



Cisco Subscriber Edge Services Manager Installation and Configuration Guide

SESM Release 3.1(7)
October 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-2147-03



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 Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, 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, Internet Quotient, 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. (0208R)

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

Copyright ©2002, Cisco Systems, Inc.

All rights reserved.



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

Preparing to Install SESM	1-1
Installation Platform Requirements	1-1
Memory and Disk Space Requirements	1-2
Java Software Considerations	1-3
Solaris Patch Requirements	1-3
Recommended and Required JVM Versions	1-3
Installing the Bundled JRE	1-3
JVM Requirements for Application Startup	1-4
Specifying an Existing JRE or JDK	1-4
Specifying the JRE or JDK in Startup Scripts	1-4
Obtaining a JDK for SESM Web Development	1-5
Requirements for Related Network Components	1-5
SSG and RADIUS Considerations	1-5
Advantages to Running an LDAP Directory During SESM Installation	1-6
Dependencies among SESM Components	1-6
Uninstalling a Previous SESM Installation	1-6

CHAPTER 2

Installing SESM 2-1

- Obtaining the SESM Installation File and License Number 2-1
 - Obtaining a License Number 2-1
 - Downloading Software from the Cisco Web Site 2-2
 - Uncompressing the Image 2-2
- Required Installation Privileges 2-3
- Installation Methods 2-3
 - Installing Using GUI Mode 2-3
 - Installing Using Console Mode 2-4
 - Installing Using Silent Mode 2-4
- Turning On the Installation Logging Feature 2-5
- Installation Parameter Descriptions 2-5
- Installation Results 2-20
- Post-Installation Configuration Tasks 2-21

CHAPTER 3

SESM Configuration Management 3-1

- Introduction 3-1
 - Java Management Extensions 3-1
 - MBean Description 3-2
 - Methods for Changing MBean Attribute Values 3-2
 - Monitoring Features 3-2
- Using the SESM Remote Management Tool 3-3
 - SESM Remote Management Overview 3-3
 - Accessing an Application's Agent View 3-4
 - Configuring the ManagementConsole MBean 3-5
 - Starting and Removing the Management Console 3-5
 - URLs for Accessing Agent Views 3-6
 - CDAT Main Window 3-6
 - Configuring Links to Agent Views on the CDAT Main Window 3-7
 - Using the Agent View 3-8
 - Using the MBean View 3-9
 - Monitoring an Application 3-12
- Directly Editing MBean Configuration Files 3-13
 - Restarting Applications after Editing 3-14
 - MBean Configuration File Names 3-14
 - MBean Configuration File Format 3-15
 - SystemProperty and Property Tags in Configuration Files 3-17
- Changing web.xml and webdefault.xml 3-18

CHAPTER 4**Configuring J2EE Containers for SESM Applications 4-1**

- J2EE Containers 4-1
- Container Requirement for the Port-Bundle Host Key Feature 4-1
- Creating WAR Files for Containers Other Than Jetty 4-2
- Jetty Container MBeans 4-2
 - Log MBean 4-3
 - Debug MBean 4-4
 - Server MBean 4-5
 - SESMSocketListener MBean 4-6
 - SESMSSSLListener MBean 4-7

CHAPTER 5**Configuring SESM Portal Applications 5-1**

- SESM Portal Application MBeans 5-1
 - Logger MBean 5-2
 - ManagementConsole MBean 5-3
 - SESM MBean 5-4
 - SESMDemoMode MBean 5-6
 - DESSMode MBean 5-6
 - SSG MBean 5-7
 - AAA MBean 5-10
 - Firewall MBean 5-11
 - WebApp MBean 5-13
 - Location MBean 5-15
- Associating SSGs with Subscriber Requests 5-16
 - Setting SSG Global and Subnet Entries 5-16
 - Using Port-bundle Host Key with Identical SSG Configurations 5-16
 - Using Port-bundle Host Key with Varying SSG Configurations 5-17
 - Specifically Mapping SSGs to Subscriber Subnets 5-18
- Configuring a Customized SESM Application 5-19
 - SESM Application Definition 5-19
 - SESM Application Names 5-20
 - Creating Configuration Files and Startup Scripts 5-20

CHAPTER 6**Configuring CDAT 6-1**

- Required Cookies Feature 6-1
- CDAT Application MBeans 6-1
 - Logger MBean 6-2
 - ManagementConsole MBean 6-2

- MainServlet MBean 6-2
- CDAT MBean 6-3
- Adding a New Application to the CDAT Main Window 6-4
- Configuring CDAT Login Values 6-4
 - Login Values for SESM Agent Views 6-4
 - Login Values for LDAP Directory Management 6-5

CHAPTER 7

- Configuring the RADIUS Data Proxy 7-1**
 - Configuring Listeners and Handlers 7-1
 - Changing Installed Configuration Options 7-2
 - Changing the RADIUS Data Proxy Mode 7-2
 - Adding Service Information to Replies 7-2
 - Using a Restricted Client List 7-3
 - RADIUS Data Proxy MBeans 7-3
 - Logger MBean 7-3
 - ManagementConsole MBean 7-3
 - RADIUSDictionary MBean 7-4
 - RDP MBean 7-4
 - RDP Protocol Handlers 7-7

CHAPTER 8

- Configuring Security Policy Engine for SESM 8-1**
 - SPE Attributes 8-1
 - Directory MBean 8-2
 - Connection MBeans 8-3
 - Extending the Directory Schema and Loading Initial RBAC Objects 8-3
 - Rerunning the SESM Installation to Update the Schema and Load RBAC Objects 8-4
 - Loading Sample Data 8-4

CHAPTER 9

- Running SESM Components 9-1**
 - Starting Applications 9-1
 - Starting the SESM Portals 9-1
 - Startup Script Names 9-2
 - Mode Argument 9-2
 - Starting RDP 9-2
 - Starting CDAT 9-3
 - Startup Script Explanation 9-3
 - Application-Specific Startup Scripts 9-3
 - Generic Startup Script 9-4

SystemProperty and Property Assignments in the Start Script	9-4
Logging On to SESM Portals	9-5
Stopping Applications	9-6
Stopping SESM Applications on Solaris and Linux	9-6
Stopping SESM Applications on Windows NT	9-7
Adding and Removing Services on Windows NT	9-7
Memory Requirements and CPU Utilization	9-7
SESM Portal Application Memory Requirements	9-8
Factors Affecting RAM	9-8
Symptoms of Insufficient Memory	9-8
SESM Portal Application CPU Utilization	9-9
RDP Memory Requirements	9-9

CHAPTER 10**Configuring SESM Features 10-1**

Automatic Service Connections	10-1
Configuring Automatic Services	10-1
Configuring a Service for Automatic Connection	10-1
Configuring SESM to Request Automatic Connections in LDAP Mode	10-2
Subscriber Experiences with Automatic Connections	10-2
Connection Status for Auto Connect Services	10-2
Pop-Up Window for Auto Connect Services	10-2
Changing the Auto Connect Property for a Service	10-3
Disconnecting Auto Connect Services	10-3
Location Awareness	10-3
Overview of Location Awareness	10-3
Location Awareness Configuration Methods	10-4
Using Location to Control the Look and Feel of Portal Pages	10-5
Location Names	10-5
Configuring Location Awareness Based on Complete ID Attributes	10-5
Using Multiple Attributes for the Same Location	10-6
Using Duplicate, Overlapping and Nested Attributes for Different Locations	10-6
Implementing Nested and Overlapping Locations	10-6
Configuring Location Awareness Based on IP Address Subnets	10-7
Demonstrating Location Awareness	10-8
Demonstration Procedure Using Complete ID Attributes	10-8
Demonstration Procedure Using Subnet Entries	10-9
Arbitrary Attributes	10-9
Description of Arbitrary Attributes	10-9
Configuring Arbitrary Attributes	10-10

- Demonstrating Arbitrary Attribute Assignments in NWSP 10-11
- Personal Firewalls 10-12
 - Overview of Firewall Features 10-12
 - My Firewall Page 10-14
 - Advanced Firewall Page 10-16
 - Configuring the Firewall Pages 10-18
 - ACLs Generated from Entries on the Firewall Pages 10-19
 - Viewing Generated ACLs 10-19
 - Generated ACLs for the My Firewall Page 10-19
 - My Firewall Example 10-21
 - Generated ACLs for the Advanced Firewall Page 10-22
 - Advanced Firewall Example 10-23
 - ACL Number Assignments 10-23
 - Subscriber Experiences with Personal Firewalls 10-25
 - Deployer-Imposed Firewalls 10-25
 - Restrictions 10-26
 - Procedure for Entering ACLs in CDAT 10-26
 - ACL Format for CDAT Entries 10-26
 - References for More Information about Access Control Lists 10-27
- Multikey Authentication 10-28
- Quality of Service 10-28

CHAPTER 11

- Deploying a Captive Portal Solution 11-1**
 - SSG and SESM Release Requirements 11-1
 - Solution Description 11-2
 - Solution Diagram 11-2
 - SESM Captive Portal Application 11-3
 - Content Applications 11-4
 - NWSP Application 11-4
 - Message Portal Application 11-4
 - Alternative Configuration Options for a Captive Portal Solution 11-5
 - Installing and Running the Sample Solution 11-6
 - Installing the Sample Solution 11-6
 - Installation Results 11-6
 - Additional Configuration Steps 11-7
 - Configuring the SSG to Match the Installed Captive Portal Solution 11-7
 - Loading Sample Profiles for Captive Portal Demonstration 11-8
 - Configuring Unique Service Logon Pages for Service Redirections 11-8
 - Starting the Sample Captive Portal Solution 11-9

MBeans in the Captive Portal Solution	11-9
MBeans in the Captive Portal Application	11-10
Logger MBean	11-10
ManagementConsole MBean	11-10
captiveportal MBean	11-11
Message Portal Application MBeans	11-13
Logger MBean	11-14
ManagementConsole MBean	11-14
SESMMBean	11-14
SESMDemoMode MBean	11-14
DESSMode MBean	11-14
messageportal MBean	11-15
Captive Portal Attributes in the NWSP WebAppMBean	11-16
Message Duration Parameters—Summary	11-17
Configuring the SSG TCP Redirect Features	11-18
Configuring SSG and Port-Bundle Host Key to Work with the Captive Portal Application	11-19
Defining Captive Portal Groups and Port Lists	11-19
Configuring Unauthenticated User Redirection	11-20
Configuring Unauthorized Service Redirection	11-20
Configuring Initial Logon Redirection	11-22
Configuring Advertising Redirection	11-22
Troubleshooting Captive Portal Configurations	11-23
Some TCP Redirection Types Not Operational	11-23
Redirection Type Turned Off in captiveportal.xml	11-24
Two Redirection Types Assigned to the Same Port in captiveportal.xml	11-24
Redirection Type Not Configured on the SSG	11-24
Redirections Continuously Occur	11-24
Redirected Networks Must Match Service Routes	11-24
Using HTTP1.1 with a Non-SESM Captive Portal Application	11-25
User Name Not Passed in Unauthenticated User Redirections	11-25

CHAPTER 12**Deploying SESM/SSG Solutions 12-1**

Communication Attributes for Interaction Between SESM and SSG	12-1
Communication Attributes for RADIUS Mode	12-3
Communication Attributes for LDAP Mode	12-6
Communication Attributes for LDAP Mode with RDP in Proxy Mode	12-9

CHAPTER 13**Troubleshooting SESM Installation and Configuration 13-1**

Diagnosing Problems	13-1
---------------------	------

- Procedures for Troubleshooting SESM Portals 13-1
- Procedures for Troubleshooting RDP 13-3
- Troubleshooting Aids 13-4
 - Log File Descriptions 13-4
 - Log File Configuration 13-4
 - Java Command Line Options 13-5
 - Obtaining License and Version Information 13-5
- Troubleshooting Tips 13-5
 - JRE and JDK Troubleshooting 13-6
 - Searching for an Existing JDK or JRE 13-6
 - Using a Pre-installed JRE or JDK 13-7
 - Recompiling a Customized JSP 13-7
 - Java Warning and Error Messages at Application Startup 13-7
 - Installation Troubleshooting 13-7
 - No X Server for a Solaris Installation 13-7
 - Incorrect Permissions 13-8
 - Files Not Found 13-8
 - Incomplete Installation or Files Installed in Incorrect Directory 13-8
 - Configuration File Location Troubleshooting 13-8
 - SESM Configuration Troubleshooting 13-8
 - Communication with SSG 13-8
 - Communication with RADIUS Server 13-9
 - Out of Memory Exceptions 13-9
 - Web Server Unavailable 13-9
 - RADIUS Configuration Troubleshooting 13-9
 - SSG Configuration Troubleshooting 13-10
 - Considerations for Subscribers Using PDA Devices 13-10

APPENDIX A

SESM Security A-1

- Java Platform Security References A-1
- Using HTTPS in SESM Portals A-1
 - HTTPS References A-2
 - Keytool and Keystore A-2
- Configuring SESM Portals to Run on SSL Ports Only A-3

APPENDIX B

Configuring an LDAP Directory for SESM Deployments B-1

- NDS Installation and Configuration Requirements B-1
 - Summary of Administrative Access to NDS B-1
 - Installation and Configuration Procedures B-2

Setting the Allow Clear Text Passwords Attribute	B-3
Sun ONE and iPlanet Installation and Configuration Requirements	B-4
Summary of Administrative Access to Sun ONE and iPlanet	B-4
Installation and Configuration Instructions	B-4

APPENDIX C**Configuring RADIUS for SESM Deployments C-1**

Configuring SSG to Communicate with the RADIUS Server	C-1
Configuring RADIUS Clients	C-1
Defining Attributes	C-2
Defining New RADIUS Attributes for SESM Deployments	C-3
SESM Predefined Attributes	C-3
Dynamically Defining Attributes in Profiles for Testing and Development	C-5
Configuring Service Profiles	C-6
Example Service Profiles	C-9
Configuring Service Group Profiles	C-10
Example Service Group Profiles	C-10
Configuring Subscriber Profiles	C-11
Example Subscriber Profiles	C-15
Configuring Next Hop Gateway Profiles	C-16
Configuring the RADIUS Accounting Feature	C-16
Configuring Cisco Access Registrar for SESM Deployments	C-17
Configuring the RADIUS Ports	C-17
Cisco SSG VSAs in Cisco Access Registrar Dictionary	C-17
Configuring NAS Clients in Cisco Access Registrar	C-17
Configuring Attribute Profiles in Cisco Access Registrar	C-17
Configuring Cisco Access Registrar Userlists and Authentication and Authorization Services	C-18
Configuring Accounting on Cisco Access Registrar	C-19
Saving the Configuration and Reloading the Server	C-19
Example RADIUS Profiles	C-19

APPENDIX D**Configuring the Bundled SESM RADIUS Server D-1**

Bundled SESM RADIUS Server Installed Location	D-1
Profile File Requirements	D-1
Defining New Attributes to the Bundled SESM RADIUS Server	D-2
Starting the Bundled SESM RADIUS Server	D-2
MBeans for the Bundled SESM RADIUS Server	D-2
Logger MBean	D-3
ManagementConsole MBean	D-3

RADIUSDictionary MBean D-3
AAA MBean D-4

APPENDIX E

SESM Load Balancing E-1

Cisco Load Balancing Solutions E-1
Configuring SESM for Load Balancing E-1
Using the Cisco IOS Server Load Balancer with SESM Portals E-2
 Load Balancing with Stickiness versus No Stickiness E-2
 Stickiness Issues with SSG Port-Bundle Host Key Feature E-2

APPENDIX F

Configuring the SSG for SESM Deployments F-1

Basic SSG Configuration F-1
Configuring the Port-Bundle Host Key Feature on SSG F-2
Sample SSG Configuration F-3

INDEX



About This Guide

This preface introduces the *Cisco Subscriber Edge Services Manager 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 services and value-added features.

Audience

This guide is intended for administrators and others responsible for installing, configuring, and running SESM applications and deploying SESM solutions.

Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	Preparing to Install SESM	Describes prerequisites to installing Cisco Subscriber Edge Services Manager (SESM) applications.
Chapter 2	Installing SESM	Describes how to install SESM software and bundled components, including the Security Policy Engine.
Chapter 3	SESM Configuration Management	Describes the methods for viewing and changing configuration values, including how to use the SESM remote management tool.
Chapter 4	Configuring a J2EE Container for SESM Applications	Describes how to change or fine-tune the J2EE container configuration after installation.
Chapter 5	Configuring SESM Portal Applications	Describes how to change the SESM portal application configuration after installation.
Chapter 6	Configuring CDAT	Describes how to change the CDAT configuration after installation.
Chapter 7	Configuring the RADIUS Data Proxy	Describes how to change the RDP configuration after installation.
Chapter 8	Configuring Security Policy Engine for SESM	Describes how to change the SPE configuration after installation.
Chapter 9	Running SESM Components	Describes how to start and stop SESM applications, including information about memory management.
Chapter 10	Configuring SESM Features	Describes how to configure location awareness, basic and advanced firewall features, automatic service connections, multikey authentication, and quality of service.
Chapter 11	Deploying a Captive Portal Solution	Describes how to configure the sample captive portal solution.
Chapter 12	Deploying an SESM/SSG Solution	Summarizes all of the attributes that control communication between components in SESM deployments.
Chapter 13	Troubleshooting SESM Installation and Configuration	Describes diagnostic procedures and methods and includes some troubleshooting tips.
Appendix A	SESM Security	Describes the security mechanisms used in SESM.
Appendix B	Configuring an LDAP Directory for SESM Deployments	Describes how to configure LDAP directories to work with SESM.
Appendix C	Configuring RADIUS for SESM Deployments	Describes the configuration steps required to include a RADIUS server in SESM deployments.
Appendix D	Configuring the Bundled SESM RADIUS Server	Describes the configuration options for the bundled SESM RADIUS server.

Chapter	Title	Description
Appendix E	SESM Load Balancing	Describes load balancing options for SESM deployments.
Appendix F	Configuring the SSG for SESM Deployments	Describes basic steps for configuring the SSG to work with SESM deployments.
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(5)*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Distributed Administration Tool Guide*
- *Cisco Subscriber Edge Services Manager Solutions Guide*
- *Cisco Subscriber Edge Services Manager 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/

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

These 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 this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

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

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing 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 online 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 with these tasks:

- 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

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

Cisco TAC inquiries 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.

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

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 this URL:

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

All customers, partners, and resellers who have a valid Cisco service 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 this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

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

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

Before calling, please 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). When you call the center, please have available your service agreement number and your product serial number.



Preparing to Install SESM

This chapter describes prerequisites to installing Subscriber Edge Services Manager (SESM) applications. It includes the following topics:

- [Installation Platform Requirements, page 1-1](#)
- [Memory and Disk Space Requirements, page 1-2](#)
- [Java Software Considerations, page 1-3](#)
- [Requirements for Related Network Components, page 1-5](#)
- [Dependencies among SESM Components, page 1-6](#)
- [Uninstalling a Previous SESM Installation, page 1-6](#)

Installation Platform Requirements

SESM applications can run on any platform that supports the Java Runtime Environment (JRE). [Table 1-1](#) lists the platforms tested in our labs.

Table 1-1 *Hardware Platforms*

Platform	Specifications
Solaris	<ul style="list-style-type: none">• Sun Ultra10 or Sun E250 (or later version)• Solaris Version 2.6 (or later version) operating system
Windows NT	<ul style="list-style-type: none">• Pentium III (or equivalent) processor• Windows NT Version 4.0, Service Pack 5 (or later version)
Windows 2000	<ul style="list-style-type: none">• Pentium III (or equivalent) processor
Linux	<ul style="list-style-type: none">• Red Hat Linux Version 7.1• SuSE Linux Version 7.3

Memory and Disk Space Requirements

The SESM applications are:

- The sample portal applications:
 - New World Service Provider (NWSP)
 - Personal Digital Assistant (PDA)
 - Wireless Access Protocol (WAP)
- Captive Portal and Message Portal applications
- Cisco Distributed Administration Tool (CDAT)
- RADIUS Data Proxy (RDP) server

The temporary disk space required for a SESM installation is approximately 50 MB on any of the supported platforms, regardless of the installation options you choose. [Table 1-2](#) shows RAM and permanent disk space requirements for a single instance of each component in SESM. These requirements are approximately the same for all of the supported platforms.

Table 1-2 RAM and Disk Space Requirements

Component Name	Disk Space (MB)	RAM
Jetty server	1.3	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, in this table, include Jetty server usage.
SESM portal applications (NWSP, WAP, and PDA)	14.6	As installed, the NWSP application uses 64 MB java reserved memory. This value is specified in the portal application start script. The “ SESM Portal Application Memory Requirements ” section on page 9-8 describes some factors to consider in sizing SESM portals for production deployments.
Captive Portal	5.1	The Captive Portal installation includes the Captive Portal and Message Portal applications.
RDP	4.1	As installed, the RDP application uses 64 MB Java reserved memory. This value is specified in the RDP start script. See the “ RDP Memory Requirements ” section on page 9-9 for more information.
Security Policy Engine (SPE) components	2.0	N/A
CDAT	6.3	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.
Tools	0.1	The tools are utilities for testing and development.

Java Software Considerations

A Java Runtime Environment (JRE) 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 JRE and the Java Development Kit (JDK). The section includes the following topics:

- [Solaris Patch Requirements, page 1-3](#)
- [Recommended and Required JVM Versions, page 1-3](#)
- [Installing the Bundled JRE, page 1-3](#)
- [JVM Requirements for Application Startup, page 1-4](#)
- [Specifying an Existing JRE or JDK, page 1-4](#)
- [Specifying the JRE or JDK in Startup Scripts, page 1-4](#)
- [Obtaining a JDK for SESM Web Development, page 1-5](#)

Solaris Patch Requirements

On older Solaris platforms, you might need to apply Solaris operating system upgrades (patches). To determine if the system requires patches, go to the Sun Microsystems Java site and start the process of downloading the JRE. 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.

Recommended and Required JVM Versions

A Java virtual machine (JVM) Version 1.3.x is recommended for running SESM applications. SESM is bundled with the following Java Runtime Environment (JRE):

- In the Solaris and Linux packages, JRE Version 1.3.1_03
- In the Windows package, JRE Version 1.3.0_03

**Note**

SESM has not been fully verified and is not supported on JVM Version 1.4.x.

Installing the Bundled JRE

The installation program determines whether to install the bundled JRE by doing the following:

1. It searches for a JDK Version 1.3.x that is already installed.
2. Failing that, it searches for a JRE Version 1.3.x that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.3.x_03.

To search for an existing JVM, the installation program looks in well-known locations. For a list of the search locations, see the [“JRE and JDK Troubleshooting” section on page 13-6](#).

If it finds a well-known location, the installation program verifies that the content is a JVM Version 1.3.x. If true, the installation program sets the JDK_HOME variable in the SESM startup scripts to point to that location and does not install the bundled JRE.

JVM Requirements for Application Startup

The SESM installation program creates and sets the `JDK_HOME` variable in the SESM application startup scripts. On application startup, the script checks the JDK or JRE version in the referenced `JDK_HOME` variable and issues error messages if the version is not appropriate for the application. Table 1-3 lists the JVM requirements for SESM application startup.

Table 1-3 Required JRE or JDK Versions

JVM Version	Startup Result
< 1.2.2	Not valid for SESM applications. None of the SESM applications will start if <code>JDK_HOME</code> points to these versions.
>= 1.2.2 and < 1.3.x	Valid for all SESM applications except for the SESM Web Services Gateway (WSG) applications. The WSG applications require JVM Version 1.3.x.
>= 1.3.x	Valid for all SESM applications. All SESM applications will start with this version. Note SESM is currently not verified and is not supported for JVM Version 1.4.x.

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/java1.3`.

Specifying the JRE or JDK in Startup Scripts

The SESM installation program sets the location of the JDK or JRE in the SESM application start scripts by setting the value for the `JDK_HOME` variable in the scripts. It sets `JDK_HOME` to the location of the JDK or JRE that it found installed on your system, or, if none was found, to the installed location of the bundled JRE.

If you change the location of the JDK or JRE after installation, or install a new version that you want the SESM applications to use, you must edit the value of `JDK_HOME` variable in the start scripts. Make the change in the following two startup files:

- Generic start 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—The RDP startup script does not call the generic start script.

Table 1-4 shows the path names of the startup scripts that you must change.

Table 1-4 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 1.3.1 recommended) must be installed on any system that web developers will use to create or modify the Java Server Pages (JSPs) for a customized SESM application. You can obtain JDK Version 1.3.1 from the Sun Java web page:

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

On systems that you will use to customize the SESM application, we recommend that you install the JDK before you install SESM. By doing so, 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 *Subscriber Edge Services Manager Web Developer Guide* 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 variable points to the directory into which you installed the JDK.

Requirements for Related Network Components

This section describes requirements of non-SESM components that might be required in SESM deployments. Topics are:

- [SSG and RADIUS Considerations, page 1-5](#)
- [Advantages to Running an LDAP Directory During SESM Installation, page 1-6](#)

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, 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.

Advantages to Running an LDAP Directory During SESM Installation

If you are installing SESM in LDAP mode, the installation program establishes communication with your LDAP directory, if possible.

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 the SESM web application or CDAT, as described in the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 8-3.

Dependencies among SESM Components

You can install all SESM components together on the same system (a typical installation), or you can install some components separately in a distributed manner (a custom installation). [Table 1-5](#) describes components that must be installed together on the same machine. The installation program detects these dependencies and enforces the correct installation.

Table 1-5 *Component Dependencies in a Distributed Installation*

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

Uninstalling a Previous SESM 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 13-8](#) for information.



Installing SESM

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

- [Obtaining the SESM Installation File and License Number, page 2-1](#)
- [Required Installation Privileges, page 2-3](#)
- [Installation Methods, page 2-3](#)
- [Turning On the Installation Logging Feature, page 2-5](#)
- [Installation Parameter Descriptions, page 2-5](#)
- [Installation Results, page 2-20](#)
- [Post-Installation Configuration Tasks, page 2-21](#)

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 2-1](#)
- [Downloading Software from the Cisco Web Site, page 2-2](#)
- [Uncompressing the Image, page 2-2](#)

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 Software 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. Provide 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** Click **Technical Support**.
- Step 4** In the popup menu, click **Software Center**.
- Step 5** Click **Web Software**.
- Step 6** Click **Cisco Subscriber Edge Services Manager**.
- Step 7** 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 2-4 for information about silent mode.

Table 2-1 shows the names of the compressed and executable files.

Table 2-1 *Installation Image Filenames*

Platform	Compressed Filename	Executable Installation Filename
Solaris	sesm-3.1.x-pkg-sol.tar	sesm_sol.bin
Linux	sesm-3.1.x-pkg-linux.tar	sesm_linux.bin
Windows NT	sesm-3.1.x-pkg-win32.zip	sesm_win.exe

Required 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 Methods

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.

Installing Using GUI Mode

GUI mode is the default installation mode. To run in this mode, execute the installation image. No command line 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. Before you start the installation, you must modify both files to match your requirements.

To prepare for silent mode:

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



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

- Step 2** Edit the values for each parameter in the file. [Table 2-2 on page 2-6](#) 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 mysesm.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 mysesm.iss
```

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.

Installation Parameter Descriptions

Table 2-2 describes the installation and configuration parameters that you enter during the installation process. You can 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 2-2 SESM Installation and Configuration Parameters

Category	Field	Explanation
General installation parameters	Installation type and license number	<p>Choose the type of installation:</p> <ul style="list-style-type: none"> • RADIUS Evaluation—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. • LDAP Evaluation—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. • Licensed—If you purchased an SESM license, choose this option and enter the license number provided by Cisco. <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>Note 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>Note You must have write privileges to the installation directory.</p> <p>To specify the installation directory, you can either: accept the displayed default installation directory, click Browse 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"> • On Solaris and Linux: /opt/cisco/sesm_3.1.x • On Windows NT: C:\Program Files\cisco\sesm_3.1.x

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
General installation parameters (continued)	Setup type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Typical—Installs all of the following components in the same directory on the same machine: <ul style="list-style-type: none"> – Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model. – Jetty—Includes the Jetty web server, the JMX server, and JNDI. – RDP—Installed only when installation type is LDAP evaluation or LDAP license. – CDAT—If the installation type is RADIUS evaluation or RADIUS license, CDAT includes only the remote management interface. If the installation type is LDAP evaluation or LDAP license, CDAT includes both the remote management and the LDAP directory management interfaces. – SPE—Installed only when installation type is LDAP evaluation or LDAP license. – Bundled SESM RADIUS Server and Proxy RADIUS Server—Installed in the tools directory for all installation types • Custom—Allows you to choose the components to install and configure from a checklist. Choose this option to: <ul style="list-style-type: none"> – Include the SESM captive portal solution in your installation. The captive portal solution supports several types of redirection capabilities for subscriber access management solutions. – Include the SESM web services gateway (WSG) application software in your installation. WSG provides a SOAP-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. – Reinstall one of the components. – Distribute the SESM components among different workstations. • Demo—Installs and configures the NWSP, WAP, and PDA applications to run in Demo mode. The configuration files are not set up to communicate with an SSG, a RADIUS server, or an LDAP directory. Choose this option when those components are not available. <p>Note If you install SESM in Demo mode and later want to run the portals in RADIUS or LDAP mode, we recommend that you perform another SESM installation in RADIUS or LDAP mode. Otherwise, you must make extensive adjustments to configuration attributes in the MBeans.</p> <p>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 the <i>Subscriber Edge Services Manager Solution Guide</i> for more information about installing and using SESM in Demo mode.</p> <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 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Configuration and Deployment	Web Application Host	<p>Specify the IP address or host name of the host on which the SESM portal applications will run. For Demo mode, you can use the value localhost.</p> <p> Caution For LDAP and RADIUS modes, this value must be a real IP address. You cannot use the values localhost or 127.0.0.1.</p>
	Web Application Port Number	<p>Specify the port on which the container (the J2EE web server) for the SESM portal applications will listen for HTTP requests from subscribers. The installation program updates the application startup scripts for NWSP, WAP, and PDA to use this value. If you want to run these applications simultaneously, you must edit the start scripts to ensure that each application uses a different port.</p> <p>The displayed default value is port 8080.</p> <p>Tip 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"> A secure socket listener (SSL) port is derived as follows: <p style="text-align: center;"><code>application port - 80 + 443</code></p> <p>When the application port is 8080, the SSL port is:</p> <p style="text-align: center;"><code>8080 - 80 + 443 = 8443</code></p> A management console port is derived as follows: <p style="text-align: center;"><code>application port + 100</code></p> <p>When the application port is 8080, the management port is:</p> <p style="text-align: center;"><code>8080 + 100 = 8180</code></p>
	SSG Deployment Option	<p>Check this option if you are deploying SESM for a solution that uses the SSG. When you choose this option, the installation program configures the SESM components to work with one or more SSGs.</p> <p>Uncheck this option if you are deploying SESM for a self care solution that does not require an SSG component. In this case, the installation program does not prompt for any SSG information. The self care solutions require LDAP evaluation or LDAP license installations.</p>

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

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
SSG details Tip Use the show run 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> Default: 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> Default: <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. Note 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. Default: 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 with Subscriber Requests](#)” section on page 5-16 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.

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
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.		
RADIUS server details	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. Default: <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. Default: <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. Default: <code>groupcisco</code> .
Note If you are installing SESM in RADIUS mode, you are finished with the installation of the standard components. If you are selected to install the captive portal solution from the custom installation window, go to the Captive Portal category later in this table.		

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
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	<p>Enter a user ID that has permissions to extend the directory schema. Use <code>cn</code> or <code>uid</code> as appropriate. For example:</p> <ul style="list-style-type: none"> For NDS, enter: <code>cn=admin, ou=sesm, o=cisco</code> For Sun ONE (or iPlanet), enter: <code>cn=Directory Manager</code> <p>Note The default configuration by the Sun ONE installation process uses <code>cn</code> for the Directory Manager. See the “Sun ONE and iPlanet Installation and Configuration Requirements” section on page B-4 for more information.</p>
	Directory admin password	<p>Enter the password for the directory administrator. This is the password you entered during directory installation and configuration. For example:</p> <ul style="list-style-type: none"> For NDS, enter the password you specified for the admin user during installation. For Sun ONE, enter the password you entered for the Directory Manager user during Sun ONE installation.

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 can not update the directory for SESM use. You must perform the updates at a later time before you run SESM web applications or CDAT. See the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 8-3 for instructions.

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
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 comes 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"> 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> <ul style="list-style-type: none"> For Sun ONE (or iPlanet), the container administrator is not the same as the directory administrator. You created this container administrator after Sun ONE installation. <pre>uid=yourAdmin,ou=sesm,o=cisco</pre>
	Directory password	Enter the password associated with the directory user ID.
Naming attribute	inetorgPerson	<p>Choose the component in distinguished name (dn) that allows access to the SESM container.</p> <ul style="list-style-type: none"> common name (cn)—NDS, for example, uses cn. unique identifier (uid)—Sun ONE, for example, uses uid for the SESM container. See the “Sun ONE and iPlanet Installation and Configuration Requirements” section on page B-4 for more information. <p>Note The SESM sample data uses cn. If you choose uid, you must edit the sample data before loading it into a Sun ONE or other directory that uses uid. See the “Loading Sample Data” section on page 8-4.</p>

Note 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.

Table 2-2 SESM Installation and Configuration Parameters (continued)


Category	Field	Explanation
RDP Configures RDP to SSG communication	RDP host	Enter the IP address or host name on which the RDP will run.  Caution Use a routable IP address. Do not use the values localhost or 127.0.0.1.
	Port number	Enter the port on which the RDP will listen. Default: 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” section on page 7-4 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. Default: <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">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.2. This value must also match the service password value you entered for the SESM portal. See the SESM “Passwords” section on page 2-10. Default: <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 “Passwords” section on page 2-10. Default: <code>groupcisco</code> .
Next hop password	Enter the password that SSG uses to request next hop tables from RDP. This password must match the value that was configured on the SSG host with the following command: <code>ssg next-hop download nextHopTableName password</code> The service-password value must be the same on all of the SSGs that communicate with this RDP server. Default: <code>nexthopcisco</code> .	

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
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"> 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. Default (non-proxy) mode—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the SPE API to send authorization requests to the LDAP directory.
	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 with the autoConnect attribute in the SESM MBean. See the "SESM MBean" section on page 5-4 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 can add more clients by adding elements to the allowedClients attribute in the RADIUSServerSocket MBean.</p> <p>If you do not check this option, the RDP accepts requests from any client (any SSG).</p>

If you choose the RDP Proxy mode option, the installation process prompts you for the following RADIUS server information.

AAA Server Details	Primary IP	Enter the IP address or the host name of the primary AAA server that you want RDP to communicate with.
	Primary port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on.
	Secondary 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 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	<p>Enter the shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers.</p> <p>Default: <code>cisco</code>.</p>

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
<p>If you choose the RDP Add client option, the installation program prompts you for the following information about one RDP client. You can add more clients by adding elements to the allowedClients attribute in the RDPMBean, RADIUSServerSocket component. See the “RDP MBean” section on page 7-4 for more information.</p>		
RDP Client	Client IP address	Enter the IP address of the SSG.
	Shared Secret	Enter the shared secret used for SSG to RDP communication. This value must match the value configured on the SSG, using the following command: <code>radius-server key SharedSecret</code>
<p>If you are performing a Custom installation and you check the Captive Portal item, the installation program prompts you for captive portal configuration information.</p>		
<p>Note The configuration information you enter in the following parameters must match TCP redirect configuration values on the SSG. The easiest way to ensure that values match in both places is to accept all of the default values presented by the installation process. Then configure the SSG based on the example captiveportal/config/ssgconfig.txt file. See Chapter 11, “Deploying a Captive Portal Solution,” for more information.</p>		
Captive Portal Server Configuration	Captive portal host	Enter the IP address or host name on which the captive portal solution will run.
	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 seven listeners in the web server, as follows: <ul style="list-style-type: none"> Subscriber redirection listener Initial logon redirection listener Advertising redirection listener Default service redirection listener Three service redirection listeners <p>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.</p> <p>Note If you use the same port number for more than one listener, some redirections will not work.</p> <p>Default: 8090</p>
	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"> Initial logon redirections Advertising redirections <p>For those redirection types, the default URIs displayed later in this installation procedure refer to pages in the Message Portal application.</p>

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
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
Main web server configuration	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"> Unauthenticated user redirection Default unconnected service redirection Specific unconnected service redirections Error handling due to captive portal misconfiguration (if a port has been used which is not configured for redirection). 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
Unauthenticated User Redirection	Enable	Check this box to configure unauthenticated user redirections.
	Port In	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. Note You must configure the SSG TCP redirect feature to send unauthenticated user redirections to this port. Default: 8090
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for unauthenticated user redirections. The default values reference the NWSP application. <ul style="list-style-type: none"> Host—Enter the name or IP address for the web server that contains the content application for unauthenticated user redirections. Port—Enter the listener port number for this content application. The default is the port number you entered for the NWSP application. URI—The absolute page name you want the subscriber to see. The default is /home, which is the NWSP logon page.


Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Initial Captivation	Enable	Check this box to configure initial logon redirections.
	Port In	Enter the port that the Captive Portal web server will listen on for initial logon redirections. Note You must configure the SSG TCP redirect feature to send initial logon redirections to this port. Default: 8091
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for initial logon redirections. The default values reference the Message Portal application. <ul style="list-style-type: none"> Host—Enter the name or IP address for the web server that contains the content application for initial logon redirections. Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application. URI—The absolute page name you want the subscriber to see. The default is /initial, which is the Message Portal greeting page.
	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
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. Note 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"> Host—Enter the name or IP address for the web server that contains the content application for advertising redirections. Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application. URI—The absolute page name you want the subscriber to see. The default is /advertising, which is the Message Portal advertising page.
	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 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Unconnected Service Redirection	Enable	Check this box to configure service redirections, including a default service redirection.
	Default Service Redirect Port In	Enter the port that the Captive Portal web server will listen on for default service redirections. Default service redirections are used for services whose address does not belong to the destination network of any of the specific service redirections. Note 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. Note 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"> The host and port values are the ones you entered earlier for the service application. The page name is /serviceRedirect, which is a generalized NWSP page. Configuration parameters in nwsp.xml define more specific pages. 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 Unconnected 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 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
CDAT	CDAT host	Enter the IP address or host name on which the CDAT application will run.  Caution Use a routable IP address. Do not use the values localhost or 127.0.0.1.
	CDAT port number	Enter the port number on which the CDAT web server will listen. The default is 8081.
Links for CDAT main window	Hosts and port numbers for remote SESM applications	The installation program prompts for host names and port numbers of all applications that you did not install during the current session. It uses this information to configure links on the CDAT main window pointing to the management consoles of these remote SESM applications. To skip the prompts for applications that you have not installed on any system or do not want CDAT to manage, click Next . For applications that you installed during the current session, the installation program already has the link information.
The installation program installs the components on your system. When it is finished installing the files, and if it successfully connected to your LDAP directory, it displays the following additional prompts about modifications to the directory.		
LDAP directory modifications	Extend schema	Choose this option if you are installing SESM to run with a new LDAP directory and you want the installation program to apply the SPE schema extensions to the directory. The 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> . 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 “ Post-Installation Configuration Tasks ” section on page 2-21. Note The schema must be extended for each LDAP directory used in the SESM deployment. If multiple instances of SESM using just one LDAP directory exist, then the schema need only be extended in one of the installs where the SPE component is selected.
	Install RBAC	Choose this option if you want the installation program to load the top-level 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. If you do not choose this option, you must install RBAC objects later, before running the SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “ Post-Installation Configuration Tasks ” section on page 2-21. Note The RBAC objects must be installed into each LDAP directory used in the SESM deployment. If multiple instances of SESM using just one LDAP directory exist, then the RBAC objects must only be loaded in one of the installs where the SPE component is selected.

Installation Results

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

- `_jvm`—(Optional) This directory contains the JRE that is shipped with SESM. If your SESM installation directory does not include `_jvm`, it means that the installation program located a suitable JSDK or JRE elsewhere on your system. See the “[Installing the Bundled JRE](#)” section on page 1-3.
- `_uninst`—This directory contains the utility to uninstall the components you just installed. To uninstall components, run the executable file in this directory.
- `captiveportal`—This directory exists only if you installed the Captive Portal solution using a Custom installation.
- `cdat`—This directory contains configuration files and libraries for CDAT.
- `dess-auth` (LDAP-mode only)—This directory contains the SPE DESS and AUTH libraries, SPE DESS schema, and sample data. The schema subdirectory contains the `README.SESM.LDIF.html` file, which explains how to manually update the LDAP directory with the SPE schema, load initial RBAC objects, and load sample data.
- `docs`—This directory contains the `apidoc` directory, which holds the Java documentation for the SESM application programmer interface (API).
- `jetty`—This directory contains the following subdirectories:
 - `bin`—Contains start scripts for Jetty server applications
 - `config`—Contains configuration files that control Jetty servlets
 - `lib`—Contains the Jetty server class libraries
- `lib`—This directory contains the SESM class libraries.
- `messageportal`—This directory exists only if you installed the Captive Portal solution using a Custom installation, and chose the Install Message Portal option during the installation.
- `nwsp`, `pda`, and `wap`—These directories contain the following subdirectories:
 - `config`—Contains a configuration file for the portal application and a demo data file.
 - `docs`—Contains the application javadoc files.
 - `webapp`—Contains the Web application, including libraries, JSPs, images, and the `WEB-INF` directory, which includes J2EE configuration files, such as `web.xml` and `web-jetty.xml`.
- `rdp`—This directory contains startup scripts, configuration files, and libraries for the RDP server.
- `redist`—This directory contains libraries from third-party companies that Cisco is redistributing. It includes the Jasper JSP framework, the JMX framework, and the JAXP XML parser framework. It also includes test tools.
- `tools`—This directory contains scripts that developers can use to precompile customized SESM JSPs, configure and start the bundled RADIUS server, and configure and start a proxy RADIUS server.
- `licensenum.txt`—This file contains the license number that you used during installation and the version number of the SESM software that you installed.

Post-Installation Configuration Tasks

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

-
- Step 1** Install and configure other software components required for your SESM solution, such as RADIUS servers, LDAP directory, and SSGs.
 - Step 2** (LDAP mode only) Update the LDAP directory with SPE schema extensions and load initial RBAC objects if you did not allow the installation program to do these tasks. See the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 8-3.
 - Step 3** (LDAP mode only) Optionally load sample data into the LDAP directory. See [“Loading Sample Data”](#) section on page 8-4.
 - Step 4** 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 with Subscriber Requests”](#) section on page 5-16.
 - Step 5** If you installed the captive portal solution, see the [“Additional Configuration Steps”](#) section on page 11-7 for instructions on configuring an SSG to work with the installed captive portal features.
 - Step 6** If you installed the RDP server and turned on the restricted client feature, you might need to add more SSGs to the RDP’s client list. The installation program accepts information for one client. See the [“Using a Restricted Client List”](#) section on page 7-3.
-

For information about starting SESM portals and logging on, see [Chapter 9, “Running SESM Components.”](#)

For information about configuring a customized SESM portal application, see the [“Configuring a Customized SESM Application”](#) section on page 5-19.



SESM Configuration Management

The SESM installation program assigns initial values to all of the key SESM attributes, using a combination of default values and values you provide during the installation. This chapter describes how to change these initial configuration values. Topics in this chapter are:

- [Introduction, page 3-1](#)
- [Using the SESM Remote Management Tool, page 3-3](#)
- [Directly Editing MBean Configuration Files, page 3-13](#)
- [Changing web.xml and webdefault.xml, page 3-18](#)

Introduction

This section introduces terms and concepts related to configuring SESM applications.

Java Management Extensions

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>

When you install the Jetty component from the SESM installation package, you are also installing a JMX server from Sun Microsystems. You can substitute any JMX-compliant 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 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. The contents of the MBean configuration files control ConfigAgent activity.

MBean Description

MBeans are Java classes that follow a model described in the JMX 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 attributes in MBeans to:

- Configure components and the communication connections between those components.

Read-write attributes in the SESM MBeans let deployers configure the application. For example, the SESM MBean configures the SESM mode; the SSG MBean configures communication between SSG and the SESM web application, the 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.

- Provide metrics about a running application.

Read-only attributes in the SESM MBeans let deployers monitor a running application. For example, the SESM MBean includes attributes for the current number of active sessions, the highest number of active sessions handled by this application so far, the number of authenticated sessions, the number of failed authentications, and so on. The SSG MBean includes attributes for the number of requests received, the number of access reject messages received, the number of timeouts, and so on.

Methods for Changing MBean Attribute Values

To change the configuration attributes in an SESM application's MBeans, you can:

- Use the SESM remote management tool—You can change the value of most MBean attributes while the SESM application is running by using the SESM remote management tool. These changes take effect immediately on the running application. You can optionally store the changes in the MBean configuration file so that they persist over application restarts.

See the [“Using the SESM Remote Management Tool”](#) section on page 3-3 for more information.

- Directly edit the application's MBean configuration file—You can change the value of some attributes by directly editing the appropriate MBean configuration file. These changes take effect the next time you start the application.

See the [“Directly Editing MBean Configuration Files”](#) section on page 3-13 for more information.

Monitoring Features

To monitor a running application, use the SESM remote management tool. You can view the current value of any read-only attribute using this tool. You can optionally set a refresh interval that automatically refreshes the window with new metric values every set number of seconds.

Using the SESM Remote Management Tool

This section describes how to use the SESM remote management tool. Topics are:

- [SESM Remote Management Overview, page 3-3](#)
- [Accessing an Application's Agent View, page 3-4](#)
- [Using the Agent View, page 3-8](#)
- [Using the MBean View, page 3-9](#)
- [Monitoring an Application, page 3-12](#)

SESM Remote Management Overview

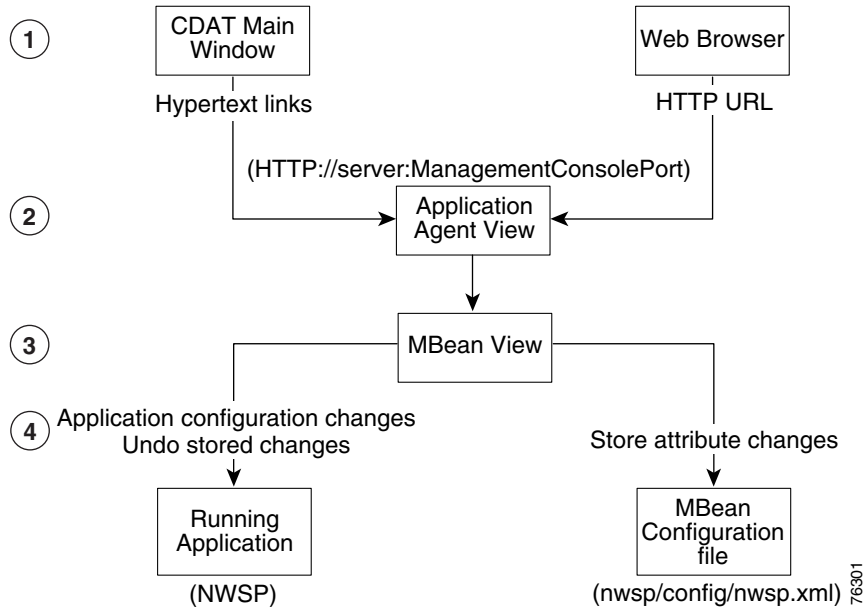
The SESM Remote Management tool provides a way to monitor and change the attributes in a running SESM application. It also provides a way to optionally store changes in the application configuration files, so that the changes persist across restarts.



Note

The SESM ManagementConsole is an adaptation of the HTML adaptor server included with the Sun example JMX server. The Cisco adaptations in this release add persistence features to the server. Plans for future SESM releases include an improved user interface.

An application's Agent View is the window into SESM remote management. [Figure 3-1](#) summarizes how to access the Agent View and the tasks you can perform from it.

Figure 3-1 Remote Management Summary

- | | |
|----------|---|
| 1 | Each SESM application has a management console, known as the Agent View. You can access an application's Agent View in two ways: <ul style="list-style-type: none"> Click a link configured on the CDAT main window—From this central location, you can conveniently access the Agent Views for all of the SESM applications. Enter the URL for the application's management console in a web browser. |
| 2 | An application's Agent View lists all of the MBeans in the running application. From the Agent View, you can access MBean Views. |
| 3 | An MBean View provides access to all of the attributes in the MBean. |
| 4 | From the MBean View, you can perform the following actions on attribute values: <ul style="list-style-type: none"> View current attribute values for the running application. Apply changes to most Read/Write attributes. Applied changes take immediate effect on the running application. Store changes in the application's configuration file. Stored changes persist for future restarts of the application. <p>Undo (revert) changes sequentially from the most recent store to the first store made in the session. The Undo action only affects the running application, even though it undoes the stored changes. To persist an undo, you must store the change.</p> |

Accessing an Application's Agent View

This section describes how to configure, start, and access an Agent View. Topics are:

- [Configuring the ManagementConsole MBean, page 3-5](#)
- [Starting and Removing the Management Console, page 3-5](#)
- [URLs for Accessing Agent Views, page 3-6](#)
- [CDAT Main Window, page 3-6](#)
- [Configuring Links to Agent Views on the CDAT Main Window, page 3-7](#)

Configuring the ManagementConsole MBean

All of the SESM applications include the ManagementConsole MBean, which configures and starts an Agent View for the application. [Table 3-1](#) describes the attributes in the ManagementConsole MBean.

Table 3-1 SESM Portal Application—ManagementConsole MBean

Attribute Name	Explanation
Port	<p>Specifies the management console port for this application.</p> <p>In the installed configuration files, the port value is a system property named:</p> <pre>management.portno</pre> <p>All of the installed startup scripts set this 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. The user must enter a user ID and password that matches values specified in AuthInfo.</p> <p>Each application has a ManageConsole MBean that configures the login values for that application's management console. You can configure different user IDs and passwords for each application or use the same values for all applications.</p> <p>You can specify multiple sets of AuthInfo information to allow multiple users access to a management console.</p> <p>The AuthInfo array has two elements:</p> <ol style="list-style-type: none"> 1. User ID—Enter a user ID that you want to have access to the management console. The default value in all of the MBean configuration files is <code>MgmtUser</code>. 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>. <p>You can add, change, and delete AuthInfo values in the configuration files or on the management console.</p> <p>Note If you use the management console to change or delete the user ID or password that you used to log on to the console, the console redisplay the logon prompts. You must log in again using the new authentication values.</p>

Starting and Removing the Management Console

All of the SESM applications are configured to start a management console on application startup.

If you do not want to start a management console for an application, comment out the following lines in the application's MBean configuration file:

```
<Action jmxname="com.cisco.sesm:name=ManagementConsole">
  <Call name="start"/>
</Action>
```

URLs for Accessing Agent Views

You can access an Agent View by typing its URL in the address field of a web browser.

The URL for accessing the Agent View must include the name of the host on which the application is running and the configured management console port number (for example, the value for management.portno). An example URL for the NWSP Agent View is:

```
http://server1:8180
```

CDAT Main Window

The CDAT main window provides the most convenient way to access Agent Views. This window contains links to all of the Agent Views for all of the SESM applications that you install. You can add additional links as you develop more applications. [Figure 3-2](#) shows the CDAT main window.

Figure 3-2 CDAT Main Window



To use the CDAT main window to access an Agent View, follow these procedures:

Step 1 Start CDAT. The CDAT startup script is located in:

```
jetty
  bin
    startCDAT
```

Step 2 Open a web browser.

Step 3 Direct the browser to the CDAT main window ([Figure 3-2](#)).

The URL for accessing CDAT must include the server name where the CDAT is running and the configured CDAT port. The default port used by the installation program is 8081. An example URL for the CDAT main window is:

```
http://server1:8081
```

Step 4 Click the hot text for the Agent View that you want to access.

Configuring Links to Agent Views on the CDAT Main Window

The SESM installation process adds a link to the CDAT main window for Agent Views to each SESM application that you install. You can add additional links as you install more instances of the applications or if you develop customized applications.

To add additional links or to change the URLs behind the existing links, edit the links attribute in the MainServlet MBean. See the [“MainServlet MBean” section on page 6-2](#) for information about the links attribute.

Using the Agent View

The Agent View displays the MBeans in a running application. Figure 3-3 shows the Agent View for a NWSP application running in LDAP mode.

Figure 3-3 Agent View

The screenshot shows the 'Agent View' window for a JMX RI/1.0 application. At the top, there is a filter box labeled 'Filter by object name:' containing the text '*:*'. Below this, a message states: 'This agent is registered on the domain **com.cisco.sesm**. This page contains 22 MBean(s).' To the right of this message is an 'Admin' button. A horizontal line separates this header from the main content area, which is titled 'List of registered MBeans by domain:'. The content is a tree view of MBeans:

- **JMImplementation**
 - [type=MBeanServerDelegate](#)
- **com.cisco.sesm.ignore**
 - [name=ManagementAdaptor](#)
- **com.cisco.sesm.jmx**
 - [name=Version](#)
- **com.cisco.sesm**
 - [agent=Configuration](#)
 - [context=sesm](#)
 - [name=Directory](#)
 - [name=Directory.type=Connection.instance=Primary](#)
 - [name=Directory.type=Connection.instance=Secondary](#)
 - [name=Logger](#)
 - [name=ManagementConsole](#)
 - [name=SESM](#)
 - [name=SSG](#)
 - [name=Version](#)
 - [name=WebApp](#)
- **org.mortbay.jetty**
 - [Debug=0](#)
 - [name=Jetty.Server=0](#)

76302

Table 3-2 explains the actions you can perform from the AgentView.

Table 3-2 Actions from the Agent View

Name	Description
Admin button	Click the Admin button at the top of the window to add a new MBean to the application. Note You should not need to add new MBeans to installed applications.
MBean links	Click an MBean in the list to navigate to the MBean View.

Using the MBean View

The MBean View displays the attributes in an MBean. Figures 3-4 and 3-5 show the MBean View for the WebApp MBean in NWSP. Table 3-3, which follows the figures, explains the numbered callouts in these figures.

Figure 3-4 MBean View—Top Portion

MBean View [JMX RI/1.0]

- **MBean Name:** com.cisco.sesm.name=WebApp
- **MBean Java Class:** com.cisco.sesm.webapp.config.WebAppMBean

[Back to Agent View](#) Reload 1 2 Unusable

MBean description:

com.cisco.sesm.webapp.config.WebAppMBean

List of MBean attributes: 3

Name	Type	Access	Value
confirmAtAccountLogoff	boolean	RW	<input checked="" type="radio"/> True <input type="radio"/> False
confirmAtServiceLogoff	boolean	RW	<input checked="" type="radio"/> True <input type="radio"/> False
confirmAtServiceLogon	boolean	RW	<input type="radio"/> True <input checked="" type="radio"/> False
credentialMaxLength	int	RW	<input type="text" value="20"/>
defaultURI	java.lang.String	RW	<input type="text" value="/home"/>
dimensions	com.cisco.sesm.webapp.config.DimensionData[]	RW	Type Not Supported: [[Lcom.cisco.sesm.webapp.config.DimensionData;@21302
serviceLogonURI	java.lang.String	RW	<input type="text" value="/serviceLogon"/>
serviceNotGivenURI	java.lang.String	RW	<input type="text" value="/status"/>
serviceStartURI	java.lang.String	RW	<input type="text" value="/serviceStart"/>
serviceSubscriptionURI	java.lang.String	RW	<input type="text" value="/subscriptionManage"/>
sessionTimeOut	int	RW	<input type="text" value="7200"/>

Apply 4

76306

Figure 3-5 MBean View—Bottom Portion

Apply

List of MBean operations: **5**

[Description of addDimensionAttribute](#)

void **addDimensionAttribute** (java.lang.String [param0](#)
 (java.lang.String [param1](#)
 (java.lang.String [param2](#)

[Description of addDimension](#)

void **addDimension** (int [param0](#)
 (java.lang.String [param1](#)
 (java.lang.String [param2](#)

[Description of addDimension](#)

void **addDimension** (int [param0](#)
 (java.lang.String [param1](#)

[Description of undo](#)

void **undo** **6**

[Description of store](#)

void **store** **7**

76306

Table 3-3 Actions from the MBean View

Figure Key	Name	Description
1	Reload interval Reload button	A reload obtains new information from the application and reloads the page. <ul style="list-style-type: none"> The reload interval specifies the number of seconds between automatic reloads. You can change the reload interval here. The change takes effect immediately. If the reload interval is 0 (the default), use the Reload button to manually reload the view.
2	Unregister button	Makes the MBean inaccessible to the running application. Do not use this button.

Table 3-3 Actions from the MBean View (continued)

Figure Key	Name	Description
3	MBean attributes	<p>Lists all of the attributes in the MBean. From this section, you can:</p> <ul style="list-style-type: none"> • Display a short description of the attribute—Click the attribute name. For more detail about any attribute, see the appropriate chapter in this manual. • Change the value of read-write attributes • Monitor metrics (read-only attributes) <p>To change an attribute value, do one of the following, depending on the attribute type:</p> <ul style="list-style-type: none"> • Integers and strings—Type the attribute value in the Value column. • Booleans—Choose the desired radio button. • Arrays: <ul style="list-style-type: none"> – If the Value column contains the phrase “Type Not Supported”—Choose one of the buttons from the MBean Operations section. – If the Value column contains a hotlink phrase “view the values of <i>attribute</i>”—Click the link, which takes you to another page that lists the array elements and current values. Use the appropriate operation in the MBean Operations section to add or change element values.
4	Apply button	Sends the attribute changes to the running application. The change takes effect immediately on the running application unless you receive an error message stating otherwise.
5	MBean operations	Lists operations that you can perform against the MBean. The list is different for each MBean. However, all MBeans include the Store and Undo operations, described below.
6	Undo button	<p>Reverts the running application to the state before the last store. All store operations are captured and can be undone, in sequential order starting with the last change first. You can reverse a previously stored undo. Table 3-4 shows how the Undo operation works.</p> <p>Note The Undo operation applies to the running application only. To save an Undo action to the configuration files (that is, undo the changes stored in the configuration file), click the Store button again.</p>
7	Store button	<p>Saves the attribute changes in the appropriate configuration file (for example, nwsp.xml). This action persists the changes for future application restarts. The Store button has the following effects on the MBean in the configuration file:</p> <ul style="list-style-type: none"> • Deletes any <SystemProperty> or <Property> tags used in the MBean in the originally-installed configuration file. The Store button saves the currently defined value of all attributes in the MBean, regardless of how those values were derived. The Store operation is not aware of property definitions or values assigned by the startup script. • Deletes comments in the MBean. • Includes all read-write attributes in the MBean, whereas the installed configuration files might include only the most commonly changed attributes. • Deletes a <Call> tag inside a <Configure> tag. If the <Call> element sets an attribute value, the rewritten MBean contains the attribute assignment performed in a different way. However, if the <Call> element is performing an action other than setting an attribute value, the action is lost. The correct way to call methods is to use the <Action> tag.

Table 3-4 Sequential Store and Undo Operations

Action	Attribute Value in the Running Application	Attribute Value in the Configuration File
Startup	5	5
Change the value to 10 in the MBean View	5	5
Apply the change	10	5
Store the change	10	10
Undo	5	10
Store	5	5

Monitoring an Application

The SESM application MBeans include read-only attributes that provide activity, performance and memory metrics. You can monitor these metrics from the same MBean View that you use to change the values of read-write attributes.

Some useful monitoring features on the MBean View are:

- **Reload period**—Set an automatic refresh rate by changing the reload period. The browser automatically refreshes the attributes values at the rate specified by the reload period. The default reload period is 0, which turns off the automatic refresh feature.
- **Reload button**—If you do not set an automatic reload period, you can refresh the read-only values at any time by clicking the Reload button.

Figure 3-6 shows metrics in the SESM MBean in the NWSP application.

Figure 3-6 Metrics in the SESM MBean in the NWSP Application

MBean View

[JMX RI/1.0]

- **MBean Name:** com.cisco.sesm.name=SESM
- **MBean Java Class:** com.cisco.sesm.core.model.SESMMBean

Reload Period in seconds:

[Back to Agent View](#)

5 Reload

Unregister

MBean description:

SESM Mode configuration.

List of MBean attributes:

Name	Type	Access	
activeAuthenticatedSessions	int	RO	0
activeSessions	int	RO	0
authenticatedSessions	int	RO	0
authenticationFailures	int	RO	0
authenticationSPI	java.lang.String	RO	com.cisco.sesm.spis.radius.RADIUSAuthe
authenticationTime	long	RO	0
authorizationSPI	java.lang.String	RO	com.cisco.sesm.spis.dess.DESSAuthorizati
authorizationTime	long	RO	0
autoConnect	boolean	RW	<input type="radio"/> True <input checked="" type="radio"/> False

76307

Directly Editing MBean Configuration Files

You can use a text editor to directly edit any of the SESM MBean configuration files. This section includes information related to direct editing. Topics are:

- [Restarting Applications after Editing](#), page 3-14
- [MBean Configuration File Names](#), page 3-14
- [MBean Configuration File Format](#), page 3-15
- [SystemProperty and Property Tags in Configuration Files](#), page 3-17

Restarting Applications after Editing

If you change configuration values by directly editing the configuration files, you must stop and restart the SESM application and its Jetty server before the changes take effect. If you deployed SESM in LDAP mode, you also must stop and restart RDP.

See [Chapter 9, “Running SESM Components,”](#) for instructions on stopping and starting applications.

MBean Configuration File Names

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.

[Table 3-5](#) lists all of the MBean configuration files in SESM deployments.

Table 3-5 Summary of MBean Configuration Files

Component	File Path Name	Description
Container (Jetty)	jetty config nwsp.jetty.xml wap.jetty.xml pda.jetty.xml cdat.jetty.xml captiveportal.jetty.xml messageportal.jetty.xml	These files configure Jetty server containers See the “Jetty Container MBeans” section on page 4-2 for information.
SESM web portals	nwsp config nwsp.xml wap config wap.xml pda config pda.xml	These files configure the following items for the web portals: <ul style="list-style-type: none"> • SESM mode and other deployment options. • Communication between SESM applications and SSG, as appropriate. • Communication between SESM applications and RADIUS servers. • Logging and debugging for the SESM application. See the “SESM Portal Application MBeans” section on page 5-1.
Captive portal solution	captiveportal config captiveportal.xml messageportal config messageportal.xml	These files configure captive portal options and behavior. See Chapter 11, “Deploying a Captive Portal Solution,” for more information.
RDP	rdp config rdp.xml	This file configures: <ul style="list-style-type: none"> • RDP options and RDP communication with SSG • Optionally, RDP communication with a RADIUS server • Logging and debugging for RDP See the “RADIUS Data Proxy MBeans” section on page 7-3.

Table 3-5 Summary of MBean Configuration Files (continued)

Component	File Path Name	Description
CDAT	cdat config cdat.xml	This file configures: <ul style="list-style-type: none"> System resource usage for the CDAT application Logging and debugging for the CDAT application Agent View links on the CDAT main window See the “ CDAT Application MBeans ” section on page 6-1 for more information.
SPE	applicationName config dessauth.xml For example: nwsp/config/dessauth.xml pda/config/dessauth.xml wap/config/dessauth.xml rdp/config/dessauth.xml cdat/config/dessauth.xml	The dessauth.xml files configure LDAP directory security and connection attributes, SPE caching, and SPE logging. Each SESM application has its own version of the dessauth.xml file. See the “ SPE Attributes ” section on page 8-1 for more information.

MBean Configuration File Format

This section summarizes the MBean file format Mdefined in `xmlconfig.dtd`. The purpose of this summary is to provide enough information for you to easily edit the configuration files.

Use the following example as a reference while reading the format guidelines that follow. The example configures the Logger, Version, and ManagementConsole MBeans for SESM portals.

```
<XmlConfig>

<!-- ===== -->
<Instantiate order="1"
    class="com.cisco.sesm.jmx.LoggerMBean"
    jmxname="com.cisco.sesm:name=Logger"/>

<Instantiate order="5"
    class="com.cisco.sesm.jmx.VersionMBean"
    jmxname="com.cisco.sesm.jmx:name=Version" />

<Instantiate order="99"
    class="com.cisco.sesm.jmx.AgentView"
    jmxname="com.cisco.sesm:name=ManagementConsole"/>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=Logger">
  <Set name="debug" type="boolean">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"><Property name="application.home"
default="." />/logs/yyyy_mm_dd.application.log</Set>
  <Set name="logFrame" type="boolean">false</Set>
  <Set name="logThread" type="boolean">false</Set>
  <Set name="logStack" type="boolean">false</Set>
  <Set name="logToErr" type="boolean">false</Set>

```

```

    <Set name="trace"      type="boolean">true</Set>
    <Set name="warning"   type="boolean">true</Set>
  </Configure>
<!-- ===== -->
<Action jmxname="com.cisco.sesm:name=ManagementConsole">
  <Call name="start"/>
</Action>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:jmx:name=Version">
  <Set name="verbose" type="boolean">false</Set>
</Configure>

<!-- ===== -->
<Configure jmxname="com.cisco.sesm:name=ManagementConsole">
  <Set name="port" type="int"><Property name="management.portno" default="8180"/></Set>
  <Set name="authInfo">
    <Array class="com.sun.jdmk.comm.AuthInfo">
      <Item>
        <New class="com.sun.jdmk.comm.AuthInfo">
          <Set name="password">MgmtPassword</Set>
          <Set name="login">MgmtUser</Set>
        </New>
      </Item>
    </Array>
  </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 `<Instantiate>`, `<Configure>`, and `<Action>` elements.
- An `<Instantiate order = x>` element 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.

- An `<Action>` element calls methods on an MBean.
- 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

ConfigAgent can match a registered MBean by both class and name.

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

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

Where:

attributeName is the MBean parameter name whose value is being set. Do not change any *attributeName*.

dataType is the required data type of the value you specify. Do not change *dataType* unless the change is related to application development. The *dataType* can be: none (which defaults to string), string, int, boolean, URL, an Array element, a Map element, or a New element.

value is the attribute 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.

Any <Call> tag inside a <Configure> tag disappears if you persist the MBean with the remote management tool. If the <Call> element is setting an attribute value, the rewritten MBean contains the attribute assignment performed in a different way. However, if the <Call> element was used to perform an action other than setting an attribute value, the action is lost. The correct way to call methods is to use the <Action> tag.

- 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, Call, Array, or Map elements after any Arg elements. These nested elements are applied to the created or returned object.
- The <Action> tag calls a method defined within the class.
- A <SystemProperty> or <Property> tag might appear inside a <Set> or <Call> tag.



Note The default values assigned in these tags are not used if a value is assigned in the start script. You must remove any use of the setting in the appropriate startup script for the default values in the configuration files to take effect. See the next section, “[SystemProperty and Property Tags in Configuration Files](#)”, for more information.

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 with the JMX server.

- Configures an MBean—The <Configure> tag causes ConfigAgent to configure an MBean. ConfigAgent can configure existing MBeans and MBeans that are registered later. ConfigAgent configures an MBean if there is a matching entry in the XML file for that MBean. The <Set> tag sets attribute values for the MBean.
- Performs actions on an MBean—The <Action> tag causes ConfigAgent to perform the specified action. For example, ConfigAgent can start an MBean.

SystemProperty and Property Tags in Configuration Files

The installed MBean configuration files use <SystemProperty> and <Property> tags as the value for some attributes. Both tags use the features of a Java system property. The difference between the two tags is:

- SystemProperty tags—The property value applies to the Java virtual machine (VM). All applications running in the same container are configured to use the same value.

Table 3-6 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 application	applicationName webapp WEB-INF web.xml	This file defines J2EE application parameters, including parameters related to Java Server Pages (JSPs). There is a separate web.xml file for each web application.
SESM application	applicationName webapp WEB-INF web-jetty.xml	This file is required for the port-bundle host key feature. See “Container Requirement for the Port-Bundle Host Key Feature” section on page 4-1 for more information.



Configuring J2EE Containers for SESM Applications

The SESM installation process performs all required configurations for running the SESM applications in Jetty containers. Use this chapter if you want to change or fine-tune the J2EE container configuration after installation. This chapter contains the following topics:

- [J2EE Containers, page 4-1](#)
- [Container Requirement for the Port-Bundle Host Key Feature, page 4-1](#)
- [Creating WAR Files for Containers Other Than Jetty, page 4-2](#)
- [Jetty Container MBeans, page 4-2](#)

J2EE Containers

SESM portals and CDAT are J2EE web applications. They must run in a J2EE web server. The web server is the *container* for the applications that run in it. The SESM installation program installs and configures Jetty servers as the containers for the SESM portal applications and CDAT. Deployers can create a web archive (WAR) file from the installation and deploy SESM applications in other containers.

Container Requirement for the Port-Bundle Host Key Feature

Before you deploy SESM applications in containers other than Jetty, determine if your solution requires the port-bundle host key feature on the Service Selection Gateway (SSG). For solutions that use SSG, we recommend enabling the port-bundle host key feature.



Note The Jetty server is currently the only J2EE-compliant server that can support the port-bundle host key feature.

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. To do this, the Jetty server uses the `PortBundleHandler`, an extension that allows access to the request handling part of the server API and thus get the remote port number.

The `PortBundleHandler` is added to the Jetty container by the following file under the SESM application directory (nwsp, for example):

```
nwsp
  webapp
    WEB-INF
      web-jetty.xml
```

Jetty version 4.1.0RC6 is bundled with SESM Release 3.1(7). This Jetty version adds the contents of `web-jetty.xml`. In Jetty versions earlier than Version 4, the port bundle handler must be added in the `nwsp.jetty.xml` file.

Creating WAR Files for Containers Other Than Jetty

You can create web archive (WAR) files to use in deploying the sample SESM applications in non-Jetty web containers. To create a WAR file, use the `jar` command on the `webapps` directory under the desired SESM application. For example, to create a WAR file for NWSP on a Solaris system, enter the following commands:

```
cd installDir/nwsp/webapp
jar cf0 ../nwsp.war *
```

For instructions about deploying an application using a WAR file, see the documentation for the container you are using.

The installed configuration is specific to a Jetty container. If you choose to deploy the SESM applications in a container other than Jetty, you must make changes to the container MBeans. For example, you must change class or object names. You might need to add MBeans.

Jetty Container MBeans

A Jetty container uses the following MBeans:

- [Log MBean, page 4-3](#)
- [Debug MBean, page 4-4](#)
- [Server MBean, page 4-5](#)
- [SESMSocketListener MBean, page 4-6](#)
- [SESMSSSLListener MBean, page 4-7](#)

To change attributes in these MBeans, you can use either of the following methods:

- Edit the container's MBean configuration file:

```
jetty
  config
    nwsp.jetty.xml
    wap.jetty.xml
    pda.jetty.xml
    cdat.jetty.xml
```

- Make changes using the Agent View running on the application's management port. For example, the Agent View for the NWSP application provides access to both the application and the container MBeans.



Note Containers do not have their own management consoles.

Log MBean

The Log MBean enables the Jetty server debugging and logging mechanisms and configures the information that appears in the jetty log file. [Table 4-1](#) describes the attributes in the Log MBean.

Table 4-1 Jetty Container—Log MBean

Attribute Name	Explanation
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 the log messages include frame details. Installed default: false
logOneLine	Installed default: false
logStackSize	Controls whether or not the log messages include an indication of stack depth. Installed default: false
logStackTrace	Controls whether or not the log messages include trace information. Installed default: false
logTags	Installed default: true
logTimeStamps	Installed default: true
append	Indicates if messages overwrite existing contents (false) or are appended to the existing file (true). Installed default: true

Table 4-1 Jetty Container—Log MBean (continued)

Attribute Name	Explanation
retainDays	Indicates the number of days to keep an old log file before deleting it. Installed default: 31
filename	Specifies the log filename and path, as follows: <i>application.home/logs/yyyy_mm_dd.jetty.log</i> Where: <ul style="list-style-type: none"> <i>application.home</i>—A property whose value is set in the SESM start script. See Table 9-1 on page 9-5. logs—A constant. All log files appear in the logs subdirectory under the application directory. <i>yyyy_mm_dd</i>—The year, month, and day that the file was created. .jetty.log—A constant identifying the Jetty log files.

Debug MBean

The Debug MBean enables or disables the Jetty server debugging mechanism. [Table 4-2](#) describes the attributes in the DebugMBean.

Table 4-2 Jetty Container—Debug MBean

Attribute Name	Explanation
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
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

Server MBean

The Server MBean configures a request log, which records all incoming HTTP requests. [Table 4-3](#) describes the attributes in the Server MBean.

Table 4-3 Jetty Container—Server MBean

Attribute Name	Explanation
RequestLog	<p>Creates a new class with one argument, which specifies the name and location of the request log. The installed value is:</p> <pre>application.home/logs/yyyy_mm_dd.request.log</pre> <p>Where:</p> <ul style="list-style-type: none"> <i>application.home</i>—A property whose value is set in the SESM start script. See Table 9-1 on page 9-5. logs—A constant. All log files appear in the logs subdirectory under the application directory. yyyy_mm_dd—The year, month, and day that the file was created. The installation program uses the appropriate path name delimiter for the installation platform. .request.log—A constant identifying an HTTP request file.
retainDays	<p>Indicates the number of days to keep a log file before deleting it.</p> <p>Installed default: 90</p>
append	<p>Indicates whether or not to append messages to an existing file or to create a new file for each application instance.</p> <p>Installed default: true</p>
<Call addWebApplication>	<p>This call adds the SESM application to run on the web server. It uses five positional arguments:</p> <ol style="list-style-type: none"> The first positional argument specifies the virtual host name for the web server application. The second positional argument specifies the context path for locating the web server application. For example, / or /pathname/*. The third positional argument identifies the location of the application. The value is: <pre>application.home/webapp</pre> <p>Where <i>application.home</i> is a system property whose value is set in the start script.</p> The fourth positional argument identifies the location of the webdefault.xml file for this application. The value is: <pre>jetty.home/config/webdefault.xml</pre> <p>Where <i>jetty.home</i> is a system property whose value is set in the start script.</p> The fifth positional argument specifies whether or not web archive (WAR) files are used. Valid values are TRUE and FALSE. <p>The first three arguments define the location of the web server application.</p> <pre>host/context/application</pre> <p>The SESM start script derives the values for <i>application.home</i> and <i>jetty.home</i> from an expected (installed) directory structure. To change these values, edit the start script.</p>

SESMSocketListener MBean

The SESMSocketListener MBean configures the port that the Jetty server listens on for HTTP requests from subscribers. [Table 4-4](#) describes the attributes in the SESMSocketListener MBean.


Table 4-4 Jetty Container—SESMSocketListener MBean

Attribute Name	Explanation
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>Note The startup script sets this system property. Unless you alter the start 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>Default: 8080</p> <p>Installed value: The SESM installation program sets the <code>application.portno</code> in the startup script to the application port that you provided during the installation process.</p>
minThreads	<p>Sets the minimum number of threads that this listener maintains during periods of low load. This listener always has 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 the length of time 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 the length of time that the web server waits for a request 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>

SESMSSLListener MBean

The SESMSSLListener MBean configures the port that the Jetty server listens on for requests from subscribers on the Secure Sockets Layer (SSL). [Table 4-5](#) describes the attributes in the SESMSSLListener MBean.

Table 4-5 Jetty Container—*SESMSSLListener MBean*

Attribute Name	Explanation
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>Note 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 maintains during periods of low load. The listener always has 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. Sample keystore files are included in the installation for each portal application. For example:</p> <pre>jetty.home/config/nwspkeystore</pre> <p>Where:</p> <p><i>jetty.home</i>—A 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> Caution 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 “Using HTTPS in SESM Portals” section on page A-1 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.



Configuring SESM Portal Applications

This chapter describes the configurable attributes and options for the SESM portals. The chapter includes the following topics:

- [SESM Portal Application MBeans, page 5-1](#)
- [Associating SSGs with Subscriber Requests, page 5-16](#)
- [Configuring a Customized SESM Application, page 5-19](#)

SESM Portal Application MBeans

The SESM installation process uses default values and values you enter during installation to configure the sample portal applications. Read this section if you want to change or fine-tune configuration after installation.

The SESM portal applications use the following MBeans:

- [Logger MBean, page 5-2](#)
- [ManagementConsole MBean, page 5-3](#)
- [SESM MBean, page 5-4](#)
- [SESMDemoMode MBean, page 5-6](#)
- [DESSMode MBean, page 5-6](#)
- [SSG MBean, page 5-7](#)
- [AAA MBean, page 5-10](#)
- [Firewall MBean, page 5-11](#)
- [WebApp MBean, page 5-13](#)
- [Location MBean, page 5-15](#)

To change attributes in these MBeans, you can either:

- Make changes using the Agent View running on the application management port. For example, use the Agent View for NWSP. You can access the Agent View from the CDAT main window.
- Edit the application MBean configuration file. For example, edit the nwsp.xml file for NWSP.

The installation process configures all three of the sample portal applications (NWSP, WAP, and PDA) using the same default port numbers. These port numbers are:

- Application port—8080
- Application management port—8180

Each sample portal application uses a different MBean configuration file. The files are located in a directory named for the application under the SESM installation directory:

```
nwsp
  config
    nwsp.xml
wap
  config
    wap.xml
pda
  config
    pda.xml
```

Logger MBean

The Logger MBean 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. [Table 5-1](#) describes the attributes in the Logger MBean.

Table 5-1 SESM Portal Application—Logger MBean

Attribute Name	Explanation
debug	<p>Turns debugging on or off. That is, it controls whether Log.debug calls executed by the SESM application are displayed in the log file.</p> <p>Note Logging remains on regardless of this value. That is, all Log.trace and Log.warning calls executed in the SESM application are written to the log file regardless of the value of the debug attribute. To turn off logging, comment out the entire Logger MBean.</p> <p>Values for this attribute are:</p> <ul style="list-style-type: none"> • 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. • 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. <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>

Table 5-1 SESM Portal Application—Logger MBean (continued)

Attribute Name	Explanation
debugThreads	<p>Specifies a specific thread name for which to show debugging messages. You can specify multiple thread names, separating them using a comma. For example: 6,13,22. 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. Enter a list of thread names separated by commas.</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 MAX, MED, or LOW.</p> <p>Installed default: LOW</p>
logDateFormat	<p>Specifies format of dates in the log file.</p> <p>Installed default: yyyyMMdd:HHmmss.SSS</p>
logFile	<p>Specifies the filename and location for the logging (tracing) of business events performed by the SESM application. The installed default is:</p> <pre>application.home/logs/yyyy_mm_dd.application.log</pre> <p>Where:</p> <ul style="list-style-type: none"> • <i>application.home</i>—A property whose value is set in the SESM start script. See Table 9-1 on page 9-5. • <i>logs</i>—A constant. All log files appear in the logs subdirectory under the application directory. • <i>yyyy_mm_dd</i>—The year, month, and day that the file was created. • <i>application.log</i>—A constant identifying the application log files.
logFrame	<p>Controls whether or not to log the calling member function.</p> <p>Installed default: false</p>
logStack	<p>Controls whether or not to log stack traces.</p> <p>Installed default: false</p>
logThread	<p>Controls whether or not to log thread IDs. Installed default: true</p>
logToErr	<p>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.</p> <p>Installed default: true</p>
trace	<p>Controls whether or not to log trace messages. These messages indicate entry and exit to code points.</p> <p>Installed default: true</p>
warning	<p>Controls whether or not to log warning messages (nonfatal exceptions). Installed default: true</p>

ManagementConsole MBean

The ManagementConsole MBean configures the portal's management console port, including valid user names and passwords for accessing the console. See the [“Configuring the ManagementConsole MBean” section on page 3-5](#) for more information.

