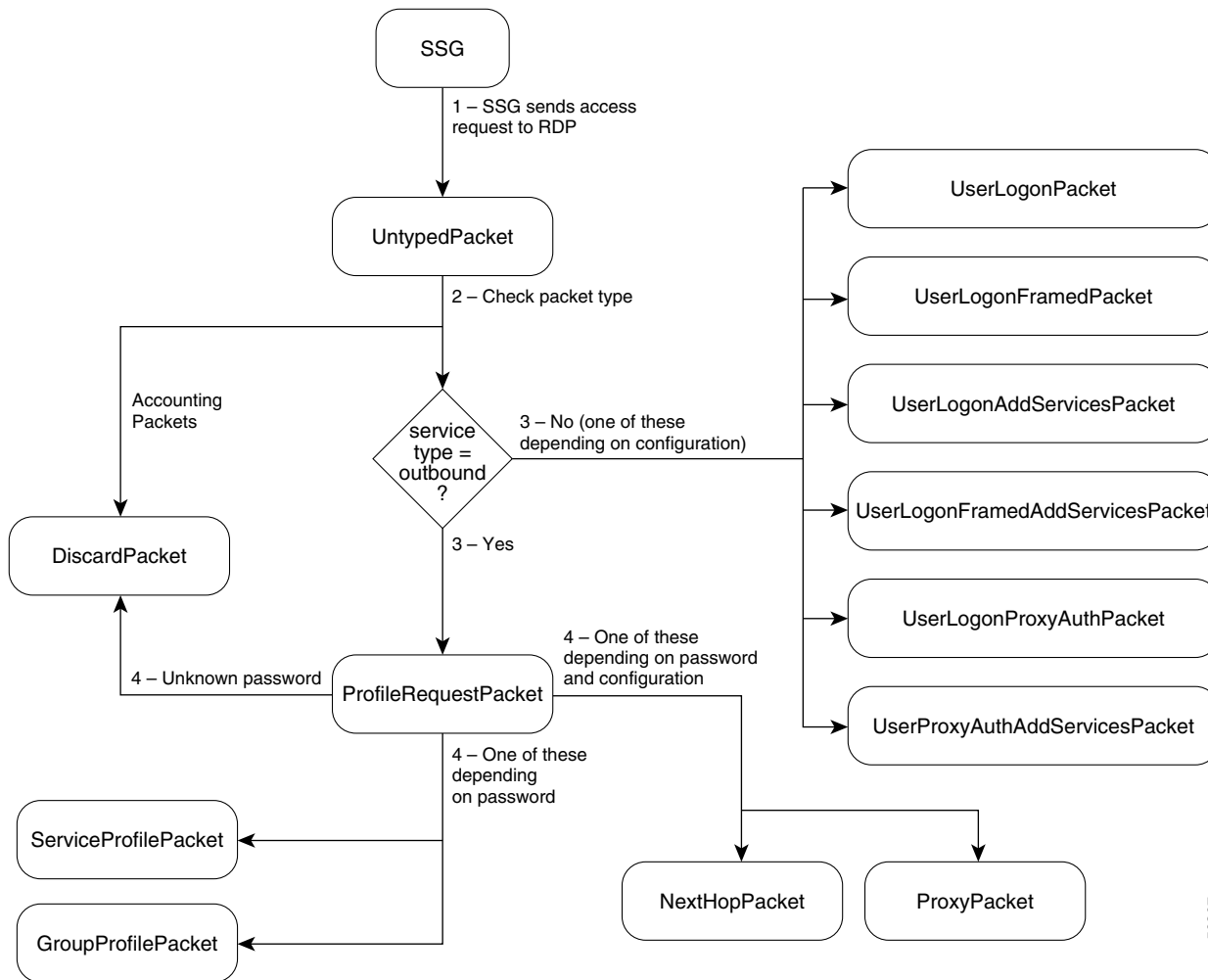
Table E-1 describes the RDPPacket classes included with the installed RDP application.

**Table E-1 RDPPacket Classes and Methods**

Class	Methods
RDPPacket	getType—If the request is an Access Request, this method prompts you with Untyped. Otherwise, the method prompts you with Unknown.
DiscardPacket	handle—Returns null. (That is, it silently discards the request.)
RejectPacket	handle—Returns an Access Reject message.
UntypedPacket	getType—If the request contains the AV Service-Type with the value <code>Outbound</code> , then the method ProfileRequest appears. Otherwise, this method prompts you with UserLogon.
ProfileRequestPacket	getType—If the request contains a password that matches a password defined by the <code>PASSWORD:</code> attribute, this method displays the attribute's value. Otherwise, this method prompts you with Unknown.
ProxyPacket	handle—Proxies the request to an AAA server. Requires a parameter to define the name of the AAA MBean.
ServiceProfilePacket	handle—Uses the DESS API to create a service profile response.
GroupProfilePacket	handle—Uses the DESS API to create a group profile response.
NextHopPacket	handle—Uses the DESS API to create a next hop gateway response.
UserLogonAddServicesPacket	handle—Uses the DESS API to authenticate and authorize a subscriber. All services and groups the subscriber is subscribed to appear.
UserLogonPacket	handle—Uses the DESS API to authenticate a subscriber. If the subscriber is using PPP, the subscriber's auto-logon services appear.
UserProxyAuthAddServicePacket	handle—Proxies the request to a AAA server, but uses DESS to add authorization information. Requires a parameter to define the name of an AAA MBean.
UserProxyAuthPacket	handle—Proxies the request to an AAA server, but uses DESS to add authorization information for auto-logon services if the user is a PPP user. Requires a parameter to define the name of an AAA MBean.

Figure E-1 shows how RDP processes a request from SSG. A detailed explanation follows the figure.

Figure E-1 RDP Request Processing



A request from SSG is processed in the following way:

1. The initial packet is handled by the base class. The `getType` method returns `Untyped`.
2. An `Untyped` packet is handled by the `UntypedPacket` class.
3. The `getType` method returns one of the following types:
  - If the packet contains the AV pair `service-type = Outbound`, `getType` returns `ProfileRequest` packet.
  - Otherwise, `getType` returns one of the `UserLogon` request packets, depending on values in the MBean configuration file.

4. A ProfileRequest packet is handled by the ProfileRequestPacket class. This class narrows the type again using the PASSWORD: attributes set in the rdp.xml file. If the password in the request (prepended with the string PASSWORD:) matches any of the password attributes set in the rdp.xml file, the getType method returns the packet type associated with the password in the corresponding <Call name="setAttribute"> element. Password attributes identify the following types of requests:
  - ServiceRequest—The ServiceRequest packet handler uses the DESS API to retrieve a list of services that this subscriber is authorized to access.
  - GroupRequest —The GroupRequest packet handler uses the DESS API to retrieve a list of services that this subscriber is authorized to access through group membership.
  - ProxyNextHop—The ProxyNextHop packet handler passes the request to the RADIUS server identified in the AAA MBean in the rdp.xml file.
  - If the password does not match any of the above, getType returns Unknown. An Unknown packet is handled by the RejectPacket packet handler.

See the “RDPPacketFactory” section in [Table 6-6 on page 6-32](#) for information about how to set these password values.

## Processing Requests in Proxy Mode

When RDP is running in Proxy mode, profile requests are forwarded to a RADIUS server. This section describes the configuration entries in rdp.xml that make this happen. The section discusses the following entries from the installed rdp.xml file.

```
<Call name="setAttribute">
  <Arg>PASSWORD:nexthopcisco</Arg>
  <Arg>ProxyNextHop</Arg>
</Call>

<Call name="addType">
  <Arg>ProxyNextHop</Arg>
  <Arg>com.cisco.aggbu.rdp.ProxyPacket;NextHop</Arg>
</Call>

<Configure name="com.cisco.aggbu:name=AAA,connection=NextHop">
```

If a ProfileRequestPacket has the password nexthopcisco (this is an example; your password value might be different), it is typed ProxyNextHop. The <Call name="addType"> element for ProxyNextHop maps the packet to the ProxyPacket class.

The ProxyPacket class accepts a string in its constructor which identifies the connection object that will handle the request. The string after the class name and semicolon in the <Call name="addType"> element is passed to the ProxyPacket class constructor. This connection object name matches the connection object configured by the AAA MBean.





## Sample MBean Configuration Files

This appendix contains sample MBean configuration files. It includes the following sections:

- [Sample Container MBean Configuration File, page F-1](#)
- [Sample Application MBean Configuration File, page F-3](#)
- [Sample RDP MBean Configuration File, page F-13](#)
- [Sample CDAT MBean Configuration File, page F-16](#)
- [Sample SPE MBean Configuration File, page F-18](#)
- [Sample Captive Portal Configuration File, page F-19](#)
- [Sample Message Portal Configuration File, page F-24](#)

### Sample Container MBean Configuration File

An example jetty/config/nwsp.jetty.xml file follows.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2001, 2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container specific configuration for the NWSP web application.
Container independant configuration can be found at:
      $INSTALLROOT/nwsp/config/nwsp.xml
-->

-->

<XmlConfig>

  <!-- ===== -->
  <Instantiate order="10" class="org.mortbay.jetty.jmx.LogMBean"/>
  <Instantiate order="11" class="org.mortbay.jetty.jmx.DebugMBean"/>
  <Instantiate order="12"
    class="org.mortbay.jetty.jmx.HttpServerMBean"
    jmxname="org.mortbay.jetty:name=Jetty,Server=0"/>

  <!-- ===== -->
  <Configure jmxname="org.mortbay.jetty:name=Log,OutputStreamLogSink=0">
    <Set name="append" type="boolean">true</Set>
    <Set name="filename"><SystemProperty name="application.log"
default="./logs"/>/yyyy_mm_dd.jetty.log</Set>
    <Set name="logTimezone"></Set>
    <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS' '</Set>
    <Set name="logLabels" type="boolean">>false</Set>
    <Set name="logOneLine" type="boolean">>false</Set>
  </Configure>
</XmlConfig>
```

```

    <Set name="logStackSize" type="boolean">false</Set>
    <Set name="logStackTrace" type="boolean">false</Set>
    <Set name="logTags" type="boolean">true</Set>
    <Set name="logTimeStamps" type="boolean">true</Set>
    <Set name="retainDays" type="int">31</Set>
</Configure>

<Configure class="org.mortbay.jetty.jmx.DebugMBean" >
  <Set name="debug" type="boolean">false</Set>
  <Set name="debugPatterns"></Set>
  <Set name="debugTriggers"></Set>
  <Set name="verbose" type="int">0</Set>
  <Set name="suppressStack" type="boolean">false</Set>
  <Set name="suppressWarnings" type="boolean">false</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0">
  <Call name="addListener">
    <Arg>
      <New class="org.mortbay.http.SocketListener">
        <Set name="port"><SystemProperty name="application.portno"
default="8080"/></Set>
        <Set name="minThreads">5</Set>
        <Set name="maxThreads">255</Set>
        <Set name="maxIdleTimeMs">60000</Set>
        <Set name="maxReadTimeMs">60000</Set>
      </New>
    </Arg>
  </Call>

  <Call name="addListener">
    <Arg>
      <New class="org.mortbay.http.SunJsseListener">
        <Set name="port"><SystemProperty name="application.ssl.portno"
default="8130"/></Set>
        <Set name="MinThreads">5</Set>
        <Set name="MaxThreads">255</Set>
        <Set name="MaxIdleTimeMs">50000</Set>
        <Set name="Keystore"><SystemProperty name="jetty.home"
default=". "/>/config/nwspkeystore</Set>
        <Set name="Password">OBF:1vny1z1o1x8e1vnw1vn61x8g1z1u1vn4</Set>
        <Set name="KeyPassword">OBF:1u2u1wml1z7s1z7a1wnl1u2g</Set>
      </New>
    </Arg>
  </Call>

  <Set name="logSink">
    <New class="org.mortbay.util.OutputStreamLogSink">
      <Arg><SystemProperty name="application.log"
default="./logs"/>/yyyy_mm_dd.request.log</Arg>
      <Set name="retainDays">90</Set>
      <Set name="append">true</Set>
    </New>
  </Set>

  <!-- NWSP web application -->
  <Call name="addWebApplication">
    <Arg></Arg>
    <Arg></Arg>
    <Arg><SystemProperty name="application.home" default=". "/>/docroot</Arg>
    <Arg><SystemProperty name="jetty.home" default=". "/>/config/webdefault.xml</Arg>
    <Arg type="boolean">FALSE</Arg>
    <Call name="addHandler">

```



```

        <Arg type="int">0</Arg>
        <Arg><New class="com.cisco.sesm.jetty.PortBundleHandler"/></Arg>
    </Call>
</Call>

<Call name="start"/>

</Configure>

</XmlConfig>

```

## Sample Application MBean Configuration File

This section contains two sample files:

- [RADIUS Mode Deployment, page F-3](#)
- [LDAP Mode Deployment, page F-8](#)

## RADIUS Mode Deployment

The following nwsp/config/nwsp.xml file shows a RADIUS mode deployment.

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/kesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container independent configuration for the NWSP web application.
Container specific configuration can be found at:
$INSTALLROOT/$CONTAINER/config/nwsp.xml
-->

<XmlConfig>
<!-- ===== -->
<Instantiate order="1"
class="com.cisco.sesm.jmx.LoggerMBean"
jmxname="com.cisco.sesm:name=Logger"/>

<Instantiate order="99"
class="com.sun.jdmk.comm.HtmlAdaptorServer"
jmxname="com.cisco.sesm:name=ManagementConsole">
<Arg type="int">
<SystemProperty name="management.portno"/>
</Arg>
<Arg>
</Arg>
<Array class="com.sun.jdmk.comm.AuthInfo">
<Item>
<New class="com.sun.jdmk.comm.AuthInfo">
<Arg>MgmtUser</Arg>
<Arg>MgmtPassword</Arg>
</New>
</Item>
</Array>
</Arg>
</Instantiate>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=Logger">
<Set name="debug" type="boolean"><SystemProperty name="nwsp.debug"
default="false"/></Set>

```

```

    <Set name="debugPatterns"></Set>
    <Set name="debugThreads"></Set>
    <Set name="debugVerbosity">LOW</Set>
    <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS</Set>
    <Set name="logFile"><SystemProperty name="application.log"
default="./logs"/>/>yyyyMMdd.application.log</Set>
    <Set name="logFrame" type="boolean">>false</Set>
    <Set name="logStack" type="boolean">>false</Set>
    <Set name="logThread" type="boolean">>true</Set>
    <Set name="logToErr" type="boolean"><SystemProperty name="nwsp.logToErr"
default="false"/></Set>
    <Set name="trace" type="boolean">>true</Set>
    <Set name="warning" type="boolean">>true</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=ManagementConsole">
    <Call name="start"/>
</Configure>

<!-- ===== -->
<Configure class="com.cisco.sesm.core.model.SESMMBean"
    jmxname="com.cisco.sesm:name=SESM">
    <Call name="defineMode">
        <Arg>Demo</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoAuthenticationService</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoAuthorizationService</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoConnectionService</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoServiceProfileService</Arg>
    </Call>
    <Call name="defineMode">
        <Arg>RADIUS</Arg>
        <Arg>com.cisco.sesm.spis.radius.RADIUSAuthentication</Arg>
        <Arg>com.cisco.sesm.spis.radius.RADIUSAuthorization</Arg>
        <Arg>com.cisco.sesm.spis.radius.RADIUSServiceConnection</Arg>
        <Arg>com.cisco.sesm.spis.radius.RADIUSServiceProfile</Arg>
    </Call>
    <Call name="defineMode">
        <Arg>LDAP</Arg>
        <Arg>com.cisco.sesm.spis.radius.RADIUSAuthentication</Arg>
        <Arg>com.cisco.sesm.spis.dess.DESSAuthorizationService</Arg>
        <Arg>com.cisco.sesm.spis.radius.RADIUSServiceConnection</Arg>
        <Arg>com.cisco.sesm.spis.dess.DESSServiceProfileService</Arg>
    </Call>
    <!--
    - This determines the SESM model mode of operation. A mode of operation
    - determines how SESM connects to hardware.
    -->
    <Set name="mode"><SystemProperty name="sesm.mode" default="RADIUS"/></Set>
    <!--
    - This boolean turns on or off the capability to perform
    - single sign-on. In single sign on mode, a user only has to
    - authenticate once and SESM merely checks that the user has
    - been authenticated.
    -->
    <Set name="singleSignOn" type="boolean">>true</Set>
    <!--
    - This boolean determines whether or not services are auto-connected
    - by SESM during sign-on.
    -->
    <Set name="autoConnect" type="boolean">>false</Set>
    <!--
    - This is the number of seconds between clearing group
    - and service caches.

