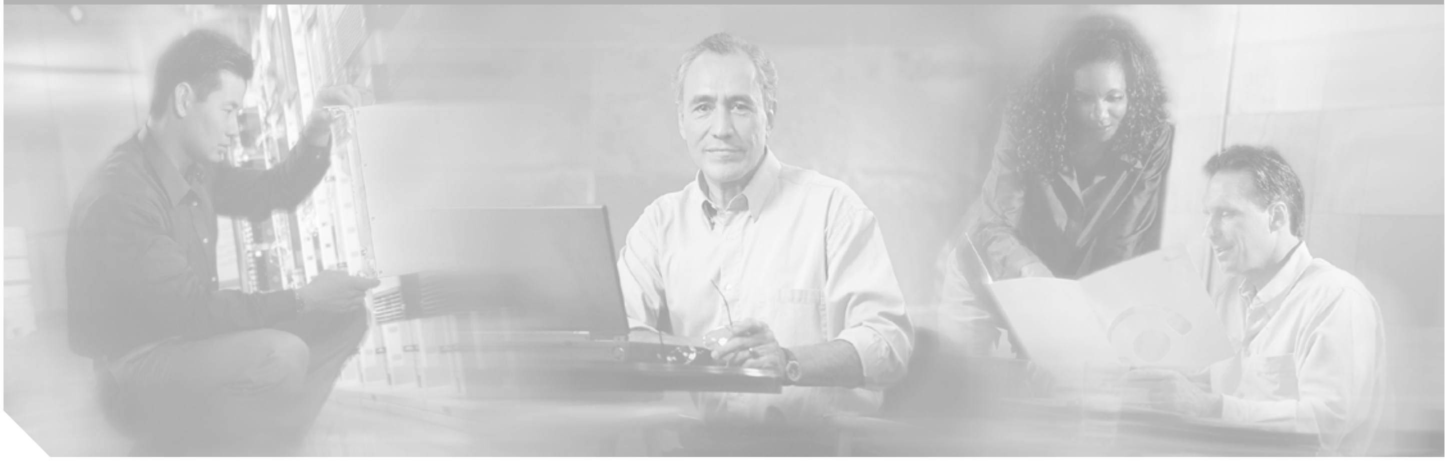


Cisco Subscriber Edge Services Manager Solutions Guide

SESM Release 3.1(9)
April 2003

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-2862-02

Cisco Subscriber Edge Services Manager Solutions Guide

CONTENTS

About This Guide

This preface introduces the *Cisco Subscriber Edge Services Manager Solutions 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 describes the features, capabilities, and deployment options of the Cisco Subscriber Edge Services Manager (Cisco SESM) product.

Audience

This guide is intended for anyone who is planning, managing, or customizing an SESM deployment or requires an understanding of SESM capabilities.

Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	SESM Introduction	Describes the components in the SESM product.
Chapter 2	SESM Features	Describes the features and capabilities of the SESM applications.

Chapter	Title	Description
Chapter 3	SESM Solutions for Service Selection and Connection with SSG	Describes the main features of the service selection and connection solution.
Chapter 4	SESM Solutions for Subscriber Self-Care	Describes the main features of the self-care solutions.
Appendix A	Establishing a Testing Environment for SESM	Describes the tools for establishing a testing environment for SESM deployments.
Appendix B	Using the SESM Web Services Gateway	Describes how to install, start, and use the WSG application and example client.
Index	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(9)*
- *Cisco Subscriber Edge Services Manager Solutions Guide*
- *Cisco Subscriber Edge Services Manager Quick Start Guide*
- *Cisco Subscriber Edge Services Manager Installation Guide*
- *Cisco Subscriber Edge Services Manager Deployment Guide*
- *Cisco Subscriber Edge Services Manager Web Portal Guide*
- *Cisco Subscriber Edge Services Manager Captive Portal Guide*
- *Cisco Subscriber Edge Services Manager RADIUS Data Proxy Guide*
- *Cisco Subscriber Edge Services Manager Troubleshooting Guide*
- *Cisco Subscriber Edge Services Manager Application Management Guide*

- *Cisco Distributed Administration Tool Guide*
- *Cisco Subscriber Edge Services Manager Web Developer 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 deployement, 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 a global, world-class, customer-focused, easy-to-use, highly integrated application for doing business with Cisco anytime, anywhere. Cisco.com helps 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, 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, have your service agreement number and your product serial number available.

CHAPTER 1

SESM Introduction

This chapter introduces the Cisco Subscriber Edge Services Manager (SESM). The chapter includes the following topics:

SESM Overview

The Cisco Subscriber Edge Services Manager (SESM) is an extensible set of applications for providing on-demand value-added services and access control at the network edge. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM solutions to provide value-added services to their subscriber base or management capabilities to their administrators.

SESM solutions consist of customized web portals that implement the deployer’s business model, show branded identities, offer customized and branded web page content, and control the subscriber experience with personalized web page content based on subscriber attributes such as location, access device, browser preferences, language, and interests. Captive portal features can further control subscriber experiences by capturing subscriber requests and redirecting browsers.

SESM Value-Added Services

Some examples of value-added services that can be offered through SESM portal applications are:

- One-stop, on-demand service selection—SESM supports service selection by issuing connection requests to a cooperating network access device.
- Network and service access control.

- Messaging and advertising—These services can be incorporated with other SESM solutions, such as service selection, or they can stand alone, for example, for a subscriber base whose only service is automatically connected Internet access.
- Subscriber account self-management and service self-subscription—These services allow individual subscribers to control and manage their account information. In SESM Release 3.1(5), these self-care applications require a deployment using an LDAP directory and the extensions provided by the Cisco Security/Subscriber Policy Engine (SPE) software. Self-care services can be incorporated with other SESM solutions or stand alone.
- Firewall provisioning—SESM provides the interface for subscribers to control traffic to and from their connection. The deployer can also issue traffic filters, which take precedence over the personal filters entered by subscribers.
- Profile provisioning—A customized SESM portal could act as an administrative tool to provision subscribers and push profiles or selected profile information to a RADIUS database or other operational support system (OSS).

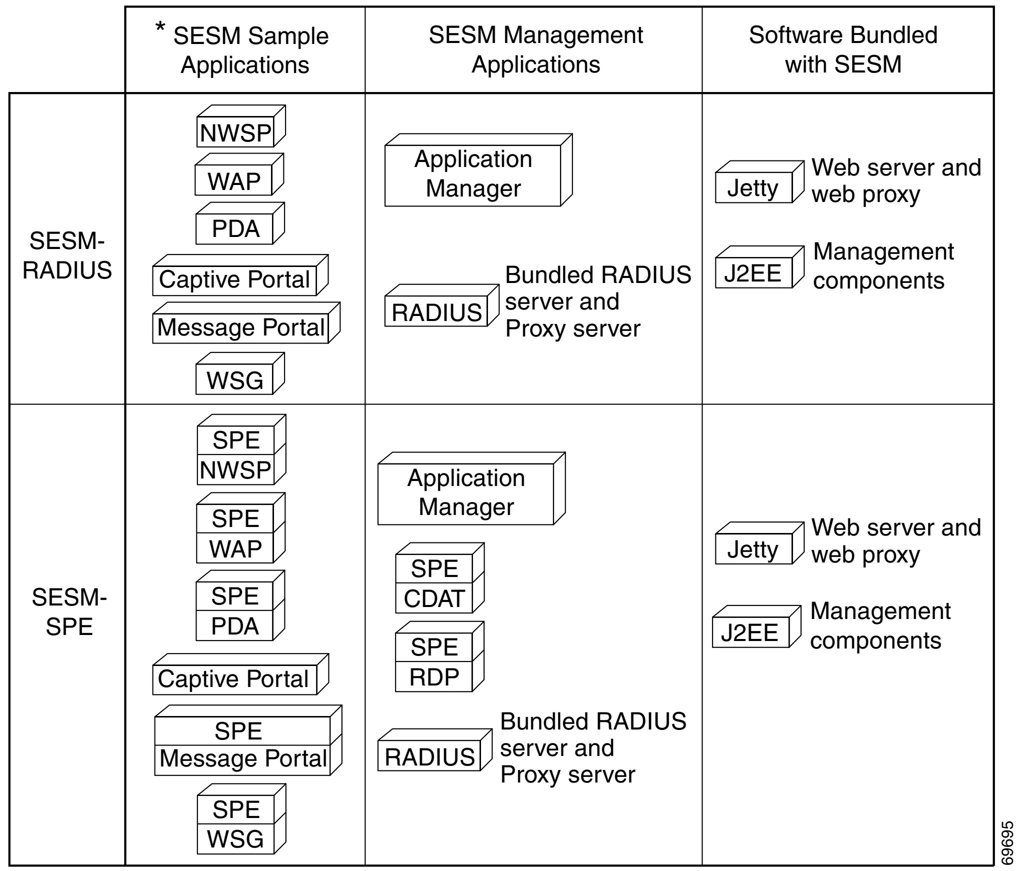
SESM Applications

SESM is an extensible Java2 Enterprise Edition (J2EE) compliant suite of applications and components for developing, deploying, and managing customized and branded web portal applications. SESM includes the following applications:

- Application Manager—A web-based tool from which administrators can view and change configuration attributes for running applications. Most changes are persisted across restarts.
- Cisco Distributed Administration Tool (CDAT)—A web-based tool from which administrators can maintain data in the SESM container in an LDAP directory
- RADIUS Data Proxy (RDP) server—A multipurpose RADIUS server that can transform RADIUS requests into SPE API calls to work with SPE extensions.
- Sample portal applications that you can install and configure for demonstration purposes or as a starting point for customizations:
  - New World Service Provider (NWSP) portal—A comprehensive example of most features offered by the SESM web development kit.
  - Wireless Access Protocol (WAP) portal—Designed specifically for deployment in the mobile wireless industry.
  - Personal Digital Assistant (PDA) portal—Shows web pages formatted for a PDA device.
- Sample captive portal solution—Includes the following applications:
  - Captive Portal application—A gateway application for use with the SSG and other applications in a captive portal solution. The default configuration for this application redirects subscriber browsers to either the Message Portal application or the NWSP application.
  - Message Portal application—Produces sample greetings and advertising pages to demonstrate SESM captive portal features.
- Bundled SESM RADIUS server—A RADIUS server that reads and processes profiles in Merit format. This server is useful for developing and testing SESM customizations.
- Web Services Gateway (WSG)—The Web Services Gateway (WSG) application enables third-party web portals and subscriber management systems to integrate with the SESM and SSG solution.