SESM MBean

The SESM MBean configures SESM features and options, including the SESM mode. [Table 5-2](#) describes the attributes in the SESM MBean.

Table 5-2 SESM Portal Application—SESM MBean

Attribute Name	Explanation
mode	<p>An SESM portal runs in one of the following modes.</p> <ul style="list-style-type: none"> • RADIUS—In this mode, the SESM web application communicates with SSG and a RADIUS server. • LDAP—In this mode, the SESM web application communicates with SSG and an LDAP directory. • 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. <p>The value for mode is a Java system property named: <code>sesm.mode</code></p> <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.) To change the mode, you can:</p> <ul style="list-style-type: none"> • Reinstall the software. • Edit the MBean configuration files, changing the mode and other attributes, as appropriate. • 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"> – On Solaris: <code>jetty/bin/startNWSP.sh -mode {Demo RADIUS LDAP}</code> – On Windows: <code>jetty\bin\startNWSP.cmd {Demo RADIUS LDAP}</code> • 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.
singleSignOn	<p>Enables or disables the single sign-on feature.</p> <ul style="list-style-type: none"> • true—Subscribers only need to authenticate during a session. Single sign-on offers the following advantages: <ul style="list-style-type: none"> – 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. – Subscribers do not need to reauthenticate if SESM automatic memory management clears sessions from the SESM portal. – 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. • false—Subscribers are required to reauthenticate for all of the cases described above. <p>Installed default: true</p>

Table 5-2 SESM Portal Application—SESM MBean (continued)

Attribute Name	Explanation
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"> • false—SESM does not send connection requests to SSG • true—SESM sends connection requests to SSG <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"> • 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. • 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.
profileCache Period	<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. If this value is 0 or undefined, the application calculates a value as: profileCachePeriod * 2.</p> <p>Installed default: 1200</p>
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"> • 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. • 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. <p>Installed default: false</p>
memRequired	<p>The minimum memory that must be available for the application to create a new SESM session or authenticate a subscriber. If this amount of memory is not available, the subscriber receives a "server busy" message.</p> <p>SESM applications include automatic memory management features that constantly work to free unused memory. If this attribute is set correctly, the application does not run out of memory. If this attribute is set too small, the application might run out of memory and terminate abnormally.</p> <p>The installed default is correct for the NWSP application. You might need to adjust the value for customized applications.</p> <p>If subscribers are receiving the server busy message too frequently, increase the amount of memory reserved for the application. This value is set in the startup script. See the "SESM Portal Application Memory Requirements" section on page 9-8 for more information.</p> <p>Installed default: 10485760</p>

SESMDemoMode MBean

The SESMDemoMode MBean configures SESM in demo mode. [Table 5-3](#) describes the attributes in the SESMDemoMode MBean.

Table 5-3 SESM Portal Application—SESMDemoMode MBean

Attribute Name	Explanation
demoDataFile	<p>Specifies the file that contains data for Demo mode. The installed value is:</p> <p style="text-align: center;"><i>application.home/config/aaa.properties</i></p> <p>Where:</p> <p style="text-align: center;"><i>application.home</i> is a system property</p> <p>The SESM start script derives the value for application.home from an expected (installed) directory structure. To change the value of application.home, edit the start script.</p>

DESSMode MBean

The DESSMode MBean configures SPE attributes used by the SESM application. [Table 5-4](#) describes the attributes in the DESSMode MBean.

Table 5-4 SESM Portal Application—DESSMode MBean

Attribute Name	Explanation
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>
naming	<p>The component in distinguished name (dn) that the LDAP directory uses to allow access to the directory. For example:</p> <ul style="list-style-type: none"> • cn—Indicates the common name (cn) used in an NDS directory • uid—Indicates the unique identifier (uid) used in an iPlanet directory

SSG MBean

The SSG MBean configures communication between SESM web applications and SSGs. The MBean also includes attributes that determine which SSG should handle a subscriber request. [Table 5-5](#) describes the attributes in the SSG MBean.

Table 5-5 SESM Portal Application—SSG MBean

Object	Attribute Name	Explanation
SSG	SSGIPPolicyClass	<p>Sets the policy to use for mapping SSGs to subscribers.</p> <p>Installed default: <code>com.cisco.sesm.ssg.DefaultSSGIPPolicy</code></p> <p>The <code>DefaultSSGIPPolicy</code> is implemented using the attributes described in the rest of this table. Other policies are subsets of <code>DefaultSSGIPPolicy</code>. Deployers might also implement customized policies of their own.</p> <p>See the javadoc for more information.</p>
Global attributes The global attributes apply to all SSGs that the SESM web application might communicate with. To determine how an SSG is configured, use the show run command on the SSG host.	PORT	<p>The global value for RADIUS ports on the SSG hosts. This value must match the value 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 ssg radius-helper key 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>

Table 5-5 SESM Portal Application—SSG MBean (continued)

Object	Attribute Name	Explanation
SSG global attributes (continued)	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. If the SESM portal times out while waiting for responses from the SSG, try adjusting this value lower.</p> <p>Installed default: 20</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>
	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"> • true—The SSGs have port-bundle host key enabled with a 0 bundle length. • false—The SSGs do not have port-bundle host key enabled. • If BUNDLE_LENGTH is non-zero, this switch is ignored, because a nonzero value implies the use of the host key feature.
	MIN_LOCAL_PORT MAX_LOCAL_PORT	<p>Together, these two attributes specify a range of UDP ports for RADIUS protocol requests from the SESM portal application to the SSG. By using these attributes, you restrict the source ports used by NWSP to only the ports in the specified range.</p> <p>For example, you might want to restrict port usage if a firewall separates SESM from other components. In that case, you can configure the firewall to allow traffic through the specified range of ports.</p> <p>You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.</p>

Table 5-5 SESM Portal Application—SSG MBean (continued)

Object	Attribute Name	Explanation
<p>SSG subnet entries</p> <p>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.</p> <p>See the “Associating SSGs with Subscriber Requests” section on page 5-15 for more information about using subnet entries.</p>	<p>Subnet entries use positional arguments.</p>	<p>The format for a subnet entry is:</p> <pre data-bbox="737 363 1143 516"><Call name="setSubnetAttribute"> <Arg>subnetAddress</Arg> <Arg>subnetMask</Arg> <Arg>argumentName</Arg> <Arg>argumentValue</Arg> </Call></pre> <p>The call to setSubnetAttribute has four positional arguments:</p> <ol style="list-style-type: none"> 1. <i>subnetAddress</i> is the subnet for which you are explicitly setting a value, overriding the globally set value. 2. <i>subnetMask</i> is the mask that can be applied to the subscriber’s IP address to derive the subnet. 3. <i>argumentName</i> is the argument that you are explicitly setting: <ul style="list-style-type: none"> – 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—The host key bundle length used on the SSG. Overrides the globally-set bundle length. 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>This value must match the value used in the following command on the SSG host:</p> <pre data-bbox="784 1304 1027 1325">ssg port-map length</pre> <ul style="list-style-type: none"> – IP—Explicitly sets the IP address for the SSG that services the specified <i>subnetAddress</i>. – THROTTLE—The maximum number of simultaneous requests that SESM portals can send to the SSG. Overrides the globally set throttle value. – SESSION_LOCATION and SESSION_BRAND—The location or brand associated with the specified subnet. Valid values are defined as arbitrary properties in the WebApp MBean. See the “Configuring Location Awareness” section on page 5-22 for more information. – MIN_LOCAL_PORT and MAX_LOCAL_PORT—The range of UDP ports used by the SESM portal to send messages to the SSG. Overrides the globally set range. 4. <i>argumentValue</i> is the value for <i>argumentName</i>.

AAA MBean

The AAA MBean configures communication between the SESM web application and the RADIUS servers, which occurs only when the SESM application is running in RADIUS mode.

Table 5-6 describes the attributes in the AAA MBean.

Table 5-6 SESM Portal Application—AAA MBean

Attribute Name	Explanation
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
maxRetries	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. Default: <code>servicecisco</code>
serviceGroupPassword	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>

Firewall MBean

The Firewall MBean configures fields on the NWSP My Firewall page. [Table 5-7](#) describes the attributes in the Firewall MBean. For more information about configuring and using the SESM firewall features, see the “[Personal Firewalls](#)” section on page 10-12.

Firewall Protocols and Applications

The Firewall MBean defines a list of firewall protocols and firewall applications, which are SESM concepts used in a different way than the OSI protocol and application concepts. You can specify ACLs on firewall applications, but not on firewall protocols.

- A firewall protocol defines components used to build the firewall applications. They consist of any Layer 3 or Layer 4 protocol and an optional port. (The combination of a lower layer protocol and a port might define an OSI layer 7 application, such as FTP.) For example, the following are some firewall protocols, shown as they are defined to the Firewall MBean:

```
<Key>ip</Key>
<Value>ip</Value>

<Key>tcp</Key>
<Value>tcp</Value>

<Key>ftp</Key>
<Value>tcp, 21</Value>

<Key>https</Key>
<Value>tcp, 443</Value>

<Key>imap</Key>
<Value>tcp, 143</Value>
```

- The firewall applications are the items that are displayed on the My Firewall page in the Applications/Protocols column. They are the items on which ACLs are applied. A firewall application consists of one or more firewall protocols. For example:

```
<Key>ip</Key>
<Value>ip</Value>

<Key>tcp</Key>
<Value>tcp</Value>

<Key>ftp</Key>
<Value>ftp</Value>

<Key>email</Key>
<Value>smtp, pop2, pop3, imap</Value>

<Key>www</Key>
<Value>http, https</Value>
```

SESM includes many predefined firewall protocols and firewall applications. You can see all of these predefined values by accessing the NWSP Agent View. In the Firewall MBean, click in the value column for the read-only attributes AllApplicationDescriptions and AllProtocolDescriptions.

You can use the customProtocols and customApplications attributes in the Firewall MBean to define additional firewall protocols and firewall applications.

Table 5-7 SESM Portal Application—Firewall MBean

Attribute Name	Explanation
customProtocols	<p>Defines additional firewall protocols. Each item in the array consists of two elements:</p> <ul style="list-style-type: none"> • Key—Names the firewall protocol. The name can be anything. • Value—The lower layer protocol (OSI Layer 3 or 4 protocol) and an optional port, separated by a comma. The lower layer protocol value must be a protocol that the SSG host is configured to accept. <p>For example:</p> <pre data-bbox="467 579 699 630"><Key>tcp</Key> <Value>tcp</Value></pre> <pre data-bbox="467 659 748 709"><Key>ftp</Key> <Value>tcp, 21</Value></pre> <p>See the “Firewall Protocols and Applications” section on page 5-11 for a definition and more examples of firewall protocols. Several firewall protocols are predefined in SESM and do not need to be explicitly defined here.</p>
customApplications	<p>Defines additional firewall applications. Each item in the array consists of two elements:</p> <ul style="list-style-type: none"> • Key—Names the firewall application. The name can be anything. • Value—A list of firewall protocols that comprise the application, separated by commas. Valid values are the SESM predefined and custom firewall protocols. <p>To see a list of all defined protocols, open the portal’s Agent View management console and click in the value column of the AllProtocolDescriptions attribute, a read-only attribute in the Firewall MBean.</p> <pre data-bbox="467 1121 699 1171"><Key>ftp</Key> <Value>ftp</Value></pre> <pre data-bbox="467 1201 787 1251"><Key>www</Key> <Value>http,https</Value></pre> <p>See the “Firewall Protocols and Applications” section on page 5-11 for a definition and more examples of firewall applications.</p>

Table 5-7 SESM Portal Application—Firewall MBean (continued)

Attribute Name	Explanation
displayApplications	<p>Specifies the firewall applications that appear on the NWSP My Firewall page, in the Applications/Protocols column. Items in this list must be defined as predefined or custom firewall applications. To see a list of all defined applications, open the portal's Agent View management console and click in the value column of the AllApplicationsDescriptions attribute, a read-only attribute in the Firewall MBean.</p> <p>The text that represents the application on the My Firewall page is configured as a resource bundle in the portal application's directory. For example, for NWSP, resources are in:</p> <pre>nwsp/webapp/WEB-INF/classes/messages[_locale].properties.</pre> <p>The portal searches its resource bundles for the resource <i>firewallAppNameDescription</i>, where <i>firewallAppName</i> is the application defined in the Firewall MBean. If a matching resource is not found, then <i>firewallAppName</i> is displayed on the My Firewall page. For example, consider the following firewall application:</p> <pre>www</pre> <p>The portal searches for a resource named <i>wwwDescription</i>, and displays the text in the appropriate language on the My Firewall page. (In the installed files, this is World-Wide-Web for the en locale.) If the <i>wwwDescription</i> resource did not exist, then <i>www</i> would appear on the My Firewall page.</p>
direction	<p>Specifies direction (in or out) for the default access control direction in the ACLs created by SESM. See the “ACLs Generated from Entries on the Firewall Pages” section on page 10-19 for more information about created ACLs.</p> <p>Value values for direction are:</p> <ul style="list-style-type: none"> • in—Upstream, from the subscriber • out—Downstream, to the subscriber <p>All connections have a return path. A block on in also affects traffic traveling in the opposite direction, and vice-versa. For any ACL, the choice of whether to control the in or out direction is a matter of preference.</p>
returnOption	<p>Sets the return option for TCP applications. Recommended values are: permit and default. Default refers to the Permit/Deny All Else button on the My Farewell page.</p> <p>Default: permit</p> <p>Note You can alter the My Firewall JSP to add a button allowing the subscriber to choose the TCP return option. The JSP contains commented-out code for an ipPermission button, which you could copy to implement a return TCP permission button.</p>

WebApp MBean

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 5-8 describes the attributes in the WebApp MBean.

Table 5-8 SESM Portal Application—WebApp MBean

Attribute Name	Explanation
confirmAtServiceLogon	Controls whether or not the application prompts the user for confirmation before it acts on a request to start a service. Default: FALSE
confirmAtServiceLogoff	Controls whether or not the application prompts the user for confirmation before it acts on a request to log off. Default: TRUE
confirmAtAccountLogoff	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
disconnectWhenUnsubscribe	Controls whether SESM requests the SSG to disconnect an existing service connection if the subscriber unsubscribes from that service. Applies to LDAP mode only.
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
usernameMinLength usernameMaxLength passwordMinLength passwordMaxLength	These attributes control the length of user names and passwords. A value of 0 is valid for usernameMinLength and passwordMinLength. Configuration files from SESM releases earlier than Release 3.1(7) that use the credentialMaxLength attribute are valid. The value in credentialMaxLength sets usernameMaxLength and passwordMaxLength values. Defaults for usernameMinLength and passwordMinLength: 1 Defaults for usernameMaxLength and passwordMaxLength: 30
prepaidRedirectionURL serviceNotGivenURI defaultURI serviceSubscriptionURI noSubscribePermissionURI serviceStartURI serviceLogonURI	These attributes are related to the captive portal solution. See Table 11-4 on page 11-16 for explanations of these attributes.
addDimension entries	You can create arbitrary attributes and associate them with subscriber requests in the manner described in the “Arbitrary Attributes” section on page 10-9 .

Location MBean

The Location MBean defines locations and associated attributes for the location awareness feature based on complete ID attributes. [Table 5-9](#) describes the attributes in the Location MBean. For more information about configuring location awareness, see [“Location Awareness” section on page 10-3](#).

Table 5-9 *SESM Portal Application—Location MBean*

Attribute Name	Explanation
locationService	Defines the SESM class containing the logic for location determination. You can change this attribute to point to a customized service provider interface (SPI) class.
locations	<p>Defines an array of location values. Each location in the array consists of the following items:</p> <p>Note Configure locations by editing the configuration file, not by using AgentView.</p> <ul style="list-style-type: none"> • name—Names the location. The <i>location</i> can be any value, but it must match your intended usage. • parameters—An array of one or more elements defining the attributes for the location. Each item in the parameters array consists of a class name and attribute values required for the class. The following class names are valid: <ul style="list-style-type: none"> – com.cisco.sesm.core.location.IPRangeParam—Associates this location with a specified range of edge session IP addresses. The edge session IP address is the value passed from the SSG to SESM in standard RADIUS attribute number 8, FRAMED_IP_ADDRESS. <p>IPRangeParam requires two attributes defining the start and end of the IP address range</p> <pre><New class="com.cisco.sesm.core.location.IPRangeParam"> <Set name="start" type="String">10.0.0.0</Set> <Set name="end" type="String">10.10.0.0</Set> </New></pre> – com.cisco.sesm.core.location.VPIRangeParam—Associates this location with a specified range of virtual path identifier (VPI). The edge session VPI is the value passed from the SSG to SESM in the RADIUS VSA (attribute number 26), Account-Info subattribute (number 250), subattribute code \$VP. Although SSG passes both the VPI and the virtual channel identifier (the VPI/VCI attribute), SESM Release 3.1(7) uses only the VPI. <p>VPIRangeParam requires two attributes defining the start and end of the VPI range.</p> <pre><New class="com.cisco.sesm.core.location.VPIRangeParam"> <Set name="start" type="int">1</Set> <Set name="end" type="int">2</Set> </New></pre> – com.cisco.sesm.core.location.SubInterfaceParam—Associates this location with a specified subinterface. Subinterface ranges are not permitted in SESM Release 3.1(7). The edge session subinterface is the value passed from the SSG to SESM in the RADIUS VSA (attribute number 26), Account-Info subattribute (number 250), subattribute code \$SI. Some examples of subinterface values are: Ethernet0/0, FastEthernet4/0, or ATM2/0. <p>SubInterfaceParam requires one attribute defining the subinterface to associate with the location:</p> <pre><New class="com.cisco.sesm.core.location.SubInterfaceParam"> <Set name="subInterface" type="String">Ethernet0/0</Set> </New></pre> <p>The parameters array can define multiple attributes for a location. In that case, an edge session is associated with the location only when the session attributes match all of the attributes defined for the location.</p>

Associating SSGs with Subscriber Requests

A typical SESM deployment consists of multiple SSGs. The installation process configures communication with one SSG when you choose the appropriate options. This section describes how to configure communication with additional SSGs. It includes the following topics:

- [Setting SSG Global and Subnet Entries, page 5-16](#)
- [Using Port-bundle Host Key with Identical SSG Configurations, page 5-16](#)
- [Using Port-bundle Host Key with Varying SSG Configurations, page 5-17](#)
- [Specifically Mapping SSGs to Subscriber Subnets, page 5-18](#)

Setting SSG Global and Subnet Entries

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 the SESSION_LOCATION and SESSION_BRAND attributes.

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

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 the port-bundle host key feature unless you require 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 Port-Bundle Host Key Feature on SSG, page F-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 using 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. When the SESM installation program prompts you, enter the globally-configured values in Step 2. These values are saved as global elements in the SSG MBean, 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 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 single 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>
```

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 hard coded 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.

- 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.

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.



Configuring CDAT

This chapter describes how to configure the Cisco Distributed Administration Tool (CDAT) application. The chapter includes the following topics:

- [Required Cookies Feature, page 6-1](#)
- [CDAT Application MBeans, page 6-1](#)
- [Adding a New Application to the CDAT Main Window, page 6-4](#)
- [Configuring CDAT Login Values, page 6-4](#)

Required Cookies Feature

Make sure that the cookies feature is enabled on the browser in which you are running CDAT. If the CDAT application tends to log off unexpectedly, check the browser cookies setting.

CDAT Application MBeans

The CDAT application uses the following MBeans:

- [Logger MBean, page 6-2](#)
- [ManagementConsole MBean, page 6-2](#)
- [MainServlet MBean, page 6-2](#)
- [CDAT MBean, page 6-3](#)

To change attributes in these MBeans, you can use either of the following methods:

- Edit the CDAT MBean configuration files:

```
cdat
  config
    cdat.xml
    dessauth.xml
    lib.xml
```

- Make changes using the Agent View running on the CDAT management port. The installation process uses the following default port numbers for CDAT:
 - CDAT port—8081
 - CDAT management port—8181

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs CDAT application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the “[Logger MBean](#)” section on page 5-2 for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the management console port for CDAT, including valid user names and passwords for accessing the console. See the “[Configuring the ManagementConsole MBean](#)” section on page 3-5 for more information.

MainServlet MBean

The MainServlet MBean configures the list of links in the CDAT main window. The SESM installation program configures initial links. Use this MBean to change those links or add new ones. The initial links configured by the installation program link to:

- Management consoles for all of the installed SESM applications, which can include NWSP, CDAT, RDP, and captive portal.
- LDAP directory management logon page

[Figure 3-2 on page 3-6](#) shows the CDAT main window with the above-mentioned links. [Table 6-1](#) describes the attributes in the MainServlet MBean.

Table 6-1 CDAT Application—MainServlet MBean

Attribute Name	Explanation
links	<p>Specifies the links to display on the CDAT main window, such as the links to the logon pages that provide access to:</p> <ul style="list-style-type: none"> LDAP directory maintenance Remote management of SESM applications. Each application has a separate link to a logon page that allows access to an AgentView for that application. <p>The links attribute is an array. For each link, provide the following information:</p> <ul style="list-style-type: none"> label—The static text that appears on the CDAT window to identify the link. For example, the installed file uses Manage NWSP to identify the remote management function for NWSP: URI—The HTTP address that points to the target page. To point to the management console for an SESM application, use that application's host name and management console port. For example: <pre>http://server1:8180/</pre> <p>The SESM startup scripts set the management port to <code>application.port + 100</code>. For example, if you installed NWSP using the default port value 8080, its management port is:</p> <pre>8080 + 100 = 8180</pre> <p>Similarly, if you installed CDAT using the default port value 8081, the startup script sets its management port to:</p> <pre>8081 + 100 = 8181</pre> linkText—The active text that the user clicks to go to the URI. For example, the installed file uses the text AgentView as the active text for the link to the NWSP management console.

CDAT MBean

The CDAT MBean configures resource attributes for an LDAP directory management session in CDAT. [Table 6-2](#) describes the attributes in the CDAT MBean.

Table 6-2 CDAT Application—CDAT MBean

Attribute Name	Explanation
naming	<p>The component in distinguished name (dn) that your LDAP directory uses to allow access to the directory.</p> <ul style="list-style-type: none"> cn—NDS, for example, uses common name cn. uid—iPlanet, for example, uses unique identifier (uid).
sessionTimeout	<p>The maximum period of inactivity allowed after logging into a CDAT directory management session. When this time period elapses with no activity, CDAT logs the user out. Values are in seconds. A negative value prevents the user from ever being logged out. Changes to this attribute value take effect for subsequent logins.</p> <p>Default: 600</p>

Table 6-2 CDAT Application—CDAT MBean (continued)

Attribute Name	Explanation
maxVariables	The maximum number of page/page instance variables allowed for each CDAT directory management session. This number affects how many pages can be visited before their state is lost, although it is not a one-to-one mapping. If many StateTimedOut errors are occurring, increase this number. Default: 40
queryMaxResults	The maximum number of results to return from any one query to the LDAP directory. Changes to this attribute value take immediate effect. A value of zero removes any limits. Default: 500
queryTimeout	The timeout (in milliseconds) for queries to the LDAP directory. Changes to this attribute value take immediate effect. A value of zero is an infinite timeout value. Default: 0

Adding a New Application to the CDAT Main Window

To add a new application to the CDAT main window, add an entry for it in the links attribute in the CDAT MainServlet MBean.

The links attribute must include information for each SESM application that you want to manage from CDAT. For example, if you deploy multiple instances of NWSP, each instance must be configured in the links attribute.

Configuring CDAT Login Values

This section describes how to configure the login values for the CDAT management functions:

- [Login Values for SESM Agent Views, page 6-4](#)
- [Login Values for LDAP Directory Management, page 6-5](#)

Login Values for SESM Agent Views

On the CDAT main window, the links for managing SESM applications point to each application's management console port. When you initially go to a management console port, you are prompted to log on.

The logon values are configured in the AuthInfo attribute in the Management Console MBean in *each* application's MBean configuration file. See the [“Configuring the ManagementConsole MBean” section on page 3-5](#) for more information, including the default user name and password values in the installed files.

You can configure different user IDs and passwords for each application's Agent View or use the same values for all applications.

Login Values for LDAP Directory Management

On the CDAT main window, the link for managing the LDAP directory points to the CDAT directory manager login window.

Before any administrator can log into the CDAT Directory Manager function, the directory schema must be extended, some initial RBAC rules and roles must be loaded into the directory, and an initial administrator must be created.

- The easiest way to extend the schema and load initial RBAC objects is to allow the SESM installation program to perform these tasks. See the [“Extending the Directory Schema and Loading Initial RBAC Objects” section on page 8-3](#) for instructions and alternatives.
- The easiest way to create the initial administrator is to load the SESM sample LDAP data into the directory. See the following file in the SESM installation directory for instructions:

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

For more information about the sample data, logging into CDAT, and creating CDAT administrators, see the *Cisco Distributed Administration Tool Guide*.



Configuring the RADIUS Data Proxy

The RADIUS Data Proxy (RDP) translates RADIUS protocol messages into LDAP protocol messages with SPE DESS extensions. RDP is available for installation when you install SESM in LDAP mode. This section describes how to configure the RDP application. Topics are:

- [Configuring Listeners and Handlers, page 7-1](#)
- [Changing Installed Configuration Options, page 7-2](#)
- [RADIUS Data Proxy MBeans, page 7-3](#)
- [RDP Protocol Handlers, page 7-7](#)

Configuring Listeners and Handlers

RDP receives RADIUS protocol messages on one listener. The listener is configured in the RDP MBean.

RDP processes the messages using multiple handlers. Each handler performs some processing and calls the next handler. The chain of handlers that processes a message is configured in the RDP MBean and is determined by:

- The basic configuration options that you specify during installation.
- The type of message; for example, requests for authorization or authentication use different handlers than requests to obtain profile information.

The RDP application is easily extensible because the chain of handlers is configurable in the MBeans. New handlers can be plugged in to handle new or customized configuration requirements.



Note

To maintain the correct processing sequence for the installed RDP application, do not change the name and nexthandler attributes in the RDP MBeans.

See the [“RDP Protocol Handlers” section on page 7-7](#) for a summary of the chain of RDP handlers that processes RADIUS protocol messages in the installed RDP application.

Changing Installed Configuration Options

RDP configuration options are chosen and configured during RDP installation. This section describes how to change those configuration options. The topics are:

- [Changing the RADIUS Data Proxy Mode, page 7-2](#)
- [Adding Service Information to Replies, page 7-2](#)
- [Using a Restricted Client List, page 7-3](#)

Changing the RADIUS Data Proxy Mode

The RDP can run in the following modes:

- **Default (non-proxy) mode**—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the SPE API to send authorization requests to the LDAP directory.
- **Proxy mode**—In this mode, RDP forwards authentication requests to a configured RADIUS server. RDP uses the SPE API to send authorization requests to the directory.

If you use Proxy mode, see the [“RADIUS Data Proxy MBeans” section on page 7-3](#) for important information about configuring subscriber profiles.

To change the RDP mode, we recommend that you reinstall the RDP component.



Note

The alternative is to manually edit the configuration files, commenting out the inappropriate handlers, removing the comments surrounding other handlers, and configuring those handlers.

RDP can also run in LOCAL mode, during which it obtains profiles from a Merit flat file. This mode is useful for testing environments. To switch to LOCAL mode, use the LOCAL attribute in the RDP MBean.

Adding Service Information to Replies

To change this option, we recommend that you reinstall the RDP component.



Note

The alternative is to manually edit the configuration files, commenting out the inappropriate handlers, removing the comments surrounding other handlers, and configuring those handlers.

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.

Do not choose this option if memory is a consideration on the SSG device. Instead, you can configure the SESM application to initiate automatic connections with the autoConnect attribute in the SESM MBean. See the [“SESM MBean” section on page 5-4](#) for more information.

Using a Restricted Client List

This option is easily changed after installation. For instructions, see the `addClientList` attribute in the “RDP MBean” section on page 7-4.

RADIUS Data Proxy MBeans

RDP uses the following MBeans:

- [Logger MBean, page 7-3](#)
- [ManagementConsole MBean, page 7-3](#)
- [RADIUSDictionary MBean, page 7-4](#)
- [RDP MBean, page 7-4](#)

To change attributes in these MBeans, you can either:

- Edit the RDP MBean configuration files:

```
rdp
  config
    rdp.xml
tools
  config
    erp.xml
```

- Make changes using the Agent View running on the RDP management port.

Default port numbers used by the installation process are:

- RDP port—1812
- RDP management port—1912

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs RDP application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the “[Logger MBean](#)” section on page 5-2, for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the RDP management console port, including valid user names and passwords for accessing the console. See the “[Configuring the ManagementConsole MBean](#)” section on page 3-5 for more information.

RADIUSDictionary MBean

All SESM applications, including the RDP, internally predefine the standard RADIUS attributes and the Cisco SSG vendor-specific attributes (VSAs). You can define additional attributes, such as additional Cisco VSAs or third-party VSAs, in the RADIUSDictionary MBean. When you define attributes in this MBean, you can use the defined attribute names in the profiles on the LDAP directory.

For a list of the standard RADIUS attributes that are predefined in SESM, see [Table C-2 on page C-4](#). For a list of the Cisco SSG VSAs that are predefined in SESM, see [Table C-3 on page C-4](#).

[Table 7-1](#) describes the attributes in the RADIUSDictionary MBean.

Table 7-1 RDP—RADIUSDictionary MBean

Attribute Name	Explanation
dynamicAttributes	<p>An array of new attribute definitions. To define a new attribute, add a new item to this array. The format for an item is:</p> <pre>name(radiusAttributeId, vendorId, vendorSubattribute, datatype)</pre> <p>Where:</p> <ul style="list-style-type: none"> <i>name</i>—The new attribute name. <i>radiusAttributeId</i>—Use attribute value 26, the vendor-specific attribute. <i>vendorId</i>—A RADIUS vendor ID. <i>vendorSubattribute</i>— A unique number that distinguishes this attribute from other VSAs for the same vendor. <i>datatype</i>—One of the following values: BINARY, STRING, INTEGER, IPADDRESS. When datatype is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string. <p>An example follows:</p> <pre>demoVSA(26, 1, 1, BINARY)</pre> <p>Other valid syntax formats are represented below:</p> <pre>name([[type=]26],[vendorId=]vendorId,[vendorType=]vendorType,[dataType=]dataType)</pre> <p>For example:</p> <pre>demoVSA(type=26, vendorId=1, vendorType=1,dataType=INTEGER)</pre>

RDP MBean

The RDP MBean configures the RDP listener, including its thread pool and sockets (ports), and all of the handlers. [Table 7-2](#) describes the configurable attributes in the RDP MBean.



Note

Unless you are customizing the RDP application, the attributes in [Table 7-2](#) are the only ones you should change. All other attributes affect the processing sequence of the RDP protocol handler. See the [“Changing Installed Configuration Options” section on page 7-2](#) for more information.

Table 7-2 RDP—RDP MBean

Attribute Name	Explanation
handler	Defines the type of listener being configured. The value must be RDP to configure an RDP protocol handler.
dump	<ul style="list-style-type: none"> true—Displays all RADIUS messages on the console (stderr) false—Does not display messages Default: true
The following attribute is in the DESSAuthenticationHandler class.	
authAttributes	This attribute specifies the RADIUS attributes to use in subscriber authentication, in addition to the USER_NAME attribute. USER_NAME is always required and should not appear in the list. Any other standard RADIUS attribute can be used for authentication. Typical values are: <ul style="list-style-type: none"> USER_PASSWORD CALLED_STATION_ID (APN) CALLING_STATION_ID (MSISDN) NAS_IDENTIFIER See the “Multikey Authentication” section on page 10-28 for more information.
The following attributes are in the DESSServiceProfileHandler, DESSGroupProfileHandler, and DESSNextHopProfileHandler classes.	
servicePassword	RDP requires passwords to obtain service, group, and next hop profiles. The SSG sets the password in the request. The values you configure here must match the values configured on the SSG, or, in the case of the groupPassword, in SESM configuration. If the configured password does not match the password in a profile, RDP returns an access-reject message. <ul style="list-style-type: none"> servicePassword—Requests containing this password value are requests for a single service profile. RDP uses the SPE API to obtain a list of authorized services for a subscriber. This servicePassword must match the password configured on the SSG with the following command: <pre>ssg service-password servicePassword</pre> groupPassword—Requests containing this password value are requests for a service group profile. RDP 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. The groupPassword value must match the password configured on the SESM portal in the serviceGroupPassword attribute in the AAA MBean. nextHopPassword—Requests containing this password value are requests for a next hop table profile. RDP 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: <pre>ssg next-hop download nextHopTableName password</pre>
groupPassword	
nextHopPassword	
Note	The following attributes are in RDP MBean, RADIUSListener=RDP,component=Threadpool
minThreads	Sets the minimum number of threads that this listener maintains during periods of low load. This listener always has system resources allocated for this number of threads. Default: 5

Table 7-2 RDP—RDP MBean (continued)

Attribute Name	Explanation
maxThreads	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. Default: 255
Note The following attributes are in RDP MBean, RADIUSListener=RDP,component=RADIUSServerSocket	
secret	The shared secret that must be used in RADIUS protocol messages sent to the bundled SESM RADIUS server. This attribute sets a global shared secret for all clients. To specify different shared secrets for each client, use the allowedClients attribute.
localPort	The port the RADIUS server listens on. It uses the same port for RADIUS Accounting-Requests and Access-Requests. The installed configuration file defines this attribute as a Java system property, which is assigned a value at run time: <i>application.portno</i>
allowedClients	Configures a list of clients from which the server can accept requests. Also configures shared secrets. Turn this feature on and off as follows: <ul style="list-style-type: none"> • Allow any client to access the RDP—Comment out the allowedClients attribute in the XML file, or remove all clients from the allowedClients list. • Restrict client access—Uncomment the allowedClients attribute in the XML file. <p>Note If you do not see the allowedClients attribute in the Agent View, check the configuration file (the XML file). The allowedClients attribute might be commented out. If so, remove the comment characters, save the XML file, and then restart the RDP.</p> <p>RDP clients are SSGs. You can add more clients by adding more elements to the allowedClients attribute. An element in allowedClients attribute has the following format:</p> <pre>{hostName IPAddress}[:localSecret]</pre> <p>Where:</p> <p><i>hostName</i> or <i>IPAddress</i> identify a client (an SSG, for example) that has access to the RDP.</p> <p><i>localSecret</i> identifies the secret that this client uses for RADIUS communication. If the client is an SSG, this value must match the shared secret configured on the SSG device:</p> <pre>radius-server key SharedSecret</pre>
Note The following attributes are in RDP MBean, PROXY=ProxyHandler,component=RADIUSClientSocket. This component is used only when RDP is configured in Proxy mode.	
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 server returns responses or timeout messages for previous requests. Default: 256
timeOut	The number of seconds that RDP waits before timing out RADIUS packets that it sends to the AAA server. Default: 4000

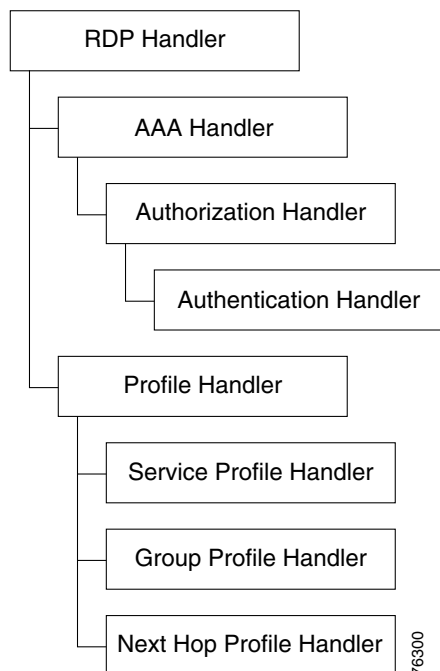
Table 7-2 RDP—RDP MBean (continued)

Attribute Name	Explanation
maxRetries	The number of times RDP resends packets to the AAA server if no response is received. 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 RDP. The shared secret must be the same for the primary and secondary servers. It must match the secret specified when you configured RDP 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

RDP Protocol Handlers

Figure 7-1 shows the processing sequence that RDP uses for handling packets.

Figure 7-1 RDP Handlers



Each protocol handler has a special purpose:

- RDP handler—Determines whether the request requires the AAA handler or Profile handler.
- AAA Handler—Coordinates handling of AVPairs, authorization, and authentication.
- Authorization Handler—Adds a service list to the ACCESS-ACCEPT response.
- Authentication Handler—Authenticates the request and adds other attributes to the response, including:
 - Adds extra AV pairs to the response. This includes firewall settings and any other AV pairs set in CDAT.
 - Generates IP pool names from primary services and adds the pool name.
 - Adds the home URL.
 - Adds TCP redirect attributes.
 - Adds idle timeout and session timeout attributes.



Note

When RDP is running in Proxy mode, RDP performs all of the above authentication work using information in the profile obtained from a RADIUS server. If you are using Proxy mode, be sure to add these attributes to the subscriber profiles on the RADIUS server, as opposed to the ones on the LDAP server.

- Profile Handler—Handles profile requests and passes them on to the appropriate specific profile handler.
- Service Profile Handler—Handles a service profile request.
- Group Profile Handler—Handles a service group profile request.
- Next Hop Profile Handler—Handles a next hop table profile request.



Configuring Security Policy Engine for SESM

This chapter describes how to configure the Security Policy Engine (SPE) component to work with SESM applications. The chapter includes the following topics:

- [SPE Attributes, page 8-1](#)
- [Extending the Directory Schema and Loading Initial RBAC Objects, page 8-3](#)
- [Loading Sample Data, page 8-4](#)

SPE Attributes

SPE uses the following MBeans:

- [Directory MBean, page 8-2](#)
- [Connection MBeans, page 8-3](#)—Two connection MBeans might be configured:
 - Connection MBean, instance=Primary
 - Connection MBean, instance=Secondary

The SPE MBeans are used by any application that incorporates the SPE, which could include SESM portals deployed in LDAP mode, the RDP server, and the CDAT application. Each application has its own version of SPE MBeans.

To change attributes in the SPE MBeans, you can either:

- Edit the SPE MBean configuration file in the appropriate SESM application config directory:

```
applicationName
  config
    dessauth.xml
```

- Make changes using the Agent View for an application that incorporates SPE APIs.



Note

The SPE component does not have its own management console. Rather, the SPE MBeans are managed from the application's MBean list, on the application's management console.

Directory MBean

The Directory MBean configures logging and caching attributes for executing classes in the SPE APIs. [Table 8-1](#) describes the attributes in the Directory MBean.

Table 8-1 SPE—Directory MBean

Attribute Name	Explanation
connectionNameRoot	Root name of the individual connection Mbeans. This MBean searches for other mbeans that begin with this name and assumes that those MBeans are connections to the directory.
factory	Do not change the installed value.
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 each 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 <code>cacheMaxObjects</code> , 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
cacheMinFreeMem	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: $cacheSize = (JavaVirtualMemory - applCodeSize) * (100\% - cacheMinFreeMem)$ Where: <i>JavaVirtualMemory</i> is the maximum virtual memory size specified at application startup time with the <code>jvm</code> argument. The installed startup scripts use the following values: <ul style="list-style-type: none"> The <code>startNWSP</code> script uses 64 MB The <code>runrdp</code> script uses 20 MB <i>applCodeSize</i> is the application size. The NWSP is approximately 18 MB. <i>cacheMinFreeMem</i> is the percentage of JVM that must remain available after the application is loaded into memory. For example, the <i>cacheSize</i> for NWSP is 90% of 14 MB, or 12.6 MB: $cacheSize = (32\text{ MB} - 18\text{ MB}) * (100\% - 10\%)$ Default: 10

Table 8-1 SPE—Directory MBean (continued)

Attribute Name	Explanation
cacheSessionTimeout	Specifies the timeout of inactive client sessions in seconds. Default: 600
cacheExpireInterval	Specifies the interval in seconds after which the cache attempts to expire objects. Note 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. Default: 600
cacheObjectTimeout	Specifies the number of seconds before objects time out. Default: 600

Connection MBeans

The Connection MBeans configure location and security attributes required to connect to an LDAP directory. If you configure and deploy two LDAP directories for failover protection, make sure to configure two instances of the connection MBean, using the appropriate connection information for the primary and secondary directories. The connection MBean names are:

- Connection, instance=Primary
- Connection, instance=Secondary

Table 8-2 describes the attributes in the Connection MBeans.

Table 8-2 SPE—Connection MBeans

Attribute Name	Explanation
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.

Extending the Directory Schema and Loading Initial RBAC Objects

For SESM deployments running in LDAP mode, you must make the following modifications 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*.
- Load 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 update activities. If you did not choose these options during installation, you must perform these updates before running CDAT or SESM applications in LDAP mode.

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

- Perform a custom SESM installation, installing just the SPE component, to make the updates. See the following section [“Rerunning the SESM Installation to Update the Schema and Load RBAC Objects”](#) for instructions.
- Perform the updates manually using native administration tools and commands. See the following file in the SESM installation directory for instructions:

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

Rerunning the SESM 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 **Update schema** and **Install RBAC**.
-

Loading Sample Data

The SESM installation includes sample data that you can optionally load into the LDAP directory, after the SPE extensions are applied. The sample data is located in:

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

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

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



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 9-1](#)
- [Logging On to SESM Portals, page 9-5](#)
- [Stopping Applications, page 9-6](#)
- [Adding and Removing Services on Windows NT, page 9-7](#)
- [Memory Requirements and CPU Utilization, page 9-7](#)

Starting Applications

This section describes the startup scripts for SESM applications. Topics are:

- [Starting the SESM Portals, page 9-1](#)
- [Starting RDP, page 9-2](#)
- [Starting CDAT, page 9-3](#)
- [Startup Script Explanation, page 9-3](#)
- [SystemProperty and Property Assignments in the Start Script, page 9-4](#)

Starting the SESM Portals

SESM portals are J2EE web applications that run 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 dess-auth configuration files.

Starting RDP

Start RDP using the following script:

Platform	Script
Solaris and Linux	rdp/bin/runrdp.sh
Windows NT	rdp\bin\runrdp.cmd

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 located in the Jetty server's bin directory.

Starting CDAT

Start CDAT using the following script:

Platform	Script
Solaris and Linux	jetty/bin/startCDAT.sh
Windows NT	jetty\bin\startCDAT.cmd

CDAT is a J2EE application; therefore, 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.

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 path names 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 5-20](#) 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.

Table 9-1 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 start 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 start script sets \$APPDIR to <code>applicationName</code> under the installation directory. The <code>applicationName</code> parameter is passed from the application specific startup script (for example, <code>startNWSP.sh</code>).	<code>installDir</code> <code>nwsp</code> or <code>installDir</code> <code>rdp</code> or <code>installDir</code> <code>cdat</code>
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 the application specific startup script (for example, <code>startNWSP.sh</code>).	Specified during installation. The default is 8080 for the NWSP, WPA, and PDA portal applications. The default is 8081 for CDAT.
application.ssl.portno=\$SSLPORTNO	application.ssl.portno is the port that the web server listens on for secure HTTPS requests from subscribers.	The startup script sets \$SSLPORTNO to <code>\$PORTNO - 80 + 443</code> .
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 SESM Portals

To access SESM portals, such as NWSP, 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** Make sure the web browser has Javascript enabled.
- Step 4** 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 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 the portal URL.

Step 5 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 C, "Configuring RADIUS for SESM Deployments,"](#) 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 Refer to the *Subscriber Edge Services Manager Solutions Guide* for instructions on 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 9-6](#)
- [Stopping SESM Applications on Windows NT, page 9-7](#)

Stopping SESM Applications on Solaris and Linux

To stop SESM applications on Solaris and Linux, execute the stop scripts listed in [Table 9-2](#). None of the scripts accept arguments.

Table 9-2 *SESM Stop Scripts on the Solaris and Linux Platforms*

Application	Stop Script Path Names (Solaris and Linux platforms only)
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 9-3 lists the names and locations of the scripts that add and remove services.

Table 9-3 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 9-8](#)
- [SESM Portal Application CPU Utilization, page 9-9](#)
- [RDP Memory Requirements, page 9-9](#)

SESM Portal Application Memory Requirements

This section provides some guidelines for sizing the memory requirements for SESM deployments in production mode.

Factors Affecting RAM

The following factors affect java virtual memory requirements for SESM portal applications:

- Deployment mode—RADIUS mode RAM requirements per logged in user are less than LDAP mode requirements
- Number of users simultaneously logged in
- Application footprint
- (LDAP mode only) DESS cache size—The additional functionality provided in LDAP mode is supported with database caching. Caching significantly increases the required RAM for SESM applications. The DESS cache size is an additional RAM requirement to consider over and above the other factors listed above. Cache size is configurable. The “[Directory MBean](#)” section on [page 8-2](#) describes how to set the DESS cache size.

Another consideration is the logon rate, which can affect transitory memory use.

Use the following formula to determine memory requirements for your installation:

$$\text{requiredJavaMemory} = \text{reservedMem} + (\text{maxConcurrentUsers} * \text{KBPerUser})$$

- *requiredJavaMemory* is the amount of Java virtual memory to reserve for use by the SESM portal application. The generic startup script (jetty/bin/start.sh) sets the Java virtual memory using an argument to the java command. The following line is near the end of the start script:

```
$JAVA $SERVER -Xms64m -Xmx64m \
```

The first -X argument is the initial memory to reserve. The second -X argument is the maximum memory. We recommend using the same value for both.

- *reservedMem* represents the initial memory requirement for the application before subscribers begin to log on. Initial memory varies by application and depends on how many classes are loaded. A value from 10 to 15 MB is a reasonable estimate.
- *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 varies depending on the size of the profiles. Suggested values are:
 - For RADIUS mode: 5 KB per subscriber.
 - For LDAP mode: 17 KB per subscriber.

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

SESM Portal Application CPU Utilization

CPU utilization by an SESM portal application increases as the rate of new logons increases. [Table 9-4](#) 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 9-4 *SESM Portal CPU Utilization*

SESM Mode	Logon Rate Sustained until Maximum Users Reached ¹	Maximum Users	CPU Utilization on Sun Sparc U5-10 400-MHz server
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

RDP RAM requirements are affected by the following factors:

- Number of users simultaneously logged in and logon rates
- Application footprint
- DESS cache size—Cache size is configurable. The [“Directory MBean” section on page 8-2](#) describes how to set the DESS cache size.

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. Increase memory by editing the RDP startup script.



Configuring SESM Features

This chapter describes how to configure the following SESM features:

- [Automatic Service Connections, page 10-1](#)
- [Location Awareness, page 10-3](#)
- [Arbitrary Attributes, page 10-9](#)
- [Personal Firewalls, page 10-12](#)
- [Multikey Authentication, page 10-28](#)
- [Quality of Service, page 10-28](#)

Automatic Service Connections

An automatically connected service is a service that SSG connects 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 Services, page 10-1](#)
- [Subscriber Experiences with Automatic Connections, page 10-2](#)

Configuring Automatic Services

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 C-6 on page C-11](#) 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, reinstall RDP.

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 10-1](#) 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's home URL is set to an autoconnect 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 correct. 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 the SESM session expires, the SSG reconnects all auto connect services.

The SESM session might expire, for example, because the subscriber closed the browser or navigated away from the SESM pages. When the 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.

Location Awareness

This section describes the SESM location awareness features. It includes the following topics:

- [Overview of Location Awareness, page 10-3](#)
- [Configuring Location Awareness Based on Complete ID Attributes, page 10-5](#)
- [Configuring Location Awareness Based on IP Address Subnets, page 10-7](#)
- [Demonstrating Location Awareness, page 10-8](#)

You can enhance location awareness features with arbitrary attributes, as described in the “[Arbitrary Attributes](#)” section on page 10-9.

Overview of Location Awareness

The SESM location awareness feature relies on the physical location characteristics of an edge session. SESM obtains this location information from the SSG as part of the session’s initial connection request. The specific attributes used to determine the location, and hence the location branding, are configurable.

The location attributes can consist of the client IP address, client subnet, MAC address, VPI/VCI, SSG subinterface, and MSISDN, depending on the network deployment, and are valid even before the session authenticates.

The SESM portal can use the location as a dimension in the user shape to help determine the resources to use in the returned JSPs.

**Note**

Location and locale are two different dimensions of the user shape. The locale dimension identifies subscriber language and character set preferences. SESM obtains the locale from the subscriber browser settings. The locale is available before the subscriber authenticates.

Some examples of using location information in customized SESM portals are:

- Location-based branding—Brand the portal pages and offer free or different services accordingly.
- Personalized portals—Taylor the subscriber experience based on location characteristics.
- Access policies—Allow free services to a certain segment of subscribers based on connection characteristics, such as VPI ranges or subinterface ranges. For example, location awareness could permit certain subscribers from a certain location to gain access to the Internet service without authentication.
- Redirections—Redirect all browsers with particular location characteristics to a specified portal page.

Location Awareness Configuration Methods

SESM offers two ways to configure location awareness. [Table 10-1](#) describes these two methods.

Table 10-1 Location Attributes

Feature	MBean	Attributes That Determine Location	Restrictions
Location awareness using complete ID attributes Note This is the recommended method for defining location awareness.	Location MBean	One of the following attributes or a combination of attributes: <ul style="list-style-type: none"> • Subscriber IP address range • Virtual path identifier (VPI) range • Subinterface, such as an Ethernet interface More attributes might be added in future releases.	Requires the SSG complete ID feature in one of the following Cisco IOS releases: <ul style="list-style-type: none"> • Release 12.3(1)T • Release 12.2(8)B, X train
Location awareness using IP subnets	SSG MBean	One of the following: <ul style="list-style-type: none"> • If the port-bundle host key feature is used—SSG IP address subnetwork ranges • If the port-bundle host key feature is not used—Subscriber IP address subnetwork ranges 	Does not work if load balancing is implemented. Will be phased out in future releases.

If both of the above location awareness methods are configured for the same SESM portal, the location derived from the IP subnet method takes precedence. If the session does not match the criteria configured for the IP subnet method (in the SSG MBean), then the portal examines the complete ID criteria in the Location MBean.

Using Location to Control the Look and Feel of Portal Pages

When the SESM portal identifies the location (based on configured attributes), it sets the “LOCATION” attribute in the SESMSession object created for the subscriber. For the location determination to be meaningful, the portal must use the “LOCATION” attribute. For example:

- The portal can use the location as a dimension in the user shape to help determine the resources to use in the returned JSPs. NWSP uses this method to determine a location-specific image to use in the NWSP banner. See the *Subscriber Edge Services Manager Web Developer Guide* for more information about the user shape mechanism, the location attribute in the locationDimension.jsp, and the SESMSession object.
- The portal can associate attributes to a location using the SESM arbitrary attributes feature. See the “Arbitrary Attributes” section on page 10-9 for more information.

Location Names

Any value is acceptable for a location name, but the name must match the intended uses. For example:

- NWSP uses the location dimension in the user shape to return different images on JSP pages based on location. To implement this usage, NWSP uses the configured location name to identify the subdirectory containing the correct image for each location. Therefore, the configured names must match the subdirectory names. For examples, see the following:

```
nwsp
  webapp
    london
    newyork
    paris
```

- NWSP associates arbitrary attributes to locations. The location names in the arbitrary attributes configuration must match the names used in location awareness configuration. For examples, see the “Configuring Arbitrary Attributes” section on page 10-10.

Configuring Location Awareness Based on Complete ID Attributes

The complete ID is the complete set of identifying attributes available about an edge session. SSG makes this set of attributes available to SESM. The SESM location awareness feature uses a subset of the complete ID attributes. The complete ID attributes that are currently supported for location awareness are listed in [Table 10-1](#).



Note

To use location awareness based on complete ID, your SSG platforms must be running Cisco IOS Release 12.3(1)T or the X train for Release 12.2(8)B.

Use the Location MBean to define location names and the attributes that are associated with each location. For information about the Location MBean, see the “Multikey Authentication” section on page 10-28.

Using Multiple Attributes for the Same Location

You can use multiple attributes to define a location. For example, the installed `nwsp.xml` file configures a “paris” location that applies to all sessions with a VPI from 1 to 3 on the subinterface ATM3/0. Both requirements must match for the location to apply to a session.

Each attribute definition in a location is restricted to one value or one range. However, you can define more than one location with the same name using the same attributes, but with different attribute values. For example, you could define two “london” locations, each one using a different IP address range.

Using Duplicate, Overlapping and Nested Attributes for Different Locations

This section describes the situation when a session’s attributes match the criteria for more than one location. SESM offers two ways to resolve the location in these cases:

- Identify the first matching location—The portal associates the first location whose configured attributes match all of the attributes of the edge session. The ordering of locations in the configuration file is important. NWSP implements location awareness using this method.
- Identify all matching locations—This feature provides a way to process nesting and overlapping locations. The portal must be customized to process all matching locations in some way. To implement this feature, see the next section.

Implementing Nested and Overlapping Locations

To implement nested or overlapping locations, you can customize the portal to use the `getLocations` method. This method returns an iterator over all the locations that match the attributes for the session, in the order that the locations appear in the configuration file.

Overlapping Locations

Overlapping locations occur when there is a possibility of sessions existing that match more than one location. They may or may not be defined on the basis of the same parameter types.

In the following example, two locations overlap for sessions with a client IP address in the range 10.4.0.0 to 10.8.0.0.

- Location A is defined for client IP range 10.0.0.0 to 10.8.0.0.
- Location B is defined for client IP range 10.4.0.0 to 10.32.0.0.

In the following example, two locations overlap for sessions with a client IP address in the range 10.0.0.0 to 10.8.0.0 that are connected via the subinterface Ethernet 0/0.

- Location A is defined for client IP range 10.0.0.0 to 10.8.0.0.
- Location B is defined for the sub-interface Ethernet 0/0.

Nested Locations

Nested locations are a specialization of the overlapping concept. Nesting occurs when one location is a subset of another. In the following example, Location A is nested inside location B.

- Location A is defined for the sub-interface ATM0 and VPI number 1 to 3.
- Location B is defined for the sub-interface ATM0.

When defining nested interfaces, it is usually best to define the smallest location first. In the example above, this would be Location A. This is because only the first match is returned when looking for a single location, so any nested locations would effectively get hidden if they were not placed in the configuration before the location they are nested inside.

There is no restriction on how deeply locations can be nested.

Configuring Location Awareness Based on IP Address Subnets

To configure locations based on IP address subnets, use the SSG MBean. Use `setSubnetAttribute` entries with the `SESSION_LOCATION` argument. The following example from `nwsp.xml` shows the attributes required for location awareness:

```
<Call name="setSubnetAttribute"><Arg>ipAddress</Arg><Arg>mask</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>location</Arg></Call>
```

[Table 5-5 on page 5-7](#) describes how to format subnet entries. The following points relate specifically to location awareness:

- *ipAddress* and *mask* indicate one of the following:
 - A range of subscriber IP addresses (a subnet)—Use the IP address and Mask fields to indicate a subnet of IP addresses to associate with the same location. If port-bundle host key is configured on the SSG, the range will apply to SSG IP addresses, rather than subscriber IP addresses.
 - A specific IP address—The IP address is that of the client, or, if port-bundle host key is configured on the SSG, one of the SSG IP addresses specified in the port-bundle host key port map configuration.
- *location* is the location you want to associate with *ipAddress*. Any value is acceptable, but it must match your intended uses.
- Any value is acceptable, but it must match your intended uses. For example:
 - NWSP uses different images for each location. The images are stored in subdirectories whose

Example 1—Location Associated with Subscriber IP Addresses

The following example associates locations with subscriber subnets. The example associates a different subscriber network with each of the three example locations defined in Step 2. In the NWSP application, when subscribers from the 144.0.0.0 network point their browsers to the NWSP URL, they receive a page containing the words New York under the NWSP logo.

```
<Call name="setSubnetAttribute"><Arg>10.0.0.0</Arg><Arg>255.0.0.0</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>1.0.0.0</Arg><Arg>255.0.0.0</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
<Call name="setSubnetAttribute"><Arg>144.0.0.0</Arg><Arg>255.0.0.0</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>newyork</Arg></Call>
```

Example 2—Location Associated with SSG IP Address

When the port-bundle host key feature is configured on the SSG, location must be associated with an SSG IP address, rather than the subscriber's IP address. In the following example, the IP address is an SSG source IP address included in the port mappings during port-bundle host key configuration.

```
<Call name="setSubnetAttribute"><Arg>10.52.199.20</Arg><Arg>255.255.255.255</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
```

Demonstrating Location Awareness

The NWSP application illustrates location awareness by changing the look of the banner on the NWSP logon page. The location determines which city name appears in the NWSP logo. The installed `nwsp/docroot` directory includes subdirectories for three locations: `london`, `paris`, and `newyork`. These subdirectories contain the images used in this demonstration. If you want to use different city values, you must provide the corresponding images. The application code that displays the banner is in `locationDimension.jsp`.

Demonstration Procedure Using Complete ID Attributes

To demonstrate location awareness based on Complete ID attributes, use the following procedure:

- Step 1** Install SESM in RADIUS or LDAP mode, using a typical or custom installation. (Do not use Demo.)



Note You cannot use Demo mode to show location awareness using complete ID attributes.

- Step 2** Comment out the location subnet entries in the SSG MBean.

- Step 3** Edit the Location MBean to include a specific IP address for the “paris” location. Use the IP address of a client machine that is available for the demonstration. Use the same IP address in the start and end parameters.

For example:

```
<Set name="name">london</Set>
<Set name="parameters">
<Array class="com.cisco.sesm.core.location.LocationParameter">
<Item>
<New class="com.cisco.sesm.core.location.IPRangeParam">
<Set name="start" type="String">needIPAddress</Set>
<Set name="end" type="String">needIPAddress</Set>
</New>
</Item>
</Array>
</Set>
```

- Step 4** Add a new location to the Location MBean for “newyork.” (Use this value because the installed files include a subdirectory and an image for the newyork value.) For example, insert these lines into the locations array:

```
<Item>
<New class="com.cisco.sesm.core.location.Location">
<Set name="name">newyork</Set>
<Set name="parameters">
<Array class="com.cisco.sesm.core.location.LocationParameter">
<Item>
<New class="com.cisco.sesm.core.location.IPRangeParam">
<Set name="start" type="String">needIPAddress</Set>
<Set name="end" type="String">needIPAddress</Set>
</New>
</Item>
</Array>
</Set>
</New>
</Item>
```

- Step 5** Start NWSP using the NWSP startup script.
- Step 6** Open browsers on each of the client systems.
- Step 7** From each browser, go to the SESM URL. For example, go to `http://serverName:8080`.
- Step 8** Notice the images in the banners on each browser. One should say London; the other should say New York.
- Step 9** On a third machine, repeat steps 7 through 9. The banner should not include a city name, because the third browser's IP address is not associated with any location in the configuration file.
-

Demonstration Procedure Using Subnet Entries

To demonstrate location awareness based on subnet entries, use the following procedure:

- Step 1** Install SESM in Demo mode.
- Step 2** Edit `setSubnetAttribute` parameters in the SSG MBean to include specific IP addresses for two different client machines that are available for the demonstration. For example:
- ```
<Call name="setSubnetAttribute"><Arg>NEED_REAL_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
 <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>NEED_REAL_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
 <Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
```
- Step 3** Start NWSP using the NWSP startup script.
- Step 4** Open browsers on each of the client systems.
- Step 5** From each browser, go to the SESM URL. For example, go to `http://serverName:8080`.
- Step 6** Notice the images in the banners on each browser. One should say London; the other should say Paris.
- Step 7** On a third machine, repeat steps 7 through 9. The banner should not include a city name, because the third browser's IP address is not associated with any location in the configuration file.
- 

## Arbitrary Attributes

This section describes the arbitrary attribute feature. It includes the following sections:

- [Description of Arbitrary Attributes, page 10-9](#)
- [Configuring Arbitrary Attributes, page 10-10](#)
- [Demonstrating Arbitrary Attribute Assignments in NWSP, page 10-11](#)

## Description of Arbitrary Attributes

The arbitrary attribute feature lets the deployer create any arbitrary attribute and associate it with other known attributes. To use the arbitrary attribute feature, you configure a multidimensional table consisting of the known attribute values and the arbitrary attributes you are associating.

For example, NWSP uses arbitrary attributes to associate URLs with locations. In this case, the elements in the multi-dimensional table are as follows:

- One dimension of the table consists of the location values, which must be defined using the location awareness feature.
- Another dimension is the URL to associate with each location.

At run time, SESM constructs a reference table holding all of the configured values. The arbitrary attribute values are available for use by the SESM portal. For example, NWSP uses arbitrary attributes associated with locations to help determine the initial URL for an Internet service pop-up window.

## Configuring Arbitrary Attributes

To configure the SESM portal to associate arbitrary attribute values to locations, use the following procedure:

**Step 1** In the WebApp MBean, use `addDimension` calls to configure the arbitrary attribute reference table.

**Step 2** The format for an `addDimension` call is:

```
<Call name="addDimension">
 <Arg type="int">attributeID</Arg>
 <Arg>attributeKey</Arg>
 <Arg>attributeResult</Arg>
```

An example from `nwsp.xml` is:

```
<Call name="addDimension">
 <Arg type="int">1</Arg>
 <Arg>london</Arg>
 <Arg>http:\\www.london.com</Arg>
```

Where:

- *attributeID* identifies a category of entries in the attribute table. Use the same *attributeID* for all entries associated with the same purpose.
- *attributeKey* identifies the location values. For example, the installed WebApp MBean includes the values `london`, `paris`, and `newyork`. The location values must be defined in the location awareness feature.



**Note** Make sure the location values match exactly the definitions used for location awareness. For example, the “London” and “london” are considered different values.



**Note** The user shape mechanism and the `addDimension` calls are different features. The user shape mechanism has no dependencies on any values defined in the `addDimension` calls.

- *attributeResult* defines a URL that you want to associate with the *attributeKey*.



## Demonstrating Arbitrary Attribute Assignments in NWSP

The arbitrary attribute used in this demo determines the first URL that the browser attempts to display after the subscriber connects to an Internet service. The code that implements this demo is in `initUser.jsp`. The code determines the initial URL as follows (the second item uses the arbitrary attribute feature):

1. If the subscriber request was captured by the SESM Captive Portal application, the subscriber's initial URL request is used.
2. Otherwise, if a location in an `addDimension` call matches the `LOCATION` attribute from the `SESMSession` object, the URL associated with the location is used.
3. Otherwise, if the subscriber profile includes a non-blank `H` attribute, that URL is used.

### Demonstration Procedure

To demonstrate the use of an arbitrary attribute to control an item on a JSP page, use the following procedure.

- 
- Step 1** Configure location awareness. You can use either location awareness method: subnets configured in the SSG MBean, or complete ID attributes configured in the Location MBean.
- Step 2** Edit the parameters to the `addDimension` calls in the WebApp MBean. Make sure the second argument in the `addDimension` call matches exactly the location strings you defined for location awareness. The installed `nwsp.xml` file contains the following lines:
- ```
<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>
```
- Step 3** Start NWSP using the NWSP startup script.
- Step 4** Start a browser on a system whose location was configured in Step 1.
- Step 5** Go to the NWSP URL.
- Step 6** Login using the following values:
- RADIUS mode demos:
 - User: radiususer
 - Password: cisco
 - LDAP mode demos:
 - User: golduser
 - Password: cisco
- Step 7** Select the Internet service from the NWSP service list (if the Internet service was not automatically configured.)

A service pop-up window appears, attempting to go to the URL in the `addDimension` call. For example, the london location attempts to go to `www.london.com`.

**Note**

If you configured the Captive Portal application, the browser's original request is honored instead of the arbitrary attribute associated with the location.

Personal Firewalls

This section describes how to configure and use the SESM personal firewall features. Topics are:

- [Overview of Firewall Features, page 10-12](#)
- [My Firewall Page, page 10-14](#)
- [Advanced Firewall Page, page 10-16](#)
- [Configuring the Firewall Pages, page 10-18](#)
- [ACLs Generated from Entries on the Firewall Pages, page 10-19](#)
- [Subscriber Experiences with Personal Firewalls, page 10-25](#)
- [Deployer-Imposed Firewalls, page 10-25](#)
- [References for More Information about Access Control Lists, page 10-27](#)

Overview of Firewall Features

The SESM personal firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on web portal pages. Deployers can also apply firewall controls on subscriber traffic.

The NWSP application includes two personal firewall pages:

- **My Firewall page**—This is a basic firewall page that allows subscribers to create filters on specific applications and protocols. The subscriber can choose to permit or deny all traffic for each of the applications/protocols. The list of applications and protocols that appears on the My Firewall page is preconfigured by the deployer in the Firewall MBean.
- **Advanced Firewall page**—This page provides a way for the subscriber to create more specific filters than the basic page. They can create filters that permit or deny traffic for specific source and destination IP addresses, ranges of IP addresses, or ports.

The deployer-imposed firewall controls cannot be changed by the subscriber. The deployer-imposed controls are added to subscriber profiles using CDAT. These controls have a higher priority and can therefore override the personal firewalls entered by subscribers.

Required Deployment Options

The SESM firewall features are supported only when SESM is running in LDAP mode with RDP deployed in non-Proxy mode. The SSG (or some other cooperating network element that can process extended access control lists) is required.

Underlying Technology

The underlying technology for the SESM personal firewall features is extended access control lists (ACLs). The ACLs are attributes in subscriber profiles in an LDAP directory.

The ACLs are stored in the subscriber profiles as a standard RADIUS attribute with number 26 (vendor specific attribute), subattribute number 1 (Cisco AV-pair). A subscriber profile might have many ACL entries, which together determine which traffic is permitted and denied on the connection.

The ACLs are added to the profile in two ways:

- The SESM portal creates the ACLs and adds them to the profile as a result of subscriber entries on the portal firewall pages.
- Deployer administrators manually create correctly formatted ACLs and enter them in the subscriber profile using CDAT.

SESM and SSG (or another cooperating network element) implement the personal firewall ACLs as follows:

- SSG sends an access-request message to RDP.
- During authentication processing, RDP obtains the subscriber profile from the directory and includes all of the profile information, including the ACLs, in the access request reply it sends back to the SSG.
- The SSG applies the ACLs against traffic to and from the subscriber's connection.

Firewall Priorities

The SSG or other cooperating network element applies the ACLs in a subscriber's profile, in a prioritized order, to each packet. When the conditions specified in an ACL match the packet, the permit or deny action specified in the ACL is applied to the packet, and no further ACLs are examined for that packet. The order in which ACLs are applied affects the filtering outcome.

In the SESM ACLs in a subscriber profile, priority is based on an ACL number. (The lowest ACL number is applied first.) The ACL numbering scheme used by SESM enforces the following general priorities:

- Administrative ACLs have the highest priority. These ACLs are entered by the deployer in CDAT should contain ACL numbers in the range from 100 to 109. It is up to the administrators entering the ACLs to enforce this convention.
- ACLs generated from the Advanced Firewall page have the next priority. The SESM portal automatically assigns these ACL numbers.
- ACLs generated from the My Firewall page have the lowest priority. The SESM portal automatically assigns these ACL numbers.

See the [“ACL Number Assignments” section on page 10-23](#) for a description of how SESM assigns the ACL numbers to ensure that the most specific ACLs are applied first, and the more general ACLs last.

My Firewall Page

Figure 10-1 shows the NWSP My Firewall page as it appears if there are no ACLs in the subscriber profile, or if the only ACLs in the profile are deployer-imposed ACLs. (Deployer-imposed ACLs are ones with ACL numbers in the 100 to 109 range.)

Figure 10-1 My Firewall Page in NWSP



A description of the My Firewall page follows.

- Firewall Enabled or Disabled—When the page displays, this button indicates whether any subscriber-entered filters exist for this subscriber:
 - Enabled—At least one subscriber-entered filter exists in the subscriber’s profile. The filters can be those entered on the My Firewall or Advanced Firewall page. Administrative ACLs, if any exist in the profile, are not considered.
 - Disabled—This subscriber profile contains no subscriber-entered filters. If the window opens with Enabled selected, and the subscriber clicks **Disabled** followed by **OK**, it deletes all subscriber-entered filters from the subscriber profile. The action does not delete administrative ACLs if the administrator used the reserved administrative ACL numbers (numbers 100 through 109.)



Note

Once deleted, the ACLs cannot be retrieved. They must be reentered. The deployer might want to customize the NWSP My Firewall page to remove the Disable button or move the button to the Advanced Firewall page.

- Permit All Else or Deny All Else buttons

When a subscriber profile contains one or more ACLs, an implicit default denies all other traffic not addressed by the existing ACLs. This deny-all-else implicit default is imposed by the Cisco router hosting the SSG or other cooperating network element.

The Permit All Else or Deny All Else radio buttons offer a way for the subscriber to explicitly impose a default behavior. A deployer could decide not to display these buttons and allow the implicit behavior to operate. In this case, the page would not need the Deny button next to each application.

When firewalls are enabled, the subscriber must consider whether to permit or deny traffic for each of the applications listed on the Firewall page. To do this, the subscriber can:

- Consider each application separately, and select whether to permit or deny traffic for it.
- Allow the default action to apply. They choose the default action by selecting either the Permit All Else or Deny All Else button.

- Applications/Protocols

Lists the applications available for firewall settings. This list is configured by the deployer, as described in the [“Configuring the Firewall Pages” section on page 10-18](#). For each application in the list, the subscriber can specify whether to deny or permit traffic. The ACLs that NWSP generates for this page will specify that all source and all destination IP addresses are subject to the control being defined in the ACL.



Note The subscriber can use the Advanced Firewall Page to obtain finer control in the ACLs, such as specifying specific IP addresses or ports that are subject to the control.

- Permit/Deny/Default buttons—The portal determines the initial setting for each item in the Application/Protocol list, as follows:
 - If no ACLs exist or if only one ACL exists in the subscriber’s profile for the application/protocol, **Default** is selected. In a typical production deployment, most applications initially appear in the default state, because there are no specific ACLs in the subscriber profiles.
 - If the application/protocol has more than one ACL in the subscriber profile:
 - If all ACLs have the same permission (that is, all are permit or all are deny), then the corresponding **Permit** or **Deny** is selected.
 - Otherwise, if some ACLs specify permit and others deny, then **Default** is selected for that application.

First Time Access of My Firewall Page

The default state of a subscriber profile is one in which no ACLs are defined. The first time the subscriber goes to the My Firewall page, the settings are:

- Firewall Disabled—Indicating that there are no ACLs imposing any controls on traffic to or from the subscriber.
- Deny All Else—Ignore this button when firewalls are disabled.
- For all applications and protocols, the Default buttons are selected.

When ACLs exist in the subscriber profile, the SESM portal analyzes the ACLs and renders the page based on the ACLs, as described in the previous section.

Advanced Firewall Page

Figure 10-2 shows the Advanced Firewall page.

Figure 10-2 Advanced Firewall Page in NWSP

Advanced Firewall

The entries on this page work independently of those on the basic page and override those wherever applicable.

Any / Specific Address	IP Address	Mask	IP Protocol	IP Protocol Number	Application Protocol	Port Number	Permit	Deny	Delete Entry
From me to these destinations:									
Add a new entry:									
<input type="radio"/>	<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	=	<All>	<input type="text"/>	<input type="radio"/>	<input type="radio"/>
To me from these sources:									
Add a new entry:									
<input type="radio"/>	<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	=	<All>	<input type="text"/>	<input type="radio"/>	<input type="radio"/>

OK Go Back Reset

76726

A description of the Advanced Firewall page follows.

- From me/To me entries—Subscribers can enter filters for upstream or downstream traffic.
 - From me to these destinations— These entries filter messages that the subscriber can initiate. The filters are based on the destination IP address, port, protocol, and application entered by the subscriber.

The source is the subscriber. In the NWSP application, the source IP address for these entries is always set to “any” and source port is not specified. SESM developers can alter the Advanced Firewall JSP, adding fields to let the subscriber enter source IP address and port.

The ACLs generated from these entries are known as inacIs. The inacIs specify filters for traffic travelling upstream into the SSG host or other routing device. For more information about inacIs, see the [“References for More Information about Access Control Lists”](#) section on page 10-27.

- To me from these sources—These ACLs filter messages that the subscriber can receive. The filters are based on the source IP address, port, protocol, or application entered by the subscriber.

The destination is the subscriber. In the NWSP application, the destination IP address for these entries is always set to “any” and destination port is not specified. SESM developers can alter the Advanced Firewall JSP, adding fields to let the subscriber enter destination IP address and port.

The ACLs generated from these entries are known as outacIs. The outacIs specify filters for traffic travelling downstream, out from the SSG host or other routing device. For more information about outacIs, see the [“References for More Information about Access Control Lists”](#) section on page 10-27.

See the *Subscriber Edge Services Manager Web Developer Guide* and the SESM javadoc for more information about development options for JSP pages.

- Any/Specific Address—Indicates whether this ACL applies to any IP address or to specific IP addresses provided in the IP Address and Mask fields.
- IP Address and Mask—Specifies the source or destination IP address or address range that is being permitted or denied. Any ACL can specify IP addresses. Be sure to click the Specific Address radio button (above) if you are including an IP address.

The mask for ACLs is inverted from the more familiar net mask. Bits in the mask are zero if the respective bit in the address should match. For example, if the ACL should filter addresses x.x.x.0, then the mask is 0.0.0.255.

- IP Protocol—Specifies the Internet protocol to filter:
 - Any IP—Filters all IP traffic.
 - tcp—Filters TCP traffic.
 - udp—Filters UDP traffic.
 - <0-255>—Filters traffic based on a protocol number specified in the IP Protocol Number field.
- IP Protocol Number—A number in the range 0 through 255. Protocol numbers refer to protocol configurations on the SSG host or other routing device. For example, TCP corresponds to the protocol number 6.
- Port Operator (=, !=, >, <)—Valid only when IP Protocol is TCP or UDP. The operator applies to the application protocol port number. (Each application protocol name is an alias to a port number.) The operator is used to compare the port in a packet to the port specified in the ACL.
 - = requires the port values to match
 - != requires that the port values not match
 - > requires that the port in the packet be greater than the port value specified in the ACL
 - < requires that the port in the packet be less than the port value specified in the ACL
- Application Protocol—Valid only when IP Protocol is TCP or UDP. An ACL can filter on a specific application carried on the TCP or UDP protocols. (On the SSG host or other routing device, each application is configured on a unique port. The ACLs filter on those port numbers or the aliases to those port numbers.) To specify the application port to filter, either:
 - Choose <0-65535> from this drop down list and provide the appropriate port number in the Port Number field.

Choose an application from the Application drop down list. This list consists of all of the application port aliases configured in the Firewall MBean for TCP. The corresponding port number automatically appears in the Port Number field.

In NWSP, the Application drop down list is meaningful only when IP Protocol is TCP. If IP Protocol is UDP, the subscriber must choose <0-65535> and explicitly enter the correct UDP port number in the Port Number field.



Note

If the subscriber chooses an application from the list when IP Protocol is UDP, NWSP uses the port number that corresponds to the selected application. The deployer could customize NWSP to implement a separate drop down list for UDP applications. Alternatively, the deployer could remove the Internet Protocol and Internet Protocol Number fields, making TCP the default, in which case the existing list of applications would always be appropriate.

- Port Number—Valid only when IP Protocol is TCP or UDP and Application Protocol is <0-65535>. Enter the application port to filter. The port number must match the port configured for the application or protocol on the SSG host device or other cooperating network element.
- Permit—Adds the permit keyword to the generated ACL. The permit keyword allows a message to travel to its destination when the message matches the conditions in the ACL.
- Deny—Adds the deny keyword to the generated ACL. The deny keyword prevents a message from traveling to its destination when the message matches the conditions in the ACL..
- Delete Entry—Deletes this ACL from the subscriber profile. If this is a new entry, using this button has no effect on the subscriber profile.



Note To be added to the subscriber profile, a new entry must have either the Permit or Deny button selected.

- The three action buttons at the bottom of the window are:
 - OK—Adds the changes to the subscriber profile.
 - Go Back— It cancels any changes you made on the page since last using OK and returns to the My Firewall page
 - Reset—Cancels any changes you made on the page since last using OK and redisplay the page, showing the settings that currently exist in the subscriber profile.

Configuring the Firewall Pages

To configure the SESM firewall features, use the Firewall MBean, described in the [“Firewall MBean” section on page 5-11](#).

Configuring the Application/Protocol List on the My Firewall Page

The Application/Protocol list on the My Firewall page is configured by the deployer as follows:

- The applications that appear in the list are configured in the Firewall MBean.
- The displayed text that represents an application in the list is obtained from a resource bundle in the portal application’s directory.

Configuring the Drop Down Lists on the Advanced Firewall Page

The contents of the drop down lists on the Advanced Firewall page are configured by the deployer as follows:

- The IP Protocol drop down list shows the list of Internet protocols configured in the Firewall MBean.
- The Application/Protocol drop down list shows the port aliases configured for TCP applications in the Firewall MBean.



Note Developers can customize the Advanced Firewall JSP, hardcoding options rather than using the values obtained from the Firewall MBean.

ACLs Generated from Entries on the Firewall Pages

This section describes the ACLs that are automatically generated by the SESM portal. The section includes the following topics:

- [Viewing Generated ACLs, page 10-19](#)
- [Generated ACLs for the My Firewall Page, page 10-19](#)
- [Generated ACLs for the Advanced Firewall Page, page 10-22](#)
- [ACL Number Assignments, page 10-23](#)

Viewing Generated ACLs

The deployer administrators can view all ACLs in a subscriber profile using CDAT. The ACLs appear in the Local RADIUS attribute field. The field contains all ACLs automatically generated by the SESM portal as a result of subscriber actions on the basic and advanced firewall pages, as well as any administrative ACLs directly entered by the deployer.

Depending upon CDAT privileges, which are assigned within CDAT, the administrator might be permitted to add, change and delete ACLs from the profile through CDAT.

NWSP does not provide a way for subscribers to view the generated ACLs.

Generated ACLs for the My Firewall Page

This section describes the ACLs that are automatically generated by NWSP from entries on the My Firewall page. The My Firewall page always results in ACLs that filter on:

- Any source and any destination address.
- A specific port number associated with the chosen application.

Subscribers must use the Advanced Firewall page to create ACLs that filter on specific addresses or multiple port numbers.

The ACLs generated from the My Firewall page are in the following form:

```
[inacl# | outacl#]Number=permission protocol any any eq portNumber [established]
```

Where:

- *inacl#* or *outacl#* is used, depending on the value of the direction attribute in the Firewall MBean.
 - *inacl#*—Applies the ACL to upstream traffic, which is traffic from the subscriber
 - *outacl#*—Applies the ACL to downstream traffic, which is traffic to the subscriber

All TCP connections require a return path. A block on upstream traffic also affects the traffic traveling in the opposite direction, and vice-versa, if there is no ACL allowing established connections in the same direction as the block. For example, blocks on downstream traffic and an ACL allowing established connections on downstream traffic would allow the TCP upstream traffic.

The choice of whether to control the in or out direction in the My Firewall ACLs is a matter of preference for the deployer to decide. All ACLs generated from the My Firewall page use the same direction.

- *Number* is in the range from 110 to 196. SESM assigns the ACL number as described in the “[ACLs Generated from Entries on the Firewall Pages](#)” section on page 10-19.

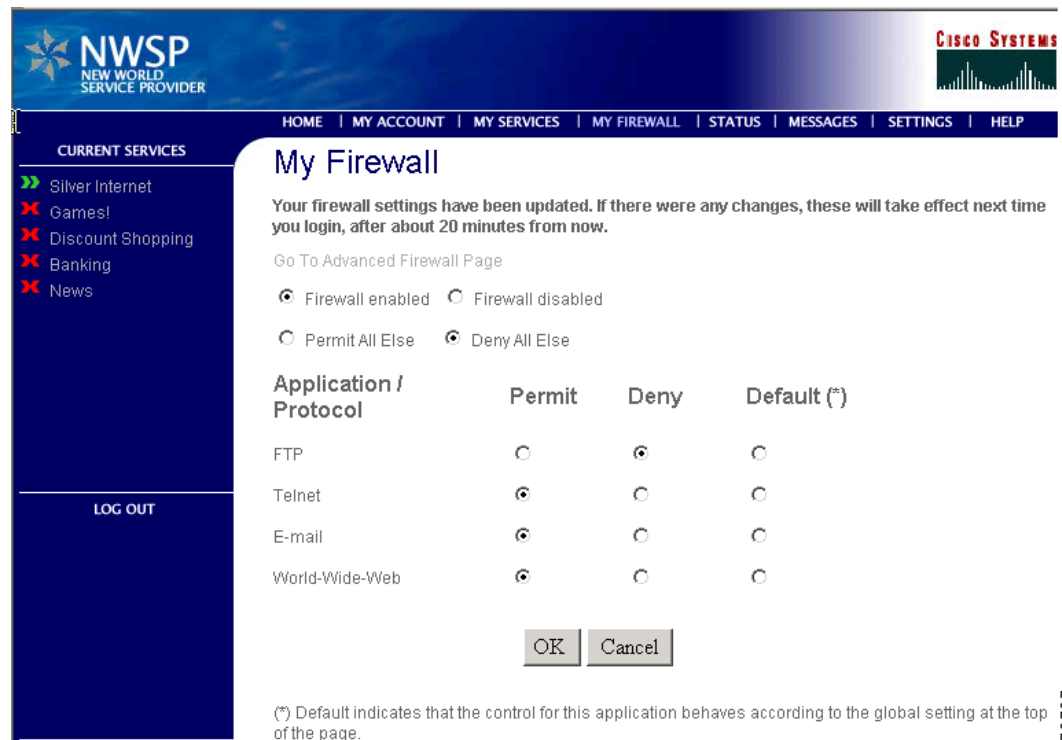
- *permission* is one of the following values:
 - permit
 - deny
- *protocol* is the configured protocol for the application, as defined in the Firewall MBean. Examples are tcp, udp, ip, and so on.
- “any any” are keywords in the source IP address and destination IP address fields. The keyword “any” specifies that all source and all destination IP addresses are subject to the control being defined in this ACL. Subscribers must use the Advanced Firewall page to create filters on specific IP addresses.
- “eq” is a keyword in the operator field. The keyword “eq” specifies that the filter applies to traffic whose source or destination port matches (equals) the value in *portNumber*. All ACLs generated from the My Firewall page use the “eq” keyword. Subscribers must use the Advanced Firewall page to specify other operators.
- *portNumber* is the port number related to the application, as defined in the Firewall MBean.
- *established* is a keyword used in the automatically generated ACLs for TCP return connections. In the Firewall MBean, an application named return is configured. Also in the Firewall MBean, the ReturnOption attribute specifies the permission to use in the TCP return connection ACLs.

For more information, see the [“Firewall MBean” section on page 5-11](#).

My Firewall Example

Figure 10-3 shows an example My Firewall page.

Figure 10-3 My Firewall Example



The settings shown in Figure 10-3 result in the following ACLs:

```
Cisco_AV:ip:inacl#196=deny ip any any
```

```
Cisco_AV:ip:outacl#196=deny ip any any
```

```
Cisco_AV:ip:outacl#129=permit tcp any any established
```

```
Cisco_AV:ip:inacl#128=deny tcp any any eq 21
```

```
Cisco_AV:ip:inacl#128=permit tcp any any eq 23
```

```
Cisco_AV:ip:inacl#158=permit tcp any any eq 25
```

```
Cisco_AV:ip:inacl#158=permit tcp any any eq 109
```

```
Cisco_AV:ip:inacl#158=permit tcp any any eq 110
```

```
Cisco_AV:ip:inacl#158=permit tcp any any eq 143
```

```
Cisco_AV:ip:inacl#138=permit tcp any any eq 80
```

```
Cisco_AV:ip:inacl#138=permit tcp any any eq 443
```

Generated ACLs for the Advanced Firewall Page

This section describes the ACLs that are automatically generated by the SESM portal based on subscriber entries on the Advanced Firewall page. The ACLs generated from the Advanced Firewall page are in the following form:

```
{inacl# | outacl#}Number=permission protocol {any | sourceIPAddress sourceMask} [operator port]
{any | destinationIPAddress destinationMask} [operator port] [established]
```

Where:

- *inacl#* or *outacl#* is used, depending on which section on the Advanced Firewall page the subscriber used:
 - *inacl#*—The subscriber entered the ACL in the “From me to these destinations” section. The ACL applies to upstream traffic, which is traffic from the subscriber.
 - *outacl#*—The subscriber entered the ACL in the “To me from these sources” section. The ACL applies to downstream traffic, which is traffic to the subscriber.

All connections have a return path. A block on upstream traffic also affects the traffic traveling in the opposite direction, and vice-versa. The choice of whether to control the in or out direction in the Advanced Firewall is a matter of preference for the subscriber.

- *Number* is in the range from 110 to 196. SESM assigns the ACL number as described in the [“ACLs Generated from Entries on the Firewall Pages” section on page 10-19](#).
- *permission* matches the choice selected by the subscriber on the Advanced Firewall page:
 - permit
 - deny
- *protocol* is the protocol that the subscriber selected from the drop down list on the Advanced Firewall page (ip, tcp, or udp.)
- *sourceIPAddress sourceMask*—The values entered by the subscriber in “To me from these sources” entries.
- *operator port*—The operator matches the subscriber selection on the Advanced Firewall page. Operator values in ACLs are: eq, ne, lt, gt.
- *destinationIPAddress destinationMask* —The values entered by the subscriber in “From me to these destinations” entries.
- *portNumber* is the port number related to the protocol, as defined in the Firewall MBean.

Advanced Firewall Example

Figure 10-4 shows sample settings on the Advanced Firewall page.

Figure 10-4 Advanced Firewall Example

Any / Specific Address	IP Address	Mask	IP Protocol	IP Protocol Number	Application Protocol	Port Number	Permit	Deny	Delete Entry	
From me to these destinations:										
<input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	=	ftp	<input type="text"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="text"/>	<input type="text"/>	any IP	<input type="text"/>	=	<All>	<input type="text"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Add a new entry:										
<input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	=	<All>	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
To me from these sources:										
<input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	=	ftp	<input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="text"/>	<input type="text"/>	any IP	<input type="text"/>	=	<All>	<input type="text"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Add a new entry:										
<input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	=	<All>	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

OK Go Back Reset

The settings shown in Figure 10-4 result in the following ACLs:

```
Cisco_AV:ip:inacl#118=permit tcp any any eq 21
```

```
Cisco_AV:ip:outacl#118=deny tcp any eq 21 any
```

```
Cisco_AV:ip:inacl#193=permit ip any any
```

```
Cisco_AV:ip:outacl#193=permit ip any any
```

ACL Number Assignments

ACL numbers affect the order in which the SSG or other cooperating network element applies ACLs to the packet. Lower numbers are processed first. ACL processing stops the first time the ACL conditions match the packet information, and the deny or permit action in the matching ACL is carried out. The ACL number, therefore, can affect the filtering outcome.

ACL numbers are not permanent. Each time a subscriber uses the firewall pages to add or change ACL entries, the SESM portal reexamines all ACLs in the subscriber's profile and reassigns ACL numbers.

When the portal assigns ACL numbers to the automatically generated ACLs, it enforces the conventions and priorities described in Table 5-1.

Table 10-2 ACL Numbers for Automatically Generated ACLs

Priority	ACL Number	Explanation
Highest Priority	100 - 109	Reserved for administrative ACLs.
	110 - 119	ACLs from the Advanced Firewall page, when no application is specified. The explanation below for the 3rd digit applies to these ACLs as well.
	120 - 189	<p>ACLs from the My Firewall page. The numbers within this range are assigned as follows:</p> <ul style="list-style-type: none"> • 1st digit—Is always 1 (1xx) • 2nd digit—Indicates the number of ACL entries that currently exist in the subscriber’s profile for the same application: <ul style="list-style-type: none"> – 12x—Applications with 1 ACL entry – 13x—Applications with 2 ACL entries – ...and so on – 18x—applications with 7 or more ACL entries • 3rd digit—Indicates how specific the IP addresses and ports are, with lower numbers (higher priority) given to ACLs containing the most specific address and port information: <ul style="list-style-type: none"> – 1x0—Not used. – If neither source nor destination addresses are “any”: <ul style="list-style-type: none"> 1x1—Both source and destination ports are specified 1x2—Either source or destination port is specified 1x3—Neither source nor destination port is specified – If either source or destination addresses is “any” <ul style="list-style-type: none"> 1x4—Both source and destination ports are specified 1x5—Either source or destination port is specified 1x6—Neither source nor destination port is specified – If both source and destination ports are “any” <ul style="list-style-type: none"> 1x7—Both source and destination ports are specified 1x8—Either source or destination port is specified 1x9—Neither source nor destination port is specified <p>Example: A profile contains two ACLs for the same application, both with specific source addresses, destination addresses of “any”, and no ports. The ACL number for both is 136.</p>
190 not used 191 - 193	<p>Internet protocol (IP) settings on the Advanced Firewall page:</p> <ul style="list-style-type: none"> • 191—Both source and destination addresses are specified • 192—Either source or destination address is specified • 193—Neither source nor destination address is specified 	
Lowest priority	194 - 196	<p>Internet protocol (IP) settings on the My Firewall page:</p> <ul style="list-style-type: none"> • 194—Both source and destination addresses are specified • 195—Either source or destination address is specified • 196—Neither source nor destination address is specified

Subscriber Experiences with Personal Firewalls

This section describes how the personal firewall feature works from the subscriber point of view.

Creating Personal Firewalls

Subscribers create their personal firewalls by clicking radio buttons on the My Firewall page. The SESM portal creates the ACLs based on the information from the My Firewall page and adds the ACLs to the subscriber profile in the LDAP directory.

When New ACLs Take Effect

Although the LDAP directory is updated with the new information, the new ACLs do not take effect until a subscriber reauthenticates (logs out and logs in again). Also, the RDP cache must be refreshed, which by default takes 10 minutes. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time.

Interaction Between Entries on the My Firewall and Advanced Firewall Pages

The ACLs created from the Advanced Firewall pages have higher priority than ACLs created from the My Firewall page. Therefore, the subscriber might see filtering information on the My Firewall page that does not get applied to traffic because it is overridden by filters on the Advanced Firewall page.

Similarly, ACLs created by administrators (if they use the reserved ACL numbers 100 through 109) have the highest priority. Therefore, the subscriber might see filters on either the My Firewall or Advanced Firewall page that does not get applied to traffic because it is overridden by the administrative filters.

Safeguards

SESM and SSG include the following safeguards regarding firewalls:

- Subscribers cannot inadvertently deny themselves access to the SSG or the default network. SSG does not apply ACLs if the packet is going to the default network.
- Subscribers cannot inadvertently deny themselves access to open garden services. SSG does not use the subscriber's personal ACLs on packets coming from and going to open-garden services or in local-forwarding. (A set of host ACLs might apply in these cases.)
- ACLs generated from the Firewall pages are correctly formatted.
- Subscribers must have the SESMFirewall permission to use the firewall pages. Subscriber permissions are assigned in CDAT, in the user and group windows.
- Administrators must have the appropriate permissions to add or update user profiles. Administrator permissions are assigned in CDAT.

Deployer-Imposed Firewalls

This section describes how to configure and use the administrative firewall feature. It includes the following topics:

- [Restrictions, page 10-26](#)
- [Procedure for Entering ACLs in CDAT, page 10-26](#)
- [ACL Format for CDAT Entries, page 10-26](#)

Restrictions

Deployer-imposed firewalls can be used in conjunction with the subscriber self-configured firewalls, with the following restrictions:

- You should test the ACLs before moving them to a production environment.
In SESM Release 3.1(7), you must enter a correctly formatted ACL in CDAT. CDAT does not analyze or validate your ACL entry.



Caution

The SSG does not allow a subscriber to authenticate if the profile contains an incorrectly formatted ACL.

- You should create ACLs using ACL numbers in the range from 100 to 109.
The ACL numbers from 100 to 109 are reserved for administrator use. By using these numbers, you ensure that these ACLs are processed first, making them the highest priority.
If you create ACLs in CDAT using ACL numbers in the range from 110 to 196, (the ACLs reserved for use by the subscriber self-configured ACLs), you risk the following:
 - You might interfere with the personal firewall settings created by the subscriber.
 - You provide the opportunity for the subscriber to reverse your settings.

Procedure for Entering ACLs in CDAT

To enter deployer-imposed ACLs, use the following procedure:

-
- Step 1** Start the CDAT application.
 - Step 2** Log in as an administrator with permissions to modify subscriber profiles.
 - Step 3** Access the subscriber or group profile.
 - Step 4** Enter the ACLs in the Local RADIUS attribute field, using the format described in the following section.
 - Step 5** If a subscriber is currently logged into an SESM session, the new ACLs do not take effect until the subscriber reauthenticates (logs out and logs in again). Also, the RDP cache needs to be refreshed, which by default takes 10 minutes. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time.
-

ACL Format for CDAT Entries

This section describes the format of the firewall entries in the Local RADIUS attribute field in CDAT. The ACLs entered in CDAT can use the full range of ACL options as described in the Cisco IOS documentation for extended ACLs.

The general format for the Local RADIUS attribute field is:

attribute:value

In the case of the firewall ACL entries:

- attribute* is Cisco_AV
- value* is the ACL whose format is described below

The format of the ACLs entered by administrators is:

```
Cisco_AV:ip:directionacl#ACLnumber=permission protocol source destination
```

Where:

- *direction* is one of the following:
 - in
 - out
- *acl#* is a required string
- *ACLnumber* is in the range from 100 to 109. The numbers indicate priority in the ACL evaluation. ACLs with the lowest numbers are analyzed first. The order is important because ACL processing stops when the first match occurs.

ACLs whose numbers are in the range 100 to 109 will have higher priority than any ACLs created by subscribers using the My Firewall page. (The range of ACL numbers reserved for use by the My Firewall page is 110 to 196.)

ACLs whose numbers are in the range 100 to 109 cannot be modified by the subscriber (because the My Firewall page will not modify ACLs whose numbers are in that range), although the subscriber can delete those ACLs along with all others with the Disable Firewall button.

- *permission* is one of the following values: permit or deny
- *protocol* is the configured protocol for the application, as defined in the Firewall MBean. Examples are tcp, udp, ip, and so on.
- *source* and *destination* are in the form:

```
{any | IPaddress mask} [portOperator portNumber]
```

where *portOperator* values are: lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). The range operator requires two port numbers. All other operators require one port number.

Example

The following examples, using ACL number 100, were set by an administrator in CDAT.

```
Cisco_AV:ip:inacl#100=permit tcp any 10.0.0.0 0.0.0.0 eq 80
```

```
Cisco_AV:ip:outacl#100=permit tcp any any established
```



Note

There is an implicit deny at the end of an ACL list. When an ACL list exists, only explicitly permitted traffic is permitted.

References for More Information about Access Control Lists

The SESM firewall feature creates extended ACLs. For more information about ACL formats and processing, refer to the Cisco IOS documentation on extended ACLs. The following references point to documentation for Cisco IOS Release 12.2:

- Configuration Guide—In the *Configuring IP Services* guide, see the “Filtering IP Packets Using Access Lists” section. The online link is:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#xtocid14

- Command reference—In the *Cisco IOS IP Command Reference, Volume 1 of 3, Addressing and Services*, see the “IP Services Commands” section. The online link is:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fipras_r/1rfip1.htm

Multikey Authentication

To implement multikey authentication:

1. Add the authentication fields to the portal logon page.

This step requires portal customization. SESM is installed with an example 3-field authentication page that you can implement. The example authentication fields are: username, password and telephone number. (Telephone number is the RADIUS attribute CALLING_STATION_ID).

To change the NWSP logon page to prompt for these three keys and process them:

- a. Edit `nwsp/webapp/WEB-INF/web.xml`.
- b. Change the following line:
`<servlet-class>com.cisco.sesm.webapp.control.AccountLogonControl</servlet-class>`
to: `<servlet-class>com.cisco.sesm.webapp.control.AccountLogon3KeyControl</servlet-class>`
- c. Change the following line:
`<param-value>/pages/accountLogon.jsp</param-value>`
to: `<param-value>/pages/accountLogon3Key.jsp</param-value>`

2. In LDAP mode, configure RDP to authenticate on the same fields that are specified on the logon page.

You can configure RDP to use any number of fields for authentication. Any standard RADIUS attribute field is a valid key.

- a. Edit the `DESSAuthenticationHandler` Mbean from the RDP management console, or manually edit `rdp.xml`.
 - b. Add items to the `AuthAttribute` attribute. To configure with the installed example in NWSP that uses three keys, make sure the following items are listed in `AuthAttribute`, in this order: `USER_PASSWORD`, `CALLING_STATION_ID`. (The `USER_NAME` attribute is always used for authentication and should not appear in the `AuthAttribute` array.)
3. In RADIUS mode, logic to authenticate with multiple keys must exist in the RADIUS server you are using. Verify that this logic exists with your RADIUS server vendor.
 4. Make sure that the subscriber profiles includes the values against which to authenticate. In LDAP mode, administrators can enter the APN and NAS identifier attributes as group values. See the *Cisco Distributed Administration Tool Guide* for more information.

Quality of Service

Quality of Service (QoS) features control IP traffic transmission rates. The QoS features in SESM deployments are implemented using SSG hierarchical policing features. See the SSG documentation for information about enabling and configuring hierarchical policing. See the “[Related Documentation](#)” section on page -xv for an URL to the online location of SSG documents.

SSG supports per-subscriber and per-service hierarchical policing. The parameters that implement these policies are specified in subscriber and service profiles:

- To implement per-subscriber policies—Use the Q attribute in the subscriber profiles.
- To implement per-service policies—Use the Q attribute in a service profile.

See the [“Configuring Service Profiles” section on page C-6](#) and the [“Configuring Subscriber Profiles” section on page C-11](#) for a summary of RADIUS profile formats. See the *Cisco Distributed Administration Tool Guide* for information about creating profiles in an LDAP directory.



Deploying a Captive Portal Solution

This chapter describes how to configure the SESM sample captive portal solution. The chapter contains the following topics:

- [SSG and SESM Release Requirements, page 11-1](#)
- [Solution Description, page 11-2](#)
- [Installing and Running the Sample Solution, page 11-6](#)
- [MBeans in the Captive Portal Solution, page 11-9](#)
- [Configuring the SSG TCP Redirect Features, page 11-18](#)
- [Troubleshooting Captive Portal Configurations, page 11-23](#)

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 guide assumes that you are using SESM applications.

Solution Description

This section describes the SESM captive portal solution. It contains the following topics:

- [Solution Diagram, page 11-2](#)
- [SESM Captive Portal Application, page 11-3](#)
- [Content Applications, page 11-4](#)
- [Alternative Configuration Options for a Captive Portal Solution, page 11-5](#)

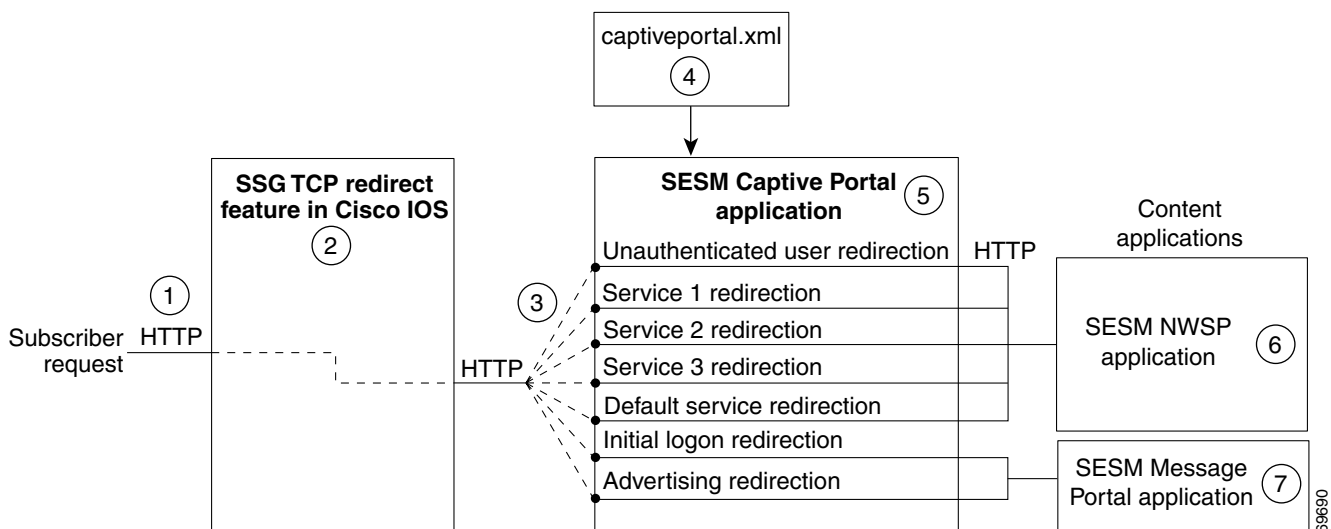
Solution Diagram

Figure 11-1 illustrates how the components in the SESM captive portal solution work together to provide appropriate content to the subscriber.


Note

Figure 11-1 shows the sample solution configured using all of the default values provided by the SESM installation program. There are many possible variations to this default deployment.

Figure 11-1 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"> • 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). • Each type of redirection must use a different port value. The port number identifies the type of redirection to the SESM Captive Portal application.

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.

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.

[Table 11-1](#) 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.

Table 11-1 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	The service name that was requested in the original request. The NWSP application uses this value to log on to the service.
Service redirection	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.
	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.
Initial logon and advertising redirections	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. Duration attributes exist on both the SSG side and the SESM side. See the "Message Duration Parameters—Summary" section on page 11-17 .
	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 11-1 on page 11-3](#) for a description of the parameters that the Captive Portal application forwards to the NWSP application.

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 11-1](#) for a description of the parameters that the Captive Portal application forwards to the Message Portal application.

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 Some 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 the redirection type on the SSG.

Eliminating Some J2EE Listeners

The web server container in which the captive portal application runs is configured with a separate listener for each TCP redirect port you configured. That is, separate listeners exist 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 requires that you enter 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 and Running the Sample Solution

This section describes how to install and configure the sample captive portal solution in the quickest possible configuration. To alter the default configuration after installation, see the “[MBeans in the Captive Portal Solution](#)” section on page 11-9.

This section includes the following topics:

- [Installing the Sample Solution](#), page 11-6
- [Installation Results](#), page 11-6
- [Additional Configuration Steps](#), page 11-7
- [Starting the Sample Captive Portal Solution](#), page 11-9

Installing 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 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 11-7 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
  webapp
  docs
```

```
messageportal
  config
    messageportal.xml
  webapp
  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 11-7](#)
- [Loading Sample Profiles for Captive Portal Demonstration, page 11-8](#)
- (Optional) [Configuring Unique Service Logon Pages for Service Redirections, page 11-8](#)

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 11-1. If not, upgrade the Cisco IOS release before proceeding.
- Step 2** Make sure that basic SSG functionality is enabled and configured, as described in the “[Basic SSG Configuration](#)” section on page F-1.
- 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 displays default inputs for captive portal group names and port numbers. These defaults correspond to values used in the TCP redirect commands in the ssgconfig.txt file. If you change these captive portal group names or port numbers, you must make corresponding changes to the port numbers in the ssgconfig.txt file.

- Step 4** Edit `ssgconfig.txt` as follows:
- You *must* edit the placeholder IP addresses. Change them to the actual network IP addresses you entered during captive portal installation.
 - If you changed the displayed defaults for captive portal group names or the incoming port numbers, then you must edit those values in `ssgconfig.txt` to match the values you entered during captive portal installation.
- Step 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 11-24.
- 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 Captive Portal 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 9, “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).

MBeans in the Captive Portal Solution

This section describes the MBeans in the captive portal solution. The topics are:

- [MBeans in the Captive Portal Application, page 11-10](#)
- [Message Portal Application MBeans, page 11-13](#)
- [Captive Portal Attributes in the NWSP WebAppMBean, page 11-16](#)

MBeans in the Captive Portal Application

The captive portal application uses the following MBeans:

- [Logger MBean, page 11-10](#)
- [ManagementConsole MBean, page 11-10](#)
- [captiveportal MBean, page 11-11](#)

To change attributes in these MBeans, you can use either of the following methods:

- Edit the captive portal MBean configuration file:

```
captiveportal
  config
    captiveportal.xml
```

- Make changes using the Agent View running on the Captive Portal management port. The installation process uses the following default port numbers for captive portal:
 - Captive portal port—8090
 - Captive portal management port—8190

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs captive portal application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the “[Logger MBean](#)” section on page 5-2 for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the management console port for CDAT, including valid user names and passwords for accessing the console. See the “[Configuring the ManagementConsole MBean](#)” section on page 3-5 for more information.

captiveportal MBean

Table 11-2 explains attributes in the captiveportal MBean.

Table 11-2 *captiveportal MBean*

Attribute Name	Explanation
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"> • true—The captive portal application performs an HTTP redirect to an appropriate content application. • 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.
host	<p>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.</p>

In the installed configuration files, the following attributes are assigned 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.

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"> • <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"> – serviceportal.host (usually the NWSP IP address) – messageportal.host (usually the Message Portal IP address) • <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"> – serviceportal.port – messageportal.port • <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"> – For user redirections: /home, which is the NWSP logon page. – For initial logon redirections: /initial, which is the Message Portal greetings page. – For advertising redirections: /advertising, which is the Message Portal advertising page. <p>The default values for the system properties and the URIs were set during installation in the URL Out fields.</p>
---	---

Table 11-2 captiveportal MBean (continued)

Attribute Name	Explanation
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"> • userRedirect.port • initialCaptive.port • advertisingCaptive.port <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>Note The SSG TCP redirect commands also accept a duration attribute. See the “Message Duration Parameters—Summary” section on page 11-17 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"> 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. If you change a port value, also change the SSG configuration to send the service redirection to the same port value. 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. <p>Note 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> <ol style="list-style-type: none"> 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.

Table 11-2 captiveportal MBean (continued)

Attribute Name	Explanation
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"> • userRedirectURLParam • serviceRedirectURLParam • serviceRedirectServiceParam • serviceRedirectSubscriberParam • messageRedirectURLParam • messageRedirectSubscriberParam • messageRedirectDurationParam 	<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>

Message Portal Application MBeans

The Message Portal application uses the following MBeans:

- [Logger MBean, page 11-14](#)
- [ManagementConsole MBean, page 11-14](#)
- [SESMMBean, page 11-14](#)
- [SESMDemoMode MBean, page 11-14](#)
- [DESSMode MBean, page 11-14](#)
- [messageportal MBean, page 11-15](#)

To change attributes in these MBeans, you can use either of the following methods:

- Edit the Message Portal MBean configuration file:

```
messageportal
  config
    messageportal.xml
```

- Make changes using the Agent View running on the messageportal management port. The installation process uses the following default port numbers for message portal:
 - Message portal port—8085
 - Message portal management port—8185

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs Message Portal application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the “[Logger MBean](#)” section on page 5-2, for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the management console port for the Message Portal application, including valid user names and passwords for accessing the console. See the “[Configuring the ManagementConsole MBean](#)” section on page 3-5 for more information.

SESMMBean

The SESMMBean is required in all SESM portal applications. It sets the SESM mode for the application. The “[SESM MBean](#)” section on page 5-4 describes this MBean.

For the Message Portal application, the mode attribute must be one of the following:

- LDAP, if the mode for the Captive Portal application is LDAP.
- 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.)

SESMDemoMode MBean

The SESMDemoMode MBean is required in all SESM portal applications that are running in Demo mode. See the “[SESMDemoMode MBean](#)” section on page 5-6 for more information about this MBean.

If you run the message portal application in Demo mode, it obtains subscriber profiles from the file identified in this MBean. You can add interests (hobbies) to subscriber profiles in the demo data file using the \$AA subattribute, as described in [Table C-6 on page C-11](#), “[Attributes in Subscriber Profiles](#)”.

DESSMode MBean

The DESSMode MBean is required in all SESM portal applications that are running in LDAP mode. See the “[DESSMode MBean](#)” section on page 5-6 for more information about this MBean.

messageportal MBean

Table 11-3 explains the configuration attributes in the messageportal MBean.

Table 11-3 *messageportal MBean*

Attribute Name	Explanation
defaultPage	<p>For advertisement redirections, specifies the default page to redirect to if:</p> <ul style="list-style-type: none"> • The subscriber profile does not contain any interests • The ignoreProfile attribute is set to true • The interestPages attribute indicates that the default page should be used for a specific interest.
defaultURL	<p>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).</p>
defaultDuration	<p>Optional. This value is used if the Captive Portal application does not forward a CPDURATION parameter.</p> <p>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.</p> <p>Note The SSG TCP redirect commands also accept a duration attribute. See the “Message Duration Parameters—Summary” section on page 11-17 for more information.</p>
ignoreProfile	<p>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:</p> <ul style="list-style-type: none"> • true—Ignore the interest field. Redirect to the page specified in the defaultPage attribute. • false—Redirect to a page based on the first interest in the subscriber profile. <p>Note In RADIUS mode, this attribute must be set to true. The interest attribute is not available with RADIUS profiles.</p>
redirectOn	<p>For initial logon and advertisement redirections, indicates action to take after the captivation duration elapses:</p> <ul style="list-style-type: none"> • 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. • false—Do not issue another redirection. The message or advertisement page remains displayed until the subscriber enters another URL.

Table 11-3 *messageportal MBean (continued)*

Attribute Name	Explanation
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>

Captive Portal Attributes in the NWSP WebAppMBean

The NWSP portal is the content application for unauthenticated user redirection and service redirections. The NWSP application contains the WebApp MBean. [Table 11-4](#) explains configuration attributes in the WebAppMBean that are directly related to the captive portal solution.

Table 11-4 *Captive Portal Attributes in the WebAppMBean*

Attribute Name	Explanation
prepaidRedirectionURL	<p>For service redirections when the SSG prepaid feature is enabled, tells NWSP which page to redirect to if the prepaid limit for the requested service is reached. No redirection occurs if this attribute is null or empty.</p> <p>The default value that exists after installation is the NWSP recharge page.</p>
serviceNotGivenURI	<p>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.</p> <p>The default value that exists after installation is the NWSP status page.</p>

Table 11-4 Captive Portal Attributes in the WebAppMBean (continued)

Attribute Name	Explanation
defaultURI	<p>For service redirections, tells NWSP which page to redirect to if:</p> <ul style="list-style-type: none"> • The service specified in the HTTP request from the Captive Portal application is not available. • The service exists, the subscriber is not subscribed to it, and the subscriber does not have permission to visit the subscription page. • Any other unexpected conditions <p>The default value that exists after installation is the NWSP home page.</p>
serviceSubscriptionURI	<p>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.</p> <p>The default value that exists after installation is:</p> <ul style="list-style-type: none"> • In LDAP mode, the NWSP subscriptionManage page. • In RADIUS mode, the NWSP displays the page specified in the defaultURI attribute.
noSubscribePermissionURI	<p>For service redirections, tells NWSP which page to redirect to if the subscriber is not subscribed to the requested service and:</p> <ul style="list-style-type: none"> • The application is running in RADIUS mode, or • The application is running in LDAP mode, and the subscriber does not have the permission to self-subscribe to services. <p>The default value that exists after installation is the NWSP home page.</p>
serviceStartURI	<p>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.</p> <p>The default value that exists after installation is the NWSP serviceStart page.</p>
serviceLogonURI	<p>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.</p> <p>The default value that exists after installation is the NWSP serviceLogon page.</p>

Message Duration Parameters—Summary

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 are too early and do not take place.

Durations on the SSG Side

On the SSG side, the message duration controls the length of time 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 11-19](#)
- [Defining Captive Portal Groups and Port Lists, page 11-19](#)
- [Configuring Unauthenticated User Redirection, page 11-20](#)
- [Configuring Unauthorized Service Redirection, page 11-20](#)
- [Configuring Initial Logon Redirection, page 11-22](#)
- [Configuring Advertising Redirection, page 11-22](#)

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

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. (is that true?). 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—Summary”](#) section on page 11-17 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 captive 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 `initialCaptive`. 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 `initialCaptive` group is associated with initial logon redirections. The message captivation lasts for 10 seconds, unless the subscriber profile overrides that value. 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 initialCaptive
    server 10.0.1.4 8091
  redirect port-list ports to initialCaptive
  redirect captive initial default group initialCaptive 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—Summary”](#) section on page 11-17 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 captive 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 `advertisingCaptive`. 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 `advertisingCaptive` group is associated with advertising redirections. The captivation lasts for 5 seconds 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 advertisingCaptive
    server 10.0.1.4 8092
  redirect port-list ports to advertisingCaptive
  redirect captive advertising default group advertisingCaptive 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 11-23
- [Redirections Continuously Occur](#), page 11-24
- [User Name Not Passed in Unauthenticated User Redirections](#), page 11-25

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 11-24
- [Two Redirection Types Assigned to the Same Port in `captiveportal.xml`](#), page 11-24
- [Redirection Type Not Configured on the SSG](#), page 11-24

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 11-24](#)
- [Using HTTP1.1 with a Non-SESM Captive Portal Application, page 11-25](#)

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 occurs 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 11-19](#).
- 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.



Deploying SESM/SSG Solutions

This section describes the attributes that control communication between components in SESM deployments. 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 12-1](#)
- [Communication Attributes for RADIUS Mode, page 12-3](#)
- [Communication Attributes for LDAP Mode, page 12-6](#)
- [Communication Attributes for LDAP Mode with RDP in Proxy Mode, page 12-9](#)

Communication Attributes for Interaction Between SESM and SSG

The section applies to all SESM deployments, regardless of the SESM mode.

[Figure 12-1](#) shows the attributes whose values must match for successful communication between an SESM web application and SSG. [Table 12-1](#) describes how to set these attributes on both sides of the communication.

Figure 12-1 Attributes for SESM to SSG Communication in All Modes

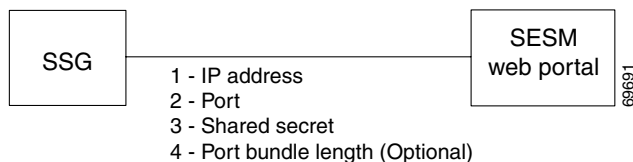


Table 12-1 Setting Attributes for SESM to SSG Communication in All Modes

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 show run to view the settings.
	<ol style="list-style-type: none"> IP Address—Use the following command to specify the network that the SESM web application is running on: <code>ssg default-network networkIPAddress mask</code>
	<ol style="list-style-type: none"> 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: <code>ssg radius-helper auth-port port</code>
	<ol style="list-style-type: none"> Shared Secret—Use the following command to specify the shared secret used in RADIUS protocol communication between the SSG and the SESM web application: <code>ssg radius-helper key secret</code>
	<ol style="list-style-type: none"> (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: <code>ssg port-map length bits</code> Note Additional commands are required on SSG to enable and configure the host key feature. For more information, see the “Configuring the Port-Bundle Host Key Feature on SSG” section on page F-2.
On the SESM web application side	<ol style="list-style-type: none"> 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):
	<ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> PORT global attribute PORT subnet attribute—Overrides the global setting if all of the SSGs are not configured the same.
	<ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> SECRET global attribute SECRET subnet attribute—Overrides the global setting if all of the SSGs are not set the same.
	<ol style="list-style-type: none"> Host Key Port Bundle Length—Use the following attributes to set the port-bundle length to match the settings on the SSG hosts. <ul style="list-style-type: none"> BUNDLE_LENGTH global attribute BUNDLE_LENGTH subnet attribute—Overrides the global setting if all of the SSGs are not configured the same.

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 We strongly recommend 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 12-2 shows the attributes whose configured values must match. Table 12-2 describes how to set these attributes on each side of the communication.

Figure 12-2 Communication Attributes in a RADIUS Mode Deployment

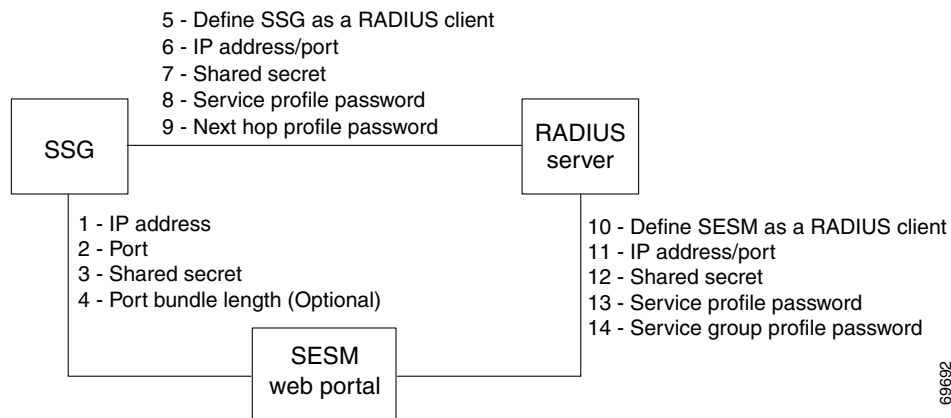


Table 12-2 Setting Communication Attributes in a RADIUS Mode Deployment

Configuring Communication Between an SESM Application and SSG		
On the SESM and SSG Sides	1 to 4	See Table 12-1 , “Setting Attributes for SESM to SSG Communication in All Modes”
Configuring Communication Between a RADIUS Server and SSG		
On the RADIUS Side	Set these values using the RADIUS product’s native configuration procedures:	
	5.	Define SSG as a RADIUS Client—Define SSG as a NAS client.
	6.	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.
	7.	Shared secret—The shared secret value is specified when you define the SSG as a NAS client.
	8.	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.
	9.	(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:	
	5.	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>Note If the SSG is not supporting PPP connections, you do not need to use the aaa authentication ppp command.</p>
	6.	IP address/port—Use the following command: <pre>radius-server host RadiusHostIpAddr auth-port port</pre>
	7.	Shared secret—Use the following command: <pre>radius-server key RadiusSharedSecret</pre>
	8.	Service Password—Use the following command: <pre>ssg service-password servicePassword</pre>
	9.	(Optional) Next Hop Password—Use the following command: <pre>ssg next-hop download nextHopTableName password</pre>

Table 12-2 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:
10.	Define a RADIUS client—Define SESM as a NAS client.
11.	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.
12.	Shared secret—You set the shared secret value when you define the SESM application as a NAS client. Note 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.
13.	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.
14.	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):
10.	Define a RADIUS client—The attribute name is mode. To deploy SESM in RADIUS mode, the value for mode must be RADIUS. Note You can override the value for mode on the command line when you start the SESM application. For more information, see the “Starting the SESM Portals” section on page 9-1 .
	Set the following values in the AAA MBean in the SESM application configuration file (nwsp.xml, for example):
11.	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"> • primaryIP • primaryPort • (Optional) secondaryIP • (Optional) secondaryPort
12.	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.
13.	Service Password—The attribute name is servicePassword. Use this attribute to provide SESM with the generic password used in the service profiles.
14.	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:

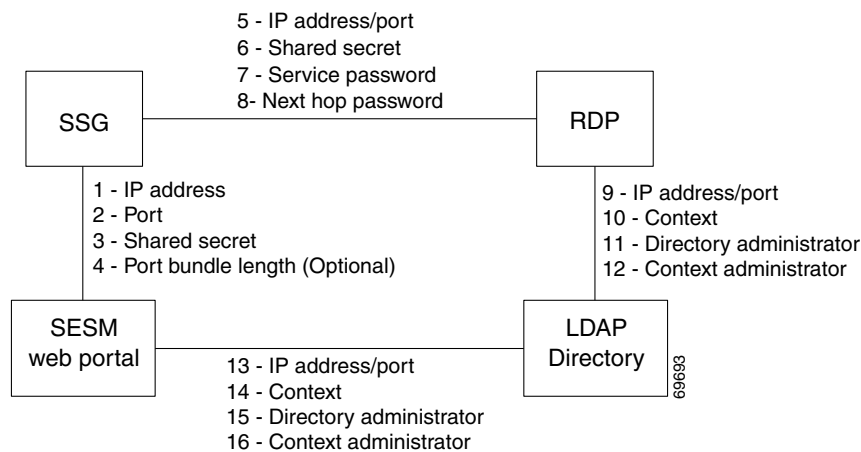
- RADIUS IP address and port—The RADIUS clients must know the IP address of the RADIUS server machine and the port that RADIUS uses for authentication and authorization requests. The port is set when the RADIUS server is configured. It is usually port 1812, which is the industry’s default authentication 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 12-3 shows the attributes whose configured values must match on each side of the communication to successfully deploy SESM in LDAP mode. Table 12-3 describes how to set these attributes on each side of the communication.

Figure 12-3 Communication Attributes in an LDAP Mode Deployment



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 12-3 Setting Communication Attributes in an LDAP Mode Deployment

Configuring Communication Between an SESM Web Application and SSG		
On the SESM and SSG Sides	1 to 4	See Table 12-1, “Setting Attributes for SESM to SSG Communication in All Modes”
Configuring Communication Between RDP and SSG		
On the RDP side	Set the following values in the RDP MBean on the RDP host machine.	
	5.	IP address/port—The attribute names are: <ul style="list-style-type: none"> localIPAddress—The IP Address or host name of the RDP host machine. (You cannot enter the value localhost or 127.0.0.1.) 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.
	6.	Shared secret—The attribute name is secret. This is the RADIUS protocol shared secret value used for communication between SSG and RDP.
	7.	Service password—The attribute name is servicePassword. Replace <code>servicecisco</code> with the service password set on the SSG side.
	8.	(Optional) Next hop password—The attribute name is nextHopPassword. 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.
On the SSG side	Set the following values using Cisco IOS commands on the SSG:	
	5.	IP address/port—Use the following command: <code>radius-server host RDPHostIpAddr auth-port port</code>
	6.	Shared secret—Use the following command: <code>radius-server key RDPSharedSecret</code>
	7.	Service password—Use the following command to set the key that SSG uses in service requests: <code>ssg service-password servicePassword</code>
	8.	(Optional) Next hop password—Use the following command to set the key that SSG uses in next hop table requests: <code>ssg next-hop download nextHopTableName password</code>

Table 12-3 Setting Communication Attributes in an LDAP Mode Deployment (continued)

Configuring Communication Between RDP and an LDAP Directory	
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/dessauth.xml</code>).</p> <p>9. 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. An example 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>10. Context—The attribute name is <code>context</code>. Provide the organizational unit and organization in the LDAP directory that holds the SESM data. An example 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>11. Directory administrator—The attribute names are:</p> <ul style="list-style-type: none"> principal—This must be an administrator ID that exists in the LDAP directory with permissions to extend the LDAP directory schema. An example entry is: <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"> credentials—Provide the password that goes with the principal. <p>You provide the initial values for these attributes during installation. The installation program prompts you for directory server admin information.</p> <p>12. 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>9 to 12 Use native administration tools for the LDAP directory product to configure the directory for SESM deployment. See the Appendix B, “Configuring an LDAP Directory for SESM Deployments,” for guidelines and requirements.</p>

Table 12-3 Setting Communication Attributes in an LDAP Mode Deployment (continued)

Configuring Communication Between an SESM Application and an LDAP Directory		
SPE configuration on the SESM application side	13 to 16	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 dess-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	13 to 16	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 12-4](#) shows the attributes whose configured values must match on each side of the communication between RDP in proxy mode and the RADIUS Server. [Table 12-4](#) 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 12-4 Communication Attributes in an LDAP Mode Deployment with RDP in Proxy Mode

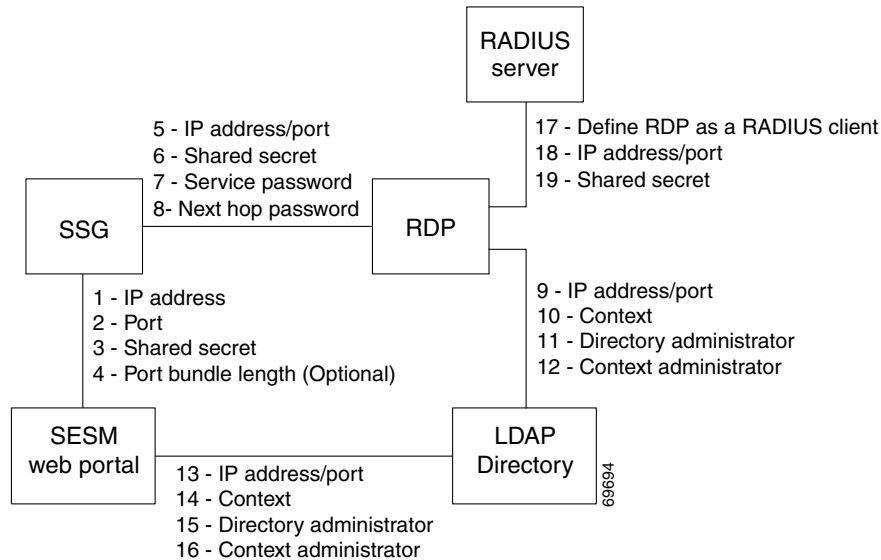


Table 12-4 Setting Communication Attributes in an LDAP Mode Deployment with RDP Proxy

Configuring Communication Between Components in LDAP Mode

See Table 12-3.	1 to 16	See Table 12-3, “Setting Communication Attributes in an LDAP Mode Deployment”
-----------------	----------------	---

Configuring Communication Between RDP and a RADIUS Server

On the RADIUS side	Set these values using the RADIUS product’s native configuration procedures:	
	17.	Set up a RADIUS Client—Define RDP as a NAS client.
	18.	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.
	19.	Shared secret—You set the shared secret value when you define the RDP application as a NAS client. Note If you are configuring primary and secondary RADIUS servers, the shared secret value must be the same on both RADIUS servers.



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 13-1](#)
- [Troubleshooting Aids, page 13-4](#)
- [Troubleshooting Tips, page 13-5](#)

Diagnosing Problems

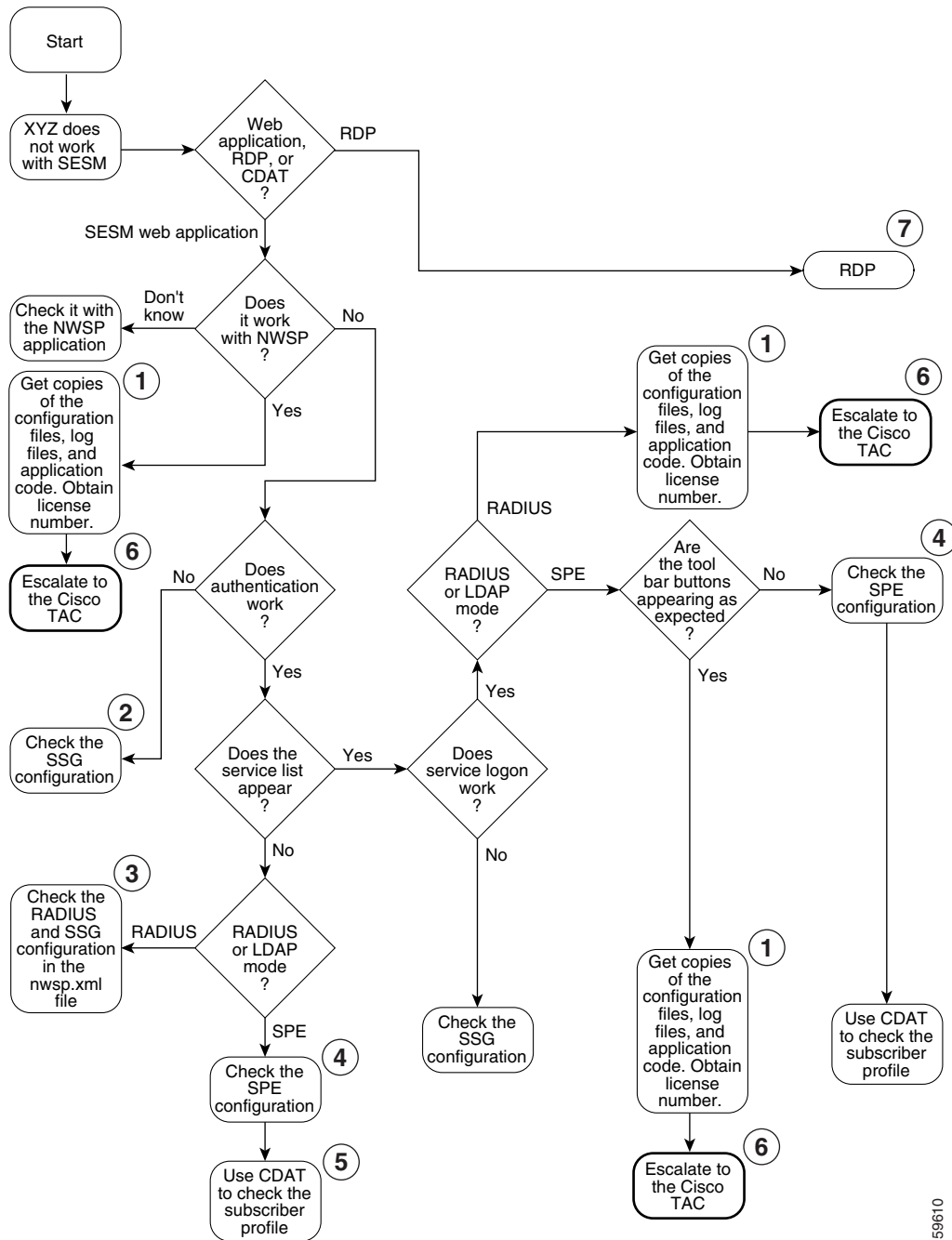
This section contains procedural charts that show you how to research a problem and identify the general area of the problem before escalating it to the Cisco Technical Assistance Center. The section includes the following procedures:

- [Procedures for Troubleshooting SESM Portals, page 13-1](#)
- [Procedures for Troubleshooting RDP, page 13-3](#)

Procedures for Troubleshooting SESM Portals

[Figure 13-1](#) shows a procedure for analyzing problems in SESM portal applications. The numbered callouts are keyed to the table that follows the figure.

Figure 13-1 Procedures for Troubleshooting SESM Portal Applications



59610

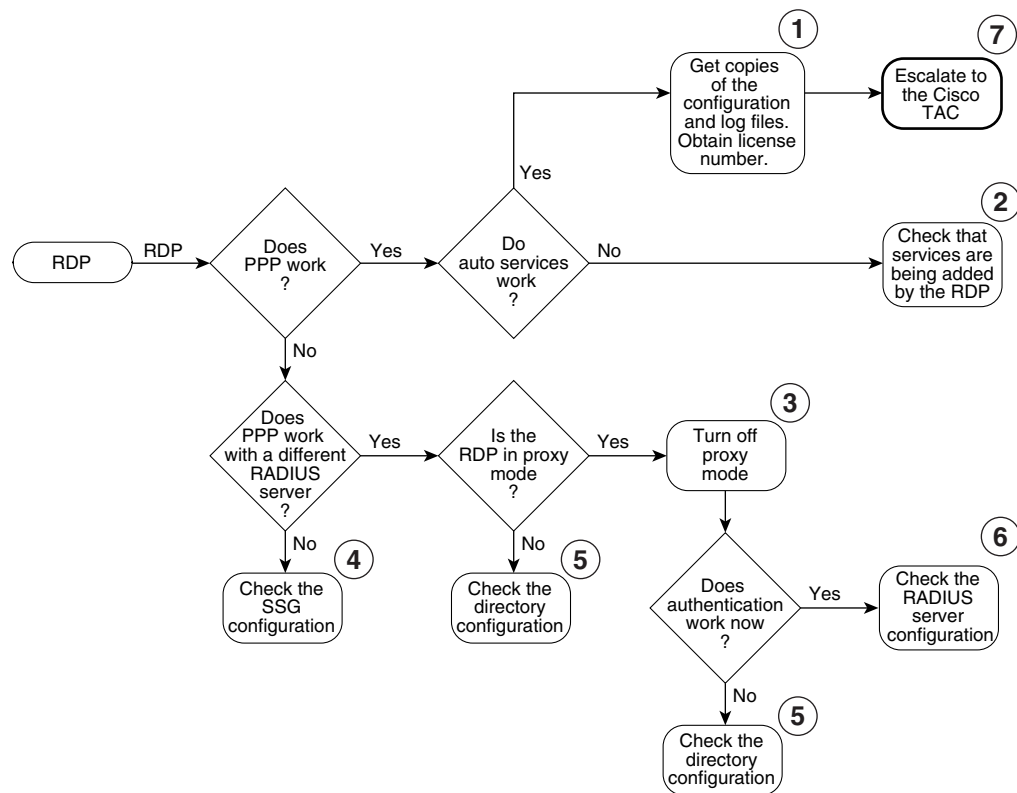
- | | |
|---|---|
| 1 | See MBean Configuration File Names , page 3-14 , Log File Descriptions , page 13-4 , and Obtaining License and Version Information , page 13-5. |
| 2 | See Basic SSG Configuration , page F-1. |
| 3 | See SSG MBean , page 5-7 and AAA MBean , page 5-10. |
| 4 | See SPE Attributes , page 8-1. |

5	Make sure the subscriber is subscribed to services and has the proper privileges to access those services. See the CDAT documentation: http://www.cisco.com/univercd/cc/td/doc/solution/sesm
6	See Obtaining Technical Assistance , page xvi.
7	See Procedures for Troubleshooting RDP , page 13-3.

Procedures for Troubleshooting RDP

Figure 13-2 shows a procedure for analyzing problems in RDP. The numbered callouts are keyed to the table that follows the figure.

Figure 13-2 Procedures for Troubleshooting RDP



59611

1	See MBean Configuration File Names , page 3-14, Log File Descriptions , page 13-4, and Obtaining License and Version Information , page 13-5.
2	See Adding Service Information to Replies , page 7-2.
3	See Changing the RADIUS Data Proxy Mode , page 7-2.
4	See Configuring the SSG for SESM Deployments , page F-1.
5	See Configuring Security Policy Engine for SESM , page 8-1.
6	See the client and server socket components in the RDP MBean , page 7-4 and RADIUS Data Proxy MBeans , page 7-3.
7	See Obtaining Technical Assistance , 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:

- [Log File Descriptions, page 13-4](#)
- [Log File Configuration, page 13-4](#)
- [Java Command Line Options, page 13-5](#)
- [Obtaining License and Version Information, page 13-5](#)

Log File Descriptions

The SESM log files can help troubleshoot SESM applications and deployments. By changing the configuration of the logging and debugging mechanisms, you can change the amount of detail reported and specify message filtering. Two of the log files have debugging mechanisms in addition to the logging features.

- **Jetty HTTP Request log**—Contains incoming HTTP requests. You can use this log file to analyze volume and traffic patterns for the web server.
- **Jetty log**—Contains logging and debugging messages from Jetty. 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.
- **Application log**—Contains logging and debugging messages from the SESM application. The logging tool logs SESM web application activity. The debugging mechanism produces messages useful to developers in debugging applications.

You can configure all three of these logs for each SESM portal application and for CDAT. RDP uses only the application log.

Log File Configuration

[Table 13-1](#) shows the MBeans that configure the log files. The MBeans control the level of verbosity in the logs, message filtering, debugging, file location, and file management.

Table 13-1 *Configuring the Log Files*

Log Type	MBean Name and Reference to More Information	Filename Attribute	Default Log Filename
Request log	Server MBean, page 4-5	RequestLog	<i>date.request.log</i>
Jetty log	Log MBean, page 4-3 Debug MBean, page 4-4	filename	<i>date.jetty.log</i>
Application log	Logger MBean, page 5-2	logFile	<i>date.application.log</i>

To change the location of a log file, change the value of the filename attributes listed in [Table 13-1](#). All of the log filename attributes use the `application.home` property, which ensures that all logs for an application are located in the same directory. The value for the `application.home` property is set by the start script at run time. See [Table 9-1 on page 9-5](#), “[Java System Properties in Startup Scripts](#)” for more information about the `application.home` property.

The installed default configuration places all log files for an application into the `logs` subdirectory under the application home directory. For example:

```
SESMinstallDir
  nwsp
    logs
```

If the `logs` directory does not exist, it is created at application runtime.

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
```

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 13-6
- [Installation Troubleshooting](#), page 13-7
- [Configuration File Location Troubleshooting](#), page 13-8
- [SESM Configuration Troubleshooting](#), page 13-8
- [RADIUS Configuration Troubleshooting](#), page 13-9
- [SSG Configuration Troubleshooting](#), page 13-10

JRE and JDK Troubleshooting

If the SESM installation program does not find an appropriate JRE, it installs the bundled JRE. See the section [“Installing the Bundled JRE” section on page 1-3](#).

This section contains the following topics:

- [Java Warning and Error Messages at Application Startup, page 13-7](#)
- [Searching for an Existing JDK or JRE, page 13-6](#)
- [Using a Pre-installed JRE or JDK, page 13-7](#)
- [Recompiling a Customized JSP, page 13-7](#)

Searching for an Existing JDK or JRE

The SESM installation program does the following when searching for a valid JDK or JRE:

1. It searches for a JDK Version 1.3.1 that is already installed.
2. Failing that, it searches for a JRE Version 1.3.1 or later that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.3.1_03.

In some cases, even though a JRE is installed, the installation program may not find it or finds a different JRE.

On Windows NT, the installation program looks in the NT Registry for the location of a JDK or JRE. It searches for the following:

\Java\1.3.1	\JavaSoft\JRE\1.3.1
\Java\1.3	\JavaSoft\JRE\1.3
\Program Files\JavaSoft\JRE\1.3.1	\Java\JRE\1.3.1
\Program Files\JavaSoft\JRE\1.3	\Java\JRE\1.3

On Solaris and Linux, the installation program looks in the following well-known locations before installing the bundled JRE:

/usr/jdk1.3.1	/usr/java1.3.1	/usr/j2sdk1.3.1	/usr/jre1.3.1
/usr/jdk1_3_1	/usr/java1_3_1	/usr/j2sdk1_3_1	/usr/jre1_3_1
/usr/jdk1.3	/usr/java1.3	/usr/j2sdk1.3	/usr/jre1.3
/usr/jdk1_3	/usr/java1_3	/usr/j2sdk1_3	/usr/jre1_3
/usr/jdk	/usr/java	/usr/j2sdk	/usr/jre
/opt/jdk1.3.1	/opt/java1.3.1	/opt/j2sdk1.3.1	/opt/jre1.3.1
/opt/jdk1_3_1	/opt/java1_3_1	/opt/j2sdk1_3_1	/opt/jre1_3_1
/opt/jdk1.3	/opt/java1.3	/opt/j2sdk1.3	/opt/jre1.3
/opt/jdk1_3	/opt/java1_3	/opt/j2sdk1_3	/opt/jre1_3
/opt/jdk	/opt/java	/opt/j2sdk	/opt/jre

Using a Pre-installed JRE or JDK

On any of the installation platforms, 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

The installed `web.xml` file points to precompiled versions of the JSPs. It does *not* reference the JSPs in `/nwsp/webapp`. Thus, changing the JSPs in `webapp` has no effect if you use the installed `web.xml` file.

If you do not see changes that you make to a JSP, do either of the following:

- Recompile the page when you run the application—See the *Subscriber Edge Services Manager Web Developer Guide* for procedures.
- Precompile the page before running the application—Run the precompile script in `tools/bin`.

Java Warning and Error Messages at Application Startup

SESM application startup 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.

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 application 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 F, “Configuring the SSG for SESM Deployments.”](#)

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 C, "Configuring RADIUS for SESM Deployments."](#)

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 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 13-9](#) 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 C-1](#) 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.

Considerations for Subscribers Using PDA Devices

This section describes how some characteristics of PDA devices might impact subscriber experiences when accessing the SESM portal.

- PDAs use basic IE browsers, which might lose the port number of the request during redirections. This characteristic might not be noticeable with simple configurations, but it is a problem with the SSG TCP redirection feature. It is therefore important to run the server on the default ports (80 for insecure connections, 443 for secure connections).
- The `webapp/decorators/httpSniff.jsp` is useful for fine-tuning the recognition of the subscriber device type. This JSP modifies the default behavior of the SESM `HttpSniffBean` decorator, which influences the shape decoration. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information about decorators.
- If a PDA device does not have an IP address, it cannot use DNS to resolve a requested URL. The result is a “Page Not Found” error.

PDAs can take between 20 to 60 seconds to get an IP address after the subscriber logs out and reinserts the PC card. If the subscriber reinserts the card immediately and tries to browse, the “Page Not Found” error is returned. However, if the subscriber waits for an IP address before browsing, the browser should be redirected appropriately.

The simplest way to verify that a PDA has an IP address is to use the WLAN card statistics utility. For example, the Cisco 350 card shows the number of unicast packets received and transmitted. Subscribers should make sure that the count is higher than 0 for received packets before attempting to login.

- PDA browsers cache easily. If a subscriber selects a web site that is cached, the cached page might display even though the subscriber is not authenticated. PDA browsers do not have controls for avoiding this behavior.



SESM Security

This appendix describes the security mechanisms used in a Subscriber Edge Services Manager (SESM) deployment. This chapter includes the following topics:

- [Java Platform Security References, page A-1](#)
- [Using HTTPS in SESM Portals, page A-1](#)
- [Configuring SESM Portals to Run on SSL Ports Only, page A-3](#)

Java Platform Security References

SESM applications inherit the security features of the Java language platform and of the J2EE framework. The following URLs describe security topics related to the Java and J2EE technology:

- For Java security software and documentation:
<http://java.sun.com/security/index.html>
- For information related to JDK 1.3:
<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/>

Using HTTPS in SESM Portals

This section contains the following topics concerning HTTPS:

- [HTTPS References, page A-2](#)
- [Keytool and Keystore, page A-2](#)

HTTPS References

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

Keytool and Keystore

The SSL part of HTTPS requires a certificate to generate the encryption key. For the Jetty web server bundled with 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/1.3/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:

<http://jetty.mortbay.com/jetty/doc/SslListener.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 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 SESM Portals to Run on SSL Ports Only

The sample applications installed with SESM provide an option on the logon page that allows the subscriber to choose between starting a secure (HTTPS) session or a standard (HTTP) session. The default configuration files start both types of listeners: one HTTP listener and one HTTPS listener to support either choice from the logon page.

To remove this option from the logon page and run the portal in secure mode only, follow these procedures:

- Step 1** To remove the secure or standard session option from the NWSP logon page, comment out the HTML in `accountLogonBody.jsp`.

```
<%-- Make this page either secure or insecure --%>
<% if (request.isSecure()) { %>
<tr>
<td colspan=2 align=center class="MediumText">
<A HREF="/insecure/home">
<l10n:resource key="standardLoginLabel">Standard</l10n:resource>
</A>
&nbsp; | &nbsp;
<l10n:resource key="secureLoginLabel">Secure</l10n:resource>
</td>
</tr>
<% } else { %>
<tr>
<td colspan=2 align=center class="MediumText">
<l10n:resource key="standardLoginLabel">Standard</l10n:resource>
&nbsp; | &nbsp;
<A HREF="/secure/home">
<l10n:resource key="secureLoginLabel">Secure</l10n:resource>
</A>
</td>
</tr>
<% } %>
```

- Step 2** In the Jetty configuration file, comment out or remove the call that starts the standard HTTP listener. For example, in `nwsp.jetty.xml`, surround the `Configure` tag for the `SESMSocketListener` for the HTTP port with comment indicators, as shown here:

```
<!-- (start comment)
<Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,SESMSocketListener=0">
  <Set name="port" type="int"><SystemProperty name="application.portno"
    default="8080"/></Set>
  <Set name="minThreads" type="int">5</Set>
  <Set name="maxThreads" type="int">255</Set>
  <Set name="maxIdleTimeMs" type="int">60000</Set>
  <Set name="maxReadTimeMs" type="int">60000</Set>
</Configure>
(end comment) -->
```

- Step 3** In the generic start script, remove the information that defines and opens a port for standard HTTP traffic.

The generic script is executed by all of the application-specific startup scripts. In `start.sh` or `start.cmd`, change:

```
MGMPORTNO=`expr $PORTNO + 100`
SSLPORTNO=`expr $PORTNO - 80 + 443`
PORTS="$PORTNO $MGMPORTNO $SSLPORTNO"
```

to:

```
MGMPORTNO=`expr $PORTNO + 100`
SSLPORTNO=1234
PORTS="$MGMPORTNO $SSLPORTNO"
```

Further down in the script, delete the `-Dapplication.portno=$PORTNO` argument, shown in bold below:

```
$JAVA $SERVER -Xms64m -Xmx64m \
  -classpath $CLASSPATH \
  -Dinstall.root=$INSTALLDIR \
  -Djetty.home=$JETTYDIR \
  -Dapplication.home=$APPDIR \
  -Dapplication.portno=$PORTNO \
  -Dapplication.ssl.portno=$SSLPORTNO \
  -Dmanagement.portno=$MGMPORTNO \
  $MODE \
  $JVMOPTIONS \
  com.cisco.sesm.jmx.Main \
  $CONFIG_FILES \
```

- Step 4** If you are running a captive portal solution, change the configured redirections to the NWSP application to use the HTTPS protocol and the HTTPS port you defined in the generic startup script.

In the `captiveportal.xml` file, change the following lines. The port numbers must match the SSL port number defined in the `serviceportal` configuration (which in the default configuration is `nwsp.xml`).

```
<Set name="userRedirectURL">
http://<SystemProperty name="serviceportal.host" default="nwsp"/>:
<SystemProperty name="serviceportal.port" default="8080"/>/home</Set>
<Set name="serviceRedirectDefaultURL">http://nwsp:8080/serviceRedirect</Set>
<Set name="errorURL">
  http://<SystemProperty name="serviceportal.host" default="nwsp"/>: <SystemProperty
name="serviceportal.port" default="8080"/>/home</Set>
```

to

```
<Set name="userRedirectURL">
  https://<SystemProperty name="serviceportal.host" default="nwsp"/>:
  <SystemProperty name="serviceportal.port" default="1234"/>/home</Set>
<Set name="serviceRedirectDefaultURL">https://nwsp:1234/serviceRedirect</Set>
<Set name="errorURL">
  https://<SystemProperty name="serviceportal.host" default="nwsp"/>: <SystemProperty
name="serviceportal.port" default="1234"/>/home</Set>
```

- Step 5** If you are using the Message Portal application in your captive portal solution, change the configured redirections to NWSP to use the HTTPS protocol and the HTTPS port you defined in the generic startup script.

In `messageportal.xml`, change the following lines:

```
<Set name="defaultURL">
  http://<SystemProperty name="serviceportal.host" default="nwsp"/>:
  <SystemProperty name="serviceportal.port" default="8080"/>/</Set>
```

to:

```
<Set name="defaultURL">
  https://<SystemProperty name="serviceportal.host" default="nwsp"/>:
  <SystemProperty name="serviceportal.port" default="1234"/>/</Set>
```



Configuring an LDAP Directory for SESM Deployments

This appendix describes how to install and configure LDAP directories to work with SESM. SESM is verified to run with the following directories:

- Novell eDirectory Version 8.5
- iPlanet Version 5.x on Solaris Version 2.6. (iPlanet Version 5.1 is recommended.)
- Sun ONE Directory Server Version 5.1 SP1 on Solaris Version 8. (Sun ONE does not run on Solaris Version 2.6.)

Topics in this appendix are:

- [NDS Installation and Configuration Requirements, page B-1](#)
- [Sun ONE and iPlanet Installation and Configuration Requirements, page B-4](#)

NDS Installation and Configuration Requirements

This section describes how to install and configure Novell eDirectory Version 8.5 to work with SESM. Topics are:

- [Summary of Administrative Access to NDS, page B-1](#)
- [Installation and Configuration Procedures, page B-2](#)
- [Setting the Allow Clear Text Passwords Attribute, page B-3](#)

Summary of Administrative Access to NDS

When you complete the procedures in the following section, your NDS directory is configured as follows:

- The following SESM container exists in the NDS directory:
 - Tree name: sesm
 - Server context: ou=sesm.o=cisco
- The Allow Clear Text Passwords option is set to true (required).

- Access to the SESM container through ConsoleOne is granted with the following distinguished name (dn) in the format shown:
 - name: cn=admin.ou=sesm.o=cisco
 - password: value you specified during the NDS installation

This administrative user has all required permissions to update the NDS directory schema and also to create and modify objects in the SESM container.

- When configuring SESM and SPE, use the following format for distinguished name:

```
cn=admin,ou=sesm,o=cisco
```

Installation and Configuration Procedures

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. Use 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
```

Step 13 Go to the following section to enable the Allow Clear Text Passwords attribute. This setting is required.

Setting the Allow Clear Text Passwords Attribute

For SESM to work with NDS, the Allow Clear Text Passwords 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 Passwords attribute is a property of the LDAP Group object of a server.

To set Allow Clear Text Passwords, follow these procedures:

Step 1 Start ConsoleOne. Run the following file:

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

Step 2 Authenticate to the NDS Directory as follows:

- In the tree, click on 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-hand panel.

Step 3 Enable the Allow Clear Text Passwords attribute 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**.
- Click **Close**.

Step 4 Exit ConsoleOne and proceed to SESM installation.

Sun ONE and iPlanet Installation and Configuration Requirements

This section describes how to install and configure Sun ONE and iPlanet to work with SESM. Topics are:

- [Summary of Administrative Access to Sun ONE and iPlanet, page B-4](#)
- [Installation and Configuration Instructions, page B-4](#)

Summary of Administrative Access to Sun ONE and iPlanet

On completion of the instructions in the following section, your Sun ONE or iPlanet directory is configured as follows:

- The following administrative user has all required permissions to update the directory schema:
 - name: cn=Directory Manager
 - password: value you specify during the directory installation
- 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 create and modify objects in the SESM container.
 - name: uid=*yourAdmin*,ou=sesm,o=cisco
where *yourAdmin* is a value you specify during container creation
 - password: a value you specify during container creation

Installation and Configuration Instructions

To install and configure Sun ONE or iPlanet to work with SESM, perform the following steps. These instructions assume that you are installing iPlanet Version 5.0 on a Solaris 2.6 system or Sun ONE Version 5.1 SP1 on a Solaris Version 8 system.

- Step 1** Log on as superuser.
- Step 2** If you have a tar file, expand it.
- Step 3** 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 asking you which components to install, select all components.
- Step 6** At 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** At the following prompt, enter the value **o=cisco**.
- ```
Suffix [dc=]:o=cisco
```
- Step 9** At the following prompt, accept the default value of **Directory Manager**.
- ```
Directory Manager DN [cn=Directory Manager]:
Password:
Password (again):
```
- Enter the password of your choice. This 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** At the following prompt, enter any port number. The configuration examples later in this procedure use the value 390.
- ```
Administration port [15197]:390
```
- Step 11** At 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 server might start automatically. If not, start it as described in the next step.
- Step 12** Start the directory server by executing the following:
- ```
/usr/iplanet/servers/start-admin
```
- Step 13** Start the console by executing the following:
- ```
/usr/iplanet/servers/startconsole
```
- 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 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**.

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 following fields. In the UserID field, enter **admin**.

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

Click **OK**.

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 ACI Name. Click **Add**. The Add User & Group window appears.

Step 23 Enter **admin** in the search field. Click **Search**: 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 or Sun ONE and proceed to the SESM installation.



Configuring RADIUS for SESM Deployments

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 C-1](#)
- [Configuring RADIUS Clients, page C-1](#)
- [Defining Attributes, page C-2](#)
- [Configuring Service Profiles, page C-6](#)
- [Configuring Service Group Profiles, page C-10](#)
- [Configuring Subscriber Profiles, page C-11](#)
- [Configuring Next Hop Gateway Profiles, page C-16](#)
- [Configuring the RADIUS Accounting Feature, page C-16](#)
- [Configuring Cisco Access Registrar for SESM Deployments, page C-17](#)
- [Example RADIUS Profiles, page C-19](#)

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 C-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 C-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
```

Defining Attributes

RADIUS servers use an attribute dictionary to define the attributes that can appear in profiles. An 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.

SESM applications, including RDP, CDAT, and the portal applications, internally predefine the standard RADIUS attributes and the Cisco SSG VSAs. You can use these predefined attributes in RADIUS and LDAP profiles whether or not they are defined in an attribute dictionary. See the [“SESM Predefined Attributes” section on page C-3](#) for predefined attribute names.

Defining New RADIUS Attributes for SESM Deployments

To define additional attributes to use in profiles, such as Cisco VSAs not predefined in the SESM code and non-Cisco VSAs, use the following methods:

- If SESM is running in RADIUS mode, define the attribute in the RADIUS server attribute dictionary. See your RADIUS server vendor's documentation for instructions and syntax. If you are using the bundled SESM RADIUS server, use the RADIUSDictionary MBean used by the bundled SESM RADIUS server. See the [“RADIUSDictionary MBean” section on page D-3](#).
- If SESM is running in LDAP mode, you can define new RADIUS attributes in the RADIUSDictionary MBean used by the RDP application. See the [“RADIUSDictionary MBean” section on page 7-4](#).

SESM Predefined Attributes

[Table C-2](#) lists the standard RADIUS attribute names that are predefined in SESM applications.

[Table C-3](#) shows the Cisco SSG VSAs that are predefined in SESM applications.

Table C-2 Standard RADIUS Attributes Predefined in SESM Applications

RADIUS Attribute Names¹		
USER_NAME	SESSION_TIMEOUT	ACCT_LINK_COUNT
USER_PASSWORD	IDLE_TIMEOUT	ACCT_INPUT_GIGAWORDS
CHAP_PASSWORD	TERMINATION_ACTION	ACCT_OUTPUT_GIGAWORDS
NAS_IP_ADDRESS	CALLED_STATION_ID	EVENT_TIMESTAMP
NAS_PORT	CALLING_STATION_ID	CHAP_CHALLENGE
SERVICE_TYPE	NAS_IDENTIFIER	NAS_PORT_TYPE
FRAMED_PROTOCOL	PROXY_STATE	PORT_LIMIT
FRAMED_IP_ADDRESS	LOGIN_LAT_SERVICE	LOGIN_LAT_PORT
FRAMED_IP_NETMASK	LOGIN_LAT_NODE	ARAP_PASSWORD
FRAMED_ROUTING	LOGIN_LAT_GROUP	ARAP_FEATURES
FILTER_ID	FRAMED_APPLETALK_LINK	ARAP_ZONE_ACCESS
FRAMED_MTU	FRAMED_APPLETALK_NETWORK	ARAP_SECURITY
FRAMED_COMPRESSION	FRAMED_APPLETALK_ZONE	ARAP_SECURITY_DATA
LOGIN_IP_HOST	ACCT_STATUS_TYPE	PASSWORD_RETRY
LOGIN_SERVICE	ACCT_DELAY_TIME	PROMPT
LOGIN_TCP_PORT	ACCT_INPUT_OCTETS	CONNECT_INFO
REPLY_MESSAGE	ACCT_OUTPUT_OCTETS	CONFIGURATION_TOKEN
CALLBACK_NUMBER	ACCT_SESSION_ID	EAP_MESSAGE
CALLBACK_ID	ACCT_AUTHENTIC	MESSAGE_AUTHENTICATOR
FRAMED_ROUTE	ACCT_SESSION_TIME	ARAP_CHALLENGE_RESPONSE
FRAMED_IPX_NETWORK	ACCT_INPUT_PACKET	ACCT_INTERIM_INTERVAL
STATE	ACCT_OUTPUT_PACKETS	NAS_PORT_ID
CLASS	ACCT_TERMINATE_CAUSE	FRAMED_POOL
VENDOR	ACCT_MULTI_SESSION_ID	

1. A hyphen (-) can replace the underbar (_) in RADIUS attribute names. The attribute names are not case-sensitive.

Table C-3 Cisco SSG VSAs Predefined in SESM Applications

RADIUS Attribute	Vendor ID	Subattribute	Name¹	Type
26	9	1	Cisco-Av	String
26	9	250	Account-Info	String
26	9	251	Service-Info	String
26	9	252	Command-Code	BINARY
26	9	253	Control-Info	String

1. The hyphen (-) and underbar (_) are interchangeable in RADIUS attribute names. The attribute names are not case-sensitive.

Dynamically Defining Attributes in Profiles for Testing and Development

SESM allows you to dynamically define a new attribute when you first use it in a profile. This feature is intended only for testing, demonstration, and development purposes. Use the dynamic attribute feature only in the following circumstances:

- The SESM portal is running in Demo mode.
- The SESM portal is running in RADIUS mode, and the RADIUS server you are using is the bundled SESM RADIUS server.
- The SESM portal is running in LDAP mode in a testing or development environment.

Dynamic attributes are defined as new subattributes under the standard RADIUS vendor-specific attribute number 26.

Valid formats are:

```
[attributeName](radiusAttributeId, vendorId, vendorSubattribute, datatype)
```



Note If you omit *attributeName*, the parentheses surrounding the attribute definition are optional, but recommended.

Where:

- *attributeName*—Is the new attribute name.

This field is optional. If it is used, subsequent profiles can use just the *attributeName*, without the attribute definition. However, you must be sure that the profile containing the attribute definition gets used before any other profiles that use only the *attributeName*.



Note To successfully use the attribute by name in a different profile, the user whose profile contains the attribute definition must log onto the portal before any user whose profile contains only the new attribute name without the definition.

If *attributeName* is not used, you use only the attribute definition in the profiles.