```

```

-->
<Set name="profileCachePeriod" type="int">600</Set>
<!--
- This is the minimum length of time in seconds that an SESMSession
- is held in memory without being accessed. SESMSessions are checked
- regularly according to the profileCachePeriod.
- If this is set to 0 (or undefined) profileCachePeriod*2 is used.
-->
<Set name="sessionCachePeriod" type="int">1200</Set>
<!--
- Turning on this option will cause the model to throw an exception when
- an attempt is made to connect a service in a mutually exclusive service
- group and another service in the group is already connected.
- If the option is turned off, the previous service will be disconnected
- automatically.
-->
<Set name="confirmMutexDisconnect" type="boolean">>false</Set>
<!--
- This sets the minimum amount of memory required before
- a SESM session can be created or authenticated.
- This is in order to prevent the application running out of memory.
-->
<Set name="memRequired" type="long">10485760</Set>
<!--
- If this is set true, sessions will be removed from memory when
- the minimum memory limit is hit.
- Turning this on will facilitate a quick recovery from a memory problem
- but will result in loss of user state. This means they will have to log
- in again if Single Sign On is disabled.
-->
<Set name="clearSessionsOnMem" type="boolean">>false</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=SESMDemoMode">
<!--
- This is the demo data file. It is in the format of a Merit
- dictionary with special extensions for this software.
-->
<Set name="demoDataFile"><SystemProperty
name="application.home"/>/config/demo.txt</Set>
</Configure>

<!-- ===== -->
<!-- Settings for the DESS SPI. -->
<Configure jmxname="com.cisco.sesm:name=DESSMode">
<!-- The time in seconds between checking the authorization tokens. -->
<Set name="tokenCheckInterval" type="int">300</Set>
<!-- The age of a token in seconds (time since last used) for it to be removed from
cache. -->
<Set name="tokenMaxAge" type="int">600</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=SSG">
<!--
- Maximum number of simultaneous requests allowed to each SSG. Extra
- requests will be placed on a queue and issued as responses are received
- or timeout.
-->
<Set name="throttle" type="int">20</Set>

<!--
- Here we define attributes for RADIUS communication with the SSG If

```

```

- we are running with Port Bundle Host key then we need only define
- the global attributes for all of the SSGs.
-->
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>TIMEOUTSECS</Arg><Arg>10</Arg></Call>
<Call name="setGlobalAttribute"><Arg>RETRIES</Arg><Arg>3</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<!--
- A non zero value here, the default should be 4, will turn Port
- Bundle Host Key on.
-->
-->
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
<Call
name="setGlobalAttribute"><Arg>PORT_BUNDLE_HOST_KEY_SWITCH</Arg><Arg>>false</Arg></Call>
<!--
- This value may be true or false. True is implied by a non zero
- BUNDLE_LENGTH. If the BUNDLE_LENGTH is non zero, then this value
- will be ignored. As a BUNDLE_LENGTH of 0 is a legal value, however,
- the Port Bundle Host Key feature can also be turned on here
- when the BUNDLE_LENGTH is 0, which it would be for persistent
- connections.

<Call
name="setGlobalAttribute"><Arg>PORT_BUNDLE_HOST_KEY_SWITCH</Arg><Arg>>true</Arg></Call>

-->

<!--
- If we need to map from a client IP address to an SSG explicitly,
- then we could have an entry like this:

<Call
name="setSubnetAttribute"><Arg>213.0.0.0</Arg><Arg>255.0.0.0</Arg><Arg>IP</Arg><Arg>195.24
5.182.2</Arg></Call>

- which would map the client subnet 213.0.0.0 to the SSG at
- 195.245.182.2 with the global parameters defined above for
- the RADIUS protocol.
-->
<!-- If we need to define a location for a subnet, say London, then we
- could do this:

<Call
name="setSubnetAttribute"><Arg>213.0.0.0</Arg><Arg>255.0.0.0</Arg><Arg>SESSION_LOCATION</A
rg><Arg>London</Arg></Call>

- See the location definitions below for illustrations of how
- attributes can be associated with locations.
-->
</Configure>

<!-- ===== -->
<!--
- Here we define attributes for RADIUS communication with the RADIUS
- servers for service and group profiles in RADIUS mode.
-->
<Configure jmxname="com.cisco.sesm:name=AAA,connection=ServiceProfile">
<Set name="throttle" type="int">256</Set>
<Set name="timeOut" type="int">4</Set>
<Set name="retryCount" type="int">3</Set>
<Set name="primaryIP">127.0.0.2</Set>
<Set name="primaryPort" type="int">1812</Set>
<Set name="secret">cisco</Set>

```

```

<Set name="secondaryIP">127.0.0.3</Set>
<Set name="secondaryPort" type="int">1812</Set>
<Set name="servicePassword">servicecisco</Set>
<Call name="open"/>
</Configure>

<Configure jmxname="com.cisco.sesm:name=AAA,connection=ServiceGroupProfile">
  <Set name="throttle" type="int">256</Set>
  <Set name="timeOut" type="int">4</Set>
  <Set name="retryCount" type="int">3</Set>
  <Set name="primaryIP">127.0.0.2</Set>
  <Set name="primaryPort" type="int">1812</Set>
  <Set name="secret">cisco</Set>
  <Set name="secondaryIP">127.0.0.3</Set>
  <Set name="secondaryPort" type="int">1812</Set>
  <Set name="serviceGroupPassword">groupcisco</Set>
  <Call name="open"/>
</Configure>

<!-- ===== -->

<Configure class="com.cisco.sesm.webapp.config.WebAppMBean"
  jmxname="com.cisco.sesm:name=WebApp">
  <!--
  - These options control different aspects of the NWSP applications
  - behaviours. These settings are used by the NWSP application to
  - control different aspects of its behaviour.
  -->
  <!-- Confirm that you want to logon onto a service as opposed
  - to single click logon. -->
  <Set name="confirmAtServiceLogon" type="boolean">FALSE</Set>
  <!-- Confirm that you want to logoff a service as opposed
  - to single click logoff. -->
  <Set name="confirmAtServiceLogoff" type="boolean">TRUE</Set>
  <!-- Confirm that you want to logoff from the application as opposed
  - to single click logoff. -->
  <Set name="confirmAtAccountLogoff" type="boolean">TRUE</Set>
  <!-- This overrides the setting in the Jetty nwsp.xml. -->
  <Set name="sessionTimeOut" type="int">7200</Set>
  <!-- Maximum length for usernames and passwords. -->
  <Set name="credentialMaxLength" type="int">30</Set>

  <!-- These identify the URI required for requests to NWSP's /serviceRedirect: -->
  <!-- service redirect when request parameter "service" is null or empty -->
  <Set name="serviceNotGivenURI">/status</Set>
  <!-- service redirect for any unexpected condition, eg if service is not available -->
  <Set name="defaultURI">/home</Set>
  <!-- service redirect for services that are not subscribed -->
  <Set name="serviceSubscriptionURI">/subscriptionManage</Set>
  <!-- service redirect when no further entry of credentials required -->
  <Set name="serviceStartURI">/serviceStart</Set>
  <!-- service redirect when further entry of credentials required -->
  <Set name="serviceLogonURI">/serviceLogon</Set>

  <!--
  - These are examples of how arbitrary properties can be used
  - in the SESM applications.
  -->
  <Call name="addDimension">
    <Arg type="int">1</Arg>
    <Arg>London</Arg>
    <Arg>http://www.london.com</Arg>

```

```

</Call>
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>Paris</Arg>
  <Arg>http://www.paris-france.org/</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>New York</Arg>
  <Arg>http://www.usa.net/newyork</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">2</Arg>
  <Arg>Acme</Arg>
  <Arg>http://www.acme.com</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">2</Arg>
  <Arg>Cisco</Arg>
  <Arg>http://www.cisco.com</Arg>
</Call>
</Configure>

</XmlConfig>

```

## LDAP Mode Deployment

The following nwsp/config/nwsp.xml file shows an LDAP mode deployment with the captive portal feature enabled. RDP was installed in normal (non-proxy) mode, with the Add Services option checked.

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container independent configuration for the NWSP web application.
Container specific configuration can be found at:
      $INSTALLROOT/$CONTAINER/config/nwsp.xml
-->

<XmlConfig>
  <!-- ===== -->
  <Instantiate order="1"
    class="com.cisco.sesm.jmx.LoggerMBean"
    jmxname="com.cisco.sesm:name=Logger"/>

  <Instantiate order="99"
    class="com.sun.jdmk.comm.HtmlAdaptorServer"
    jmxname="com.cisco.sesm:name=ManagementConsole">
    <Arg type="int">
      <SystemProperty name="management.portno"/>
    </Arg>
    <Arg>
  </Array class="com.sun.jdmk.comm.AuthInfo">
    <Item>
      <New class="com.sun.jdmk.comm.AuthInfo">
        <Arg>MgmtUser</Arg>
        <Arg>MgmtPassword</Arg>
      </New>
    </Item>
  </Array>
  </Arg>
</Instantiate>

```

```

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=Logger">
  <Set name="debug" type="boolean"><SystemProperty name="nwsp.debug"
default="false"/></Set>
  <Set name="debugPatterns"></Set>
  <Set name="debugThreads"></Set>
  <Set name="debugVerbosity">LOW</Set>
  <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS</Set>
  <Set name="logFile"><SystemProperty name="application.log"
default="./logs"/>/>yyyy_mm_dd.application.log</Set>
  <Set name="logFrame" type="boolean">>false</Set>
  <Set name="logStack" type="boolean">>false</Set>
  <Set name="logThread" type="boolean">>true</Set>
  <Set name="logToErr" type="boolean"><SystemProperty name="nwsp.logToErr"
default="false"/></Set>
  <Set name="trace" type="boolean">>true</Set>
  <Set name="warning" type="boolean">>true</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=ManagementConsole">
  <Call name="start"/>
</Configure>

<!-- ===== -->
<Configure class="com.cisco.sesm.core.model.SESMMBean"
  jmxname="com.cisco.sesm:name=SESM">
  <Call name="defineMode">
    <Arg>Demo</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoAuthenticationService</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoAuthorizationService</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoConnectionService</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoServiceProfileService</Arg>
  </Call>
  <Call name="defineMode">
    <Arg>RADIUS</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthentication</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthorization</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSServiceConnection</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSServiceProfile</Arg>
  </Call>
  <Call name="defineMode">
    <Arg>LDAP</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthentication</Arg>
    <Arg>com.cisco.sesm.spis.dess.DESSAuthorizationService</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSServiceConnection</Arg>
    <Arg>com.cisco.sesm.spis.dess.DESSServiceProfileService</Arg>
  </Call>
  <!--
  - This determines the SESM model mode of operation. A mode of operation
  - determines how SESM connects to hardware.
  -->
  <Set name="mode"><SystemProperty name="sesm.mode" default="LDAP"/></Set>
  <!--
  - This boolean turns on or off the capability to perform
  - single sign-on. In single sign on mode, a user only has to
  - authenticate once and SESM merely checks that the user has
  - been authenticated.
  -->
  <Set name="singleSignOn" type="boolean">>true</Set>
  <!--
  - This boolean determines whether or not services are auto-connected
  - by SESM during sign-on.

```

```

-->
<Set name="autoConnect" type="boolean">>false</Set>
<!--
- This is the number of seconds between clearing group
- and service caches.
-->
-->
<Set name="profileCachePeriod" type="int">600</Set>
<!--
- This is the minimum length of time in seconds that an SESMSession
- is held in memory without being accessed. SESMSessions are checked
- regularly according to the profileCachePeriod.
- If this is set to 0 (or undefined) profileCachePeriod*2 is used.
-->
-->
<Set name="sessionCachePeriod" type="int">1200</Set>
<!--
- Turning on this option will cause the model to throw an exception when
- an attempt is made to connect a service in a mutually exclusive service
- group and another service in the group is already connected.
- If the option is turned off, the previous service will be disconnected
- automatically.
-->
-->
<Set name="confirmMutexDisconnect" type="boolean">>false</Set>
<!--
- This sets the minimum amount of memory required before
- a SESM session can be created or authenticated.
- This is in order to prevent the application running out of memory.
-->
-->
<Set name="memRequired" type="long">10485760</Set>
<!--
- If this is set true, sessions will be removed from memory when
- the minimum memory limit is hit.
- Turning this on will facilitate a quick recovery from a memory problem
- but will result in loss of user state. This means they will have to log
- in again if Single Sign On is disabled.
-->
-->
<Set name="clearSessionsOnMem" type="boolean">>false</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=SESMDemoMode">
<!--
- This is the demo data file. It is in the format of a Merit
- dictionary with special extensions for this software.
-->
-->
<Set name="demoDataFile"><SystemProperty
name="application.home"/>/config/demo.txt</Set>
</Configure>

<!-- ===== -->
<!-- Settings for the DESS SPI. -->
<Configure jmxname="com.cisco.sesm:name=DESSMode">
<!-- The time in seconds between checking the authorization tokens. -->
<Set name="tokenCheckInterval" type="int">300</Set>
<!-- The age of a token in seconds (time since last used) for it to be removed from
cache. -->
<Set name="tokenMaxAge" type="int">600</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=SSG">
<!--
- Maximum number of simultaneous requests allowed to each SSG. Extra
- requests will be placed on a queue and issued as responses are received
- or timeout.
-->

```



```

-->
<Set name="throttle" type="int">20</Set>

<!--
- Here we define attributes for RADIUS communication with the SSG If
- we are running with Port Bundle Host key then we need only define
- the global attributes for all of the SSGs.
-->
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>TIMEOUTSECS</Arg><Arg>10</Arg></Call>
<Call name="setGlobalAttribute"><Arg>RETRIES</Arg><Arg>3</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<!--
- A non zero value here, the default should be 4, will turn Port
- Bundle Host Key on.
-->
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>
<!-- The following line configures a single non-hostkey SSG -->
<!-- Additional SSGs can be configured by adding further 'Call' elements -->
<!-- Remove the following call if the bundle size is ever set to > 0 -->
<!-- Arg list: <client subnet>, <subnet mask>, IP, <SSG IP address> -->
<Call
name="setSubnetAttribute"><Arg>10.20.1.0</Arg><Arg>255.255.255.0</Arg><Arg>IP</Arg><Arg>10
.4.4.4</Arg></Call>
<Call
name="setGlobalAttribute"><Arg>PORT_BUNDLE_HOST_KEY_SWITCH</Arg><Arg>>false</Arg></Call>
<!--
- This value may be true or false. True is implied by a non zero
- BUNDLE_LENGTH. If the BUNDLE_LENGTH is non zero, then this value
- will be ignored. As a BUNDLE_LENGTH of 0 is a legal value, however,
- the Port Bundle Host Key feature can also be turned on here
- when the BUNDLE_LENGTH is 0, which it would be for persistent
- connections.