Figure 1-1 shows the software included with SESM.

Figure 1-1 SESM Package Contents



* Includes SESM platform development kit

SESM Architecture

SESM solutions can be deployed independently of the access network, access type and access device. Subscribers access SESM portals using any Internet browser on any access device. They do not need to download any software or plug-ins. Supported access technologies include:

- Laptop and pocket organizer access over 802.11b
- Mobile phone access over General Packet Radio Service (GPRS)
- Digital Subscriber Line (DSL) modems
- Desktop system access over leased lines

Supported protocols include:

- Point-to-Point Protocol (PPP) over ATM or Ethernet
- Routed or Bridged Ethernet
- RFC 1483 (Multiprotocol Encapsulation over ATM)
- Wireless LANs

SESM is inherently scalable with a stateless architecture to support transparent load balancing and failover. SESM applications can run on any platform that supports the Java Runtime Environment (JRE). Platforms tested in our labs include Sun Solaris, Windows NT, Windows 2000, Red Hat Linux, and SuSE Linux.

SESM Component Descriptions

This section describes the SESM applications.

Application Manager

The SESM Application Manager is a web application that remotely manages SESM applications. It can manage multiple instances of SESM web portal and captive portal applications, RDP, CDAT, WSG, and other Application Manager instances. From a web-based GUI interface, administrators can view and change values for most attributes in the configuration files for these applications. They can also monitor application status.

CDAT

The Cisco Distributed Administration Tool (CDAT) is a web-based management tool for administrators. CDAT is a J2EE web application. It runs in a J2EE container and uses the services of a JMX server for configuration.

With CDAT, administrators can manage data in the SPE extensions to an LDAP directory. CDAT provides the means for creating and maintaining users, services, user groups, service groups, roles, and policy rules for the RBAC model.

RDP Server

The RADIUS Data Proxy (RDP) server is a RADIUS server that you can configure to:

- Map RADIUS protocol requests to LDAP protocol requests with SPE extensions—The RDP configured in this manner is a required element in any SESM deployment that includes an LDAP directory.
- Proxy RADIUS requests to another RADIUS server—The RDP sends user authentication requests to a specified RADIUS server, rather than to the LDAP directory. This option allows service providers with large RADIUS authentication and accounting services already deployed to continue to use the existing RADIUS database for authenticating subscribers. However, RDP obtains all service profile and service authorization information from an LDAP directory.

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

Web Development Kit

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

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

Sample Portal Applications

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

The SESM sample applications are fully functioning web applications that were built using the SESM development library. These applications use the services of the Jetty web server and the JMX management server.

The sample portals installed with SESM are:

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

  Deployers can customize this application to detect the type and make of various WAP devices used by their subscribers, and tailor the pages to the features of each device.
- The Personal Digital Assistant (PDA) portal illustrates web pages formatted for a PDA device. Service self-subscription features (usable only in SPE mode) are included.

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

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

Sample Captive Portal Solution

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

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

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

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

Bundled SESM RADIUS Server

All of the SESM packages include the bundled SESM RADIUS server. The SESM RADIUS server is suitable for developing, testing, and demonstrating SESM deployments. It reads and updates profiles in a Merit flat file format.

The bundled SESM RADIUS server comes with the following attributes internally predefined:

- Standard RADIUS attributes
- Cisco SSG VSAs

A configuration feature, the RADIUSDictionary MBean, lets you easily define additional attributes.

Bundled J2EE Components

The following J2EE components are bundled with SESM:

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

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

  The sample SESM portal applications and CDAT are installed with configuration files and startup scripts that are ready to run using the Jetty web server and the Sun example JMX server. RDP is installed with configuration files and a startup script that is ready to run using the JMX server.
- Jetty web server—Jetty is a J2EE-compliant server package from Mort Bay Consulting that is released under an open source license. The license puts few restrictions on usage of Jetty. For more information about the Jetty server, see:

  http://jetty.mortbay.org/

- JSP engine—The Jasper Java Server Pages (JSP) engine from Apache Software Foundation, Servlets Version 2.3 and JSP Version 1.2.

Related Software

This section describes the software components, in addition to the SESM applications, that might be required in SESM deployments. Each SESM solution has its own requirements regarding these components.

J2EE Components

The SESM applications require J2EE-compliant servers. The SESM packages bundle suitable J2EE components required for running the SESM applications.

Note The SESM packages do not include a Java Software Development Kit (JSDK), which is required for SESM development. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for recommended JSDK version numbers.

J2EE Server Requirements

The SESM portal applications and CDAT are J2EE applications. They require an HTTP (or HTTPS) listener and must run in a J2EE-compliant server container. RDP does not run in a J2EE server container.

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

Note Before deploying a J2EE server other than the Jetty server, determine whether your SESM solution requires the port-bundle host key feature on the Cisco Service Selection Gateway. The Jetty server is currently the only server that supports this feature. See the *Cisco Subscriber Edge Services Manager Deployment Guide* for more information.

JMX Server Requirements

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

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

Cisco Security Policy Engine

The Cisco Security Policy Engine (SPE) is required in solutions that incorporate:

- Subscriber self-care features
- Profile management in an LDAP directory

SPE software is bundled in the SESM-SPE package.

Introduction to Cisco SPE

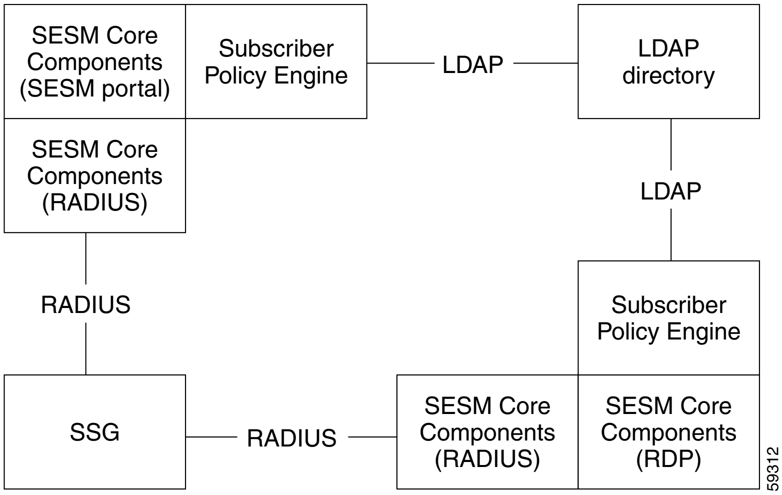
The Cisco Subscriber Policy Engine (SPE) is a policy server specifically customized to provide granular subscriber service policy. SPE combines role-based access control (RBAC) functionality with an open policy server. Service providers can create differentiated subscriber groups. Service and content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

SPE is required when SESM is deployed in SPE mode to provide the following enhanced features and capabilities:

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

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

Figure 1-2 SESM Components in SPE mode


SESM Core Components (SESM portal)
Subscriber Policy Engine
LDAP
LDAP directory
SESM Core Components (RADIUS)
LDAP
RADIUS
Subscriber Policy Engine
SSG
RADIUS
SESM Core Components (RADIUS)
SESM Core Components (RDP)
59312

SPE Software

The SESM-SPE package includes SPE. When you install applications in SPE mode using the SESM-SPE package, the installation includes the following items:

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

See the *Cisco Distributed Administration Tool Guide* for information about the RBAC model, the DESS and AUTH extensions to an LDAP directory, and how to develop subscriber and service profile information in the RBAC model.

Cisco Service Selection Gateway

The Cisco Service Selection Gateway (SSG) is a software feature module embedded in the Cisco IOS software. SESM solutions that perform service connection require the SSG. SSG can operate in standalone mode to provide Layer 2 service connection support, or it can be configured to work with SESM, which offers enhanced service-related features to subscribers.

In SESM deployments, SSG performs authentication and service connection tasks on behalf of the SESM portal. Other SSG features important in SESM deployments include:

- SSG Port-Bundle Host Key—Uniquely identifies each subscriber, which provides SESM with the following benefits:
  - Supports subscribers using overlapping and shared IP addresses
  - Eases SESM configuration by eliminating SSG to SESM server mapping requirements
- SSG TCP Redirect for Services—Enables providers to implement a captive portal, own the user experience, build a brand experience, and provide:
  - User authentication without the user needing to know the SESM URL
  - Advertising and messaging features
- SSG Open Gardens—Enables providers to specify domains that subscribers can access without service subscription (free services).
- SSG Hierarchical Policing—Ensures that a subscriber does not utilize additional bandwidth for overall service or for a specific service that is outside the bounds of the subscriber's contract with the service provider.
- SSG Prepaid—Enables real-time billing with maximum flexibility, regardless of the type of service and billing scheme. Users can be billed on a flat rate, air-time, or volume basis.
- SSG Auto logoff—Enables per-minute billing plans for services. SSG auto logoff also prevents subscribers from being charged for services that they are not able to access.

See the following SSG documentation for descriptions of these and other SSG features:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/

The SSG runs on a Cisco router or other Cisco device. The Cisco SSG feature is currently supported on the following platforms:

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

RADIUS Server

SESM works with any RADIUS server that accepts vendor-specific attributes (VSAs). Cisco VSAs define the subscriber and service profile information required in the SESM deployments. One RADIUS server to consider in your deployment is the Cisco Access Registrar, a carrier class RADIUS platform that is fully tested with SESM.

The *Cisco Subscriber Edge Services Manager Deployment Guide* describes the Cisco VSAs used in SESM deployments. The guide also describes how to configure a RADIUS server for SESM deployment, including specific information regarding the Cisco Access Registrar.

LDAP Directory

SESM portal applications deployed in SPE mode require access to an LDAP-compliant directory or relational database management system.

Some LDAP directories to consider in your deployment are:

- iPlanet Directory Server Version 5.0 (Also known as Sun ONE) from Sun Microsystems.
- Network Directory Service (NDS) eDirectory Version 8.5 from Novell, Inc.