- *radiusAttributeId*—Use attribute value 26, the vendor-specific attribute.
- *vendorId*—A RADIUS vendor ID.
- *vendorSubattribute*—A unique number that distinguishes this attribute from other VSAs for the same vendor.
- *datatype*—One of the following values: BINARY, STRING, INTEGER, IPADDRESS. When datatype is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string.

An example follows:

```
demoVSA(26, 1, 1, BINARY)
```

Other valid syntax is:

```
name([[type=]26],[vendorId=]vendorId,[vendorType=]vendorType,[dataType=]dataType)
```

Merit File Examples

In a Merit file, define a new attribute and assign a value in the following format:

```
[attributeName](attributeDefinition) = "attributeValue"
```

```
MY_ATTRIBUTE(type=26, vendorId=9, vendorType=555, dataType=INTEGER) = "34"
```

```
BINARY_ATTRIBUTE(type=26, vendorId=9, vendorType=556, dataType=BINARY) = "0x3F45"
```

```
(26,9557,IPADDRESS) = "34.43.54.240"
```

CDAT Examples

In CDAT, define a new attribute and assign a value in the Local RADIUS attributes field as follows:

```
[attributeName](attributeDefinition):attributeValue
```

For example:

```
MY_ATTRIBUTE(type=26, vendorId=9, vendorType=555, dataType=INTEGER):34
```

```
BINARY_ATTRIBUTE(type=26, vendorId=9, vendorType=556, dataType=BINARY) : "0x3F45"
```

```
(26,9,557,IPADDRESS):34.43.54.240
```

Configuring Service Profiles

Service profiles define the services that subscribers can select from an SESM web portal. You must configure a service profile for each service that will be accessible through the SESM web portal.

[Table C-4](#) 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 C-17](#) 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 `aaa.properties` file located in the NWSP config directory (for example, `nwsp/config/aaa.properties`). 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 C-4 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 on the RADIUS server. SESM obtains the service password directly from the RADIUS server. In SESM, configure this password in the <code>servicePassword</code> attribute in the AAA MBean.
Service-Type	Standard RADIUS attribute number 6. The value must be “outbound.”

Table C-4 Attributes in Service Profiles (continued)

Attribute	Description
Session-Timeout	<p>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.</p> <p>Note 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 subscriber can use the service.</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	<p>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.</p>
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"> • AauthenType—Specifies whether SSG uses the CHAP or PAP protocol to authenticate users for proxy services. • Idescription—Service description. Optional. Describes the service. • Ttype—Type of service. Optional. Valid values for <i>type</i> are: <ul style="list-style-type: none"> – P—Passthrough. This is the default. – T—Tunnel – X—Proxy. Indicates that the SSG performs proxy service. • Mmode—Service mode. Optional. Valid values for <i>mode</i> are: <ul style="list-style-type: none"> – S—Sequential mode. Prevents the subscriber from accessing any other services while connected to this service. – C—Concurrent mode. This is the default. Allows the subscriber to simultaneously log onto this service while connected to other services. • Rip_address;mask—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". • Dip_address_1[ip_address_2]—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. • Oname1[name2]...[;nameX]—Domain names. Optional. • SRadiusServerAddress;authPort;acctPort;secret—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.

Table C-4 Attributes in Service Profiles (continued)

Attribute	Description
Service-Info (continued)	<ul style="list-style-type: none"> • Gkey—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 “Configuring Next Hop Gateway Profiles” section on page C-16 for information about creating a next hop gateway table. • Uurl or Hurl—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"> – Uurl—URL for a service displayed in its own browser window. – Hurl—URL for a service displayed in a frame in the SESM portal window. <p>Note 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"> • Bsize—The PPP maximum transmission unit (MTU) for SSG as a LAC. By default, the PPP MTU size is 1500 bytes. • X—Indicates that the RADIUS authentication and accounting requests use the full user name (for example, user@service). • “QU;upstream-token-rate;upstream-normal-burst;[upstream-excess-burst];D;downstream-token-rate;downstream-normal-burst;[downstream-excess-burst]”—Indicates the hierarchical policing (quality of service) policies for this service. • Vstring—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.

Table C-4 Attributes in Service Profiles (continued)

Attribute	Description
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"> • “ip:inacl[#number]={standardACL extendedACL}”—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. • “ip:outacl[#number]={standardACL extendedACL}”—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"> – <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>. – <i>standardACL</i>—A Cisco IOS standard ACL. – <i>extendedACL</i>—A Cisco IOS extended ACL. <p>Note 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> <ul style="list-style-type: none"> • “vpdn:ip-addresses=address1[<delimiter>address2][<delimiter>address3]...”—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"> – <i>address</i>—IP address of the home gateway. – <i><delimiter></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. • “vpdn:tunnel-id=name”—VPDN tunnel ID. Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group. • “vpdn:tunnel-password=secret”—L2TP tunnel password. Specifies the secret (password) used for L2TP tunnel authentication. • “vpdn:l2tp-hello-interval=interval”—L2TP hello interval. Specifies the number of seconds for the hello keepalive interval.

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 C-5](#) briefly describes the attributes in a RADIUS service group profile.

Table C-5 Attributes in Service Group Profiles

Attribute	Description
Password	The password required to obtain the profile.
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"> “<i>Idescription</i>”—Describes the service group. If this field is omitted, the service group profile name is used. “<i>GName</i>”—Service group name. “<i>Nname</i>”—Lists the services that belong to the group. “<i>TE</i>”—Indicates that this is a mutually exclusive service group.

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 C-6](#) 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 C-17](#) 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 `aaa.properties` file located in the NWSP config directory (for example, `nwsp/config/aaa.properties`). 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 C-6 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 edge session on SSG) can remain active at any one time. When the time expires, SSG 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>Note 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.

Table C-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
Account-Info	<p>Note 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 Url or Hurl 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"> • “NserviceName”—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. • “GserviceGroupName”—Service group. Creates a folder for the service group on the subscriber's SESM web portal. The <i>serviceGroupName</i> must be defined in a service group profile. There can be multiple instances of this attribute within a subscriber profile. • “AutoConnectServiceName”—Automatic connection. Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon. <p>Note 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 “Example Subscriber Profile for Auto Services” section on page C-15 for an example.</p> <ul style="list-style-type: none"> • “Url or Hurl”—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"> – Url—URL for the home page displayed in its own browser window. – Hurl—URL for the home page displayed in a frame in the SESM browser window. <p>Note 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"> • “RIgroup;duration[;service]”—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. • “RAgroup;duration;frequency[;service]”—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.

Table C-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
Account-Info (continued)	<ul style="list-style-type: none"> • “RS”—The subscriber has SMTP forwarding capability. • “QU;upstream-token-rate;upstream-normal-burst;[upstream-excess-burst];D;downstream-token-rate;downstream-normal-burst;[downstream-excess-burst]”—Indicates hierarchical policing (quality of service) policies for this subscriber. <p>Note The \$ in a subattribute code indicates that the subattribute is used only by SESM, and not by SSG or other Cisco network devices.</p> <p>Note Deployers might see \$ subcodes in access accept messages from SSG that are not documented below. SSG uses \$ subcodes to identify information about the subscriber that it passes along for SESM use, such as MAC address, VPI/VCI, MSISDN number, and other connection information. Those codes are not documented in this guide because they are not used in subscriber profiles.</p> <ul style="list-style-type: none"> • “\$PEpermission”—Meaningful in Demo mode only, to demonstrate the LDAP mode self-management, self-subscription, and sub-account creation features. Use this attribute to assign specific permissions to the subscriber for use in a demo. The <i>permission</i> is one of the following: <ul style="list-style-type: none"> – Service Selection—The permission to perform service selection and disconnect from services is implied and does not have to be explicitly coded in the profile. – Self Manage—Use this string to demonstrate the LDAP mode feature that allows a subscriber to update their own account attributes, such as name, address, e-mail, and hobbies. – Subaccount Manage—Use this string to demonstrate the LDAP mode feature that allows a subscriber to create, delete, and manage subaccounts. The Demo mode does not create an actual subaccount; the supporting subaccount profile must be defined in the <code>aaa.properties</code> file. Define the subaccount profile and use the \$FA attribute. – Service Subscription—Use this string to demonstrate the LDAP mode feature that allows a subscriber to subscribe and unsubscribe to services and service groups. If you use this string, you must also add a \$SA or \$GA attribute. • “\$SAservice”—Meaningful in Demo mode only, to demonstrate the LDAP mode self-subscription feature. Use this attribute to list services to which the subscriber can self-subscribe. The <i>service</i> must be defined in a service profile. • “\$GAserviceGroupName”—Meaningful in Demo mode only to demonstrate the LDAP mode self-subscription feature. Use this attribute to list service groups to which the subscriber can self-subscribe. The <i>serviceGroupName</i> must be defined in a service group profile. • “\$UGuserGroupName”—Meaningful in Demo mode only to demonstrate the LDAP mode user group features, including user group branding. This subcode adds the user to a user group. The <i>userGroupName</i> can be any value. (User groups are an LDAP mode concept. RADIUS profiles do not provide a way to define valid user group names.) <p>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 <code>aaa.properties</code> file.</p>

Table C-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
Account-Info (continued)	<ul style="list-style-type: none"> <li data-bbox="358 317 1472 436">• “\$AA<i>accountAttributeName;type;attributeValue</i>”—Meaningful in Demo mode only to demonstrate the LDAP mode account self-care features. 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. Use a separate attribute line for each field. The <i>accountAttributeName</i> is a name for a field on the My Account page in the NWSP application. These are X.500 fields. See the <i>Cisco Distributed Administrator Tool Guide</i> for a list of the X.500 names. 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>. The <i>type</i> indicates a type for <i>attributeValue</i> and is one of the following: <ul style="list-style-type: none"> <li data-bbox="407 642 846 669">– S—<i>attributeValue</i> is a simple string. <li data-bbox="407 684 889 711">– V—<i>attributeValue</i> is an array of strings. The <i>attributeValue</i> indicates the value to be displayed in the field in NWSP. If type is V, surround <i>attributeValue</i> with braces ({}) and delimit each element in the array with a semicolon. For example: <pre data-bbox="396 856 841 905"> \$AAgivenName;S;James" \$AAhobbies;V;{sports;news;travel}" </pre> <li data-bbox="358 936 1472 1100">• “\$FA<i>parent</i>”—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. This subcode identifies this subscriber as a subaccount. The <i>parent</i> is the user name of the parent account and must be defined in a subscriber profile. The NWSP application running in Demo mode demonstrates subaccounts. In the <code>aaa.properties</code> file, <code>subgolduser</code> is defined as a subaccount to <code>golduser</code>. <li data-bbox="358 1121 1472 1241">• “\$SB<i>serviceBlocked</i>”—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. In a subaccount profile, this subcode identifies a service that is blocked (not available) to the subaccount. The parent account can unblock a service and make it available for subscription. The <i>service Blocked</i> must be defined in a service profile. <li data-bbox="358 1262 1472 1381">• “\$GB<i>serviceGroupBlocked</i>”—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. In a subaccount profile, this subcode identifies a service group that is blocked (not available) to the subaccount. The parent account can unblock a service group and make it available for subscription. The <i>serviceGroupBlocked</i> must be defined in a service group profile. <li data-bbox="358 1402 1472 1522">• “\$SL<i>subaccountLimit</i>”—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. In a parent account profile, this subcode defines the number of subaccounts that the parent can create. If this subcode is not included in the profile, no limit is enforced. The <i>subaccountLimit</i> is an integer value from 0 to any limit imposed by the deployer. <li data-bbox="358 1543 1472 1719">• “\$SO<i>singleSignOn</i>”—Meaningful in Demo mode only. Allows you to disable single sign-on for individual users when the SESM global sign-on is in effect. If this attribute is not defined, the default value 1 is used. Values are <ul style="list-style-type: none"> <li data-bbox="407 1650 1040 1677">– 0—Single sign-on is not permitted for this subscriber. <li data-bbox="407 1692 1146 1719">– 1 (the default)—Single sign-on is permitted for this subscriber.

Table C-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
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"> “ip:inacl[#number]={<i>standardACL</i> <i>extendedACL</i>}”—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. “ip:outacl[#number]={<i>standardACL</i> <i>extendedACL</i>}”—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"> <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>. <i>standardACL</i>—A Cisco IOS standard ACL. <i>extendedACL</i>—A Cisco IOS extended ACL. <p>Note 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 examples in this section are 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.

Example Subscriber Profile for Demo Mode

```
golduser Password = "cisco"
  Service-Type = Framed-User,
  Account-Info = "$UGgold",
  Account-Info = "Ainternet_gold",
  Account-Info = "Ninternet_gold",
  Account-Info = "Ncorporate",
  Account-Info = "Ngames",
  Account-Info = "Ndiscount_shopping",
  Account-Info = "Hhttp://www.spiderbait.com",
  Account-Info = "$PESelf Manage",
  Account-Info = "$PESubaccount Manage",
  Account-Info = "$PEService Subscription",
  Account-Info = "$SAbanking",
  Account-Info = "$GAnewsgroup",
  Account-Info = "$AAinitials;V;{A}",
  Account-Info = "$AAgender;S;female",
  Account-Info = "$AAsurname;S;Goodbody",
```

```
Account-Info = "$AAtitle;S;Miss",
Account-Info = "$AAgivenName;S;Felicity",
Account-Info = "$AAhobbies;V;{science;news;travel}"
```

See the `aaa.properties` file in the `nwps/config` directory for more examples.

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 C-4 on page C-6](#).) 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 = "G12tp-net7;192.168.1.101",
Control-Info = "G12tp-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 C-1](#).
- Add the Cisco VSAs to the RADIUS server attribute dictionary, as described in the [“Defining Attributes” section on page C-2](#).
- Configure an accounting port, as described in the [“Configuring SSG to Communicate with the RADIUS Server” section on page C-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
```

Example RADIUS Profiles

The SESM product includes sample RADIUS profiles in MERIT flat file formats. The SESM sample portal applications running in Demo mode use the profiles in these MERIT files. The installation includes a separate MERIT file for each of the sample portal applications. The files are located in the config directory under each portal application directory. For example:

```
nwsp
  config
    aaa.properties
```

■ Example RADIUS Profiles



Configuring the Bundled SESM RADIUS Server

This appendix describes the configuration options for the bundled SESM RADIUS server. Topics are:

- [Bundled SESM RADIUS Server Installed Location, page D-1](#)
- [Profile File Requirements, page D-1](#)
- [Defining New Attributes to the Bundled SESM RADIUS Server, page D-2](#)
- [Starting the Bundled SESM RADIUS Server, page D-2](#)
- [MBeans for the Bundled SESM RADIUS Server, page D-2](#)

Bundled SESM RADIUS Server Installed Location

The bundled SESM RADIUS server is installed by default in both RADIUS and LDAP mode installations. None of the SESM installation parameters affects the default configuration of the bundled SESM RADIUS server.

The installed location of configuration files and startup scripts that support the bundled SESM RADIUS server is the tools directory under your SESM installation directory:

```
tools
  bin
    startAAA
  config
    aaa.xml
    erp.xml
    aaa.properties
```

The aaa.xml and erp.xml files are MBean configuration files for the bundled SESM RADIUS server. The aaa.properties file is a sample profile file.

Profile File Requirements

The bundled SESM RADIUS server requires a profile file in MERIT format.

The default configuration points to the aaa.properties file, a sample MERIT file installed with RDP. You can change this to point to a different file by changing the aaaFilename attribute in the AAA MBean. For example, you could point to the aaa.properties file in the NWSP directory.

The bundled SESM RADIUS server loads the contents of the profile file during startup. You must restart the RADIUS server if:

- You change the `aaaFilename` attribute to point to a different file.
- You make any changes to the profiles in the referenced file.

Defining New Attributes to the Bundled SESM RADIUS Server

All SESM applications, including the bundled SESM RADIUS server, internally predefine the standard RADIUS attributes and the Cisco vendor-specific attributes (VSAs) listed in [Table C-2](#) and [Table C-3](#) on [page C-4](#).

To define additional attributes, such as Cisco VSAs not included in the above-referenced tables or other vendor VSAs:

- Define the new attribute in the [RADIUSDictionary MBean](#). New attributes defined in this MBean can be used in your profiles.
- Define the new attribute in the profile itself, as described in “[Dynamically Defining Attributes in Profiles for Testing and Development](#)” section on [page C-5](#).

Starting the Bundled SESM RADIUS Server

The bundled SESM RADIUS server is ready to run immediately after installation. To start it, execute the startup script with a port number, as follows:

- On Solaris and Linux:


```
installDir/tools/bin/startAAA.sh portNumber
```
- On Windows:


```
installDir\tools\bin\startAAA.cmd portNumber
```



Note

You can edit the start script, inserting a default port number. In that case, you do not need to specify `portNumber` on the command line.

MBeans for the Bundled SESM RADIUS Server

The bundled SESM RADIUS server uses the following MBeans:

- [Logger MBean, page D-3](#)
- [ManagementConsole MBean, page D-3](#)
- [RADIUSDictionary MBean, page D-3](#)
- [AAA MBean, page D-4](#)

To change attributes in these MBeans, you can either:

- Edit the MBean configuration files:

```
tools
  config
    aaa.xml
```

erp.xml

- Make changes using the Agent View running on the server management port. The port numbers are:
 - server port—specified at run time on the command line or in the startup script
 - management port— server port + 100

**Note**

The installation process does not add a link on the CDAT main window to this Agent View. You can add this link manually as described in [“Adding a New Application to the CDAT Main Window” section on page 6-4](#). Before creating the link, edit the startAAA script, inserting a port number that you want to consistently use to start the bundled SESM RADIUS server. Then configure the link on the CDAT window to go to the configured RDP port + 100.

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs CDAT application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the [“Logger MBean” section on page 5-2](#), for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the server management console port, including valid user names and passwords for accessing the console. See the [“Configuring the ManagementConsole MBean” section on page 3-5](#) for more information.

RADIUSDictionary MBean

All SESM applications, including this RADIUS server, internally predefine the standard RADIUS attributes and the Cisco SSG vendor-specific attributes (VSAs). You can define additional attributes, such as additional Cisco VSAs or VSAs from other vendors, in the RADIUSDictionary MBean. When you define attributes in this MBean, you can use the defined attribute names in RADIUS profiles.

**Note**

You can also define dynamic attributes directly in the profile, as described in the [“Dynamically Defining Attributes in Profiles for Testing and Development” section on page C-5](#).

For a list of the standard RADIUS attributes that are predefined in SESM, see [Table C-2 on page C-4](#). For a list of the Cisco SSG VSAs that are predefined in SESM, see [Table C-3 on page C-4](#).

[Table D-1](#) describes the attributes in the RADIUSDictionary MBean.

Table D-1 Bundled SESM RADIUS Server—RADIUSDictionary MBean

Attribute Name	Explanation
dynamicAttributes	<p>An array of new attribute definitions. To define a new attribute, add a new item to this array. The format for an item is:</p> <p><i>name(radiusAttributeId, vendorId, vendorSubattribute, datatype)</i></p> <p>Where:</p> <ul style="list-style-type: none"> <i>name</i>—Is the new attribute name. <i>radiusAttributeId</i>—Use attribute value 26, the vendor-specific attribute. <i>vendorId</i>—A RADIUS vendor ID. <i>vendorSubattribute</i>— A unique number that distinguishes this attribute from other VSAs for the same vendor. <i>datatype</i>—One of the following values: BINARY, STRING, INTEGER, or IPADDRESS. When <i>datatype</i> is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string. <p>For example:</p> <p>demoVSA(26, 1, 1, BINARY)</p> <p>Other valid syntax formats are represented below:</p> <p><i>name([[type=]26],[vendorId=]vendorId,[vendorType=]vendorType,[dataType=]dataType)</i></p> <p>For example:</p> <p>demoVSA(type=26, vendorId=1, vendorType=1,dataType=INTEGER)</p>

AAA MBean

The AAA MBean configures the AAA listener, including its thread pool and socket (port). [Table D-2](#) describes the configurable attributes in the AAA MBean.

Table D-2 Bundled SESM RADIUS Server—AAA MBean

Attribute Name	Explanation
handler	Defines the type of listener being configured. The value must be AAA to configure a bundled SESM RADIUS server.
dump	<ul style="list-style-type: none"> true—Displays all RADIUS messages on the console (stderr) false—Does not display messages <p>Default: true</p>
aaaFilename	Specifies the profile file name and path. You can change this reference to point to any file in the Merit file format. For example, you could use the NWSP aaa.properties file.
Note The following attributes are in the AAA MBean, RADIUSListener=AAA,component=Threadpool	
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>Default: 5</p>

Table D-2 Bundled SESM RADIUS Server—AAA MBean (continued)

Attribute Name	Explanation
maxThreads	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. Default: 255
Note The following attributes are in the AAA MBean, RADIUSListener=AAA,component=RADIUSServerSocket	
secret	The shared secret that must be used in RADIUS protocol messages sent to the bundled SESM RADIUS server. This attribute sets a global shared secret for all clients. To specify different shared secrets for each client, use the allowedClients attribute.
localPort	The port the RADIUS server listens on. It uses the same port for RADIUS Accounting-Requests and Access-Requests. The installed configuration file defines this attribute as a Java system property, which is assigned a value at run time: <i>application.portno</i>
allowedClients	Configures a list of clients from which the server can accept requests. Also configures shared secrets. Turn this feature on and off as follows: <ul style="list-style-type: none"> • Allow any client to access the RADIUS server—Comment out the allowedClients attribute in the XML file, or remove all clients from the allowedClients list. • Restrict client access—Uncomment the allowedClients attribute in the XML file. <p>Note If you do not see the allowedClients attribute in the Agent View, check the configuration file (the XML file). The allowedClients attribute might be commented out. If so, remove the comment characters, save the XML file, and then restart the RADIUS server.</p> <p>You can add more clients by adding more elements to the allowedClients attribute. An element in allowedClients attribute has the following format:</p> <pre>{hostName IPAddress}[:localSecret]</pre> <p>Where:</p> <p><i>hostName</i> or <i>IPAddress</i> identify a client (an SSG, for example) that has access to the server.</p> <p><i>localSecret</i> identifies the secret that this client uses for RADIUS communication.</p>



SESM Load Balancing

This chapter contains information about load balancing options for SESM deployments. It includes the following topics:

- [Cisco Load Balancing Solutions, page E-1](#)
- [Configuring SESM for Load Balancing, page E-1](#)
- [Using the Cisco IOS Server Load Balancer with SESM Portals, page E-2](#)

Cisco Load Balancing Solutions

The following Cisco load balancing solutions are available for use with SESM portals:

- Cisco IOS Server Load Balancer (Cisco IOS SLB)—A feature integrated into Cisco IOS software. Cisco IOS SLB performs Layer 4 load balancing.
- Cisco Content Services Switch 11000 (CSS 11000)—A switch that performs load balancing at Layers 4 through 7, including URL inspection.
- Cisco Content Switching Module (CSM)—A Cisco Catalyst 6500 line card that balances client traffic to farms of servers and other devices. CSM performs load balancing at Layers 4 through 7, including URL inspection.

Configuring SESM for Load Balancing

Subscriber Browsers

To participate in load balancing, the SESM clients (the subscriber browsers) must be directed to the IP address and port of the load balancing tool.

SSG Considerations

If the SESM solution requires SSGs, the load balancing tool must be accessible on the SSG default network.

Using the Cisco IOS Server Load Balancer with SESM Portals

This section contains important information about using the Cisco IOS SLB to load balance traffic among multiple instances of SESM portals.

Load Balancing with Stickiness versus No Stickiness

The Cisco IOS SLB stickiness feature controls whether all TCP connections from the same client session must be handled by the same server or can be load balanced among multiple servers. While a TCP connection is active, all packets from that client are sent to the same server regardless of the stickiness setting. The stickiness setting is relevant after the first TCP connection is released and the session is controlled by the web server.

- **Stickiness**—The load balancing tool makes all subsequent TCP connections from the same client session, received within the configured stickiness duration, to the server used for the original connection.
- **No stickiness**—The load balancing tool is free to distribute subsequent TCP connections among all available servers.



Caution

Do not enable stickiness if your deployment uses SSGs with port-bundle host key enabled. For more information, see [“Stickiness Issues with SSG Port-Bundle Host Key Feature”](#) below.



Tip

With no stickiness, we recommend configuring SESM portals with single signon enabled. Otherwise, subscribers might be required to authenticate multiple times during a session—once for each new SESM portal instance that handles requests during a subscriber session. In general, we recommend using single signon enabled in all SESM deployments. It allows subscribers to close their browsers or navigate away from the SESM portal and return later without having to reauthenticate.

Stickiness Issues with SSG Port-Bundle Host Key Feature

Stickiness in a Layer 4 load balancing tool is based on the client's IP address. When port-bundle host key is enabled, multiple subscribers have the same IP address (the SSG port-map source ip address). As a consequence, when Stickiness is enabled on the IOS-SLB, all TCP connections for all clients with the same port map IP address (using the same SSG), are directed to the same SESM server. This is not the desired effect.



Note

In general, we recommend enabling the port-bundle host key on SSGs and avoiding the stickiness option in a Layer 4 load balancing tool.

No stickiness works well whether the port-bundle host key option is enabled or disabled.



Configuring the SSG for SESM Deployments

This appendix shows the minimum required configuration for the Cisco Service Selection Gateway (SSG) to work with a Subscriber Edge Services Manager (SESM) deployment.

For more information about configuring SSG, including optional features and more explanation of the required configurations described in this appendix, see the SSG documentation. The “[Related Documentation](#)” section in the preface of this guide includes an online link to SSG documentation.

Basic SSG Configuration

This section shows the required commands for configuring SSG to work with SESM portals.

Step 1 To enable the SSG, enter:

```
ip cef
ssg enable
```

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

Step 2 To identify the network where the SESM portal is running, enter:

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

where *IPaddress* and *mask* identify the network where the SESM portal is running.

Step 3 To configure the port on which the SSG will listen for SESM requests, enter:

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

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

Step 4 To specify the shared secret for password encryption between SSG and the SESM portal, enter:

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

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

Step 5 To have the SSG cache subscriber profiles obtained during authentication, enter:

```
ssg profile-cache
```

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

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

Step 6 To configure the SSG to perform RADIUS authentication, the minimum configuration is:

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

**Note**

In LDAP mode, the RADIUS server is the SESM RADIUS Data Proxy (RDP) server.

Step 7 To configure communication between SSG and the RADIUS server, enter:

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

where:

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

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

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

password is the RADIUS shared secret for password encryption

Step 8 To specify the password that SSG uses to query the RADIUS server for service profiles, enter:

```
ssg service-password serviceProfilePassword
```

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

Step 9 Every service must be bound to an uplink interface. If the service binding is not defined in the next-hop table on the SSG device, then the service must be bound by using the **ssg bind service** command.

Step 10 (Optional but recommended) Configure the SSG port-bundle host key feature as described in the following section.

Configuring the Port-Bundle Host Key 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.

**Note**

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

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

lowPort is the lowest SESM port

highPort is the highest SESM port

SESMaddress is the IP address of SESM

If 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 SESM applications.

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

Current configuration : 4499 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c7200-1
!
boot system flash disk0:c7200-g4js-mz.v122_4_b_throttle
```

The following lines configure AAA authentication.

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

```
!ip cef
!
!
```

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

```
!!
ssg enable

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

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