<Call
name="setGlobalAttribute"><Arg>PORT_BUNDLE_HOST_KEY_SWITCH</Arg><Arg>>true</Arg></Call>

-->

<!--
- If we need to map from a client IP address to an SSG explicitly,
- then we could have an entry like this:

<Call
name="setSubnetAttribute"><Arg>213.0.0.0</Arg><Arg>255.0.0.0</Arg><Arg>IP</Arg><Arg>195.24
5.182.2</Arg></Call>

- which would map the client subnet 213.0.0.0 to the SSG at
- 195.245.182.2 with the global parameters defined above for
- the RADIUS protocol.
-->
<!-- If we need to define a location for a subnet, say London, then we
- could do this:

<Call
name="setSubnetAttribute"><Arg>213.0.0.0</Arg><Arg>255.0.0.0</Arg><Arg>SESSION_LOCATION</A
rg><Arg>London</Arg></Call>

- See the location definitions below for illustrations of how
- attributes can be associated with locations.
-->
</Configure>

```

```

<!-- ===== -->
<!--
- Here we define attributes for RADIUS communication with the RADIUS
- servers for service and group profiles in RADIUS mode.
-->
<!-- Uncomment and modify this element when run in RADIUS mode
<Configure jmxname="com.cisco.sesm:name=AAA,connection=ServiceProfile">
  <Set name="throttle" type="int">256</Set>
  <Set name="timeOut" type="int">4</Set>
  <Set name="retryCount" type="int">3</Set>
  <Set name="primaryIP">127.0.0.1</Set>
  <Set name="primaryPort" type="int">1812</Set>
  <Set name="secret">cisco</Set>
  <Set name="secondaryIP">127.0.0.2</Set>
  <Set name="secondaryPort" type="int">1812</Set>
  <Set name="servicePassword">servicecisco</Set>
  <Call name="open"/>
</Configure>

<Configure jmxname="com.cisco.sesm:name=AAA,connection=ServiceGroupProfile">
  <Set name="throttle" type="int">256</Set>
  <Set name="timeOut" type="int">4</Set>
  <Set name="retryCount" type="int">3</Set>
  <Set name="primaryIP">127.0.0.1</Set>
  <Set name="primaryPort" type="int">1812</Set>
  <Set name="secret">cisco</Set>
  <Set name="secondaryIP">127.0.0.2</Set>
  <Set name="secondaryPort" type="int">1812</Set>
  <Set name="serviceGroupPassword">groupcisco</Set>
  <Call name="open"/>
</Configure>
-->

<!-- ===== -->

<Configure class="com.cisco.sesm.webapp.config.WebAppMBean"
  jmxname="com.cisco.sesm:name=WebApp">
  <!--
- These options control different aspects of the NWSP applications
- behaviours. These settings are used by the NWSP application to
- control different aspects of its behaviour.
-->
  <!-- Confirm that you want to logon onto a service as opposed
- to single click logon. -->
  <Set name="confirmAtServiceLogon" type="boolean">FALSE</Set>
  <!-- Confirm that you want to logoff a service as opposed
- to single click logoff. -->
  <Set name="confirmAtServiceLogoff" type="boolean">TRUE</Set>
  <!-- Confirm that you want to logoff from the application as opposed
- to single click logoff. -->
  <Set name="confirmAtAccountLogoff" type="boolean">TRUE</Set>
  <!-- This overrides the setting in the Jetty nwsp.xml. -->
  <Set name="sessionTimeOut" type="int">7200</Set>
  <!-- Maximum length for usernames and passwords. -->
  <Set name="credentialMaxLength" type="int">30</Set>

  <!-- These identify the URI required for requests to NWSP's /serviceRedirect: -->
  <!-- service redirect when request parameter "service" is null or empty -->
  <Set name="serviceNotGivenURI">/status</Set>
  <!-- service redirect for any unexpected condition, eg if service is not available -->
  <Set name="defaultURI">/home</Set>
  <!-- service redirect for services that are not subscribed -->
  <Set name="serviceSubscriptionURI">/subscriptionManage</Set>

```

```

<!-- service redirect when no further entry of credentials required -->
<Set name="serviceStartURI"/>/serviceStart</Set>
<!-- service redirect when further entry of credentials required -->
<Set name="serviceLogonURI"/>/serviceLogon</Set>

<!--
- These are examples of how arbitrary properties can be used
- in the SESM applications.
-->
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>London</Arg>
  <Arg>http://www.london.com</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>Paris</Arg>
  <Arg>http://www.paris-france.org</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>New York</Arg>
  <Arg>http://www.usa.net/newyork</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">2</Arg>
  <Arg>Acme</Arg>
  <Arg>http://www.acme.com</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">2</Arg>
  <Arg>Cisco</Arg>
  <Arg>http://www.cisco.com</Arg>
</Call>
</Configure>

</XmlConfig>

```

## Sample RDP MBean Configuration File

An example rdp.xml file follows. See [Appendix E, “RDP Packet Handlers,”](#) for more information about this MBean and the possibilities for extending RDP functionality with customized packet handlers.



### Note

The contents of this MBean is different depending on the options you checked during RDP installation. (The packet handlers are different.) The following file shows RDP installed in normal (non-proxy) mode, with the Add Services and Add Client options checked.

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container independent configuration for the RDP application.
Container specific configuration can be found at:
      $INSTALLROOT/$CONTAINER/config/rdp.xml
-->

<XmlConfig>
  <!-- ===== -->

```

```

<Instantiate order="1"
  class="com.cisco.sesm.jmx.LoggerMBean"
  jmxname="com.cisco.sesm:name=Logger" />

<Instantiate order="97"
  class="com.cisco.sesm.rdp.RDPPacketFactoryMBean"
  jmxname="com.cisco.sesm:name=RDPPacketFactory" />

<Instantiate order="98"
  class="com.cisco.sesm.rdp.RDPMBean"
  jmxname="com.cisco.sesm:name=RDP" />

<Instantiate order="96"
  class="com.sun.jdmk.comm.HtmlAdaptorServer"
  jmxname="com.cisco.sesm:name=ManagementConsole">
  <Arg type="int">
    <SystemProperty name="management.portno"/>
  </Arg>
  <Arg>
</Array class="com.sun.jdmk.comm.AuthInfo">
  <Item>
    <New class="com.sun.jdmk.comm.AuthInfo">
      <Arg>MgmtUser</Arg>
      <Arg>MgmtPassword</Arg>
    </New>
  </Item>
</Array>
  </Arg>
</Instantiate>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=Logger">
  <Set name="debug" type="boolean"><SystemProperty name="rdp.debug"
default="false"/></Set>
  <Set name="debugPatterns"></Set>
  <Set name="debugThreads"></Set>
  <Set name="debugVerbosity">LOW</Set>
  <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS</Set>
  <Set name="logFile"><SystemProperty name="application.log"
default="./logs"/>/>yyyy_mm_dd.application.log</Set>
  <Set name="logFrame" type="boolean">>false</Set>
  <Set name="logStack" type="boolean">>false</Set>
  <Set name="logThread" type="boolean">>true</Set>
  <Set name="logToErr" type="boolean"><SystemProperty name="rdp.logToErr"
default="false"/></Set>
  <Set name="trace" type="boolean">>true</Set>
  <Set name="warning" type="boolean">>true</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=ManagementConsole">
  <Call name="start"/>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=RDPPacketFactory">
  <Call name="addType">
    <!-- The untyped handler looks for the service type AV in the packer to
- determine whether the request is for a service profile (service
- type == outbound) or a user profile (no service type)-->
  <Arg>Untyped</Arg>
  <Arg>com.cisco.sesm.rdp.UntypedPacket</Arg>
  </Call>
  <Call name="addType">

```

```

    <!-- There are six user logon handlers; userLogonPacket (authenticates),
    - UserLogonFramedPacket (authenticates and adds a Service-type=2
    - (Framed user) ), UserLogonFramedAddServicesPacket (authenticates
    - and adds a Service-type=2 and services, i.e. authorizes),
    - UserLogonAddServices (authenticates and authorizes),
    - UserProxyAuthPacket (authenticates via a proxy) and
    - UserProxyAuthAddServicePacket (authenticates via a proxy and
    - authorizes) -->
    <Arg>UserLogon</Arg>
    <Arg>com.cisco.sesm.rdp.UserLogonFramedAddServicesPacket</Arg>
  </Call>
  <Call name="addType">
    <Arg>ProfileRequest</Arg>
    <!-- Attempts to match the password to the PASSWORD: attribute and
    - return the matching value -->
    <Arg>com.cisco.sesm.rdp.ProfileRequestPacket</Arg>
  </Call>
  <!-- Following attribute and type handle service profiles -->
  <Call name="setAttribute">
    <Arg>PASSWORD:servicecisco</Arg>
    <Arg>ServiceRequest</Arg>
  </Call>
  <Call name="addType">
    <Arg>ServiceRequest</Arg>
    <Arg>com.cisco.sesm.rdp.ServiceProfilePacket</Arg>
  </Call>
  <!-- Following attribute and type handle group profiles -->
  <Call name="setAttribute">
    <Arg>PASSWORD:groupcisco</Arg>
    <Arg>GroupRequest</Arg>
  </Call>
  <Call name="addType">
    <Arg>GroupRequest</Arg>
    <Arg>com.cisco.sesm.rdp.GroupProfilePacket</Arg>
  </Call>
  <!-- Following attribute and type handle next hop profiles -->
  <Call name="setAttribute">
    <Arg>PASSWORD:nexthopcisco</Arg>
    <Arg>NextHopRequest</Arg>
  </Call>
  <Call name="addType">
    <Arg>NextHopRequest</Arg>
    <Arg>com.cisco.sesm.rdp.NextHopPacket</Arg>
  </Call>
  <Call name="addType">
    <Arg>Unknown</Arg>
    <!-- Does not respond to the request -->
    <Arg>com.cisco.sesm.rdp.DiscardPacket</Arg>
  </Call>
  <!-- Example use of a Proxy handler.
    String after ';' is name of AAA connection (see AAAMBean below)
  <Call name="addType">
    <Arg>ProxyNextHop</Arg>
    <Arg>com.cisco.sesm.rdp.ProxyPacket;Proxy</Arg>
  </Call>
  -->
</Configure>

<!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=RDP">
<Set id="RDPsecret" name="secret">cisco</Set>
<Set name="localIPAddress">10.3.3.1</Set>
<Set name="localPort" type="int"><SystemProperty name="application.portno"
default="1812"/></Set>

```

```

    <Set name="minThreads" type="int">10</Set>
    <Set name="maxThreads" type="int">256</Set>
    <Set name="maxIdleTimeMs" type="int">10000</Set>
    <!-- This option turns on 3-key authentication. When this is set, one of the -->
    <!-- RADIUS attributes in the access request is matched to the attribute in the -->
    <!-- user profile in the directory -->
    <Set name="threeKeyAuth" type="boolean">>false</Set>
    <!-- When 3-key authentication is turned on, this option determines which RADIUS -->
    <!-- attribute is used for authentication. Typical values are: -->
    <!-- CALLED_STATION_ID (APN) = 30 -->
    <!-- CALLING_STATION_ID (MSISDN) = 31 -->
    <!-- NAS_IDENTIFIER = 32 -->
    <Set name="authAttribute" type="int">31</Set>
    <!-- This section is used for specifying a client list for the RADIUS server -->
    <!-- This variable turns client list usage on or off. -->
    <!-- If it is off, the client list that follows has no effect. -->
    <Set name="useClientList" type="boolean">>true</Set>
    <!-- The following line is an example client specification that can be -->
    <!-- copied and modified to create a client list. -->
    <!-- The parameters are: -->
    <!-- String: client name -->
    <!-- String client IP address -->
    <!-- String shared secret -->
    <Call name="addClient">
        <Arg>SSG-first</Arg>
        <Arg>10.4.4.4</Arg>
        <Arg>cisco</Arg>
    </Call>
    <!-- End of client list section -->
    <Call name="startRDP"/>
</Configure>

<!-- ===== -->
<!-- Uncomment and modify this element when run in proxy mode -->
<Configure jmxname="com.cisco.sesm:name=AAA,connection=Proxy">
    <Set name="throttle" type="int">256</Set>
    <Set name="timeOut" type="int">4</Set>
    <Set name="retryCount" type="int">1</Set>
    <Set name="primaryIP">127.0.0.2</Set>
    <Set name="primaryPort" type="int">1812</Set>
    <Set id="AAASecret" name="secret">cisco</Set>
    <Set name="secondaryIP">127.0.0.3</Set>
    <Set name="secondaryPort" type="int">1812</Set>
    <Call name="open"/>
</Configure>
-->

</XmlConfig>

```

## Sample CDAT MBean Configuration File

An example cdat.xml file follows.