The *Cisco Subscriber Edge Services Manager Deployment Guide* describes how to configure an LDAP server for SESM deployments, including specific information regarding iPlanet and NDS.

Supported Platforms

This section describes the application servers and browsers for SESM deployments.

Application Servers

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

Note The SESM applications include the web portal applications, the Captive Portal application, RDP, and CDAT.

Table 1-1 Server Systems for the SESM Applications

Platform	Specifications
Solaris	• Sun Ultra10 or Sun E250 (or later version) • Solaris Version 2.6 (or later version) operating system
Windows NT	• Pentium III (or equivalent) processor • Windows NT Version 4.0, Service Pack 5 (or later version)
Windows 2000	• Pentium III (or equivalent) processor
Linux	• Red Hat Linux Version 7.1 • SuSE Linux

Browsers

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

Table 1-2 lists the browsers and devices for which the SESM sample portal applications are designed. The *Cisco Subscriber Edge Services Manager Web Developer Guide* includes information about obtaining and configuring simulators.

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

Table 1-2 Browsers for the SESM Sample Portal Applications

SESM Portal Application	Device	Other Requirements
NWSP Message Portal	• Desktop browsers – Netscape Release 4.x and later – Internet Explorer Release 5.x and later • WAP devices and simulators • PDA devices and simulators	• Java script enabled
WAP	WAP devices and simulators	
PDA	PDA devices and simulators	

SESM Packages

The SESM software is available in the following packages.

- SESM-SPE—This package integrates the Cisco Subscriber Policy Engine (SPE) product with the SESM product. SPE provides access to an LDAP compliant directory or relational database management system (RDBMS) for maintaining subscriber and service information. In addition, the SPE role-based access control (RBAC) model facilitates bulk administration of large subscriber populations.

  SPE also provides self-care functionality for SESM web applications, including:

  - Subscriber account registration
  - Subscriber account self-care
  - Subscriber subaccount management
  - Subscriber self-subscription to services

  Various proxy options available with the SESM RADIUS Data Proxy (RDP) component permit the integration of existing RADIUS infrastructure. Domain-based proxying can proxy to multiple servers, based on the IP domain in subscriber and service names.

- SESM-RADIUS—This package installs SESM to obtain subscriber and service information using the RADIUS protocol.

  This package does not support the self-care features listed above and firewall provisioning. To combine those features with existing RADIUS infrastructure, use a SESM-SPE package with proxy options.

Each package is available in versions appropriate for the Sun Solaris, Linux, or Windows platforms.

Subscriber and Service Profiles

SESM solutions require detailed data about subscribers and the services they are authorized to use. We refer to this data as profiles:

- Subscriber profiles—Define authentication information, subscribed services, and information about connection and service options and preferences for each subscriber.
- Service profiles—Define connection information for the services that subscribers can subscribe and connect to.

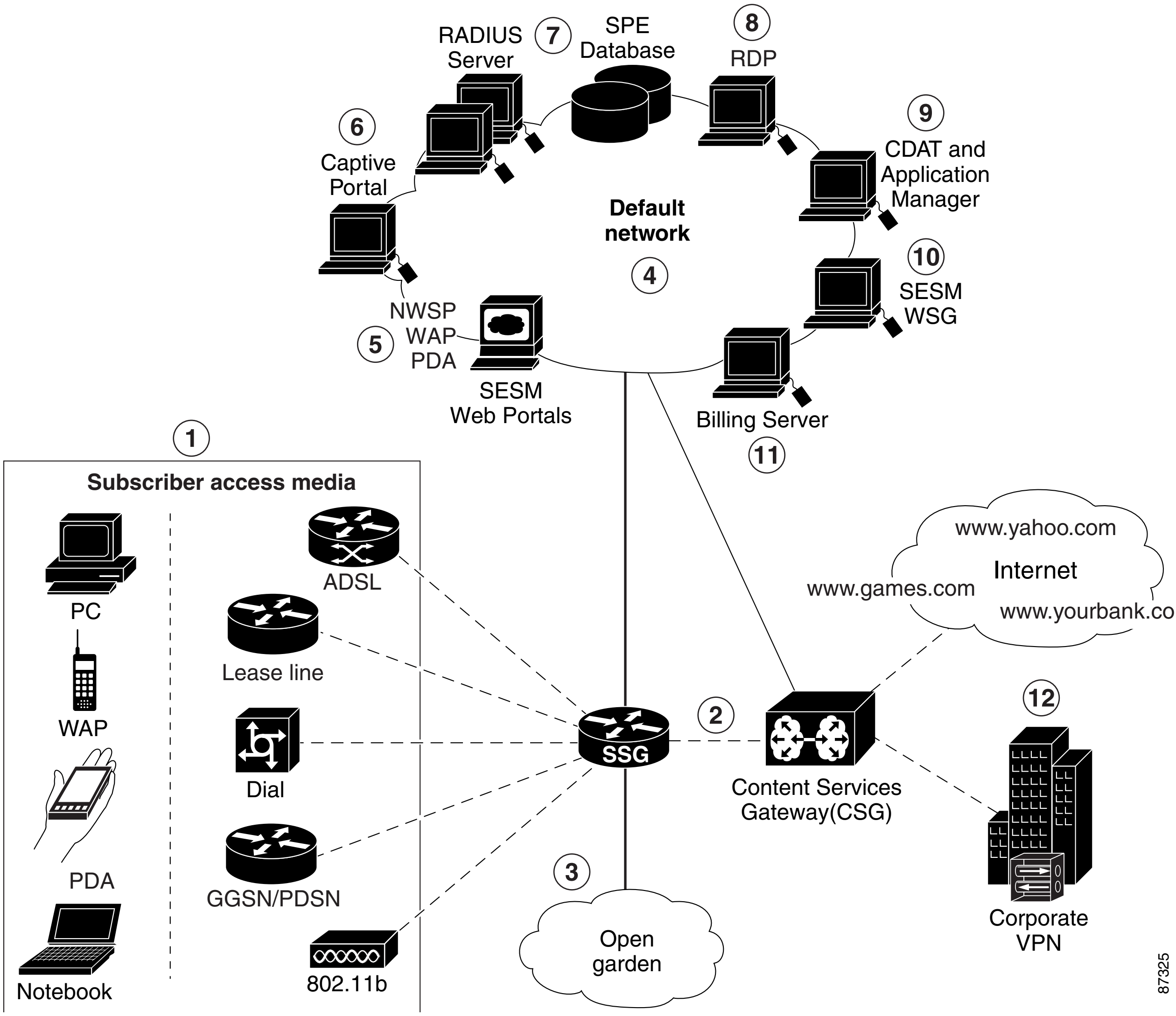
The SESM solution integrates with any one or a combination of the following options to obtain subscriber and service data:

- An AAA database managed and accessed by a RADIUS server.
- An SPE database (an LDAP directory or RDBMS) accessed through the Cisco SPE application programming interface (API). In SESM deployments, the Cisco Distributed Administration Tool (CDAT) manages the subscriber and service profiles in the database.
- A flat file in Merit format, accessed by an appropriately configured RDP application or SESM portals running in Demo mode.

SESM Reference Network Diagram

The following figure shows SESM applications in a hypothetical deployment. Actual deployments might not use all of the components shown.

Figure 1-3 SESM Network Diagram



1	Subscriber access media—SESM applications and solutions are independent of the access media.
2	Service Selection Gateway (SSG)— Most SESM solutions work with and require a Cisco gateway such as the SSG. The SSG is a feature in the Cisco IOS software running on a Cisco device. The SSG provides authentication, service connection, connection management, and SESM session capabilities. The SESM portals provide the subscriber's interface to SSG for those services. Content Services Gateway (CSG)—An optional gateway that provides content billing services to the SESM solution.
3	Open garden—The open garden is an SSG feature that allows subscriber access to preconfigured networks without authentication. Packets destined for open garden networks are not accounted for nor subject to access control by the SSG.

4	Default network—The SESM applications must run on systems on the SSG default network. The default network (and open gardens, if configured) are always accessible to subscribers.
5	SESM web portals—Subscribers access the SESM portal using a web browser. The portal provides the following features: subscriber interface to SSG; one-stop access to services; location-based branding; firewall provisioning; access to the Cisco Subscriber Policy Engine (SPE) self-care features such as registration, service subscription, account maintenance, and subaccount management. The access provider (the SESM deployer) presents these features on personalized browser pages shaped by dimensions such as access device, language preference, and location. The SESM packages include three sample web portal applications: New World Service Provider (NWSP), Wireless Access Protocol (WAP), and Personal Digital Assistant (PDA). The captive portal applications are also SESM web portals.
6	Captive portals—Captive portal applications are specialized SESM web portals that work with the SSG and other SESM web portals to capture, analyze, and redirect packets for various purposes, including messaging, advertising, or displaying logon pages in response to unauthenticated access attempts and unconnected service requests.
7	Profiles—SESM solutions are based on subscriber and service data stored in RADIUS or SPE databases.
8	SESM RADIUS Data Proxy (RDP)—The RDP application is a RADIUS server compliant with RFC 2865 and is the required RADIUS server for SESM SPE-mode deployments. RDP provides access to profiles on the SPE database. Deployers can configure RDP to proxy requests to other RADIUS servers or flat files. Domain-based proxying forwards requests to multiple RADIUS servers based on the IP domain in subscriber and service names.
9	Cisco Distributed Administration Tool (CDAT)—CDAT is a web-based GUI tool for managing the SPE extensions in an LDAP directory. CDAT provides the means for creating and maintaining user (subscriber) and service profiles, user groups, service groups, roles, and policy rules for the RBAC model. Application Manager—The Application Manager is a web-based GUI for remotely managing SESM applications in a distributed deployment. The managed applications can be SESM web portals, captive portals, RDP, CDAT, WSG, and the Application Manager itself. Administrators use the Application Manager to access the configuration attributes in the Java Management Extensions (JMX) MBeans used by these SESM applications.
10	Web Services Gateway (WSG)—The SESM WSG application provides a Simple Objects Access Protocol (SOAP)-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. Any client application can interface with SSG through the WSG using SOAP over HTTP communication.
11	Billing server—A third-party billing server is required if the SSG Prepaid feature is included in the solution.
12	Services—SESM applications work in conjunction with the Cisco gateway components to provide a one-stop interface for activating multiple services. SESM can provide the activation interface for any service type supported by the gateway component. Service information exists in the service profiles.