```
ssg port-map enable
ssg port-map destination range 8080 to 8080 ip <sesmIPAddress>
ssg port-map destination range 8443 to 8443 ip <sesmIPAddress>
>
ssg port-map source ip Loopback0
!
!
ssg bind service passthrough1 FastEthernet4/0
ssg bind service proxy1 FastEthernet4/0
ssg bind service 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 1812 acct-port 1813 timeout 10 retransmit 3
key cisco
radius-server retransmit 3
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
call rsvp-sync
!
mgcp profile default
dial-peer cor custom
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
end
c7200-1#

```



Symbols

- \$MGMTPORTNO [9-5](#)
- \$SSLPORTNO [9-5](#)
- \$ subattributes [C-13](#)
- \$ variables, in start scripts [9-5](#)

A

AAA

See RADIUS

aaa.properties file [5-6, C-19, D-1, D-4](#)

aaa.xml [D-1, D-2](#)

aaaFilename attribute [D-4](#)

AAA MBean [5-10](#)

access accept messages [C-13](#)

access control lists

See ACLs

access reject messages [13-9](#)

Account-Info, Demo mode [C-13](#)

accounting

RADIUS [C-1, C-16](#)

solutions [C-16](#)

ACLs [10-12](#)

Advanced Firewall page [10-16, 10-22](#)

established keyword in [10-20](#)

format in CDAT [10-26](#)

generated [10-19](#)

My Firewall page [10-19, 10-21](#)

numbers [10-23, 10-26, 10-27](#)

priorities [10-23](#)

RADIUS profiles [C-9, C-15](#)

restrictions [10-26](#)

viewing in CDAT [10-19](#)

addDimension call [5-14](#)

addHandler [4-2](#)

addListener [4-6, 4-7](#)

Add Services option [2-14](#)

AddWebApplication [4-5](#)

administrative firewalls [10-25](#)

Advanced Firewall page [10-16](#)

advertisingCaptiveDuration attribute [11-12, 11-18](#)

advertisingCaptiveOn attribute [11-11, 11-24](#)

advertisingCaptivePort attribute [11-12](#)

advertisingCaptiveURL attribute [11-11](#)

advertising redirection

configuring [2-17, 11-11, 11-15, 11-22](#)

duration [2-17](#)

hobbies [11-8, 11-16](#)

HTTP query parameters [11-3](#)

port [2-17](#)

profile attributes [C-12](#)

Agent View

accessing [3-4, 3-6](#)

description [3-3, 3-4](#)

links on CDAT main window [2-19, 3-7](#)

URLs [3-6](#)

using [3-8](#)

AllApplicationsDescriptions attribute [5-13](#)

Allow Clear Text Passwords [B-3](#)

allowedClients attribute [7-6, D-5](#)

AllProtocolDescriptions attribute [5-12](#)

alternative configurations, captive portal [11-5](#)

alwaysGetAllAttributes attribute [8-2](#)

apidoc [2-20](#)

APIs

SESM [5-19](#)
 APN [C-11](#)
 append attribute [4-3, 4-5](#)
 application.home [4-4, 4-5, 5-3, 9-5](#)
 application.log [4-5, 5-3, 13-4](#)
 application.portno [9-5](#)
 application.ssl.portno [9-5](#)
 applications

- startup scripts [9-3](#)
- stopping [9-6](#)

 applications list, on firewall pages [5-11, 5-13, 10-17, 10-18](#)
 Apply button, AgentView [3-11](#)
 attributes, arbitrary

- configuring [10-10](#)
- demonstrating [10-11](#)
- description [10-5, 10-9](#)
- URL [10-11](#)

 attributes, configuration

- changing values [3-2](#)
- persisting changes [3-11](#)

 attributes, RADIUS

- defining new [7-4, C-3, C-5, D-2, D-4](#)
- defining new in RDP [7-4](#)
- dictionary [C-2](#)
- predefined [C-3](#)

 authAttributes attribute [7-5](#)
 authentication

- multikey [7-5, 10-28](#)
- NDS [B-3](#)
- RDP [7-8](#)
- setting RADIUS port [C-1](#)
- type [C-7](#)

 AuthInfo attribute [3-5](#)
 autoConnect attribute [5-5](#)
 automatic connections

- configuring [10-1, C-12](#)
- description [10-1](#)
- disconnecting [10-3](#)
- RADIUS configuration example [C-15](#)

RDP [5-5](#)
 self-care, LDAP mode [10-3](#)
 status [10-2](#)
 troubleshooting [10-2](#)
 autopolicing [10-28](#)

B

blocked services [C-14](#)
 branding [5-9, 10-4](#)
 BUNDLE_LENGTH attribute [5-8, 5-9, 12-2](#)
 bundled RADIUS server [D-1](#)
 burst rates [C-8, C-13](#)

C

cacheExpireInterval [8-3](#)
 cacheMinFreeMem [8-2](#)
 cacheObjectTimeout [8-3](#)
 cacheSessionTimeout [8-3](#)
 caching

- cache size [8-2](#)
- directory data [8-2](#)
- memory usage [8-2](#)
- profiles [5-5](#)
- RDP [10-3](#)
- SESM [5-5](#)
- SPE attributes [8-2](#)

 captiveportal.jetty.xml [3-14](#)
 captiveportal.xml [3-14, 11-10, 11-11, 11-24](#)
 Captive Portal application

- alternatives [11-5](#)
- benefits [11-5](#)
- configuring [11-11](#)
- description [11-3](#)
- installing [2-15](#)
- IP address [2-15](#)
- ports [2-15](#)

- running secure mode [A-4](#)
- captiveportal MBean [11-11](#)
- captive portal solution
 - alternative configurations [11-5](#)
 - configuration files [3-18](#)
 - diagram [11-2](#)
 - eliminating J2EE listeners [11-5](#)
 - eliminating redirection types [11-5](#)
 - example profiles [11-8](#)
 - groups [11-19](#)
 - installing [2-7, 11-6](#)
 - NWSP role [11-4](#)
 - required Cisco IOS releases [11-1](#)
 - startup scripts [11-9](#)
 - troubleshooting [11-23](#)
- CDAT
 - configuring [6-1](#)
 - cookies [6-1](#)
 - entering ACLs [10-26](#)
 - installing [2-7, 2-19](#)
 - links on main window [2-19, 6-3](#)
 - logging in [6-3, 6-5](#)
 - logging on [8-3](#)
 - main window [3-6, 3-7](#)
 - MBean [6-3](#)
 - port number [2-19](#)
 - session tuning [6-3](#)
 - starting [9-3](#)
 - stopping [9-6](#)
 - timeouts [6-4](#)
 - viewing generated ACLs [10-19](#)
 - virtual memory [8-2](#)
- cdat.jetty.xml [4-2](#)
- cdat.xml [3-15, 6-1](#)
- certificates
 - keystore [A-2](#)
 - SESM license [2-1](#)
- CHAP [C-7](#)
- Cisco Access Registrar [C-17](#)
- Cisco-AVpairs [C-9, C-15](#)
- Cisco IOS, required releases
 - captive portal features [11-1](#)
 - complete ID [10-4](#)
 - port-bundle host key [F-2](#)
 - TCP redirect commands [11-7](#)
- Clear Text Passwords [B-3](#)
- clients
 - RADIUS server [12-5, C-1](#)
 - RDP [2-14, 2-15](#)
 - restricted for bundled RADIUS server [D-5](#)
 - restricted for RDP [7-6](#)
 - SSG subnets [2-9](#)
- Client subnet attribute [2-9](#)
- cn [2-12, 5-6, 6-3, B-2](#)
- comments, in MBeans [3-11](#)
- common name
 - See cn
- complete ID [10-4, 10-5, 10-8](#)
- compressed images [2-2](#)
- concurrent services [C-7](#)
- config.xml [12-9](#)
- ConfigAgent [3-1, 3-16, 3-17, 5-19](#)
- configuration files
 - customizing [5-20](#)
 - DTD [3-15](#)
 - editing [3-14](#)
 - MBean [3-1](#)
 - names [3-14](#)
 - path names in web.xml [13-8](#)
 - See also J2EE; MBeans
- confirmAtAccountLogoff attribute [5-14](#)
- confirmAtServiceLogoff attribute [5-14](#)
- confirmAtServiceLogon attribute [5-14](#)
- confirmMutexDisconnect attribute [5-5](#)
- connections
 - See automatic connections;services; directory
- Connection MBean [8-3](#)
- connectionNameRoot attribute [8-2](#)

- console
 - installation mode [2-4](#)
 - iPlanet [B-6](#)
 - management [2-8, 3-5](#)
 - NDS (ConsoleOne) [B-2, B-3](#)
- constructing MBeans [3-17](#)
- containers
 - directory [2-12, 8-2, 12-8](#)
 - for port-bundle host key [4-1](#)
 - Jetty [4-2](#)
 - other than Jetty [4-2](#)
 - See J2EE containers
 - WAR files [4-2](#)
 - See also J2EE; Jetty server
- content applications [11-4](#)
- context
 - attribute [8-2](#)
 - directory [12-8](#)
 - iPlanet and Sun ONE [B-4](#)
 - NDS [B-1](#)
 - path attribute [4-5](#)
- cookies [6-1, C-8](#)
- core model [2-7](#)
- CPDURATION query parameter [11-3, 11-18](#)
- CPSUBSCRIBER query parameter [11-3, 11-25](#)
- CPURL query parameter [11-3](#)
- CPU utilization [9-7](#)
- credentialMaxLength attribute [5-14](#)
- credentials attribute, SPE [8-3](#)
- customApplications attribute [5-12](#)
- custom installations [2-7](#)
- customizing applications [2-20](#)
- customProtocols attribute [5-12](#)
- debugPatterns attribute [4-4, 5-2](#)
- debugThreads attribute [5-3](#)
- debugVerbosity attribute [5-3](#)
- defaultDuration attribute [11-15, 11-18](#)
- default network [F-2](#)
- defaultPage attribute [11-15](#)
- defaultURI attribute [5-14, 11-17](#)
- defaultURL attribute [11-15](#)
- defineServiceRedirect attribute [11-12](#)
- demo data file [11-14](#)
- demoDataFile attribute [5-6](#)
- Demo mode
 - attributes [5-4](#)
 - blocked services [C-14](#)
 - data [5-6](#)
 - installing [2-7](#)
 - profiles [C-13](#)
 - self-subscription [C-13](#)
 - single sign-on [C-14](#)
 - switching to [5-4](#)
- demos
 - arbitrary attributes [10-11](#)
 - location awareness [10-8](#)
- deployer-imposed firewalls [10-12, 10-25](#)
- deployment modes, switching [2-7](#)
- DESS
 - configuration file [3-15](#)
- dessauth.xml [3-15, 6-1, 8-1](#)
- DESSMode MBean [5-6, 11-14](#)
- DESSPrincipal attribute, SPE [8-2](#)
- DESSusecasedata.ldf file [8-4](#)
- destination
 - service [C-7](#)
 - URL [11-9](#)
- dictionary, RADIUS [C-2](#)
- direction attribute [5-13](#)
- directory
 - caching [8-2](#)
 - configuring for SESM [B-1](#)

D

- debug attribute [4-4, 5-2](#)
- debugging [4-3, 5-2, 13-4](#)
- Debug MBean [4-4](#)

connection information [2-11, 8-3](#)
 container [2-12, 8-2, 12-8](#)
 context [12-8](#)
 extending schema [2-19, 8-3](#)
 failover [8-3](#)
 installation results [2-20](#)
 IP address [2-11, 8-3, 12-8](#)
 logging activity [8-2](#)
 meta schema [2-12](#)
 organization [2-12, 12-8](#)
 password [2-11, 8-3](#)
 portal communication [12-9](#)
 ports [2-11, 8-3, 12-8](#)
 RDP communication [12-8](#)
 running during SESM install [1-6](#)
 sample data [8-4](#)
 user ID [2-11, 8-3, 12-8](#)
 Directory MBean [8-2](#)
 disconnecting autoconnect services [10-3](#)
 disconnectWhenUnsubscribe attribute [5-14](#)
 disk space [1-2](#)
 displayApplications attribute [5-13](#)
 distinguished name
 See dn
 dn [2-12, 5-6, 6-3](#)
 DNS [C-7](#)
 domain names [C-7](#)
 downloading SESM [2-2](#)
 DTD [3-15](#)
 dump attribute [7-5, D-4](#)
 duplicate locations [10-5, 10-6](#)
 duration
 advertising redirection [2-17, 11-22](#)
 initial logon redirection [2-17](#)
 parameters [11-17](#)
 in Cisco IOS commands [11-22, 11-23](#)
 in HTTP requests [11-3](#)
 in RADIUS profiles [C-12](#)
 timing of [11-4](#)

dynamic attribute definitions [C-5](#)
 dynamicAttributes attribute [7-4, D-4](#)

E

edge session, SSG [C-11](#)
 editing configuration files [3-14](#)
 encryption [A-2](#)
 erp.xml [7-3, D-1, D-3](#)
 error redirections [2-16](#)
 errorURL attribute [11-13](#)
 established keyword, in ACLs [10-20](#)
 evaluation licenses [2-6](#)
 example
 captive portal profiles [11-8](#)
 service group profiles [C-10](#)
 service profiles [C-9](#)
 subscriber profiles [C-15](#)
 examples
 ACLs [10-21, 10-23](#)
 profiles [C-19](#)
 exceptions, out of memory [9-8, 13-9](#)
 executables
 adding Windows services [9-7](#)
 installation [2-2](#)
 startup scripts [9-1](#)
 stop scripts [9-6](#)
 explicit IP address, SSG [5-9](#)
 extended access control lists [10-12](#)
 See also ACLs
 extending directory schema [2-19, 8-3](#)

F

factory attribute [8-2](#)
 failover, LDAP directory [8-3](#)
 features
 configuring [10-1](#)

filename attribute, in Log MBean [4-4](#)

files

- [.iss](#) [2-4](#)
- [.properties](#) [2-4](#)
- [aaa.properties](#) [5-6, C-19, D-1, D-4](#)
- [aaa.xml](#) [D-1, D-2](#)
- [captiveportal.jetty.xml](#) [3-14](#)
- [captiveportal.xml](#) [3-14, 11-10, 11-11, 11-24](#)
- [cdat.jetty.xml](#) [4-2](#)
- [cdat.xml](#) [3-15, 6-1](#)
- [dessauth.xml](#) [3-15, 6-1, 8-1](#)
- DESS configuration file [3-15](#)
- DESSusecasedata.ldf [8-4](#)
- [erp.xml](#) [7-3, D-1, D-3](#)
- installation image names [2-1, 2-2](#)
- installation results [2-20](#)
- J2EE configuration [3-18](#)
- keystore [A-2](#)
- [lib.xml](#) [6-1](#)
- [licensenum.txt](#) [2-6](#)
- MBean configuration [3-1](#)
- [messageportal.xml](#) [3-14, 11-13, 11-15](#)
- [nwsp.jetty.xml](#) [3-14, 4-2](#)
- [nwsp.xml](#) [3-14, 5-2, 11-16](#)
- [pda.jetty.xml](#) [3-14](#)
- [pda.xml](#) [3-14, 5-2](#)
- [rdp.xml](#) [3-14, 7-3](#)
- README.SESM.LDIF.html [2-20](#)
- [ssgconfig.txt](#) [11-7](#)
- startup scripts [9-3](#)
- [wap.jetty.xml](#) [3-14](#)
- [wap.xml](#) [3-14, 5-2](#)
- WAR [4-2](#)
- [web.xml](#) [2-20, 3-18](#)
- [web.xml](#) file [13-8](#)
- [webdefault.xml](#) [3-18](#)
- [webdefaults.xml](#) [3-18](#)
- [web-jetty.xml](#) [2-20, 3-19, 4-2](#)
- [xmlconfig.dtd](#) [3-15](#)

See also logs

Firewall MBean [5-11](#)

firewalls

- administrative [10-25](#)
- Advanced Firewall page [10-16](#)
- applications list [5-11, 5-12, 5-13, 10-17, 10-18](#)
- configuring [10-18](#)
- deployer-imposed [10-12, 10-25](#)
- description [10-12](#)
- established keyword [10-20](#)
- generated ACLs [10-19](#)
- My Firewall page [10-14](#)
- priorities [10-13](#)
- protocols [5-11, 5-12](#)
- subscriber experiences [10-25](#)
- viewing ACLs in CDAT [10-19](#)

See also ACLs

frames [C-8, C-12](#)

frequency, in advertisement redirections [11-22, C-12](#)

full name, in service profiles [C-8](#)

G

- generated ACLs [10-19](#)
- generic start script [9-4, A-3](#)
- global attributes, SSG [5-7, 5-16](#)
- greetings page
 - See initial logon redirection
- group password
 - See service groups
- groupPassword attribute [7-5](#)
- groups
 - captive portal [11-5, 11-7, 11-19](#)
- GUI installation mode [2-3](#)

H

handler attribute [7-5, D-4](#)

- handlers
 - port-bundle host key [4-2](#)
 - RDP [7-1, 7-8](#)
 - hardware platforms [1-1](#)
 - hierarchical policing [10-28, C-8, C-13](#)
 - hobbies, captive portal advertisement [11-8, 11-14, 11-16](#)
 - home
 - application [9-5](#)
 - JDK [1-4](#)
 - jetty [9-5](#)
 - home page, URLs [C-12](#)
 - host attribute [11-11](#)
 - HTML Adaptor server [3-3, 3-5](#)
 - HTML frames [C-8, C-12](#)
 - HTTP
 - configuring listener port [2-8](#)
 - errors [13-4](#)
 - mode, removing [A-3](#)
 - processing requests [11-2](#)
 - redirections [2-16, 11-3](#)
 - request log [13-4](#)
 - SocketListener [4-6, 4-7](#)
 - Version 1.1 [11-25](#)
 - HTTPS
 - description [A-2](#)
 - keystore [4-7](#)
 - keystore file [A-2](#)
 - running secure-only mode [A-3](#)
 - HttpServer MBean [4-5](#)
-
- inacls [10-16, 10-22](#)
 - inetorgPerson attribute [2-12](#)
 - initialCaptiveDuration attribute [11-12, 11-18](#)
 - initialCaptiveOn attribute [11-11, 11-24](#)
 - initialCaptivePort attribute [11-12](#)
 - initialCaptiveURL attribute [11-11](#)
 - initializing MBeans [3-17](#)
 - initial logon redirection
 - configuring [2-17, 11-11, 11-15, 11-22](#)
 - duration [2-17](#)
 - HTTP query parameters [11-3](#)
 - port [2-17](#)
 - profile attributes [C-12](#)
 - initial URL [10-11](#)
 - installing
 - captive portal solution [2-7, 2-15, 11-6](#)
 - CDAT [2-7, 2-19](#)
 - custom [2-7](#)
 - Demo mode [2-7](#)
 - directory [2-6](#)
 - image for [2-1](#)
 - individual components [2-7](#)
 - iPlanet [B-4](#)
 - JDK [1-5](#)
 - JRE [1-3](#)
 - license [2-6](#)
 - logging during [2-5](#)
 - Message Portal application [2-15](#)
 - modes [2-3](#)
 - NDS [B-1](#)
 - NWSP [2-8](#)
 - PDA [2-8](#)
 - portal applications [2-7](#)
 - prerequisites [1-1](#)
 - RDP [2-7, 2-13](#)
 - results [2-20, 11-6](#)
 - SESM components [2-7](#)
 - SPE [2-7](#)
 - Sun ONE [B-4](#)
- idle timeout
 - services [C-7](#)
 - sessions [C-11](#)
 - ignoreProfile attribute [11-15](#)
 - images
 - downloading installation [2-2](#)
 - referenced in JSPs [5-20](#)

temporary disk space for [1-2](#)
 typical [2-7](#)
 WAP [2-8](#)
 WSG [2-7](#)

interestPages attribute [11-16](#)
 interests attribute [11-14, 11-16](#)

Internet service, initial URL [10-11](#)

IP addresses

- Captive Portal application [2-15](#)
- directory [2-11, 8-3, 12-8](#)
- load balancing [E-1](#)
- location awareness [10-4](#)
- RADIUS server [2-10, 2-14, 12-4, 12-5](#)
- RDP [2-13, 12-7](#)
- RDP clients [2-15](#)
- SSG [2-9, 12-2, 12-3, F-3](#)
- troubleshooting RADIUS server [13-9](#)

IP attribute [5-9](#)

iPlanet

- Console [B-6](#)
- dn [2-12, 5-6, 6-3](#)
- installing [B-1, B-4](#)
- password [2-11](#)
- tree and context [B-4](#)
- uid [2-11, 2-12](#)

iss file [2-4](#)

J

J2EE containers [3-1, 4-1, 13-9](#)
 J2EE listeners, eliminating [11-5](#)
 Jasper JSP framework [2-20](#)

Java

- memory usage [13-9](#)
- memory use [5-5, 9-8](#)
- security [A-1](#)
- virtual memory [8-2, 9-8](#)

javadoc [2-20](#)

Java Management Extensions

See [JMX](#)

Java Secure Sockets Extension [A-2](#)

Java system properties

- See [system properties](#)

JAXP XML parser, installing [2-20](#)

JDK

- installing [1-5](#)
- locating [1-4, 13-6](#)
- messages at startup [13-7](#)
- preinstalled [13-7](#)
- SESM startup scripts [1-4](#)
- specifying location [1-4](#)

JDK_HOME [1-4, 1-5, 9-4](#)

jetty.home [4-5, 4-7, 9-5](#)

jetty.log [4-4, 13-4](#)

Jetty server

- certificates [A-2](#)
- configuring [4-2](#)
- installing [2-7](#)
- log files [13-4](#)
- port-bundle host key [4-1, 4-2](#)
- starting [9-1](#)
- stopping [9-6](#)
- troubleshooting [13-4, 13-9](#)
- See also [J2EE containers](#)

JIT relocation message [13-7](#)

JMX

- description [3-1](#)
- HTML Adaptor server [3-5](#)
- installing framework [2-20](#)
- path [2-20](#)
- server [3-1, 3-3, 5-19](#)

JRE

- installing [1-3](#)
- locating [1-4, 13-6](#)
- messages at startup [13-7](#)
- preinstalled [13-7](#)
- SESM startup scripts [1-4](#)
- specifications [1-3](#)

- specifying location [1-4](#)
 - JSPs
 - description [5-19](#)
 - framework path [2-20](#)
 - installing framework [2-20](#)
 - precompiling [2-20](#)
 - recompiling [1-5](#)
 - recompiling after changing [13-7](#)
 - JSSE [A-2](#)
 - JVM
 - arguments [9-8](#)
 - location [1-4, 9-4](#)
 - RDP [9-9](#)
 - jvm arguments
 - changing [13-9](#)
-
- K**
- KeyPassword attribute [4-7](#)
 - keys, next hop gateway [C-8, C-16](#)
 - keystore [4-7, A-2](#)
 - Keystore attribute [4-7](#)
 - keytool facility [A-2](#)
-
- L**
- LDAP directory
 - See directory
 - LDAP mode
 - communication attributes summary [12-6](#)
 - setting [5-4](#)
 - lib.xml [6-1](#)
 - license
 - obtaining number [2-1, 2-6](#)
 - types, for installation [2-6](#)
 - licensenum.txt file [2-6, 2-20](#)
 - links, on CDAT main window [2-19](#)
 - links attribute [6-3](#)
 - Linux
 - stopping applications [9-6](#)
 - supported platforms [1-1](#)
 - well-known locations for JRE [13-6](#)
 - load balancing [E-1](#)
 - configuring with SSG [E-1](#)
 - port-bundle host key [E-2](#)
 - SESM IP address for [E-1](#)
 - stickiness [E-2](#)
 - loads, SSG tuning [5-8](#)
 - LOCAL attribute [7-2](#)
 - locale [10-4](#)
 - LOCAL mode, RDP [7-2](#)
 - localPort attribute [7-6, D-5](#)
 - LOCATION attribute [10-5](#)
 - location awareness
 - compared to locale [10-4](#)
 - complete ID [10-4, 10-5, 10-8](#)
 - configuring [5-15, 10-4](#)
 - demonstrating [10-8](#)
 - description [10-3](#)
 - duplicates [10-6](#)
 - images [10-5](#)
 - IP subnets [10-4](#)
 - location names [10-5](#)
 - nested [10-6](#)
 - overlapping [10-6](#)
 - parameters [5-9](#)
 - URLs [10-11](#)
 - user shape [10-5](#)
 - Location MBean [5-15, 10-4](#)
 - locations attribute [5-15](#)
 - locationService attribute [5-15](#)
 - logDateFormat attribute [4-3, 5-3](#)
 - logFile attribute [5-3](#)
 - logFrame attribute [5-3](#)
 - Logger MBean [5-2](#)
 - logging off
 - portal applications [5-14](#)

- with automatic connections [10-3](#)
 - logging on
 - to AgentView [6-4](#)
 - to CDAT [6-3, 6-5, 8-3](#)
 - to portal applications [9-5](#)
 - to services [11-8, 11-11, 11-17](#)
 - with automatic connections [10-2](#)
 - logLabels attribute [4-3](#)
 - Log MBean [4-3](#)
 - logOneLine attribute [4-3](#)
 - logs
 - application.home [4-4, 9-5](#)
 - application.log [5-3, 13-4](#)
 - configuring [4-3, 5-2](#)
 - directory activity [8-2](#)
 - file names [13-4](#)
 - filenames [4-4, 5-3](#)
 - installation activity [2-5](#)
 - jetty.home [9-5](#)
 - jetty.log [4-4, 13-4](#)
 - Jetty server activity [4-3](#)
 - portal activity [5-2](#)
 - RDP console [7-5](#)
 - request.log [4-5, 13-4](#)
 - turning off [5-2](#)
 - logStack attribute [5-3](#)
 - logStackSize attribute [4-3](#)
 - logStackTrace attribute [4-3](#)
 - logTags attribute [4-3](#)
 - logThread attribute [5-3](#)
 - logTimeStamps attribute [4-3](#)
 - logTimezone attribute [4-3](#)
 - logToErr attribute [5-3](#)
 - configuring [3-5](#)
 - port [2-8, 3-5, 9-4](#)
 - removing [3-5](#)
 - starting [3-5](#)
 - See also HTML Adaptor server
 - ManagementConsole MBean [3-5, 5-3](#)
 - mapping SSGs to clients [5-7, 5-18](#)
 - MASK attribute [5-7, 5-9](#)
 - masks [2-9, 5-19](#)
 - MaxIdleTimeMs attribute [4-7](#)
 - maxIdleTimeMs attribute [4-6](#)
 - maximum length, usernames and passwords [5-14](#)
 - maximum transmission unit [C-8](#)
 - maxReadTimeMs attribute [4-6](#)
 - MaxThreads attribute [4-7](#)
 - maxThreads attribute [4-6, 7-6, D-5](#)
 - maxVariables attribute [6-4](#)
 - MBeans
 - AAA [5-10](#)
 - captiveportal [11-11](#)
 - CDAT [6-3, 7-3, 11-10, 11-13, D-2](#)
 - changing [3-1](#)
 - changing attribute values [3-2](#)
 - comments in [3-11](#)
 - ConfigAgent [3-17](#)
 - Connection [8-3](#)
 - constructing and initializing [3-17](#)
 - Debug [4-2, 4-4](#)
 - description [3-2, 3-17](#)
 - DESSMode [5-6, 11-14](#)
 - Directory [8-1, 8-2](#)
 - Firewall [5-11](#)
 - Jetty [4-2](#)
 - Location [5-15, 10-4](#)
 - Log [4-2, 4-3](#)
 - Logger [5-2, 7-3, 11-10, 11-13, D-2](#)
 - MainServlet [6-2](#)
 - ManagementConsole [5-3, 7-3, 11-10, 11-13, D-2](#)
 - messageportal [11-15](#)
-
- M**
- MainServlet MBean [6-2](#)
 - management.portno [9-5](#)
 - management console

- property tags in [3-11](#)
- RADIUSDictionary [7-4](#)
- RDP [7-4](#)
- read-only attributes [3-2](#)
- read-write attributes [3-2](#)
- Server [4-5](#)
- SESM [5-4, 11-14](#)
- SESMDemoMode [5-6, 11-14](#)
- SESMSocketListener [4-6](#)
- SESMSSLListener [4-7](#)
- SSG [5-7, 10-4](#)
- WebApp [5-13, 11-16](#)
- MBean View [3-4, 3-9](#)
- memory
 - argument in startup script [9-8](#)
 - directory cache [8-2](#)
 - exceptions [9-8, 13-9](#)
 - portal applications [5-5, 9-8](#)
 - RDP [9-9](#)
 - requirements summary [1-2](#)
 - reserved [9-8](#)
 - setting java virtual memory [9-8](#)
 - SSG [5-5, 7-2](#)
 - use [5-5, 9-8](#)
- memRequired attribute [5-5](#)
- message duration
 - See duration
- messageportal.host [11-11](#)
- messageportal.jetty.xml [3-14](#)
- messageportal.port [11-11](#)
- messageportal.xml [3-14, 11-13, 11-15](#)
- Message Portal application
 - configuring [11-15](#)
 - description [11-4](#)
 - installing [2-15](#)
 - ports [2-16](#)
 - running in secure mode only [A-4](#)
 - timing of durations [11-4](#)
- messageportal MBean [11-15](#)
- messageRedirectDurationParam attribute [11-13](#)
- messageRedirectSubscriberParam attribute [11-13, 11-25](#)
- messageRedirectURLParam attribute [11-13](#)
- messages
 - at startup [13-7](#)
- meta schema, directory [2-12](#)
- Microsoft Windows
 - adding and removing services [9-7](#)
 - platform specifications [1-1](#)
 - stopping applications [9-7](#)
- minimum length, usernames and passwords [5-14](#)
- MinThreads attribute [4-7](#)
- minThreads attribute [4-6, 7-5, D-4](#)
- missing files [13-8](#)
- mode
 - argument to startup scripts [9-2](#)
 - attribute [5-4](#)
 - concurrent service [C-7](#)
 - configuration setting [5-4](#)
 - console installation [2-4](#)
 - GUI installation [2-3](#)
 - installation [2-3](#)
 - RDP [7-2](#)
 - running secure-only mode [A-3](#)
 - sequential service [C-7](#)
 - silent installation [2-4](#)
 - switching deployment [2-7, 5-4](#)
 - system property [5-4](#)
- modes
 - RDP [7-2](#)
 - secure [A-3](#)
- monitoring applications [3-2, 3-12](#)
- MSISDN [C-11](#)
- MTU, PPP [C-8](#)
- multikey authentication [7-5, 10-28](#)
- mutually exclusive service groups [5-5, C-10](#)
- My Firewall page [5-11, 10-14](#)

N

naming attribute [2-12, 6-3](#)

NAS [C-1, C-2, C-11](#)

NDS

- Allow Clear Text Passwords [B-3](#)
- authenticating [B-3](#)
- container cn [2-12](#)
- directory cn [2-11](#)
- directory dn [2-12, 5-6, 6-3](#)
- directory password [2-11](#)
- installing [B-1](#)
- tree and context [B-1](#)

nested locations [10-6](#)

next hop

- gateway [C-8, C-16](#)
- password [2-13, 7-5, 12-4](#)

nextHopPassword attribute [7-5](#)

noSubscribePermissionURI attribute [5-14, 11-17](#)

Novell eDirectory

- See NDS

NWSP

- installing [2-7](#)
- port [2-8](#)
- role in captive portal solution [11-4](#)
- starting [9-1](#)
- virtual memory [8-2](#)

nwsp.jetty.xml [3-14, 4-2](#)

nwsp.xml [3-14, 5-2, 11-16](#)

O

organization, LDAP directory [2-12, 12-8](#)

original subscriber URL

- See URLs

outacls [10-16, 10-22](#)

out of memory exception [13-9](#)

out of memory exceptions [9-8](#)

overlapping locations [10-6](#)

P

PAP [C-7](#)

parent account, Demo mode [C-14](#)

passthrough services [C-7](#)

passwordMaxLength attribute [5-14](#)

passwordMinLength attribute [5-14](#)

passwords

- Allow Clear Text Passwords [B-3](#)
- attributes for RDP [12-7](#)
- directory [2-11, 8-3](#)
- directory container [2-12](#)
- keystore [4-7](#)
- length [5-14](#)
- next hop [2-13, 7-5](#)
- service [2-10, 2-13, 5-10, 7-5, 12-4, 12-5, 13-9](#)
- service group [2-10, 2-13, 7-5](#)

path names, of configuration files [13-8](#)

PDA

- application port [2-8](#)
- installing [2-7](#)

pda.jetty.xml [3-14](#)

pda.xml [3-14, 5-2](#)

permissions

- Demo mode [C-13](#)
- LDAP directory [2-11, 2-12](#)
- required for installation [2-3, 13-8](#)

persisting attribute changes [3-11](#)

personal firewalls [10-12](#)

platforms, hardware [1-1](#)

policies, mapping SSG to clients [5-7](#)

poolSize attribute [8-3](#)

PORT_BUNDLE_HOST_KEY_SWITCH attribute [5-8](#)

portals

- configuring [2-8, 5-1](#)
- CPU utilization [9-7](#)
- defined as NAS client [C-2](#)
- directory communication [12-9](#)
- J2EE containers [4-1](#)

- logging on [9-5](#)
- memory requirements [9-7](#)
- names [5-20, 9-3](#)
- ports [2-8](#)
- RADIUS communication [2-10, 12-5](#)
- running in secure mode [A-3](#)
- SSG communication [2-9, 12-2](#)
- starting [9-3](#)
- stopping [9-6](#)
- timeouts [5-8](#)
- troubleshooting [13-1](#)
- PORT attribute [5-7, 5-9, 12-2](#)
- PortBundleHandler [4-2](#)
- port-bundle host key
 - bundle length [5-8, 12-2, 12-3](#)
 - Cisco IOS release [F-2](#)
 - configuring [4-2, F-2](#)
 - description [4-1, 5-16](#)
 - IP addresses [F-3](#)
 - Jetty [4-1](#)
 - Jetty server [4-2](#)
 - load balancing [E-2](#)
 - location awareness [10-4](#)
 - port bundles [2-9, 5-18](#)
- port-lists [11-19](#)
- port-map [F-3](#)
- ports
 - accounting [C-1](#)
 - advertising redirection [2-17](#)
 - application.portno [9-5](#)
 - application.ssl.portno [9-5](#)
 - authentication [C-1](#)
 - Captive Portal application [2-15](#)
 - CDAT [2-19](#)
 - directory [2-11, 8-3, 12-8](#)
 - initial logon redirection [2-17](#)
 - Jetty listener [4-6](#)
 - management.portno [9-5](#)
 - management console [2-8, 3-5, 9-4, 9-5](#)
 - Message Portal application [2-16](#)
 - portal applications [2-8, 9-3, 9-5](#)
 - RADIUS server [2-10, 2-14, 5-10, 7-7, 12-4](#)
 - RDP [2-13, 12-7](#)
 - service redirection [2-18](#)
 - SSG [2-9, 5-7, 5-9, 12-2, 13-8](#)
 - SSL [2-8, 4-7, 9-4, 9-5, A-3](#)
 - startup scripts [9-3](#)
 - troubleshooting [13-9, 13-10](#)
 - unauthenticated user redirection [2-16](#)
- PPP
 - connections [11-20](#)
 - maximum transmission unit [C-8](#)
 - single sign-on [5-4](#)
 - subscriber profiles [C-12](#)
- precompiling JSPs [2-20](#)
- predefined attributes [C-3](#)
- prepaidRedirectionURL attribute [5-14, 11-16](#)
- primaryIP attribute [5-10, 7-7](#)
- primaryPort attribute [5-10, 7-7](#)
- principal attribute, SPE [8-3](#)
- printTraceToConsole, DESS [8-2](#)
- priorities, firewalls [10-13](#)
- privileges
 - See permissions
- profileCachePeriod attribute [5-5](#)
- profiles
 - ACLs [C-9, C-15](#)
 - caching [5-5](#)
 - defining new attributes [C-5](#)
 - examples [C-9, C-10, C-15, C-19](#)
 - for Demo mode [C-13](#)
 - next hop gateway [C-16](#)
 - PPP subscribers [C-12](#)
 - service [C-6](#)
 - service group [5-10, C-10](#)
 - subscriber [C-11](#)
- properties files [2-4](#)
 - See also system properties; aaa.properties file

Property tag, in XML files [3-11, 3-17](#)

protocols

CHAP [C-7](#)

handlers, RDP [7-8](#)

on firewall pages [5-11, 10-17](#)

PAP [C-7](#)

proxy

RDP mode [2-14, 7-2, 12-9](#)

service type [C-7](#)

Proxy mode, RDP [7-2](#)

Q

quality of service [10-28, C-8, C-13](#)

queryMaxResults attribute [6-4](#)

query parameters, HTTP redirections [11-3](#)

queryTimeout attribute [6-4](#)

R

RADIUS

\$ subattributes [C-13](#)

AAA MBean [5-10](#)

access accept messages [C-13](#)

attributes [7-4](#)

clients [12-5, C-1](#)

dictionary [7-4, C-2](#)

mode [5-4, 12-3](#)

password [F-2](#)

predefined attributes [C-3](#)

primary server [2-10, 2-14](#)

requirements for SESM installation [1-5](#)

secondary server [2-10, 2-14, 12-5](#)

RADIUS Data Proxy

See RDP

RADIUSDictionary MBean [7-4](#)

RADIUS server

accounting port [C-1, C-16](#)

authentication port [C-1](#)

bundled SESM [D-1](#)

installing bundled [2-7](#)

portal communication [2-10, 2-14, 12-5, 13-9](#)

RDP communication [12-10](#)

SSG communication [12-4, 13-9](#)

troubleshooting [13-9](#)

See also ports

radius-server parameter [13-10](#)

RADIUS shared secret

configuring on RADIUS server [C-2](#)

with portals [2-10](#)

with RDP [2-14](#)

with SSG [2-9](#)

RAM [1-2, 9-8, 9-9](#)

RBAC [2-19, 8-3](#)

RDP

adding clients [2-14, 7-6](#)

Add Services option [2-14, 7-2](#)

authentication [7-8](#)

automatic connections [5-5, 7-2, 10-2](#)

caching [10-3](#)

client IP addresses [2-15](#)

console messages [7-5](#)

defining new attributes [7-4](#)

directory communication [12-8](#)

handlers [7-1, 7-5](#)

installing [2-7, 2-13](#)

IP address [2-13, 12-7](#)

listeners [7-1](#)

LOCAL mode [7-2](#)

memory requirements [9-9](#)

modes [7-2](#)

next hop password [2-13, 7-5](#)

port [2-13, 12-7](#)

protocol handlers [7-8](#)

RADIUS communication [2-14, 12-10](#)

restricted client feature [2-13, 2-14, 7-6, D-5](#)

service password [2-13, 12-7](#)

shared secret [2-13, 2-14, 2-15](#)
 SSG communication [2-13, 12-7](#)
 starting [9-2](#)
 stopping [9-6](#)
 troubleshooting [13-3](#)
 virtual memory [8-2](#)
 See also Proxy mode; RDP
 rdp.xml [3-14, 7-3](#)
 RDP MBean [7-4](#)
 README.SESM.LDIF.html file [2-20](#)
 read-only attributes, in MBeans [3-2](#)
 read-write attributes, in MBeans [3-2](#)
 recompiling JSPs [1-5, 13-7](#)
 redirectOn attribute [11-15](#)
 refresh interval [3-2](#)
 registering MBeans [3-17](#)
 releases
 See Cisco IOS
 Reload button [3-10](#)
 reload interval [3-10](#)
 remote management tool [3-3](#)
 See also Agent View
 request.log [4-5, 13-4](#)
 reserved memory [9-8](#)
 restricted client feature
 See RDP
 retainDays attribute [4-4, 4-5](#)
 RETRIES attribute [5-7](#)
 retryCount attribute [5-10, 7-7](#)
 returnOption attribute [5-13](#)
 roles, loading [2-19](#)

S

sample LDAP data [8-4](#)
 schema, extending [2-19, 8-3](#)
 secondaryIP attribute [5-10, 7-7](#)
 secondaryPort attribute [5-10, 7-7](#)
 SECRET attribute [5-7, 5-9, 12-2](#)
 secret attribute [5-10, 7-6, 7-7](#)
 secure socket listener
 See SSL
 security [A-1](#)
 self-subscription, Demo mode [C-13](#)
 sequential service mode [C-7](#)
 Server MBean [4-5](#)
 servers
 See Jetty Server; J2EE; JMX; RADIUS Server
 service
 connection [5-14](#)
 cookies [C-8](#)
 destinations [C-7](#)
 groups
 in service profiles [C-12](#)
 mutually exclusive [5-5, C-10](#)
 password [2-10, 2-13, 5-10, 7-5, 12-5](#)
 profiles [C-10](#)
 idle timeout [C-7](#)
 logons [11-8, 11-11, 11-17](#)
 names [2-18, C-12](#)
 next hop gateway [C-8](#)
 object, SSG [C-7](#)
 passthrough [C-7](#)
 password [7-5](#)
 proxy [C-7](#)
 query parameter in HTTP redirection [11-3](#)
 routes [11-24](#)
 status [10-2](#)
 timeouts [C-7](#)
 tunnel [C-7](#)
 types [C-10](#)
 URL [11-3](#)
 See also automatic connections; profiles
 service group name, Demo mode [C-13](#)
 serviceGroup Password attribute [5-10](#)
 serviceLogonURI attribute [5-14, 11-17](#)
 serviceNotGivenURI attribute [2-18, 5-14, 11-4, 11-16](#)
 servicePassword attribute [5-10, 7-5](#)

- serviceportal.host [11-11](#)
- serviceportal.host system property [2-16](#)
- serviceportal.port [2-16, 11-11](#)
- service proxy [C-7](#)
- serviceRedirectDefaultURL attribute [11-9, 11-12](#)
- service redirection
 - configuring [2-18, 11-11, 11-20](#)
 - content application for [2-16](#)
 - HTTP query parameters [11-3](#)
 - logon pages [11-8](#)
 - ports [2-18](#)
 - service names [2-18](#)
 - service routes [11-24](#)
 - shared address space [11-21](#)
 - URL [11-12](#)
- serviceRedirectOn attribute [11-11, 11-24](#)
- serviceRedirectServiceParam attribute [11-13](#)
- serviceRedirectSubscriberParam attribute [11-13, 11-25](#)
- serviceRedirectURLParam attribute [11-13](#)
- serviceStartURI attribute [5-14, 11-17](#)
- serviceSubscriptionURI attribute [5-14, 11-17](#)
- serviceURL query parameter [11-3](#)
- sesm.mode [5-4](#)
- SESMDemoMode MBean [5-6, 11-14](#)
- SESM MBean [5-4, 11-14](#)
- SESMSession object [10-5](#)
- SESMSocketListener MBean [4-6](#)
- SESMSSLListener MBean [4-7](#)
- SESSION_BRAND [5-9](#)
- SESSION_LOCATION [5-9](#)
- sessionCachePeriod attribute [5-5](#)
- sessionTimeout attribute [5-14](#)
- sessionTimeout attribute [6-3](#)
- session timeouts [C-11](#)
- setSubnetAttribute call [5-9](#)
- setup type [2-7](#)
- shared address spaces, service redirection [11-21](#)
- shared secret
 - configuring on RADIUS [C-2](#)
 - description [12-3](#)
 - RADIUS and portals [2-10, 5-10, 7-7, 12-5, 13-9](#)
 - RADIUS and SSG [2-9, 5-7, 12-2, 12-4, F-2](#)
 - RDP and RADIUS [2-14](#)
 - RDP and SSG [2-13, 2-15, 12-7](#)
 - SSG and portals [13-8](#)
 - troubleshooting [13-10](#)
- silent installation mode [2-4](#)
- single sign-on [5-4, 10-3, C-14](#)
- singleSignOn attribute [5-4](#)
- SMTP redirection [C-13](#)
- Solaris
 - patches [1-3](#)
 - platform specifications [1-1](#)
 - stopping applications [9-6](#)
 - well-known locations for JRE [13-6](#)
- source ip command [F-3](#)
- space requirements [1-2](#)
- SPE
 - caching [8-2](#)
 - configuration file [8-1](#)
 - installing [2-7](#)
 - virtual memory [8-2](#)
- specifications
 - disk space [1-2](#)
 - Java [1-3](#)
 - RAM [1-2, 9-8, 9-9](#)
- SSG
 - clients to RDP [2-15](#)
 - complete ID [10-4, 10-5, 10-8](#)
 - configuring [2-9, 5-16, F-1](#)
 - defining as NAS client [C-2](#)
 - duration parameters [11-18](#)
 - edge session [C-11](#)
 - explicit IP address [5-9](#)
 - global attributes [5-7, 5-16](#)
 - IP address [2-9, 12-2, 12-3, F-3](#)
 - load balancing [E-1](#)
 - mapping clients [5-16](#)

- mapping policies [5-7](#)
- mapping subnets [2-9, 5-18](#)
- MBean [5-7, 10-4](#)
- memory [5-5, 7-2](#)
- port [12-2, 12-3](#)
- portal communication [2-9, 12-2](#)
- port-map [F-3](#)
- RADIUS server communication [12-4, 13-9](#)
- RADIUS server ports [2-9, C-1](#)
- RDP communication [2-13, 12-7](#)
- releases [10-4, 11-7, F-2](#)
- requirements during SESM installation [1-5](#)
- service object [C-7](#)
- shared secret [2-9, 2-13, F-1](#)
- subnet attributes [5-9, 5-16](#)
- tuning SESM loads [5-8](#)
- See also TCP redirections; port-bundle host key
- ssgconfig.txt [11-7, 11-8](#)
- SSGIPPolicyClass [5-7](#)
- SSL [2-8, 4-7, 9-4](#)
 - certificates [A-2](#)
 - port number [9-5](#)
 - running secure-only mode [A-3](#)
- stackTrace, DESS [8-2](#)
- starting
 - bundled RADIUS server [D-2](#)
 - CDAT [9-3](#)
 - error messages [13-7](#)
 - Jetty server [9-1](#)
 - portals [9-1](#)
 - RDP [9-2](#)
- startup scripts
 - application names in [5-20, 9-3](#)
 - application-specific [9-3](#)
 - captive portal [11-9](#)
 - customizing [5-20](#)
 - description [9-3](#)
 - failure [13-4](#)
 - generic [9-4](#)
 - HTTPS mode [A-3](#)
 - Java system properties [3-18, 9-4, 9-5](#)
 - JDK_HOME [1-4, 9-4](#)
 - JDK reference [1-4, 1-5](#)
 - JRE reference [1-4](#)
 - jvm arguments [9-8, 13-9](#)
 - memory [9-8, 9-9](#)
 - mode argument [9-2](#)
 - port references [9-3](#)
 - status, of services [10-2](#)
 - stickiness [E-2](#)
 - stopping SESM processes [9-6](#)
 - Store button [3-11](#)
 - subinterface, in location awareness [10-4](#)
 - subnet attributes, SSG [2-9, 5-9, 5-16](#)
 - subscriber name [11-3](#)
 - subscriber profiles
 - See profiles
 - Sun ONE
 - dn [2-12](#)
 - installing [B-1, B-4](#)
 - password [2-11](#)
 - tree and context [B-4](#)
 - uid [2-11, 2-12](#)
 - Sun Solaris
 - See Solaris
 - support, technical [2-6](#)
 - suppressStack attribute [4-4](#)
 - suppressWarnings attribute [4-4](#)
 - system properties [3-17, 9-4, 9-5](#)
 - SystemProperty tag, in XML files [3-11, 3-17](#)

T

 - tar files [2-2](#)
 - TCP redirections
 - configuring [11-7](#)
 - eliminating types [11-5](#)
 - SMTP forwarding [C-13](#)

types [11-3](#)

See also advertising redirection; initial logon redirection; service redirection; unauthenticated user redirection

technical support [2-6](#)

Telnet interface [F-3](#)

temporary disk space [1-2](#)

This [10-22](#)

THROTTLE attribute [5-8](#)

throttle attribute [5-10, 7-6](#)

timeOut attribute [5-10, 7-6](#)

timeouts

- CDAT [6-4](#)
- portals [5-8](#)
- service [C-7](#)
- service profile [C-7](#)
- session [C-11](#)

TIMEOUTSECS attribute [5-7](#)

tokenCheckInterval attribute [5-6](#)

tokenMaxAge attribute [5-6](#)

tools directory [2-20](#)

trace attribute [5-3](#)

traceFileName, DESS [8-2](#)

traceLevel, DESS [8-2](#)

tree, LDAP directory [12-8, B-1, B-4](#)

troubleshooting

- automatic connections [10-2](#)
- captive portal solution [11-23](#)
- CDAT [6-1](#)
- configuration file location [13-8](#)
- diagnostic procedures [13-1](#)
- JRE location [13-6](#)
- RDP [13-3](#)
- SESM portal applications [13-1, 13-8](#)
- web server [13-9](#)

tuning CDAT sessions [6-3](#)

tunnel services [C-7, C-9](#)

typical installation [2-7](#)

U

uid [2-12, 5-6, 6-3, B-4](#)

unauthenticated user redirection

- configuring [2-16, 11-11, 11-20](#)
- HTTP query parameters [11-3](#)
- port [2-16](#)

unavailable web server [13-9](#)

unconnected service redirection

- See service redirection

Undo button [3-11](#)

uninstalling SESM [1-6, 2-20](#)

unique identifier [2-12, 5-6, 6-3](#)

Unregister button [3-10](#)

URL

- initial [10-11](#)
- location-based [10-11](#)
- service redirection [11-12](#)
- unconnected service redirection [11-12](#)

URLs

- AgentView [3-6](#)
- attribute for LDAP server [8-3](#)
- destination, for service redirections [11-9](#)
- home page [C-12](#)
- service [C-8](#)
- subscriber's original
 - availability [11-6, 11-15](#)
 - Captive Portal application [11-3, 11-5](#)
 - duration before redirecting [11-17](#)
 - Message Portal [11-4, 11-12, 11-15](#)
 - parameter specifying [11-3, 11-13](#)

user

- groups, in Demo mode [C-13](#)
- ID, for directory [2-11, 8-3, 12-8](#)
- ID, for directory container [2-12, 8-2](#)
- shape [10-4, 10-5](#)

username

- full name in service profiles [C-8](#)
- length [5-14](#)

query parameter in HTTP redirection [11-3](#)
 usernameMaxLength attribute [5-14](#)
 usernameMinLength attribute [5-14](#)
 userRedirectOn attribute [11-11, 11-24](#)
 userRedirectPort attribute [11-12](#)
 userRedirectURL attribute [11-11](#)
 userRedirectURLParam attribute [11-13](#)

V

vendor-specific attributes
 See VSAs
 verbose attribute [4-4](#)
 virtual
 host name [4-5](#)
 memory [8-2, 9-8, 9-9](#)
 private dial-up network (VPDN) [C-9](#)
 VPI, location awareness parameter [10-4](#)
 VSAs [C-2, C-3](#)

W

WAP
 application port [2-8](#)
 installing [2-7](#)
 wap.jetty.xml [3-14](#)
 wap.xml [3-14, 5-2](#)
 WAR files [4-2](#)
 warning
 during installation [2-11](#)
 in log files [5-2](#)
 logging configuration attribute [5-3](#)
 web.xml [2-20, 3-18, 13-8](#)
 webapp directory [2-20](#)
 WebApp MBean [5-13, 11-16](#)
 web archive files
 See WAR files
 webdefault.xml [3-18](#)

WEB-INF directory [2-20](#)
 web-jetty.xml file [2-20, 3-19, 4-2](#)
 web portals
 See portals
 Web Services Gateway [2-7](#)
 Windows
 See Microsoft Windows
 WSG [2-7](#)

X

xmlconfig.dtd [3-15](#)
 XML files
 See J2EE configuration files; files
 X server [13-7](#)

Z

zip files [2-2](#)