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2001,2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container independent configuration for the CDAT web application.
Container specific configuration can be found at:
    $INSTALLROOT/$CONTAINER/config/cdat.xml
-->

```

```

<XmlConfig>
  <!-- ===== -->
  <Instantiate order="1"
    class="com.cisco.sesm.jmx.LoggerMBean"
    jmxname="com.cisco.sesm:name=Logger" />

  <Instantiate order="99"
    class="com.sun.jdmk.comm.HtmlAdaptorServer"
    jmxname="com.cisco.sesm:name=ManagementConsole">
    <Arg type="int">
      <SystemProperty name="management.portno"/>
    </Arg>
    <Arg>
  <Array class="com.sun.jdmk.comm.AuthInfo">
    <Item>
      <New class="com.sun.jdmk.comm.AuthInfo">
        <Arg>MgmtUser</Arg>
        <Arg>MgmtPassword</Arg>
      </New>
    </Item>
  </Array>
  </Arg>
</Instantiate>

  <!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=Logger">
    <Set name="debug" type="boolean"><SystemProperty name="cdat.debug"
default="false"/></Set>
    <Set name="debugPatterns"></Set>
    <Set name="debugThreads"></Set>
    <Set name="debugVerbosity">LOW</Set>
    <Set name="logDateFormat"><SystemProperty name="cdat.logDateFormat"
default="HHmmss.SSS"/></Set>
    <Set name="logFile"><SystemProperty name="application.log"
default="./logs"/>/>yyyy_mm_dd.application.log</Set>
    <Set name="logFrame" type="boolean">>false</Set>
    <Set name="logStack" type="boolean">>false</Set>
    <Set name="logThread" type="boolean">>false</Set>
    <Set name="logToErr" type="boolean"><SystemProperty name="cdat.logToErr"
default="false"/></Set>
    <Set name="trace" type="boolean">>true</Set>
    <Set name="warning" type="boolean">>true</Set>
  </Configure>

  <!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=ManagementConsole">
    <Call name="start"/>
  </Configure>

  <!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=CDAT">
    <Set name="naming" type="String">cn</Set>
    <Set name="sessionTimeout" type="int">600</Set>
    <Set name="maxVariables" type="int">40</Set>
    <Set name="queryMaxResults" type="int">100</Set>
    <Set name="queryTimeout" type="int">0</Set>
  </Configure>
</XmlConfig>

```

# Sample SPE MBean Configuration File

An example SPE configuration file (dess-auth/config/config.xml) follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2001 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the dess-auth configuration -->

<XmlConfig>
  <!-- ===== -->
  <Instantiate order="2"
    class="com.cisco.sesm.dessauth.ConnectionMBean"
    jmxname="com.cisco.sesm:name=Directory,type=Connection,instance=Primary"
  />

  <Instantiate order="2"
    class="com.cisco.sesm.dessauth.ConnectionMBean"
    jmxname="com.cisco.sesm:name=Directory,type=Connection,instance=Secondary"
  />

  <Instantiate order="3"
    class="com.cisco.sesm.dessauth.DirectoryMBean"
    jmxname="com.cisco.sesm:name=Directory" />

  <!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=Directory,type=Connection,instance=Primary">
  <Set name="poolSize" type="int">2</Set>
  <Set name="URL">ldap://127.0.0.1:389</Set>
  <Set name="principal">cn=admin,ou=sesm,o=cisco</Set>
  <Set name="credentials"></Set>
  </Configure>

  <Configure jmxname="com.cisco.sesm:name=Directory,type=Connection,instance=Secondary">
  <Set name="poolSize" type="int">2</Set>
  <Set name="URL">ldap://127.0.0.1:389</Set>
  <Set name="principal">cn=admin,ou=sesm,o=cisco</Set>
  <Set name="credentials"></Set>
  </Configure>

  <Configure jmxname="com.cisco.sesm:name=Directory">
  <Set name="connectionNameRoot">com.cisco.sesm:name=Directory,type=Connection,*</Set>
  <Set name="factory">com.cisco.cns.security.jndi.JNDIConnection</Set>
  <Set name="context">ou=sesm,o=cisco</Set>
  <Set name="DESSPrincipal">cn=admin,ou=sesm,o=cisco</Set>
  <Set name="alwaysGetAllAttributes" type="boolean">>false</Set>

  <Set name="traceFileName"><SystemProperty name="application.log"
default="./logs"/>/>/dess.log</Set>
  <Set name="traceLevel">NONE</Set>
  <Set name="printTraceToConsole" type="boolean">>false</Set>
  <Set name="stackTrace" type="boolean">>false</Set>

  <Set name="cacheMaxObjects" type="int">50000</Set>

  <!-- Save at least cacheMinFreeMem% VM memory. -->
  <!-- i.e. Cache can occupy 100-cacheMinFreeMem% memory -->
  <Set name="cacheMinFreeMem" type="int">10</Set>

  <!-- All timeout values are in seconds -->
  <Set name="cacheSessionTimeout" type="int">600</Set>
  <Set name="cacheExpireInterval" type="int">600</Set>
```



```

<Set name="cacheObjectTimeout" type="int">600</Set>
<Call name="commit"/>
  </Configure>
</XmlConfig>

```

## Sample Captive Portal Configuration File

An example captiveportal.xml file follows:

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container independent configuration for the captiveportal web
application.
Container specific configuration can be found at:
$INSTALLROOT/$CONTAINER/config/captiveportal.jetty.xml
-->

<XmlConfig>
  <!-- ===== -->
  <Instantiate order="1"
    class="com.cisco.sesm.jmx.LoggerMBean"
    jmxname="com.cisco.sesm:name=Logger"/>

  <Instantiate order="99"
    class="com.sun.jdmk.comm.HtmlAdaptorServer"
    jmxname="com.cisco.sesm:name=ManagementConsole">
    <Arg type="int">
      <SystemProperty name="management.portno"/>
    </Arg>
    <Arg>
  <Array class="com.sun.jdmk.comm.AuthInfo">
    <Item>
      <New class="com.sun.jdmk.comm.AuthInfo">
        <Arg>MgmtUser</Arg>
        <Arg>MgmtPassword</Arg>
      </New>
    </Item>
  </Array>
  </Arg>
</Instantiate>

  <!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=Logger">
    <Set name="debug" type="boolean"><SystemProperty name="captiveportal.debug"
default="false"/></Set>
    <Set name="debugPatterns"></Set>
    <Set name="debugThreads"></Set>
    <Set name="debugVerbosity">LOW</Set>
    <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS</Set>
    <Set name="logFile"><SystemProperty name="application.log"
default="./logs"/>/>yyyy_mm_dd.application.log</Set>
    <Set name="logFrame" type="boolean">>false</Set>
    <Set name="logStack" type="boolean">>false</Set>
    <Set name="logThread" type="boolean">>true</Set>
    <Set name="logToErr" type="boolean"><SystemProperty name="captiveportal.logToErr"
default="false"/></Set>
    <Set name="trace" type="boolean">>true</Set>
    <Set name="warning" type="boolean">>true</Set>
  </Configure>

```

```

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=ManagementConsole">
  <Call name="start"/>
</Configure>

<!-- ===== -->
<Configure class="com.cisco.sesm.core.model.SESMMBean"
  jmxname="com.cisco.sesm:name=SESM">
  <!-- Only the authenticationSPI is used, but for completeness give
    a mode in each case, which requires the full set of SPIs -->
  <Call name="defineMode">
    <Arg>Demo</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoAuthenticationService</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoAuthorizationService</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoConnectionService</Arg>
    <Arg>com.cisco.sesm.spis.demo.DemoServiceProfileService</Arg>
  </Call>
  <Call name="defineMode">
    <Arg>RADIUS</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthentication</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthorization</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSConnection</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSServiceProfile</Arg>
  </Call>
  <!--
    - There is a performance consideration in retrieving the subscriber profile.
    - LDAP mode is not used, as the profile is not required. For usage
    - consistency, a mode of this name is defined here which uses the RADIUS SPIs.
  -->
  <Call name="defineMode">
    <Arg>LDAP</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthentication</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSAuthorization</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSConnection</Arg>
    <Arg>com.cisco.sesm.spis.radius.RADIUSServiceProfile</Arg>
  </Call>
  <!--
    - This determines the SESM model mode of operation. A mode of operation
    - determines how SESM connects to hardware.
  -->
  <Set name="mode"><SystemProperty name="sesm.mode" default="Demo"/></Set>
  <!--
    - This boolean turns on or off the capability to perform
    - single sign-on. In single sign on mode, a user only has to
    - authenticate once and SESM merely checks that the user has
    - been authenticated.
  -->
  <Set name="singleSignOn" type="boolean">true</Set>
  <!--
    - This is the number of seconds between clearing group
    - and service caches.
  -->
  <Set name="profileCachePeriod" type="int">600</Set>
  <!--
    - This is the minimum length of time in seconds that an SESMSession
    - is held in memory without being accessed. SESMSessions are checked
    - regularly according to the profileCachePeriod.
    - If this is set to 0 (or undefined) profileCachePeriod*2 is used.
  -->
  <Set name="sessionCachePeriod" type="int">1200</Set>
  <!--
    - This sets the minimum amount of memory required before
    - a SESM session can be created or authenticated.
    - This is in order to prevent the application running out of memory.
  -->

```

```

-->
<Set name="memRequired" type="long">10485760</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=SSG">
<!--
- Maxmimum number of simultaneous requests allowed to each SSG. Extra
- requests will be placed on a queue and issued as responses are received
- or timeout.
-->
-->
<Set name="throttle" type="int">20</Set>
<!--
- Here we define attributes for RADIUS communication with the SSG If
- we are running with Port Bundle Host key then we need only define
- the global attributes for all of the SSGs.
-->
-->
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>TIMEOUTSECS</Arg><Arg>10</Arg></Call>
<Call name="setGlobalAttribute"><Arg>RETRIES</Arg><Arg>3</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<!--
- A non zero value here, the default should be 4, will turn Port
- Bundle Host Key on.
-->
-->
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>
<Call
name="setGlobalAttribute"><Arg>PORT_BUNDLE_HOST_KEY_SWITCH</Arg><Arg>>false</Arg></Call>
<!--
- This value may be true or false. True is implied by a non zero
- BUNDLE_LENGTH. If the BUNDLE_LENGTH is non zero, then this value
- will be ignored. As a BUNDLE_LENGTH of 0 is a legal value, however,
- the Port Bundle Host Key feature can can also be turned on here
- when the BUNDLE_LENGTH is 0, which it would be for persistent
- connections.

<Call
name="setGlobalAttribute"><Arg>PORT_BUNDLE_HOST_KEY_SWITCH</Arg><Arg>>true</Arg></Call>

-->
<!--
- If we need to map from a client IP address to an SSG explicitly,
- then we could have an entry like this:

<Call
name="setSubnetAttribute"><Arg>213.0.0.0</Arg><Arg>255.0.0.0</Arg><Arg>IP</Arg><Arg>195.24
5.182.2</Arg></Call>

- which would map the client subnet 213.0.0.0 to the SSG at
- 195.245.182.2 with the global parameters defined above for
- the RADIUS protocol.
-->

</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=captiveportal">
<!--
- The install requires these booleans to turn the different features on or off.
- Disabling a particular feature can also be achieved by removing the entire
- corresponding entry, or removing the corresponding port argument.
-->
-->
<Set name="userRedirectOn" type="boolean">true</Set>

```

```

<Set name="initialCaptiveOn" type="boolean">true</Set>
<Set name="advertisingCaptiveOn" type="boolean">true</Set>
<Set name="serviceRedirectOn" type="boolean">true</Set>

<!--
- This is the URL that the Captive Portal application will redirect
- to for unauthenticated user redirects.
- It should point to the service application.
-->
<Set name="userRedirectURL">http://<SystemProperty name="serviceportal.host"
default="www.cisco.com"/>:<SystemProperty name="serviceportal.port"
default="80"/>/home</Set>

<!--
- Requests on this incoming port are for unauthenticated user redirects
-->
<Set name="userRedirectPort"><SystemProperty name="userRedirect.port"
default="8090"/></Set>

<!--
- This is the URL that the Captive Portal application will redirect
- to for default initial captive redirects.
- It should point to the message application.
-->
<Set name="initialCaptiveURL">http://<SystemProperty name="messageportal.host"
default="www.cisco.com"/>:<SystemProperty name="messageportal.port"
default="80"/>/initial</Set>

<!--
- Requests on this incoming port are for
- default initial captive redirects
-->
<Set name="initialCaptivePort"><SystemProperty name="initialCaptive.port"
default="8091"/></Set>

<!--
- Specifies the duration for the default initial captive redirects
-->
<Set name="initialCaptiveDuration">10</Set>

<!--
- This is the URL that the Captive Portal application will redirect
- to for default advertising captive redirects.
- It should point to the message application.
-->
<Set name="advertisingCaptiveURL">http://<SystemProperty name="messageportal.host"
default="www.cisco.com"/>:<SystemProperty name="messageportal.port"
default="80"/>/advertising</Set>

<!--
- Requests on this incoming port are for
- default advertising captive redirects
-->
<Set name="advertisingCaptivePort"><SystemProperty name="advertisingCaptive.port"
default="8092"/></Set>

<!--
- Specifies the duration for the default advertising captive redirects
-->
<Set name="advertisingCaptiveDuration">10</Set>

<!--
- This is the URL that the Captive Portal application will redirect

```

```

- to if an unconnected service redirect has no specific URL given in
- its configuration below. The configuration of the Service Portal
- application can be checked as to how it handles the request.
-->
<Set name="serviceRedirectDefaultURL">http://<SystemProperty name="serviceportal.host"
default="www.cisco.com"/>:<SystemProperty name="serviceportal.port"
default="80"/>/serviceRedirect</Set>

<!--
- These define service redirects, consisting of:
- incoming port, optional URL out and optional service name
- The redirect for the default group (the first listed here)
- would not have a service name specified for normal operation
-->
<Call name="defineServiceRedirect">
  <Arg><SystemProperty name="defaultServiceRedirect.port" default="8093"/></Arg>
  <Arg></Arg>
  <Arg></Arg>
</Call>

<Call name="defineServiceRedirect">
  <Arg><SystemProperty name="serviceRedirect1.port" default="8094"/></Arg>
  <Arg><SystemProperty name="serviceRedirect1.URL" default=""/></Arg>
  <Arg><SystemProperty name="serviceRedirect1.service" default="service1"/></Arg>
</Call>