SESM Application Management

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

`http://java.sun.com/products/JavaManagement`

A brief introduction to JMX terminology and its relationship to SESM application management follows:

- JMX manageable resources—Java objects instrumented to allow spontaneous management by any JMX compliant agent. Each SESM application contains JMX manageable resources.
- JMX agent— A management entity implemented in accordance with the JMX Agent Specification. For SESM, the agent is the Cisco ConfigAgent.
- Managed beans (MBeans)—Java objects that represent a JMX manageable resource. MBeans for each SESM application are specified in XML files installed in the application's config directory under the SESM installation directory.

- JMX server (also called the MBean server)—A registry for objects that are exposed to management operations by an agent. Any object that is registered with the JMX server becomes visible to the agent. In SESM applications, MBeans are registered by the ConfigAgent or by other MBeans.

Administrators can change SESM application configuration by changing the attribute values in MBeans. In SESM Release 3.1(9), use any of these ways to change MBean attribute values:

- Use the Application Manager, a web-based GUI tool. This is the preferred way to manage running SESM applications. The tool includes:
  - Operational scenarios that present the most-used attributes for quick access and adjustments.
  - Advanced screens that present all attributes.
  - A bulk upload feature for importing large mappings of subscriber subnets to SSGs.
- Manually edit the XML files associated with the application. XML files are located in the application's config directory (for example, nwsp/config/nwsp.xml). If you use this method, you must stop and restart the application before the changes take effect.
- Use the SESM Agent View, a web-based view of managed resources and associated MBeans. The Agent View is an adaptation of the Management Console provided by the HTML adaptor server, which is included with the Sun example JMX server. The Cisco adaptations add persistence features to the server.

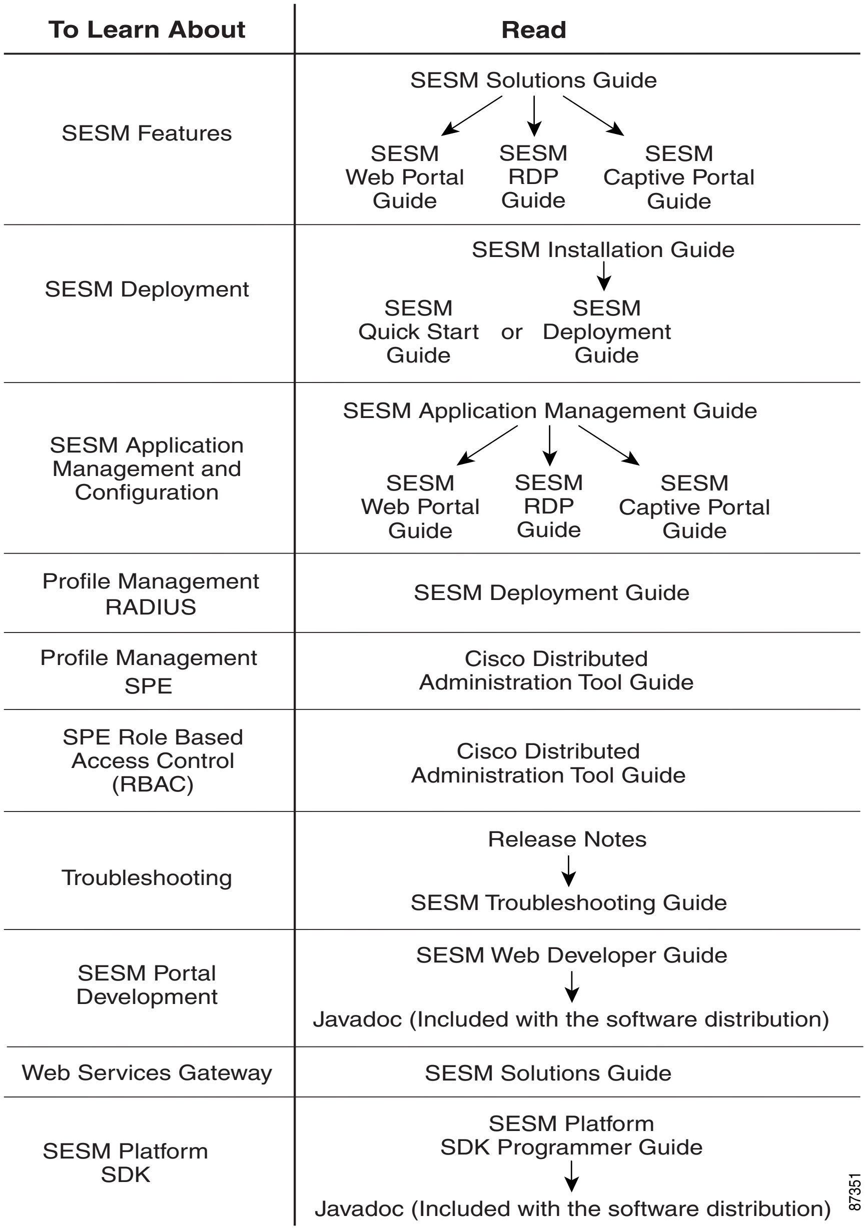
Note The Application Manager replaces the SESM Agent View. The Agent View is included in SESM Release 3.1(9) to provide convenience and continuity during migrations from previous releases.

SESM Documentation Map

Figure 1-4 can help you to locate information in the SESM documentation set. Go to the following URL to access the online version of the SESM documentation:

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

Figure 1-4 SESM Documentation Map



To Learn About	Read
SESM Features	SESM Solutions Guide ↙ ↓ ↘ SESM Web Portal Guide SESM RDP Guide SESM Captive Portal Guide
SESM Deployment	SESM Installation Guide ↓ SESM Quick Start Guide or SESM Deployment Guide
SESM Application Management and Configuration	SESM Application Management Guide ↙ ↓ ↘ SESM Web Portal Guide SESM RDP Guide SESM Captive Portal Guide
Profile Management RADIUS	SESM Deployment Guide
Profile Management SPE	Cisco Distributed Administration Tool Guide
SPE Role Based Access Control (RBAC)	Cisco Distributed Administration Tool Guide
Troubleshooting	Release Notes ↓ SESM Troubleshooting Guide
SESM Portal Development	SESM Web Developer Guide ↓ Javadoc (Included with the software distribution)
Web Services Gateway	SESM Solutions Guide
SESM Platform SDK	SESM Platform SDK Programmer Guide ↓ Javadoc (Included with the software distribution)

CHAPTER 2

SESM Features

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

- Service Selection and Connection Features with SSG, page 2-1
- Self-Care Features with SESM-SPE, page 2-5
- Captive Portal, Messaging, and Advertising Features, page 2-6
- Authentication Options, page 2-8
- Web Development Features, page 2-10
- SESM Location and Brand Awareness Features, page 2-11
- SESM Management Features, page 2-13
- Scaling, Redundancy, and Resiliency Features, page 2-15
- Accounting and Billing Interfaces, page 2-15
- Web Proxy Support, page 2-16
- Using the Web Services Gateway with Third-Party Portals, page 2-16

Service Selection and Connection Features with SSG

In solutions that use the Cisco Service Selection Gateway (SSG) to provide service connections, the SESM portal presents a service list from which the subscriber can select one or more services for connection. The connection features are implemented by SSG and controlled by attributes stored in the subscriber or service profiles. This section describes the following features:

- Service Selection from SESM Portals, page 2-2
- Service Authentication and Authorization, page 2-2
- Automatic Connections and Hidden Services, page 2-2
- Subscriber Sessions, page 2-3
- Service Status, page 2-3
- Mutually Exclusive Service Selection, page 2-4
- Service Selection by Bandwidth, page 2-4
- Supported Service Types, page 2-4

Service Selection from SESM Portals

In a service selection and connection solution, the SESM portal provides the web interface from which subscribers can:

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

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

When SESM is deployed in SPE mode, self-care features can also be offered to subscribers. See the "Self-Care Features with SESM-SPE" section on page 2-5 for more information.

Service Authentication and Authorization

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

The SESM web portal can present a service authentication page for services that require it. Service authentication can be based on user name and password. For proxy services, an option in the service profile specifies whether the CHAP or PAP protocol is used to authenticate for the service. For more information, see the chapter about RADIUS profiles in the *Cisco Subscriber Edge Services Manager Deployment Guide*.

Automatic Connections and Hidden Services

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

A hidden service is an automatically connected service that does not appear on the SESM service selection page.

A service is marked as an autoconnect service in the subscriber profile. By default, an autoconnect service is also a hidden service. Another entry in the subscriber profile can specify that the autoconnected service be included in the service selection list.

In SPE mode, the SESM portal can offer the subscriber the means to self-select or change the services that should be automatically connected and hidden.

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

Subscriber Sessions

When a subscriber successfully logs onto the SESM portal, the SSG creates an edge session for the subscriber on the SSG host platform. The session lasts until the subscriber logs off of SESM. The SSG keeps track of session status.

If the SSG port-bundle host key feature is not enabled, the SSG uses the subscriber IP address to identify a session.

If the port-bundle host key feature is enabled, the SSG uses a unique key to identify each currently logged-on subscriber, regardless of the IP address being used. The port-bundle host key is an optional feature on SSG. When enabled, the feature allows SESM portals to support the following types of subscribers:

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

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

Service Status

SESM portals can show service status in two ways.

- Status and connection metrics
- Service list images

Status and Connection Metrics

The SESM portal can display status and metrics about services that were connected during the current session. The web developer controls the types of status information and how it is presented. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information.

The sample status page in NWSP (see Figure 3-5) shows the following information about all connected services (including automatically connected services) during the current session:

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

Service List Images

The SESM web developer kit provides a way to link images indicating status to the items in the service list. NWSP uses the following images next to the items in the service list (see Figure 3-4):

- Red X—Indicates an unconnected service
- Green arrow—Indicates a connected service

Mutually Exclusive Service Selection

Mutually exclusive service selection restricts a subscriber to accessing only one service at a time in a specified group of services. One use of this feature is described in the "Service Selection by Bandwidth" section on page 2-4.

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

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

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

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

A mutually exclusive service group is defined in a service group profile.

Service Selection by Bandwidth

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

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

Supported Service Types

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

Note Service type is known as service class in CDAT.