<Call name="defineServiceRedirect">
  <Arg><SystemProperty name="serviceRedirect2.port" default="8095"/></Arg>
  <Arg><SystemProperty name="serviceRedirect2.URL" default=""/></Arg>
  <Arg><SystemProperty name="serviceRedirect2.service" default="service2"/></Arg>
</Call>

<Call name="defineServiceRedirect">
  <Arg><SystemProperty name="serviceRedirect3.port" default="8096"/></Arg>
  <Arg><SystemProperty name="serviceRedirect3.URL" default=""/></Arg>
  <Arg><SystemProperty name="serviceRedirect3.service" default="service3"/></Arg>
</Call>

<!--
- This is only used to detect loops: if the request host and this match,
- as well as the request port and the listener port, redirect to errorURL.
- Accepts a comma-separated list of aliases and/or addresses.
-->
<Set name="host">127.0.0.1</Set>

<!--
- This is the URL that the Captive Portal application will redirect
- to if it does not find a URL to redirect to for the given port that
- the request came in on. It should point to the service portal.
-->
<Set name="errorURL">http://<SystemProperty name="serviceportal.host"
default="www.cisco.com"/>:<SystemProperty name="serviceportal.port"
default="80"/>/home</Set>

<!--
- These are the parameter names passed in the query string of the URL to
- indicate the name of the service and the URL as appropriate.
- The message redirect parameters apply to initial and advertising captive
- To avoid any attempt to obtain a username by captive portal,
- the two arguments for the subscriber parameter should be empty or removed.
-->
<Set name="userRedirectURLParam">CPURL</Set>
<Set name="serviceRedirectURLParam">serviceURL</Set>
<Set name="serviceRedirectServiceParam">service</Set>

```

```

    <Set name="serviceRedirectSubscriberParam"></Set>
    <Set name="messageRedirectURLParam">CPURL</Set>
    <Set name="messageRedirectSubscriberParam">CPSUBSCRIBER</Set>
    <Set name="messageRedirectDurationParam">CPDURATION</Set>

</Configure>

<!-- ===== -->

</XmlConfig>

```

## Sample Message Portal Configuration File

An example messageportal.xml file follows:

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE XmlConfig PUBLIC "-//Cisco Systems//DTD XmlConfig 1.1//EN"
"http://www.cisco.com/sesm/xmlconfig_1_1.dtd">
<!-- Copyright (c) 2002 by Cisco Systems, Inc. All rights reserved. -->
<!-- This is the container independent configuration for the messageportal web
application.
Container specific configuration can be found at:
    $INSTALLROOT/$CONTAINER/config/messageportal.xml
-->

<XmlConfig>
  <!-- ===== -->
  <Instantiate order="1"
    class="com.cisco.sesm.jmx.LoggerMBean"
    jmxname="com.cisco.sesm:name=Logger" />

  <Instantiate order="99"
    class="com.sun.jdmk.comm.HtmlAdaptorServer"
    jmxname="com.cisco.sesm:name=ManagementConsole">
    <Arg type="int">
      <SystemProperty name="management.portno"/>
    </Arg>
    <Arg>
  <Array class="com.sun.jdmk.comm.AuthInfo">
    <Item>
      <New class="com.sun.jdmk.comm.AuthInfo">
        <Arg>MgmtUser</Arg>
        <Arg>MgmtPassword</Arg>
      </New>
    </Item>
  </Array>
    </Arg>
  </Instantiate>

  <!-- ===== -->
  <Configure jmxname="com.cisco.sesm:name=Logger">
    <Set name="debug" type="boolean"><SystemProperty name="messageportal.debug"
default="false"/></Set>
    <Set name="debugPatterns"></Set>
    <Set name="debugThreads"></Set>
    <Set name="debugVerbosity">LOW</Set>
    <Set name="logDateFormat"><SystemProperty name="messageportal.logDateFormat"
default="HHmmss.SSS"/></Set>
    <Set name="logFile"><SystemProperty name="application.log"
default="./logs"/>/>yyyy_mm_dd.application.log</Set>
  </Configure>

```

```

    <Set name="logFrame" type="boolean">false</Set>
    <Set name="logStack" type="boolean">false</Set>
    <Set name="logThread" type="boolean">false</Set>
    <Set name="logToErr" type="boolean"><SystemProperty name="messageportal.logToErr"
default="false"/></Set>
    <Set name="trace" type="boolean">true</Set>
    <Set name="warning" type="boolean">true</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=ManagementConsole">
    <Call name="start"/>
</Configure>

<!-- ===== -->
<Configure class="com.cisco.sesm.core.model.SESMMBean"
    jmxname="com.cisco.sesm:name=SESM">
    <Call name="defineMode">
        <Arg>Demo</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoAuthenticationService</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoAuthorizationService</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoConnectionService</Arg>
        <Arg>com.cisco.sesm.spis.demo.DemoServiceProfileService</Arg>
    </Call>
    <Call name="defineMode">
        <Arg>LDAP</Arg>
        <Arg>com.cisco.sesm.spis.dess.DESSAuthenticationService</Arg>
        <Arg>com.cisco.sesm.spis.dess.DESSAuthorizationService</Arg>
        <Arg>com.cisco.sesm.spis.dess.DESSServiceConnectionService</Arg>
        <Arg>com.cisco.sesm.spis.dess.DESSServiceProfileService</Arg>
    </Call>
    <!--
    - This determines the SESM model mode of operation. A mode of operation
    - determines how SESM connects to hardware.
    -->
    <Set name="mode"><SystemProperty name="sesm.mode" default="Demo"/></Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=SESMDemoMode">
    <!--
    - This is the demo data file. It is in the format of a Merit
    - dictionary with special extensions for this software.
    -->
    <Set name="demoDataFile"><SystemProperty
name="application.home"/>/config/demo.txt</Set>
</Configure>

<!-- ===== -->
<!-- Settings for the DESS SPI. -->
<Configure jmxname="com.cisco.sesm:name=DESSMode">
    <!-- The time in seconds between checking the authorization tokens. -->
    <Set name="tokenCheckInterval" type="int">300</Set>
    <!-- The age of a token in seconds (time since last used) for it to be removed from
cache. -->
    <Set name="tokenMaxAge" type="int">600</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=messageportal">

    <!-- default page to use if no interests obtained from subscriber profile -->
    <Set name="defaultPage">default.jsp</Set>
    <!-- default URL to redirect to, if none given in query string of request URL -->

```

```

    <Set name="defaultURL">http://<SystemProperty name="serviceportal.host"
default="10.50.5.1"/>:<SystemProperty name="serviceportal.port" default="8080"/></Set>
    <!-- duration in seconds, if none given in query string of request URL -->
    <Set name="defaultDuration">15</Set>
    <!-- ignore subscriber profile and only display default page -->
    <Set name="ignoreProfile" type="boolean">true</Set>
    <!-- redirect to originally requested URL after displaying message page -->
    <Set name="redirectOn" type="boolean">true</Set>

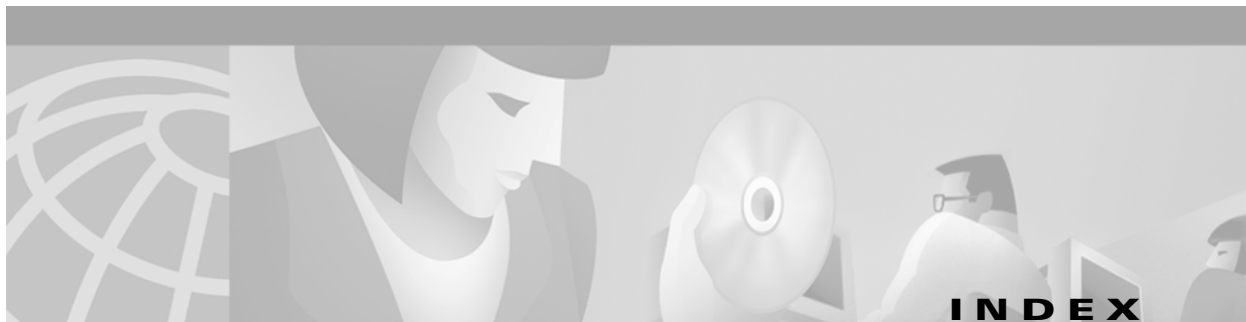
    <!-- Possible interests, obtained from subscriber profile -->
    <!-- Only the page for the first located interest is displayed -->
    <Set name="interests">
cinema,
science,
internet,
news,
sports,
travel,
finance,
community
    </Set>

    <!-- Corresponding pages, using any 1-char string to use default page instead -->
    <Set name="interestPages">
cinema.jsp,
.,
internet.jsp,
news.jsp,
sports.jsp,
travel.jsp,
finance.jsp,
community.jsp
    </Set>
    </Configure>

</XmlConfig>

```





---

## Symbols

- .iss file [5-14](#)
- .properties file [5-14](#)

---

## A

- AAA
  - See RADIUS
- AAA MBean [6-24](#)
- AAASecret attribute [6-35](#)
- access control lists
  - See ACLs
- access point name
  - See APN
- access reject message [10-12](#)
- accounting
  - interfaces [3-12](#)
  - RADIUS [D-1, D-11](#)
  - solutions [3-12, D-11](#)
- ACLs [D-6, D-10](#)
- addClient call [6-34](#)
- addDimension call [6-25](#)
- AddListener [6-11, 6-12](#)
- add services option [5-23](#)
- AddWebApplication [6-14](#)
- advertisingCaptiveDuration attribute [8-16, 8-21](#)
- advertisingCaptiveOn attribute [8-15, 8-27](#)
- advertisingCaptivePort attribute [8-16](#)
- advertisingCaptiveURL attribute [8-15](#)
- advertising redirection
  - configuring [5-27, 8-15, 8-17, 8-26](#)
  - demonstrating [8-13](#)
  - description [3-9, 8-4](#)
  - duration [5-27](#)
  - hobbies [8-10, 8-19](#)
  - HTTP query parameters [8-5](#)
  - port [5-27](#)
  - profile attributes [D-10](#)
- Allow Clear Text Passwords [5-6](#)
- alternative configurations, captive portal [8-7](#)
- alwaysGetAllAttributes attribute [6-38](#)
- always-on services [3-5](#)
- API [1-5, 1-6, 6-44](#)
- APN [3-3, 6-34, D-9](#)
- append attribute [6-9, 6-13](#)
- application.home [6-14, 7-5](#)
- application.log [6-13, 6-17, 7-5, 10-5](#)
- application.portno [7-5](#)
- application programming interface
  - See API
- applications
  - CPU utilization [7-8](#)
  - customizing [1-6, 6-44](#)
  - descriptions [1-2, 1-7](#)
  - J2EE [1-9](#)
  - list [1-2](#)
  - memory requirements [7-8](#)
  - names [7-3](#)
  - portals
    - configuring [5-17, 6-14](#)
    - customized pages [3-2](#)
    - defined as NAS client [D-2](#)
    - directory communication [9-9](#)
    - logging on [7-6](#)
    - names [6-45](#)

- personalized [3-2](#)
- ports [4-4, 5-17](#)
- RADIUS communication [5-19](#)
- RADIUS server communication [9-5](#)
- relationship to J2EE server [6-7](#)
- role [2-2](#)
- SSG communication [5-18, 9-2](#)
- stopping [7-6](#)
- timeouts [6-22](#)
- troubleshooting [10-1](#)
- sample [1-5](#)
- startup scripts [7-3](#)
- stopping [7-6](#)
- attribute dictionary [D-3](#)
- authAttribute attribute [6-34](#)
- authentication
  - 2-key [3-3](#)
  - 3-key [3-3, 6-33](#)
  - NDS [5-6](#)
  - options [3-2](#)
  - PPP clients [3-4](#)
  - processing requests for [2-5, 2-8](#)
  - reauthentication [3-4](#)
  - service [3-4](#)
  - setting RADIUS port [D-1](#)
  - single sign-on [3-4](#)
  - type [D-5](#)
  - using captive portal [8-4](#)
  - See also unauthenticated user redirections
- AuthInfo attribute [6-18](#)
- AUTH library [1-8](#)
- authorization [3-4](#)
- autoConnect attribute [6-20](#)
- automatic connections
  - changing [6-43](#)
  - configuring [6-42, D-10](#)
  - description [3-5, 6-42](#)
  - disconnecting [6-43](#)
  - RADIUS configuration example [D-11](#)

- RDP [6-20](#)
- status [6-43](#)
- troubleshooting [6-43](#)

---

## B

- bandwidths, services on different [3-6](#)
- billing interfaces [3-12](#)
- branding
  - awareness [6-44](#)
  - using MBean configuration attributes [3-11, 6-30](#)
  - using user groups [3-10, 4-9](#)
- browsers, supported [1-13, 4-4](#)
- BUNDLE\_LENGTH attribute [6-22, 6-29, 9-2](#)
- bundled software [1-8](#)

---

## C

- cacheExpireInterval [6-39](#)
- cacheMinFreeMem [6-39](#)
- cacheObjectTimeout [6-39](#)
- cacheSessionTimeout [6-39](#)
- caching
  - cache size [6-39](#)
  - directory data [6-38](#)
  - memory usage [6-39](#)
  - profiles [6-20](#)
  - RDP [6-43](#)
  - SESM [6-20](#)
  - SPE attributes [6-38](#)
- CALLED\_STATION\_ID [3-3, 6-34](#)
- CALLING\_STATION\_ID [3-3, 6-34](#)
- captiveportal.jetty.xml [8-14](#)
- captiveportal.xml [8-14, 8-15, 8-27](#)
- Captive Portal application
  - alternatives [8-7](#)
  - benefits [8-7](#)
  - configuring [8-15](#)

- description [1-7, 8-5](#)
- installing [5-24](#)
- IP address [5-24](#)
- ports [5-24](#)
- captive portal solution
  - alternative configurations [8-7](#)
  - configuration files [6-3](#)
  - demonstration [8-12](#)
  - description [1-7, 3-8, 8-1](#)
  - diagram [8-2](#)
  - eliminating J2EE listeners [8-7](#)
  - eliminating redirection types [8-7](#)
  - groups [8-22](#)
  - installing [5-16, 8-8](#)
  - NWSP role [1-7, 8-6](#)
  - prepaid services and [3-13](#)
  - required Cisco IOS releases [8-2](#)
  - sample profiles [8-10](#)
  - startup scripts [8-11](#)
  - troubleshooting [8-26](#)
- CDAT
  - configuring [6-36, 6-37](#)
  - cookies [6-36](#)
  - description [1-8](#)
  - installing [5-16, 5-21](#)
  - logging in [6-41](#)
  - MBean [6-37](#)
  - port number [5-21](#)
  - session tuning [6-37](#)
  - starting [7-3](#)
  - stopping [7-6](#)
  - timeouts [6-37](#)
  - virtual memory [6-39](#)
- cdat.jetty.xml [6-8](#)
- cdat.xml [6-36](#)
- certificates
  - obtaining license [5-11](#)
  - SSL [A-2](#)
- changing
  - configuration files [6-1](#)
  - JRE location [5-3](#)
  - JSPs [10-9](#)
- CHAP [D-5](#)
- Cisco Access Registrar [1-11, D-12](#)
- Cisco-AVpairs [D-6, D-10](#)
- Cisco Content Services Switch 11000 [2-3, 3-12](#)
- Cisco Distributed Administration Tool
  - See CDAT
- Cisco IOS, required releases
  - captive portal features [8-2](#)
  - general [1-10](#)
  - port-bundle host key [B-2](#)
  - TCP redirect commands [8-10](#)
- Cisco Service Selection Dashboard [1-2](#)
- Cisco Subscriber Policy Engine
  - See SPE
- Clear Text Passwords [5-6](#)
- clients
  - RADIUS server [9-5, D-2](#)
  - RDP [5-23, 5-24, 6-34](#)
  - RDP as RADIUS [9-11](#)
  - SSG subnets [5-18](#)
- Client subnet attribute [5-18](#)
- cn [5-5, 5-20](#)
- common name
  - See cn
- compressed images [5-12](#)
- concurrent services [B-2, D-5](#)
- config.xml [6-37, 9-9](#)
- ConfigAgent [6-2, 6-5, 6-45](#)
- configuration files
  - customizing [6-45](#)
  - editing [6-1](#)
  - location [10-11](#)
  - MBean [6-1, 6-2](#)
  - See also J2EE, MBeans
- configuring
  - automatic connections [6-42](#)

Captive Portal [8-15](#)  
 CDAT [6-37](#)  
 directory access [6-38](#)  
 Jetty server [6-8](#)  
 Message Portal [8-17](#)  
 portal applications [6-14](#)  
 RDP [6-37](#)  
 SPE [6-37](#)  
 confirmAtAccountLogoff attribute [6-25](#)  
 confirmAtServiceLogoff attribute [6-25](#)  
 confirmAtServiceLogon attribute [6-25](#)  
 confirmMutex Disconnect attribute [6-21](#)  
 connection  
   object [2-5, 2-8](#)  
   requests [2-3](#)  
   to services [6-25](#)  
   types, RDP [6-35](#)  
   See also automatic connections  
 Connection attribute [6-24](#)  
 console  
   installation mode [5-13](#)  
   iPlanet [5-8](#)  
   management [5-17, 6-18](#)  
   NDS (ConsoleOne) [5-5, 5-6](#)  
 constructing MBeans [6-2](#)  
 containers [6-7](#)  
 content applications [8-6](#)  
 context  
   attribute [6-38](#)  
   directory [9-8](#)  
   iPlanet [5-7](#)  
   NDS [5-5](#)  
   path attribute [6-14](#)  
 cookies [6-36, D-6](#)  
 core model  
   description [1-6](#)  
   installing [5-16](#)  
 CPDURATION query parameter [8-5, 8-21](#)  
 CPSUBSCRIBER query parameter [8-5, 8-28](#)

CPURL query parameter [8-5](#)  
 CPU utilization [7-8](#)  
 credentialMax Length attribute [6-25](#)  
 credentials attribute, SPE [6-38](#)  
 CSS 11000 [2-3, 3-12](#)  
 custom installations [5-16](#)  
 customizing  
   portal applications [6-44](#)  
   portal pages [3-2](#)  
   portals [1-6](#)  
   RDP [E-1](#)

---

## D

debug  
   attribute [6-10, 6-16](#)  
 debugging [10-4, 10-5](#)  
   configuring [6-9, 6-16](#)  
 debugPatterns attribute [6-10, 6-16](#)  
 debugThreads attribute [6-16](#)  
 debugTriggers attribute [6-10](#)  
 debugVerbosity attribute [6-16](#)  
 defaultDuration attribute [8-18, 8-21](#)  
 default network [1-1, 2-1, 2-3, B-2](#)  
 defaultPage attribute [8-18](#)  
 defaultURI attribute [6-25, 8-20](#)  
 defaultURL attribute [8-18](#)  
 defineServiceRedirect attribute [8-16](#)  
 demo.txt [1-11, 4-6, 6-21](#)  
 demoDataFile attribute [4-6, 6-21](#)  
 Demo mode  
   attributes [6-19](#)  
   branding example [4-9](#)  
   data [6-21](#)  
   description [1-4, 1-5](#)  
   installing [4-2, 4-4, 5-16](#)  
   logging on [4-7](#)  
   quick start [4-2](#)  
   setup option [4-4](#)

- starting [4-5](#)
  - switching to [6-19](#)
  - user IDs [4-7](#)
  - deployment modes
    - RDP [1-7](#)
    - SESM [1-4](#)
    - switching [1-5](#)
    - See also Demo mode, LDAP mode, RADIUS mode
  - DESS library [1-8](#)
  - DESSPrincipal attribute, SPE [6-38](#)
  - destination
    - service [D-5](#)
    - URL [8-11](#)
  - device awareness [3-11](#)
  - diagrams
    - captive portal solution [8-2](#)
    - LDAP mode [2-7](#)
    - RADIUS mode [2-4](#)
    - SESM network [2-1](#)
  - dictionary, RADIUS [D-3](#)
  - directory
    - access [6-38](#)
    - caching [6-38, 6-39](#)
    - configuring in SESM [5-20](#)
    - container
      - configuring [5-21, 9-8](#)
      - user ID [5-21, 6-38](#)
    - context [9-8](#)
    - extending schema [1-8, 5-29, 6-40](#)
    - installation results [5-30, 10-11](#)
    - IP address [5-20, 6-38, 9-8](#)
    - logging activity [6-38](#)
    - MBean [6-38, 6-39](#)
    - meta schema [5-20](#)
    - modifying [5-29](#)
    - organization [5-21, 9-8](#)
    - password [5-20, 6-38](#)
    - portal communication [9-9](#)
    - ports [5-20, 6-38, 9-8](#)
    - RDP communication [9-8](#)
    - running during SESM install [5-5](#)
    - supported platforms [1-11](#)
    - user ID [5-20, 6-38, 9-8](#)
  - disconnecting
    - auto connect services [6-43](#)
    - services [2-5, 2-8, 3-1](#)
  - disk space [5-2](#)
  - distinguished name
    - See dn.
  - dn [5-20](#)
  - DNS [2-3, D-5](#)
  - docroot directory [10-10](#)
  - domain names [D-5](#)
  - Domain Name System [2-3](#)
  - downloading SESM [5-11](#)
  - Dreamweaver
    - library items [3-12](#)
    - templates [3-12](#)
  - DTD [6-5, C-1](#)
  - duration
    - advertising redirection [5-27, 8-26](#)
    - demonstrating [8-13](#)
    - initial logon redirection [5-26](#)
    - parameter in HTTP requests [8-5](#)
    - parameters
      - Cisco IOS commands [8-25, 8-26](#)
      - RADIUS profile [D-10](#)
      - summary [8-21](#)
    - timing [8-6](#)
- 
- ## E
- editing configuration files [6-1](#)
  - encryption [3-7, A-2](#)
  - error redirections [5-25](#)
  - errorURL attribute [8-17](#)
  - evaluation licenses [5-15](#)
  - exceptions, out of memory [10-11](#)

## exclusive services

See mutually exclusive services

## executables

adding Windows services 7-7

installation 5-12

startup scripts 7-1

stop scripts 7-7

explicit IP address, SSG 6-29

extending directory schema 1-8, 5-29, 6-40

---

**F**

filename attribute, in LogMBean 6-9

## files

.iss 5-14

.properties 5-14

captiveportal.jetty.xml 8-14

captiveportal.xml 8-14, 8-15, 8-27

cdat.jetty.xml 6-8

cdat.xml 6-36

config.xml 6-37

configuring captive portal solution 6-3

demo.txt 4-6, 6-21

installation image names 5-10, 5-12

installation results 5-30

J2EE configuration 6-3

keystore A-2

licensenum.txt 5-15

MBean configuration 6-1

messageportal.jetty.xml 8-14

messageportal.xml 8-14, 8-17

nwsp.jetty.xml 6-8, 8-14

nwsp.xml 6-14, 8-14, 8-20

pdademo.txt 4-9

rdp.xml 6-30

ssgconfig.txt 8-9

startNWSP 4-5

startup scripts 7-3

web.xml 6-3, 8-14, 10-11

webdefault.xml 6-3, 8-14

xmlconfig.dtd 6-5

See also logging, logs

frames D-5, D-10

frequency, in advertisement redirections 8-26, D-10

full name, in service profiles D-6

---

**G**

generic startup scripts 7-4

global attributes, for SSG 6-28

global attributes, SSG 6-22, 6-28

greetings page

See initial logon redirection

group password 6-24

See service groups

GroupRequest password 6-32

groups

captive portal 8-7, 8-8, 8-10, 8-22

user, branding example 3-10

See also service groups

GUI installation mode 5-13

---

**H**

hardware platforms 1-12

hierarchical policing, SSG 3-6

hobbies, captive portal advertisement 8-10, 8-19

home page, URLs D-10

host

attribute in captive portal 8-15

SSG object 2-5, 2-8, D-9

HTML Adaptor server 6-18, 10-6

HTML frames D-5, D-10

HTTP

configuring listener port 4-4, 5-17

errors 10-4

listener 1-9

- preserving original subscriber request [8-5](#)
  - processing requests [8-3](#)
  - processing subscriber requests [2-2, 2-3](#)
  - redirections
    - after greetings or advertising [5-25](#)
    - captive portal [3-8, 8-3, 8-5](#)
    - errors [5-25](#)
    - query parameters [8-5](#)
  - request log [10-4](#)
  - security [A-1](#)
  - SocketListener [6-11](#)
  - SunJsseListener [6-12](#)
  - Version 1.1 [8-28](#)
  - HTTPS [6-12, A-2](#)
  - HttpServer MBean [6-11, 6-14](#)
- 
- I**
- idle timeout
    - services [D-4](#)
    - sessions [D-9](#)
  - ignoreProfile attribute [8-18](#)
  - images
    - downloading installation [5-11](#)
    - referenced in JSPs [3-12, 6-45](#)
    - service status indicators [3-5](#)
  - indicators, service status [3-5](#)
  - initialCaptiveDuration attribute [8-16, 8-21](#)
  - initialCaptiveOn attribute [8-15, 8-27](#)
  - initialCaptivePort attribute [8-16](#)
  - initialCaptiveURL attribute [8-15](#)
  - initializing MBeans [6-2](#)
  - initial logon redirection
    - configuring [5-26, 8-15, 8-17, 8-25](#)
    - demonstrating [8-12](#)
    - description [3-9, 8-4](#)
    - duration [5-26](#)
    - HTTP query parameters [8-5](#)
    - port [5-26](#)
    - profile attributes [D-10](#)
  - installing
    - captive portal solution [5-16, 5-24, 8-8](#)
    - CDAT [5-16, 5-21](#)
    - custom [5-16](#)
    - Demo mode [1-5, 5-16](#)
    - directory [4-4, 5-15](#)
    - image for [5-10](#)
    - individual components [5-16](#)
    - iPlanet [5-7](#)
    - JDK [5-4](#)
    - JRE [5-3](#)
    - logging during [5-13](#)
    - Message Portal application [5-24](#)
    - modes for [5-12](#)
    - NDS [5-5](#)
    - NWSP [5-17](#)
    - PDA [5-17](#)
    - portal applications [5-16](#)
    - RDP [5-16, 5-22](#)
    - results [5-30, 8-9](#)
    - SESM components [5-16](#)
    - SPE [5-16](#)
    - typical [5-16](#)
    - WAP [5-17](#)
  - interestPages attribute [8-19](#)
  - interests attribute [8-19](#)
  - internationalization [3-11](#)
  - Internet Explorer [1-13, 4-4](#)
  - IP addresses
    - Captive Portal application [5-24](#)
    - directory [5-20, 6-38, 9-8](#)
    - overlapping [3-9](#)
    - RADIUS server [5-19, 5-29, 9-4, 9-5, 9-11](#)
    - RDP [5-22, 9-7](#)
    - RDP clients [5-24, 6-34](#)
    - SSG [5-18, 9-2, 9-3, B-2](#)
    - subscriber nonroutable [3-9](#)
    - troubleshooting RADIUS server [10-11](#)

IP attribute [6-29](#)

## iPlanet

Console [5-8](#)

dn [5-20](#)

installing [5-7](#)

password [5-20](#)

tree and context [5-7](#)

uid [5-20, 5-21](#)

version [1-11](#)

See also directory

## J

### J2EE

bundled components [1-9](#)

configuration files [6-1, 6-3](#)

containers [6-7](#)

listeners, eliminating [8-7](#)

server configuration [6-7](#)

web servers [1-9, 2-2, 6-7](#)

### Java

memory usage [7-8, 10-11](#)

script [1-13](#)

security [A-1](#)

virtual memory [6-39, 7-8](#)

### Java Management Extensions

See JMX

### Java Secure Sockets Extension

See JSSE

### Java server pages

See JSPs

### Java system properties

See system properties

JAXP XML parser, installing [5-30](#)

### JDK

installing [5-4](#)

locating [5-3, 10-8, 10-9](#)

messages during installation [10-7](#)

preinstalled [10-9](#)

SESM startup scripts [5-3](#)

specifying location [5-3](#)

JDK\_HOME [5-4, 10-9](#)

jetty.home [6-12, 6-14, 7-5](#)

jetty.log [6-9, 10-5](#)

### Jetty server

certificates [A-2](#)

configuring [6-8](#)

installing [1-9, 5-16](#)

log files [10-4](#)

port-bundle host key and [1-11](#)

starting [7-1](#)

stopping [7-6](#)

troubleshooting [10-4](#)

See also J2EE

JIT relocation message [10-7](#)

### JMX

description [6-2](#)

framework, installing [5-30](#)

HTML Adaptor server [6-18, 10-6](#)

server [1-9, 6-2, 6-45](#)

### JRE

installing [5-3](#)

locating [5-3, 10-8, 10-9](#)

messages during installation [10-7](#)

preinstalled [10-9](#)

SESM startup scripts [5-3](#)

specifications [5-2](#)

specifying location [5-3](#)

### JSPs

description [3-11, 6-45](#)

engine [1-9](#)

installing framework [5-30](#)

recompiling [5-4, 10-9](#)

JSSE [6-12, A-2](#)

### jvm arguments

changing [10-11](#)

portal applications [7-8](#)

RDP [7-10](#)