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

- Passthrough—The SSG can forward traffic through any interface using normal routing or a next-hop table. Passthrough service is ideal for standard Internet access.
- Proxy—When a subscriber selects a proxy service, the SESM portal prompts for the user name and password. After authentication, the service is accessible until the user logs out from the service, logs out from the SESM portal, or is timed out.
- Tunnel—When a subscriber selects a tunnel service, SESM displays a service authentication page to obtain service connection credentials from the subscriber.

Self-Care Features with SESM-SPE

Self-care features provide subscribers with write access to their account information, so that they can maintain the information themselves.

The SESM self-care features are implemented by the SPE component and are therefore available only when SESM is deployed in SPE mode.

This section describes the following SESM self-care features:

- Account Self-Management, page 2-5
- Account Self-Registration, page 2-5
- Service Self-Subscription, page 2-5
- Subaccount Creation and Management, page 2-6
- Personal Firewalls, page 2-6

Account Self-Management

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

Account Self-Registration

The SESM self-registration feature provides a way for subscribers to create their own new account, rather than depending on a service-provider administrator to create the initial record.

Service Self-Subscription

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

Subaccount Creation and Management

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

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

Personal Firewalls

The SESM personal firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on a web portal page. The portal page presents a list of applications, configured by the deployer, that are available for firewall protection. Based on choices the subscriber makes on the portal page, SESM creates the access control list (ACL) commands that implement the traffic filters on the subscriber’s connection.

A parent account can have different filters than its subaccounts, and the parent account can restrict the subaccount from changing firewalls.

Captive Portal, Messaging, and Advertising Features

The SESM captive portal solution works with the TCP redirect features on the SSG to provide several types of subscriber captivation. With captivation, a subscriber’s original request is captured and the browser is appropriately redirected.

The SSG TCP redirect feature redirects incoming TCP packets to a specified SESM captive portal application. The SESM captive portal application issues an HTTP redirection to the subscriber’s browser, directing it to another application that returns content to the subscriber. These content applications can be SESM portals that:

- Present a session logon page to enforce authentication
- Redirect to services
- Display message pages at initial logon
- Display advertising pages at defined intervals

The following sections briefly describe these captivation types. For more information, see the *Cisco Subscriber Edge Services Manager Captive Portal Guide*.

Unauthenticated User Captivation

Unauthenticated subscribers are those who have submitted an HTTP request when there is no host object on the SSG. A host object exists only after successful authentication. Unauthenticated user captivation works as follows:

- The SSG TCP redirect feature redirects unauthenticated packets to the SESM captive portal solution.

- The SESM captive portal solution:
  - Redirects the browser to the login page of the SESM portal
  - Optionally preserves the originally requested URL and performs a second redirection after authentication to the original URL

Some benefits to implementing unauthenticated user captivation are:

- Subscribers do not need to know the URL to the SESM logon page because they are sent there automatically when they start a browser session.
- In a wireless LAN, the feature allows unauthenticated access to the default LAN network but then requires the subscriber to authenticate before accessing the Internet or other services.
- The SESM captive portal solution can redirect a subscriber to a home page URL or a predefined service address immediately after authentication.

Unconnected Service Redirection

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

Examples of how the SESM captive portal solution can support service captivations are:

- When a subscriber is not connected for a service, the captive portal solution can present a service logon page or perform the authentication on behalf of the subscriber.
- When the subscriber is not subscribed to a service, the captive portal solution can present a subscription page.
- When service connection is refused because of lack of funds in the subscriber account, the captive portal solution can present an explanation. See the "Prepaid Services" section on page 2-15 for more information.

Initial Logon Captivation

Initial logon captivation displays a message or greetings page to all subscribers immediately after authentication. This feature works as follows:

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

Initial logon captivation provides a way for providers to present important messages to their subscribers, including announcements of new services and procedures or identity and branding messages.

Advertisement Captivation

Advertisement captivation presents advertisements at specified intervals for specified durations. This feature works as follows:

- The SSG TCP redirect feature handles the interval timing mechanism. For each logged-on subscriber, when the specified interval elapses, SSG redirects the next TCP packet originating from the subscriber to the SESM captive portal application.
- The SESM captive portal solution presents the advertisement content.

Some possibilities for advertisement captivation using the SESM solution are:

- The captive portal solution can present service-specific advertisements by identifying the service name or service URL that is being requested, and presenting advertisements appropriate to users of the service.
- The SESM solution can display advertisements tailored to subscriber characteristics stored in the profile, such as hobbies, age, or gender.

Authentication Options

SESM passes authentication credentials to a cooperating network element in a RADIUS protocol format. Service providers can deploy SESM solutions using the following authentication options:

- 2-Key Authentication, page 2-8
- Authentication Using Multiple Keys, page 2-8
- Single Sign-on for PPP Clients, page 2-9
- Single Sign-on for non-PPP Clients, page 2-9
-

2-Key Authentication

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

- User name
- Password

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

Authentication Using Multiple Keys

Some deployments might require more than the standard two keys for authentication. SESM supports any number of authentication keys. The keys can be any combination of any RADIUS attribute.

Some typical fields used for authentication are:

- Access point name (APN)—This is RADIUS attribute 30, CALLED_STATION_ID. This might be a GGSN.
- MSISDN—This is RADIUS attribute 31, CALLING_STATION_ID. This might be the subscriber's MSISDN or telephone number.
- Network access server (NAS) identifier—This is attribute 32, NAS_IDENTIFIER. In SESM deployments, the SSG is the NAS.

To implement multikey authentication:

- Use the SESM web developer kit to add the authentication fields to the portal logon page.

  The SESM web developer kit does not offer a way to collect an APN or NAS identifier. This function must be performed by the cooperating network element, such as the SSG.
- If SESM is deployed 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.
- If SESM is deployed in SPE mode, you can configure the RDP Server to perform authentication using any number of standard RADIUS attributes.

  When provisioning subscriber profiles, administrators can enter the APN and NAS identifier attributes as group values. See the *Cisco Distributed Administration Tool Guide* for more information.

Single Sign-on for PPP Clients

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

Single Sign-on for non-PPP Clients

The single sign-on feature also is important for non-PPP subscribers. With single sign-on, if any subscriber authenticates using the SESM web portal, that subscriber does not need to sign on again for the duration of the session. The session exists as long as the cooperating network element has identifying information for it. For example, the SSG retains a host object until the subscriber ends the session by logging off.

This feature offers the following advantages to subscribers:

- 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 when the SESM automatic memory manager clears sessions from the SESM portal host.

Message Authentication

Beginning with SESM Release 3.1(9), SESM applications include RADIUS message authentication features. Message authentication resolves the following vulnerabilities in SESM solutions:

- Integrity of packets sent between SESM solution components—Verify that the contents of packets are not altered during transmission.
- Authentication for accounting packets—Accounting packets do not include the User-Password attribute; therefore, the shared secret MD5 encryption check cannot be performed on those packets.

In SESM Web Portals and WSG

You can configure SESM web portal and WSG applications to send the RADIUS Message-Authenticator attribute (80) in access-requests to the Cisco edge device and validate received Message-Authenticator attributes.

To configure the Message-Authenticator feature in the SESM web portal and WSG applications, set the following attribute in the SSG MBean used by the application to true.

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

In RDP

If the Message-Authenticator attribute is included in messages to RDP, the RDP validates it and responds with a Message-Authenticator attribute. If the RDP is configured to proxy authentication requests, RDP regenerates, if necessary, the Message-Authenticator attribute before proxying or responding.

These validations occur automatically in RDP without any specific configuration.

In SSG

Currently, SSG does not validate Message-Authenticator attributes and does not include the attribute in responses to SESM requests. A future release of SSG will include this capability.

Web Development Features

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

- Localization and Internationalization, page 2-10
- Java Server Pages, page 2-10
- SESM User Shape Mechanism, page 2-11
- Library Resources, page 2-11

Localization and Internationalization

SESM portals, RDP, and CDAT can support Unicode Transformation Format Version 8 (UTF-8) character representations. UTF-8 supports the traditional 1-byte character sets and double-byte character sets.

Web developers can use the following techniques to localize and internationalize SESM web portals:

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

Java Server Pages

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

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

SESM User Shape Mechanism

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

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

- The subscriber's preferred language setting in the browser sets the locale.
- The access device, browser type, and the IP address are available from the initial request.

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

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

Library Resources

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

SESM Location and Brand Awareness Features

The SESM portal can derive the location or service brand of a subscriber and present branded retail pages or different elements within a page based on those attributes.

Some examples of how you might use 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.

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.

SESM currently has three ways to configure location and brand awareness:

- Location or Brand Awareness Based on Complete ID Attributes, page 2-12

- Location or Brand Awareness Based on IP Addresses, page 2-12
- Brand Awareness Based on Subscriber Groups, page 2-12

Location or Brand Awareness Based on Complete ID Attributes

Note This is the recommended method for defining location awareness.

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:

- Subscriber IP address range
- Virtual path identifier (VPI) range
- Subinterface, such as an Ethernet interface

More attributes might be added in future releases.

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

The Location MBean used by the web portal defines location names and the attributes that are associated with each location. See the *Cisco Subscriber Edge Services Manager Web Portal Guide* for more information.

Location or Brand Awareness Based on IP Addresses

You can configure brand or location awareness based on the following IP addresses or subnets:

- 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

With this method, you configure the SSG MBean used by the web portal to assign a location or brand to the IP address associated with a request.

See the *Cisco Subscriber Edge Services Manager Web Portal Guide* for more information about how to configure branding based on IP addresses.

Brand Awareness Based on Subscriber Groups

Another way to implement brand awareness is based on subscriber groups. The group is an attribute of a subscriber profile, and a group represents a brand. The SESM portal detects the branding for a subscriber based on the group in which that subscriber is assigned and returns pages appropriate to the brand of that group.

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

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

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

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

SESM Management Features

SESM includes two web-based management tools for service provider administrators:

- Application Manager—A management tool for remotely accessing and changing configuration attributes for all SESM applications.
- CDAT—A management tool for the SPE extensions in an LDAP directory.

Note The Advanced windows in the new Application Manager replace the JMX Agent View provided as a management tool in previous releases. The AgentView is also included in SESM Release 3.1(9). However, the preferred remote management tool for SESM is the new Application Manager.

Application Manager

The Application Manager is a web application that remotely manages SESM applications. It can manage multiple instances of SESM web portal and captive portal applications, RDP, CDAT, WSG, and other Application Manager instances. These applications can be installed on the same or different systems from the Application Manager, and a firewall may exist between them.

From a web-based GUI interface, administrators can view and change values for most attributes in the configuration files for SESM applications. The tool does not permit changes to attributes if the change would disrupt the application. The application port, for example, cannot be changed.

Two types of management windows are available:

- Operational Scenarios—These windows offer convenient access to subsets of attributes that are most likely to require changes during production deployments. From these scenarios, administrators can change configuration values for running applications. The changes persist across application restarts.

  The scenarios present matrixes of attribute settings by application, enabling administrators to easily compare and change the settings for the same attribute for multiple applications of the same type.
- Advanced Windows—These windows provide access to all attributes in all MBeans used by each application. From the Advanced windows, administrators can:
  - Check the status of managed applications
  - Connect to applications that were previously unmanageable or not running, but are now available for management
  - Change attributes that are not included on the operational scenarios

– View monitoring (read-only) attribute values

VRemote Monitoring of SESM Applications

The Advanced windows include read-only attributes which contain metrics, counters, and descriptions. Administrators can use these read-only attributes to:

- Monitor portals to ensure that they are responding to HTTP requests
- Monitor RDP to ensure that it is responding to RADIUS requests
- Obtain descriptions and formatted array values
- Collect memory and activity metrics

LDAP Directory Information Management

For SPE mode deployments, CDAT provides the management interface for maintaining SESM information in the LDAP directory. From CDAT, administrators can maintain:

- Subscriber profiles
- Service profiles
- CDAT administrators
- Access policies for subscribers and CDAT administrators

See the *Cisco Distributed Administration Tool Guide* for more information about these management features.

For RADIUS mode deployments, use administrative tools provided by the vendor of the RADIUS server you are using to maintain subscriber and service profiles.

User Groups and Role Based Access Control

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

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

Support for Generic RADIUS Attributes

Administrators can enter any generic RADIUS attribute in a subscriber profile by using the LOCAL RADIUS attribute field in the CDAT interface.

Scaling, Redundancy, and Resiliency Features

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

- You can deploy multiple instances of the same SESM web portal and balance the load as you would with any web server application. The Cisco Content Services Switch 11000 is recommended for load balancing.
- Beginning with SESM Release 3.1(9), you can configure the SESM web portals to include the RADIUS Framed-IP-Address attribute in Access-Requests to the SSG. This attribute allows the load balancer, which is placed between the web portal and the SSG, to route all requests from the same session to the same SSG. The load balancer must be configured to examine the Framed-IP-Address attribute and route packets based on its value.
- The SSG port-bundle host key feature simplifies large deployments by eliminating manual mapping of subscriber subnets to SSGs.
- SESM applications are highly resilient because they are completely stateless regarding subscriber sessions. SESM applications obtain session status information from the SSG. Therefore, the SESM applications can be started and stopped without affecting a subscriber.

Accounting and Billing Interfaces

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

RADIUS Accounting

SSG can be configured to send accounting requests to a RADIUS server. The RADIUS server generates the accounting records.

Prepaid Services

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

Enhancing Prepaid Services Using SESM Captive Portal

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

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

Web Proxy Support

The SESM Release 3.1(9) Captive Portal application includes features that handle subscribers with a web-proxy configured in their browsers.

PAC File Emulation

Subscribers might have a Proxy Automatic Configuration (PAC) script configured in their browsers. When this is the case, the browser, at startup, requests the PAC file in an attempt to obtain the settings defined in the file and apply them prior to issuing any requests for a page.

For an unauthenticated subscriber in a SESM deployment, the request for the PAC file reaches the SESM Captive Portal application. In Release 3.1(9), the Captive Portal application can recognize the PAC file request and respond with its own example PAC file as a substitute. The browser session uses the settings in the Captive Portal PAC file rather than those in the original PAC file.

Web Proxy Notification Page

Subscribers might have a web proxy configured with an IP address (or DNS name) and a port. When this is the case, the browser, at startup, submits a request to the web proxy for a specific page.

For an unauthenticated subscriber in a SESM deployment, the request reaches the SESM Captive Portal application. In Release 3.1(9), the Captive Portal application can recognize the difference between a proxy request and a non-proxy or regular HTTP request. You can configure the SESM Captive Portal application to react to proxy requests by redirecting the browser to a customized message page. This page could, for example, inform the subscriber that a web-proxy is configured in the browser and how to disable it.

Web-Proxy Support

You can configure the Captive Portal application to handle a proxy request directly. In this case, when the Captive Portal application recognizes that an unauthenticated subscriber has a web proxy configured, it captures the browser and proxies a login page to the browser. After authenticating and connecting to services on the SSG, the subscriber might (depending on the specific service connections made) have access to the configured web proxy and request connection to it.

Using the Web Services Gateway with Third-Party Portals

The SESM Web Services Gateway (WSG) application provides a Simple Objects Access Protocol (SOAP)-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. Any client application can interface with SSG through the WSG using SOAP over HTTP communication.

The SESM WSG installation includes a web application configured to run in a Jetty container and a command-line client script for demonstration purposes. The WSG web application runs in RADIUS and SPE modes. It does not work in Demo mode.

In this first release, the WSG client interface enables access to the SSG for the following activities:

- Authenticating, starting, and ending sessions on the SSG

  - Obtaining session status
  - Connecting and disconnecting services

Note This first release of WSG offers a preview of future development efforts. We invite interested parties to contact us through a Cisco account representative to discuss potential uses for WSG and participate in feature planning efforts for future releases.

SESM Solutions for Service Selection and Connection with SSG

This chapter describes SESM solutions for service selection and connection. These solutions work in conjunction with the Cisco Service Selection Gateway (SSG) for network access and connection management. These solutions can work with profiles stored on either a RADIUS database or LDAP directory.

This chapter includes the following topics:

Overview

For service selection and connection solutions, the Cisco Subscriber Edge Services Manager (SESM) works in conjunction with the Service Selection Gateway (SSG) to provide robust, highly scalable connection management to services in the broadband and mobile wireless markets. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their subscribers with a web interface, or portal, for accessing multiple IP services.

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

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

Subscribers interact with SESM web portals using a standard Internet browser. They do not need to download any software or plug-ins to use the SESM web portal. After a subscriber successfully authenticates, the SESM web portal presents a list of services that the subscriber is currently authorized to use. The subscriber can gain access to one or more of those services by selecting them from the web portal. Alternatively, an automatic connection feature can automatically connect subscribers to services after authentication.

Required Cisco IOS Release for SSG

Features in SESM Release 3.1(5) require the SSG embedded in the Cisco IOS Release 12.2(4)B or later. SESM Release 3.1(5) is backward compatible and is verified to work with previously released versions of the Cisco IOS broadband release train containing the SSG feature. For example, SESM Release 3.1(5) portals can be deployed with the SSG in Cisco IOS Release 12.1(3)DC running on the Cisco 6400 UAC.

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

- *SSG Features in Release 12.2(4)B*—The online location of this document is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

- Product documentation for the device on which SSG is running

SSG Platforms

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

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

Communication Between SESM Applications and the SSG

SESM applications use command codes tunneled inside RADIUS requests to communicate with SSG. SSG distinguishes SESM requests from RADIUS requests by the presence of these command codes. SSG replies to SESM requests with either an access-accept or access-reject message.

Web Server Dependencies

Certain web server capabilities are required in SESM deployments that depend on the SSG TCP redirect feature or the port-bundle host key feature. Currently, the only web server that can provide the required capabilities is the Jetty server from Mort Bay Consulting. The rest of this section describes the dependency.

To support the above-mentioned features, SSG rewrites TCP packets destined to the default network, as follows:

- For the TCP redirect feature, SSG rewrites the destination port and IP address of the TCP packet
- For the port-bundle host key feature, SSG rewrites the source port and IP address of the TCP packet

The SSG rewrites only the TCP packet information; the corresponding values for the HTTP request contained in the TCP packet do not match. The SESM portal depends on the web server to access the socket-level values and add them to the HTTP request as request attributes. A special handler is required to perform this work. Currently, the Jetty server is the only J2EE-compliant web server that can perform this function.