**K**

KeyPassword attribute [6-12](#)  
 keys, next hop gateway [D-5, D-11](#)  
 keystore  
   certificates [A-2](#)  
   file [A-2](#)  
   password [6-12](#)  
 Keystore attribute [6-12](#)  
 keytool facility [A-2](#)

**L**

LDAP directory  
   See directory, NDS, iPlanet  
 LDAP mode  
   communication attributes summary [9-6](#)  
   description [1-5, 1-8](#)  
   diagram [2-7](#)  
   features [3-7](#)  
   setting [6-19](#)  
 LDIF command [6-41](#)  
 libraries  
   SESM [1-6, 3-12](#)  
   SPE [1-8](#)  
 license  
   number [5-15](#)  
   recorded [5-15](#)  
   types [4-4, 5-15](#)  
   types, for installation [5-15](#)  
 licensenum.txt file [5-15, 5-30](#)  
 license obtaining number [5-11](#)  
 lights, service status [3-5](#)  
 Lightweight Directory Access Protocol. See LDAP mode, directory  
 Linux  
   stopping applications [7-7](#)  
   supported platforms [1-13](#)  
   well-known locations for JRE [10-9](#)  
 load balancing [2-3, 3-12](#)  
 loads, SSG tuning [6-22](#)  
 locale awareness [3-11](#)  
 localIPAddress, RDP [6-33](#)  
 localization [3-11](#)  
 localPort, RDP [6-33](#)  
 location  
   awareness [3-10, 6-44](#)  
   parameters [6-30](#)  
 logDateFormat attribute [6-9, 6-16](#)  
 logFile attribute [6-17](#)  
 logFrame attribute [6-17](#)  
 Logger MBean [6-16](#)  
 logging  
   configuring [6-9, 6-16](#)  
   directory activity [6-38](#)  
   during installation [5-13](#)  
   Jetty server activity [6-8, 6-9](#)  
   off portal applications [3-1, 6-25](#)  
   on  
     to CDAT [6-41](#)  
     to portal applications [4-5, 7-6](#)  
     to services [3-1, 8-10, 8-12, 8-15, 8-20](#)  
     user IDs for demo [4-7](#)  
   portal activity [6-15, 6-16, 7-5](#)  
   procedures [10-4](#)  
 logLabels attribute [6-9](#)  
 LogMBean [6-9](#)  
 logOneLine attribute [6-9](#)  
 logs  
   application.log [6-17, 10-5](#)  
   jetty.home [7-5](#)  
   jetty.log [6-9, 10-5](#)  
   location [7-5, 10-4](#)  
   request.log [6-13, 10-4](#)  
 logSink class [6-13](#)  
 logStack attribute [6-17](#)  
 logStackSize attribute [6-9](#)  
 logStackTrace attribute [6-9](#)

logTags attribute [6-9](#)  
 logThread attribute [6-17](#)  
 logTimeStamps attribute [6-9](#)  
 logTimezone attribute [6-9](#)  
 logToErr attribute [6-17](#)

## M

management.portno [7-5](#)  
 management console  
   configuring [6-18](#)  
   description [10-6](#)  
   password [10-7](#)  
   port [5-17, 6-18, 7-4](#)  
   See also HTML Adaptor server  
 mapping SSGs [6-27](#)  
 MASK attribute [6-22, 6-29](#)  
 masks [5-18, 6-28](#)  
 MaxIdleTimeMs attribute [6-12](#)  
 maxIdleTimeMs attribute [6-11, 6-33](#)  
 maximum transmission unit [D-5](#)  
 maxReadTimeMs attribute [6-11](#)  
 MaxThreads attribute [6-12](#)  
 maxThreads attribute [6-11, 6-33](#)  
 maxVariables attribute [6-37](#)  
 MBeans  
   AAA [6-15, 6-31](#)  
   CDAT [6-36](#)  
   changing [6-1](#)  
   ConfigAgent [6-2](#)  
   configuration files [6-2](#)  
   constructing and initializing [6-2](#)  
   Debug [6-8](#)  
   description [6-2](#)  
   DESSMode [6-15](#)  
   Directory [6-38](#)  
   Jetty [6-8](#)  
   Log [6-8](#)  
   Logger [6-15, 6-30, 6-36](#)

ManagementConsole [6-15, 6-30, 6-36](#)  
 RDPMBean [6-31](#)  
 RDPPacketFactory [6-31](#)  
 SESM [6-15](#)  
 SESMDemoMode [6-15](#)  
 SSG [6-15](#)  
 WebApp [6-15](#)  
 memory  
   argument in startup script [7-9](#)  
   automatic management [3-4](#)  
   directory cache [6-39](#)  
   exceptions [7-9, 10-11](#)  
   portal applications [7-8](#)  
   RDP [7-10](#)  
   requirements summary [5-2](#)  
   reserved [7-8](#)  
   SSG [6-20](#)  
   usage [7-8](#)  
 Merit flat file  
   See demo.txt  
 message duration  
   See duration  
 messageportal.host [8-15](#)  
 messageportal.jetty.xml [8-14](#)  
 messageportal.port [8-15](#)  
 messageportal.xml [8-14, 8-17](#)  
 Message Portal application  
   configuring [8-17](#)  
   description [1-7, 8-6](#)  
   installing [5-24](#)  
   ports [5-25](#)  
   timing of durations [8-6](#)  
 messageRedirectDurationParam attribute [8-17](#)  
 messageRedirectSubscriberParam attribute [8-17, 8-28](#)  
 messageRedirectURLParam attribute [8-17](#)  
 meta schema, directory [5-20](#)  
 Microsoft Windows  
   adding and removing services [7-7](#)  
   platform specifications [1-12](#)

- stopping applications [7-7](#)
- MinThreads attribute [6-12](#)
- minThreads attribute [6-11, 6-33](#)
- missing files [10-10](#)
- mode
  - argument to startup scripts [7-2](#)
  - attribute [6-19](#)
  - concurrent service [D-5](#)
  - configuration setting [6-19](#)
  - console installation [5-13](#)
  - deployment [1-4](#)
  - GUI installation [5-13](#)
  - installation [5-12](#)
  - sequential service [D-5](#)
  - silent installation [5-14](#)
  - switching deployment [1-5, 6-19](#)
  - system property [6-19](#)
- See also Demo mode, LDAP mode, RADIUS mode
- MSISDN [3-3, 6-34, D-9](#)
- MTU, PPP [D-5](#)
- mutually exclusive services
  - groups [6-21, D-7, D-8](#)
  - selection [3-5](#)

---

## N

- NAS
  - clients [D-2](#)
  - identifier [D-9](#)
  - RADIUS attribute [3-3](#)
- NAS\_IDENTIFIER [3-3, 6-34](#)
- NDS
  - Allow Clear Text Passwords [5-6](#)
  - authenticating [5-6](#)
  - container cn [5-21](#)
  - directory cn [5-20](#)
  - directory dn [5-20](#)
  - directory password [5-20](#)
  - installing [5-5](#)

- tree and context [5-5](#)
- version [1-11](#)
- See also directory
- Netscape, supported version [1-13, 4-4](#)
- network access server
- network diagram [2-1](#)
- Network Directory Service
  - See NDS
- New World Service Provider application
  - See NWSP, applications
- next hop
  - gateway [D-5, D-11](#)
  - password [5-23, 6-32, 9-4](#)
  - RDP [6-35](#)
- NextHopRequest password [6-32](#)
- Novell eDirectory
  - See NDS
- NWSP
  - demonstrating [4-1](#)
  - description [1-6](#)
  - installing [5-16](#)
  - logging on [4-5](#)
  - port [4-4, 5-17](#)
  - role in captive portal solution [1-7, 8-6](#)
  - starting [7-1](#)
  - user IDs for demo [4-7](#)
  - virtual memory [6-39](#)
  - See also applications
- nwsp.jetty.xml [6-8, 8-14](#)
- nwsp.xml [6-14, 8-14, 8-20](#)

---

## O

- organization, LDAP directory [5-21, 9-8](#)
- original subscriber URL
  - See URLs
- out of memory exception [10-11](#)

**P**

- PAP [D-5](#)
- passthrough services [3-6, D-5](#)
- passwords
  - Allow Clear Text Passwords [5-6](#)
  - attributes for RDP [6-32, 9-7](#)
  - directory [5-20, 6-38](#)
  - directory container [5-21](#)
  - keystore [6-12](#)
  - management console [10-7](#)
  - next hop [5-23, 6-32](#)
  - service [5-19, 5-22, 6-24, 6-32, 9-4, 9-5, 10-12](#)
  - service group [5-19, 5-22, 6-32](#)
  - service logons [3-7](#)
- PDA
  - description [1-7](#)
  - devices [1-13](#)
  - installing [5-16](#)
  - port [4-4, 5-17](#)
  - See also applications
- pdademo.txt [4-9](#)
- permissions
  - LDAP directory [5-20, 5-21](#)
  - required for installation [4-2, 5-12, 10-10](#)
- Personal Digital Assistant application
  - See PDA, applications
- personalized portal pages [3-2](#)
- platforms
  - browsers [1-13](#)
  - hardware [1-12](#)
- poolSize attribute [6-38](#)
- PORT\_BUNDLE\_HOST\_KEY\_SWITCH attribute [6-23](#)
- portals
  - See applications
- PORT attribute [6-22, 6-29, 9-2](#)
- port-bundle host key
  - benefits [2-2, 3-9](#)
  - bundle length [6-22, 9-2, 9-3](#)
  - Cisco IOS release [B-2](#)
  - configuring [B-2](#)
  - description [1-10, 3-9, 6-25](#)
  - IP addresses [B-2](#)
  - Jetty server [1-11](#)
  - location awareness and [3-10](#)
  - port bundles [5-18, 6-27](#)
- port-lists [8-22](#)
- port-map [B-2, B-3](#)
- ports
  - accounting [D-1](#)
  - advertising redirection [5-27](#)
  - application.portno [7-5](#)
  - authentication [D-1](#)
  - Captive Portal application [5-24](#)
  - CDAT [5-21](#)
  - directory [5-20, 6-38, 9-8](#)
  - initial logon redirection [5-26](#)
  - Jetty listener [6-11](#)
  - management.portno [7-5](#)
  - management console [5-17, 6-18, 7-4](#)
  - Message Portal application [5-25](#)
  - portal applications [4-4, 5-17, 7-3](#)
  - RADIUS server [5-19, 5-29, 6-24, 9-4, 9-11](#)
  - RDP [5-22, 6-33, 9-7](#)
  - RDP proxy mode [6-35](#)
  - service redirection [5-28](#)
  - SSG [5-18, 6-22, 6-29, 9-2, 10-11](#)
  - SSL [5-17, 6-12, 7-4](#)
  - startup scripts [7-3](#)
  - troubleshooting [10-11, 10-12](#)
  - unauthenticated user redirection [5-26](#)
- PPP
  - authentication [2-3, 3-4](#)
  - connections [8-23](#)
  - maximum transmission unit [D-5](#)
  - single sign-on [3-4](#)
  - subscriber profiles [D-9](#)
  - See also single sign-on

- prepaid services [3-13](#)
- primaryIP attribute
  - portal applications [6-24](#)
  - RDP [6-35](#)
- primaryPort attribute
  - portal applications [6-24](#)
  - RDP [6-35](#)
- principal attribute, SPE [6-38](#)
- printTraceToConsole, DESS [6-38](#)
- privileges
  - See permissions
- profileCachePeriod attribute [6-20](#)
- profiles
  - caching [6-20](#)
  - examples [1-11, D-7, D-8, D-11](#)
  - next hop gateway [D-11](#)
  - PPP subscribers [D-9](#)
  - service [D-3](#)
  - service group [6-24, D-7](#)
  - subscriber [D-8](#)
  - X.500 data [3-7](#)
- properties
  - See system properties
- protocols
  - CHAP [D-5](#)
  - LDAP [1-5](#)
  - PAP [D-5](#)
  - PPP [3-4](#)
  - RADIUS [1-10](#)
  - WAP [1-2](#)
- proxy
  - RDP mode
    - configuring [5-29, 6-35, 9-10](#)
    - description [1-8, 6-30](#)
    - setting [5-23](#)
  - service type [3-6, D-5](#)

---

## Q

- queryMaxResults attribute [6-37](#)
- query parameters, HTTP redirections [8-5](#)
- queryTimeout attribute [6-37](#)
- quick start [4-2](#)

---

## R

### RADIUS

- AAA MBean [6-24](#)
- authentication retries [B-2](#)
- clients [9-5, 9-11, D-2](#)
- dictionary [D-3](#)
- IP address [9-11](#)
- Merit flat file
  - See demo.txt
- password [B-2](#)
- primary server [5-19, 5-29](#)
- proxy server and RDP [6-35](#)
- requirements during SESM installation [5-4](#)
- secondary server [5-19, 5-29, 9-5](#)

### RADIUS/DESS Proxy Server

- See RDP

### RADIUS mode

- communication attributes summary [9-3](#)
- description [1-4, 1-5, 9-3](#)
- diagram [2-4](#)
- setting [6-19](#)

### RADIUS server

- accounting port [D-1, D-11](#)
- authentication port [D-1](#)
- defining RDP as client [9-11](#)
- portal communication [5-19, 5-29, 9-5, 10-11](#)
- RDP communication [9-11](#)
- SSG communication [9-4, 10-11](#)
- supported software [1-11](#)
- troubleshooting [10-12](#)
- See also ports