Port-Bundle Host Key Feature on SSG

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

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

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

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

System Description and Network Diagram

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

Access Technologies

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

Default Networks

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

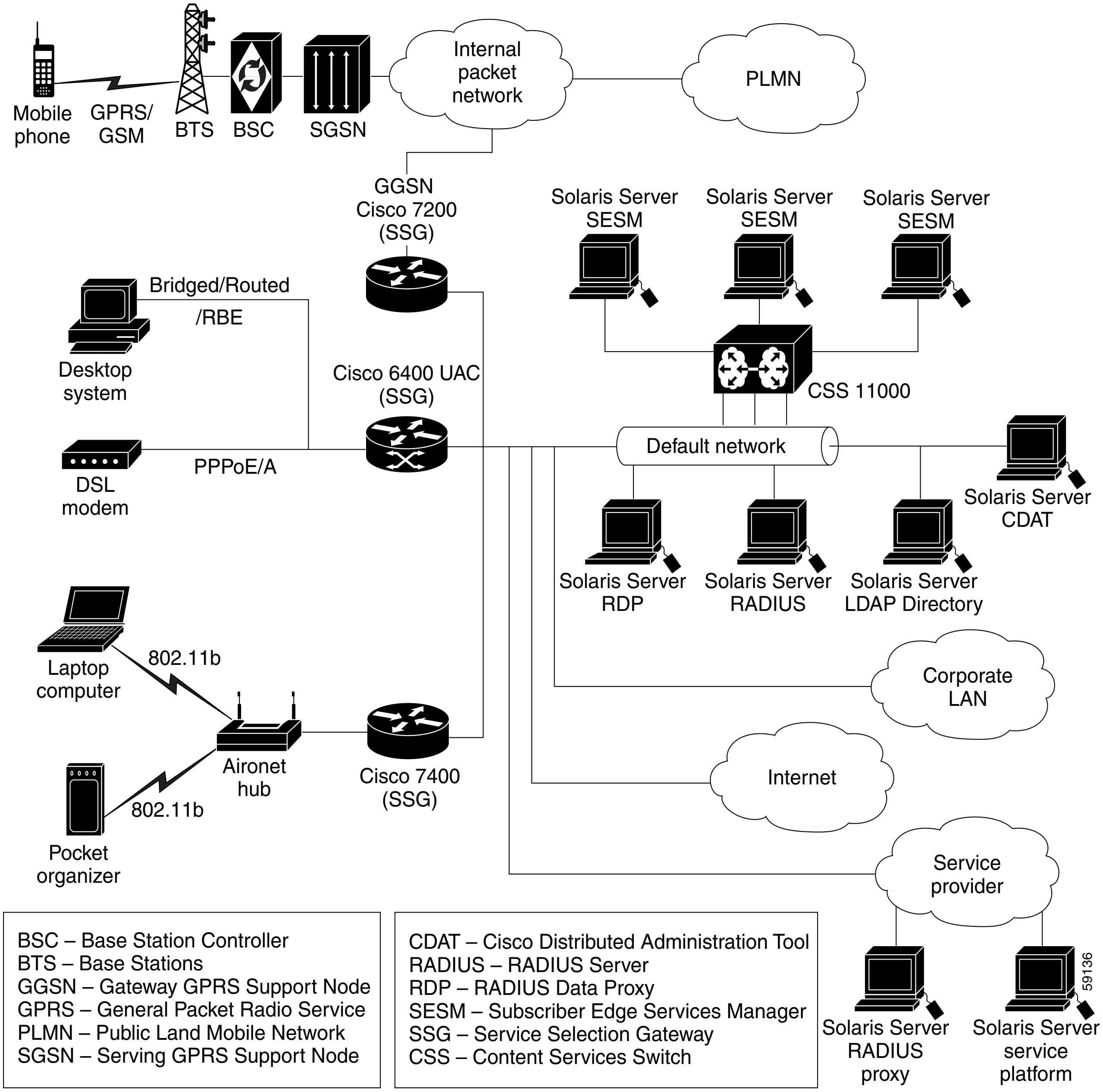
Service Selection Gateway

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

Network Diagram

Figure 3-1 is a conceptual network diagram showing SESM components, SSGs, and a default network. A typical deployment might consist of several routers of the same type, each one with its own default network, with SESM applications deployed on each of the default networks.

Figure 3-1 Network Diagram



Data Flow

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

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

- If the port-bundle host key feature is enabled on the SSG, the SSG's IP address is inserted at the source IP address of the TCP packet.
- If the port-bundle host key feature is *not* enabled, configuration parameters map client subnets to specific SSGs.

Scaling and Load Balancing

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

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

Connection Examples

This section provides some examples of how a subscriber gains access to SESM portals.

Example Using the Point-to-Point Protocol in a DSL Equal Access Deployment

This example describes the connection sequence for Point-to-Point Protocol (PPP) access to ISP services. For this example, SESM is deployed by a NAP providing equal access to several ISPs. The subscriber is a DSL subscriber using a PPP client configured on a laptop computer.

Note This example also uses the SESM captive portal features, explained in Chapter 4.

1. The subscriber launches the PPP client.
2. The PPP session is terminated on the Cisco router which is also the SSG platform.
3. System software on the router handles the PPP authentication. SSG receives notification when PPP authentication is successful. The SSG does not require further authentication.
4. The subscriber is authenticated but has no service connection. The SSG and SESM unconnected service redirection features can work together to provide the subscriber with a list of ISPs from which to choose.
   - The SSG unconnected service redirection feature intercepts the TCP packet containing the subscriber's first request. The request is redirected to an SESM application.
   - The SESM application retrieves the subscriber's profile and replies with a page containing the ISPs available to the subscriber, based on information in the profile.
   - The subscriber chooses an ISP. SESM requests the SSG to make the service connection.

Example Using Routed Wireless LAN

This example describes the connection sequence for routed access to SESM. For this example, the subscriber uses a PDA device configured for access through a wireless LAN access point.

1. The subscriber launches a web browser and sends an HTTP request. The TCP packet containing the request is routed through the SSG.
2. If the SSG TCP unauthenticated user redirect feature is configured, the subscriber can request any URL and the TCP packet is redirected to the SESM portal.
3. The SESM portal replies with the SESM logon page.
4. When the SESM portal receives the subscriber's logon information, the portal requests authentication services from the SSG. After the subscriber is authenticated, the SESM session is established.

SESM RADIUS Mode Deployment

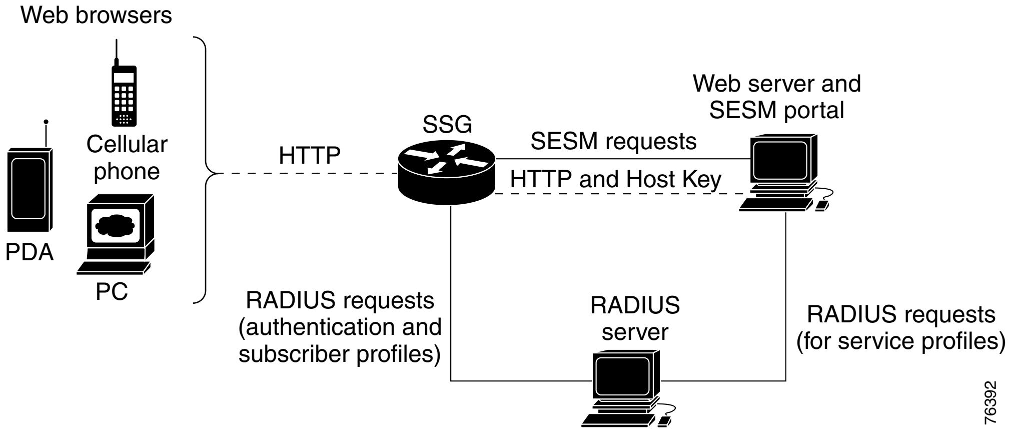
This section describes an SESM deployment using RADIUS mode. The section includes the following topics:

- RADIUS Mode Deployment Diagram, page 3-6
- Request Processing in SESM RADIUS Mode Deployments, page 3-7
- RADIUS Mode Installation and Configuration Summary, page 3-8

RADIUS Mode Deployment Diagram

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

Figure 3-2 SESM Deployed in RADIUS Mode


Web browsers
Cellular phone
PDA
PC
HTTP
SSG
Web server and SESM portal
SESM requests
HTTP and Host Key
RADIUS requests (authentication and subscriber profiles)
RADIUS server
RADIUS requests (for service profiles)
76392

SSG and the SESM portal work together to process subscriber requests. The processing sequence involves the following types of requests and associated replies:

- HTTP requests from the subscriber browser to the SESM portal—These requests are routed through the SSG to the SESM portal. If the port-bundle host key feature is enabled on the SSG, the SESM portal can support subscribers using overlapping and nonroutable IP addresses. See the "Subscriber Sessions" section on page 2-3 for more information.
- Requests from the SESM portal to SSG—SESM requests consist of proprietary command codes tunneled inside RADIUS requests.
- RADIUS protocol requests
  - From SSG to a RADIUS server—These are requests to authenticate the subscriber and obtain the subscriber profile.
  - From SESM to a RADIUS server—These are requests to obtain service profiles. The SESM portal caches the replies; therefore, these requests are required once for each service profile until the cache expires.

Request Processing in SESM RADIUS Mode Deployments

Table 3-1 describes the role of the SESM portal, SSG, and the RADIUS server in processing typical subscriber actions in RADIUS mode deployments. The mode determines where profile information is stored and obtained. Otherwise, the service selection and connection features work the same in RADIUS and SPE modes.

Table 3-1 Role of Components in SESM RADIUS Mode Deployments

Subscriber Action	Software Activity	Explanation
Subscriber logs on	Authenticate the subscriber in the system.	**1.** The HTTP request containing the logon information is routed to the SESM portal. **2.** The SESM portal initiates authentication by sending an access request to the SSG. **3.** SSG sends an access request to the RADIUS server. **4.** The RADIUS server authenticates the subscriber and returns an access-accept or access-reject message to SSG. Access-accept messages contain the subscriber profile. **5.** If the RADIUS reply is an access-accept, SSG creates an edge session on the router for the subscriber. **6.** SSG replies to the SESM request in step 2. If the reply is an access-accept, it includes the subscriber profile originally obtained from the RADIUS server.
	Display web interface with: • Personalized content • List of subscribed services	**7.** The SESM portal can analyze the subscriber profile information and determine appropriate content for this subscriber. **8.** The SESM portal ensures that it has a cached service profile for each of the services in the subscriber profile. If the cache is missing any of the profiles, the portal obtains the service profile from the RADIUS server. **9.** The SESM portal replies to the HTTP request in step 1 with the appropriate content.

Table 3-1 Role of Components in SESM RADIUS Mode Deployments (continued)

Subscriber Action	Software Activity	Explanation
Subscriber selects a service	Access the service. Display updated service connection information.	1. The service connection request from the browser is routed to the SESM portal. 2. The SESM portal sends a connection request to SSG if the subscriber is authorized to connect to that service. 3. SSG does the following: – For passthrough services, it connects the service. – For proxy or tunnel services, it sends a RADIUS authentication request to a RADIUS server. If the reply is an access-accept, SSG connects the service. – SSG replies to the SESM request in step 2. To connect the service, SSG associates this subscriber's edge session with the service. When the connection is complete, SSG allows traffic from the subscriber to the domain specified in the service profile. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.
Subscriber disconnects a service	Stop access to the service. Display updated service connection information.	1. The disconnection request from the browser is routed to the SESM portal. 2. The SESM portal sends a disconnect request to SSG. 3. SSG removes the association between the service and the subscriber's edge session and replies to the SESM request. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.

RADIUS Mode Installation and Configuration Summary

Table 3-2 summarizes the steps required to deploy SESM in RADIUS mode.