- radius-server parameter [10-12](#)
  - RADIUS shared secret
    - configuring on RADIUS server [D-2](#)
    - with portals [5-19](#)
    - with RDP [5-29](#)
    - with SSG [5-18](#)
  - RAM [5-2](#)
  - RBAC
    - description [1-3, 1-4, 1-8, 3-8](#)
    - installing [5-29](#)
    - loading [6-40](#)
    - sample data [1-8](#)
  - RDP
    - adding clients [5-23, 6-34](#)
    - add services option [5-23](#)
    - automatic connections [6-20](#)
    - caching [6-43](#)
    - client IP addresses [5-24, 6-34](#)
    - client names [5-24, 6-34](#)
    - configuring [6-30, 6-37](#)
    - customizing [E-1](#)
    - description [1-7](#)
    - directory communication [9-8](#)
    - installing [5-16, 5-22](#)
    - IP address [5-22, 9-7](#)
    - MBean [6-32, 6-33](#)
    - memory requirements [7-10](#)
    - modes [1-7](#)
    - next hop password [5-23, 6-32](#)
    - passwords [6-32](#)
    - port [5-22, 6-33, 9-7](#)
    - proxy mode
      - See proxy RDP mode
    - RADIUS communication [5-29, 6-35, 9-11](#)
    - restricted client feature [5-22, 5-23](#)
    - service password [5-22, 6-32, 9-7](#)
    - shared secret [5-22, 5-24, 5-29, 6-33, 6-34](#)
    - SSG communication [5-22, 9-7](#)
    - starting [7-2](#)
    - stopping [7-6](#)
    - troubleshooting [10-3](#)
    - tuning [6-35](#)
    - virtual memory [6-39](#)
  - rdp.xml [6-30](#)
  - RDPPacketFactory MBean [6-32](#)
  - reauthentication [3-4](#)
  - recompiling JSPs [5-4, 10-9](#)
  - redirections
    - See HTTP redirections
  - redirectOn attribute [8-12, 8-19](#)
  - redundancy [3-12](#)
  - registering MBeans [6-2](#)
  - request.log [6-13, 10-4](#)
  - reserved memory [7-8](#)
  - resiliency [3-12](#)
  - restricted client feature
    - See RDP
  - retainDays attribute [6-9, 6-13](#)
  - RETRIES attribute [6-22](#)
  - retryCount
    - attribute [6-24](#)
    - RDP [6-35](#)
  - role based access control
    - See RBAC
  - roles, loading [6-40](#)
- 
- ## S
- sample
    - applications [1-5, 1-6](#)
    - captive portal profiles [8-10](#)
    - profiles in demo.txt [1-11](#)
    - RBAC data [1-8](#)
    - service group profiles [D-8](#)
    - service profiles [D-7](#)
    - subscriber profiles [D-11](#)
  - scaling [2-3, 3-12](#)
  - schema

- extending [5-29, 6-40](#)
- extending directory [1-8](#)
- X.500 [3-7](#)
- scripts
  - See files, executables, startup scripts
- secondaryIP, RDP [6-35](#)
- secondaryIP attribute [6-24](#)
- secondaryPort, RDP [6-35](#)
- secondaryPort attribute [6-24](#)
- SECRET attribute [6-22, 6-29, 9-2](#)
- secret attribute [6-24](#)
- secure socket listener
  - See SSL
- security [A-1](#)
- self-care [3-7](#)
- self-management [3-7](#)
- self-subscription [3-4, 3-7](#)
- sequential service mode [D-5](#)
- servers
  - JMX [6-2](#)
  - supported SESM platforms [1-12](#)
  - See also web server, Jetty, RADIUS
- service
  - authentication [3-4](#)
  - authorization [3-4](#)
  - bandwidths [3-6](#)
  - concurrent [B-2](#)
  - connection [2-3, 2-5, 2-8, 6-25](#)
  - cookies [D-6](#)
  - destinations [D-5](#)
  - disconnection [2-5, 2-8, 3-1](#)
  - groups
    - in service profiles [D-9](#)
    - mutually exclusive [3-5, 6-21, D-7, D-8](#)
    - password [5-19, 5-22, 6-24, 6-32, 9-5, 9-11](#)
    - profiles [D-7, D-8](#)
  - idle timeout [D-4](#)
  - logons [3-1, 8-10, 8-12, 8-15, 8-20](#)
  - names [5-28, D-9](#)
  - next hop gateway [D-5](#)
  - object, SSG [2-5, 2-8, D-4](#)
  - passthrough [3-6, D-5](#)
  - passwords
    - See passwords
  - profiles
    - See profiles
  - proxy [3-6, D-5](#)
  - query parameter in HTTP redirection [8-5](#)
  - request password [6-32](#)
  - routes [8-28](#)
  - selection [3-1, 3-4, 3-5](#)
  - status [3-5](#)
  - subscription [3-4, 3-7](#)
  - timeouts [D-4](#)
  - tunnel [3-6, D-5](#)
  - types [3-6, D-7](#)
  - URL [8-5](#)
  - See also automatic connections
- serviceGroup Password attribute [6-24](#)
- serviceLogonURI attribute [6-25, 8-20](#)
- serviceNotGivenURI attribute [5-28, 6-25, 8-6, 8-20](#)
- servicePassword attribute [6-24](#)
- serviceportal.host [8-15](#)
- serviceportal.host system property [5-25](#)
- serviceportal.port [5-25, 8-15](#)
- service proxy [D-5](#)
- serviceRedirectDefaultURL attribute [8-11, 8-16](#)
- service redirection
  - configuring [8-15](#)
  - configuring during install [5-28](#)
  - configuring on SSG [8-24](#)
  - content application for [5-25](#)
  - demonstrating [8-12](#)
  - HTTP query parameters [8-5](#)
  - logon pages [8-10](#)
  - ports [5-28](#)
  - service names [5-28](#)
  - service routes [8-28](#)

- shared address space [8-25](#)
- troubleshooting [8-12](#)
- serviceRedirectOn attribute [8-15, 8-27](#)
- serviceRedirectServiceParam attribute [8-17](#)
- serviceRedirectSubscriberParam attribute [8-17, 8-28](#)
- serviceRedirectURLParam attribute [8-17](#)
- ServiceRequest password [6-32](#)
- serviceStartURI attribute [6-25, 8-20](#)
- serviceSubscriptionURI attribute [6-25, 8-20](#)
- serviceURL query parameter [8-5](#)
- SESM
  - core model [5-16](#)
  - MBean [6-19](#)
- sesm.mode [6-19](#)
- SESMDemoMode MBean [6-21](#)
- SESM-RADIUS [1-2](#)
- SESM-SPE [1-2](#)
  - See also SPE
- session
  - authentication [3-4](#)
  - brand awareness [6-44](#)
  - idle timeout [D-9](#)
  - location awareness [6-44](#)
  - management with port-bundle host key [3-9](#)
  - stateless in SESM [3-12](#)
  - status [3-1](#)
  - timeouts [D-9](#)
- SESSION\_BRAND [6-30](#)
- SESSION\_LOCATION [6-30](#)
- sessionCachePeriod attribute [6-20](#)
- sessionTimeOut attribute [6-25](#)
- sessionTimeout attribute [6-37](#)
- setSubnetAttribute call [6-23](#)
- setup type [4-4, 5-16](#)
- shared address spaces, service redirection [8-25](#)
- shared secret
  - configuring on RADIUS [D-2](#)
  - description [9-3](#)
  - RADIUS and portals [5-19, 6-24, 9-5, 10-11](#)
  - RADIUS and SSG [5-18, 6-22, 9-2, 9-4, B-2](#)
  - RDP and RADIUS [5-29, 6-35, 9-11](#)
  - RDP and SSG [5-22, 5-24, 6-33, 6-34, 9-7](#)
  - SSG and portals [10-11](#)
  - troubleshooting [10-12](#)
- silent installation mode [5-14](#)
- single sign-on
  - benefits [6-43](#)
  - description [2-3](#)
  - non-PPP clients [3-4](#)
  - PPP clients [3-4](#)
- singleSignOn attribute [6-20](#)
- SMTP redirection [8-4, D-10](#)
- software, bundled [1-8](#)
- Solaris
  - patches [5-3](#)
  - platform specifications [1-12](#)
  - stopping applications [7-7](#)
  - well-known locations for JRE [10-8](#)
- source ip command [B-2](#)
- SPE
  - caching [6-38](#)
  - configuration file [6-37](#)
  - configuring [6-37](#)
  - description [1-2, 1-3, 1-8, 2-7](#)
  - features [3-7](#)
  - installing [5-16](#)
  - MBean [6-38, 6-39](#)
  - virtual memory [6-39](#)
- specifications
  - disk space [5-2](#)
  - Java [5-2](#)
  - RAM [5-2](#)
- SSD [1-2](#)
- SSG
  - clients to RDP [5-24, 6-34](#)
  - configuring [2-6, 5-18, 6-25, B-1](#)
  - default network [2-1](#)
  - defining as NAS client [D-2](#)



- description [1-10](#)
- devices [1-12](#)
- duration parameters [8-21](#)
- explicit IP address [6-29](#)
- global attributes [6-22, 6-28](#)
- hierarchical policing [3-6](#)
- host object [2-5, 2-8, D-9](#)
- IP address [5-18, 9-2, 9-3, B-2](#)
- mapping subnets [5-18, 6-27](#)
- MBean [6-22](#)
- memory [6-20](#)
- network diagram [2-1](#)
- port [9-2, 9-3](#)
- portal communication [5-18, 9-2](#)
- port-map [B-2, B-3](#)
- prepaid services [3-13](#)
- processing traffic [2-2](#)
- RADIUS server communication [9-4, 10-11](#)
- RADIUS server ports [5-18, D-1](#)
- RDP communication [5-22, 9-7](#)
- requirements during SESM installation [5-4](#)
- service object [D-4](#)
- shared secret [5-18, 5-22, B-2](#)
- subnet attributes [6-23, 6-28, 6-29](#)
- tuning SESM load on [6-22](#)
- See also TCP redirections, port-bundle host key
- ssgconfig.txt [8-9](#)
- SSL [5-17, 6-8, 6-12, 7-4](#)
- stackTrace, DESS [6-38](#)
- starting
  - CDAT [7-3](#)
  - demo [4-5](#)
  - Jetty server [7-1](#)
  - MBeans [6-2](#)
  - portals [7-1](#)
  - RDP [7-2](#)
- startup scripts
  - application names in [6-45, 7-3](#)
  - application-specific [7-3](#)
  - captive portal [8-11](#)
  - customizing [6-45](#)
  - demo [4-5](#)
  - description [7-3](#)
  - failure [10-4](#)
  - generic [7-4](#)
  - Java system properties [6-6, 7-4, 7-5](#)
  - JDK reference [5-3, 5-4, 10-9](#)
  - JRE reference [5-3](#)
  - jvm arguments [10-11](#)
  - memory [7-9, 7-10](#)
  - mode argument [7-2](#)
  - port references [7-3](#)
- status
  - indicators [3-5](#)
  - of services [3-5, 6-43](#)
  - session [3-1](#)
- stopping SESM processes [7-6](#)
- subaccounts [3-7](#)
- subnet attributes, SSG [5-18, 6-23, 6-28, 6-29](#)
- subscriber name [8-5](#)
- Subscriber Policy Engine
  - See SPE
- subscriber profiles
  - configuring RADIUS [D-8](#)
  - Demo mode [4-5, 4-6](#)
  - examples [D-11](#)
  - LDAP mode [1-5](#)
  - PPP [D-9](#)
  - RADIUS mode [1-5](#)
- Sun Microsystems, sample JMX server [1-9](#)
- Sun Solaris
  - See Solaris
- support, technical [xvi, 5-15](#)
- suppressStack attribute [6-10](#)
- suppressWarnings attribute [6-10](#)
- system properties [6-6, 7-4, 7-5](#)

**T**

tar files [5-12](#)

TCP packets [2-2](#)

TCP redirections

- configuring [8-9](#)
- description [2-3, 3-8, 8-3](#)
- eliminating types [8-7](#)
- SMTP forwarding [8-4, D-10](#)
- types [8-4, 8-5](#)

See also advertising redirection; initial logon redirection; service redirection; unauthenticated user redirection

technical support [xvi, 5-15](#)

Telnet interface [B-3](#)

templates [3-12](#)

threeKeyAuth attribute [6-33](#)

throttle attribute [6-22, 6-24, 6-35](#)

timeOut attribute [6-24, 6-35](#)

timeouts [D-4, D-9](#)

- CDAT [6-37](#)
- portals [6-22](#)
- service [D-4](#)
- session [D-9](#)

TIMEOUTSECS attribute [6-22](#)

tokenCheckInterval attribute [6-21](#)

tokenMaxAge attribute [6-21](#)

trace attribute [6-17](#)

traceFileName, DESS [6-38](#)

traceLevel, DESS [6-38](#)

tree, LDAP directory [5-5, 5-7, 9-8](#)

troubleshooting

- automatic connections [6-43](#)
- captive portal solution [8-26](#)
- configuration file location [10-11](#)
- diagnostic procedures [10-1](#)
- JRE location [10-7](#)
- RDP [10-3](#)
- service redirection [8-12](#)

SESM portal applications [10-1, 10-11](#)

See also logging, debugging

tuning

CDAT sessions [6-37](#)

RDP [6-35](#)

tunnel services [3-6, D-5, D-6](#)

typical installation [4-4, 5-16](#)

**U**

uid [5-7, 5-20](#)

unauthenticated user redirection

configuring [5-26, 8-15, 8-23](#)

demonstrating [8-12](#)

description [3-8, 8-4](#)

HTTP query parameters [8-5](#)

port [5-26](#)

unavailable web server [10-11](#)

unconnected service redirection [3-9, 8-4](#)

uninstalling SESM [5-10, 5-30](#)

unique identifier [5-20](#)

URLs

attribute for LDAP server [6-38](#)

destination, for service redirections [8-11](#)

home page [D-10](#)

service [D-5](#)

subscriber's original

availability [8-8, 8-18](#)

Captive Portal application [8-3, 8-4, 8-5, 8-8](#)

duration before redirecting [8-21](#)

Message Portal [8-6, 8-16, 8-19](#)

parameter specifying [8-5, 8-17](#)

useClientList attribute [6-34](#)

user

concurrent services [B-2](#)

groups, branding example [3-10](#)

shape mechanism [3-11](#)

user groups

See branding

user ID

- demo logons [4-5, 4-7](#)
- directory [5-20, 6-38, 9-8](#)
- directory container [5-21, 6-38](#)

username

- full name in service profiles [D-6](#)
- query parameter in HTTP redirection [8-5](#)

userRedirectOn attribute [8-15, 8-27](#)

userRedirectPort attribute [8-16](#)

userRedirectURL attribute [8-15](#)

userRedirectURLParam attribute [8-17](#)

---

## V

vendor-specific attributes

- See VSAs

verbose attribute [6-10](#)

virtual

- host name [6-14](#)
- memory [6-39, 7-8, 7-10](#)
- private dial-up network (VPDN) [D-6](#)

VSAs [D-3](#)

---

## W

WAP

- description [1-6](#)
- devices [1-13](#)
- installing [5-16](#)
- port [4-4, 5-17](#)

See also applications

warning

- during installation [5-20](#)
- logging configuration attribute [6-17](#)

web.xml [6-3, 8-14, 10-11](#)

webdefault.xml [6-3, 8-14](#)

web development kit [1-6, 3-11](#)

WEB-INF directory [10-10](#)

web portals

- See applications

web servers

- configuring [6-7](#)
- role [2-2](#)
- unavailable [10-11](#)

See also J2EE, Jetty

Windows

- See Microsoft Windows

Wireless Access Protocol application

- See WAP

---

## X

X.500 user schema [3-7](#)

xmlconfig.dtd [6-5, C-1](#)

XML files

- See J2EE configuration files

X server [10-10](#)

---

## Z

zip files [5-12](#)