Table 3-2 Configuration Requirements for SESM in RADIUS Mode

Deployment Step	References[1]
1. Install and configure a RADIUS AAA server.	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the RADIUS server vendor
2. Ensure that the SSG platform is running an appropriate Cisco IOS software release.	• *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(9)*

Table 3-2 Configuration Requirements for SESM in RADIUS Mode (continued)

Deployment Step	References[1]
3. Configure SSG. Use Cisco IOS commands on the SSG platform to: – Configure SSG to listen for SESM requests. – Enable or disable the host key mechanism. – Set up SSG-to-RADIUS communication. – Configure security, routing, and other services provided by SSG. – Configure SSG TCP redirect features (optional).	• *Cisco Subscriber Edge Services Manager Deployment Guide* • SSG documentation[2]
4. Install and configure the SESM portal application and J2EE-compliant web server.	• *Cisco Subscriber Edge Services Manager Installation Guide*
5. Create user and service profiles in the RADIUS database.	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the RADIUS server vendor

[1] Go to http://www.cisco.com/univercd/cc/td/doc/solution/sesm/

[2] Go to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

SESM SPE Mode Deployment

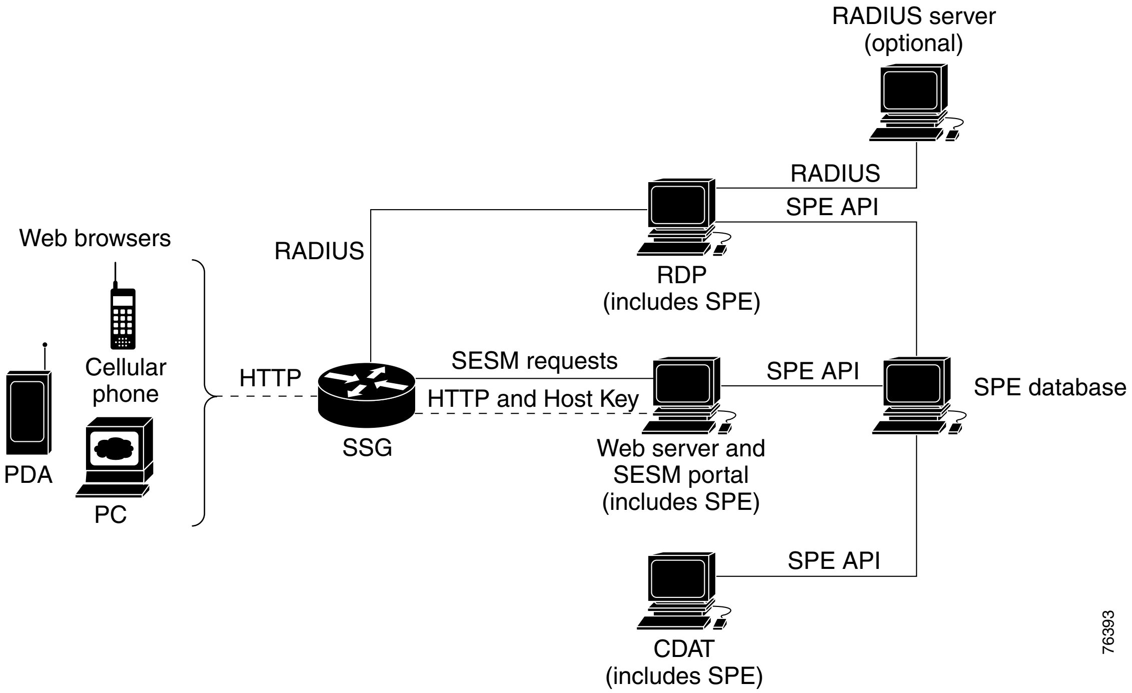
This section describes the service selection and connection solution using SESM deployed in SPE mode. The section includes the following topics:

- SPE Mode Deployment Diagram, page 3-10
- Request Processing in SESM SPE Mode Deployments, page 3-11
- SPE Mode Installation and Configuration Summary, page 3-13

SPE Mode Deployment Diagram

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

Figure 3-3 SESM Deployed in SPE Mode



In an SPE mode deployment, the Cisco Subscriber Policy Engine (SPE) provides services to SESM portals, CDAT, and RDP. The optional RADIUS server can provide user authentication services when RDP is configured in Proxy mode. SSG and SESM applications work together to process subscriber requests. The processing sequence involves the following types of requests and associated replies:

- HTTP requests from the subscriber browser to the SESM portal—These requests are routed through the SSG to the SESM portal. If the port-bundle host key feature is enabled on the SSG, the SESM portal can support subscribers using overlapping and nonroutable IP addresses. See the "Subscriber Sessions" section on page 2-3 for more information.
- Requests from the SESM portal to SSG—SESM requests consist of proprietary command codes tunneled inside RADIUS requests.
- RADIUS protocol requests from SSG to the RDP—These are requests to authenticate the subscriber and obtain the subscriber profile.

  When the RDP is running in Proxy mode, it forwards the RADIUS requests to a RADIUS server. Otherwise, RDP transforms the request into an LDAP request to the LDAP directory.
- LDAP protocol requests to the directory:
  - From RDP—These are requests for authentication and to obtain the subscriber profile.
  - From SESM—These are requests to obtain service profiles. The SESM portal caches the replies; therefore, these requests are required once for each service profile during an SESM portal run.
  - From CDAT

Request Processing in SESM SPE Mode Deployments

Table 3-3 describes the role of the SESM portal, RDP, SPE, and SSG in processing typical subscriber actions when the SESM portal is deployed in SPE mode. The mode determines where profile information is stored and obtained. Otherwise, the service selection and connection features work the same in RADIUS and SPE modes.

Table 3-3 Role of Components in an SPE Mode Deployment

Subscriber Action	Software Activity	Components Involved
Subscriber logs on	Authenticate the subscriber in the system.	**1.** The request from the browser containing the logon information is routed to the SESM portal. **2.** The SESM portal initiates authentication by sending an access request to the SSG. **3.** SSG sends a RADIUS protocol access request to the RDP. **4.** The RDP translates the request into an LDAP request to the LDAP directory. **Note** If the RDP is configured to run in Proxy Mode, RDP proxies the request to the configured RADIUS server. See the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*, Chapter 12 “Deploying SESM with SSG Solutions” for more information about the RDP Proxy mode. **5.** The LDAP directory replies to the RDP request. If access is granted (access-accept), the reply includes the subscriber profile. **6.** The RDP replies to the SSG request in step 3 with an access-accept or access-reject message. Access-accept messages contain the subscriber profile. **7.** If the reply is an access-accept message, SSG creates an edge session on the router for the subscriber. **8.** SSG replies to the SESM request in step 2. If the reply is an access-accept message, it includes the subscriber profile originally obtained from the directory in step 5.
	Display web interface with: • Personalized content • List of subscribed services	**9.** The SESM portal can analyze the subscriber profile information and determine appropriate content for this subscriber. **10.** The SESM portal ensures that it has a cached service profile for each of the services in the subscriber profile. If the cache is missing any of the profiles, the portal obtains the service profile from the LDAP directory. **11.** The SESM portal replies to the HTTP request in step 1 with the appropriate content.

Table 3-3 Role of Components in an SPE Mode Deployment (continued)

Subscriber Action	Software Activity	Components Involved
Subscriber selects a service	Access the service. Display updated service connection information.	1. The service connection request from the browser is routed to the SESM portal. 2. The SESM portal sends a connection request to SSG if the subscriber is authorized to connect to that service. 3. SSG does the following: – For passthrough services, it connects the service. – For proxy or tunnel services, it sends a RADIUS authorization request (to a RADIUS server or RDP). If the reply is an access-accept message, SSG connects the service. – SSG replies to the SESM request in step 2. To connect the service, SSG associates this subscriber's edge session with the service. When the connection is complete, SSG allows traffic from the subscriber to the domain specified in the service profile. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.
Subscriber disconnects a service	Terminate access to the service. Display updated service connection information.	1. The disconnection request from the browser is routed to the SESM portal. 2. The SESM portal sends a disconnect request to SSG. 3. SSG removes the association between the service and the subscriber's edge session and replies to the SESM request. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.
Subscriber updates an e-mail address	Update the LDAP directory.	The SESM portal sends the update to the directory using the SPE application programming interface.
Subscriber creates a subaccount	Update the LDAP directory.	The SESM portal sends the update to the directory using the SPE application programming interface.

SPE Mode Installation and Configuration Summary

Table 3-4 summarizes the installation and configuration activities for SESM in SPE mode.

Table 3-4 Configuration Requirements for SESM in SPE Mode

Activity	Reference[1]
1. (Optional) Install and configure a RADIUS server if you want to deploy RDP in Proxy mode and maintain separate profile sources for authentication (RADIUS) and authorization (LDAP).	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the RADIUS server vendor
2. Ensure that the SSG platform is running an appropriate Cisco IOS software release.	• *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(9)*
3. Configure SSG. Use Cisco IOS commands on the SSG platform to: – Configure SSG to listen for SESM requests. – Set up SSG to RADIUS communication. – Enable the host key mechanism. – Configure security, routing, and other services provided by SSG. – Configure SSG TCP redirect features (optional).	• *Cisco Subscriber Edge Services Manager Deployment Guide* • SSG documentation[2]
4. Install and configure an SPE database.	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the directory vendor
5. Install and configure the SESM software components, which include: the SESM portal applications, a J2EE-compliant web server, RDP, SPE, and CDAT.	• *Cisco Subscriber Edge Services Manager Installation Guide*
6. Load sample data and create roles, groups, and user and service profiles in the LDAP directory.	• *Cisco Distributed Administration Tool Guide*

[1] Go to http://www.cisco.com/univercd/cc/td/doc/solution/sesm/

[2] Go to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

SESM Service Selection Demo

This section describes some of the SESM features that you can demonstrate while running NWSP in Demo mode. Also see the "SESM Self-Care Demo" section on page 4-9 for demonstrations of account self-maintenance, subaccount creation, firewalls, and service self-subscription.

Step 1 Install NWSP in Demo mode. See the "Quick Start for Installing and Running Portals in Demo Mode" section on page A-2 for instructions.

Step 2 Start NWSP. The start script pathname is:

```
jetty
    bin
        startNWSP
```

See the "Starting a Demo" section on page A-5 for more information.

Step 3 Open a web browser and go to the NWSP page.

If the web browser is on the same system where NWSP is running, and you accepted the default port during installation, you can use the following URL:

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

Otherwise, the URL is:

```
    http://NWSPhostName:NWSPportNumber
```

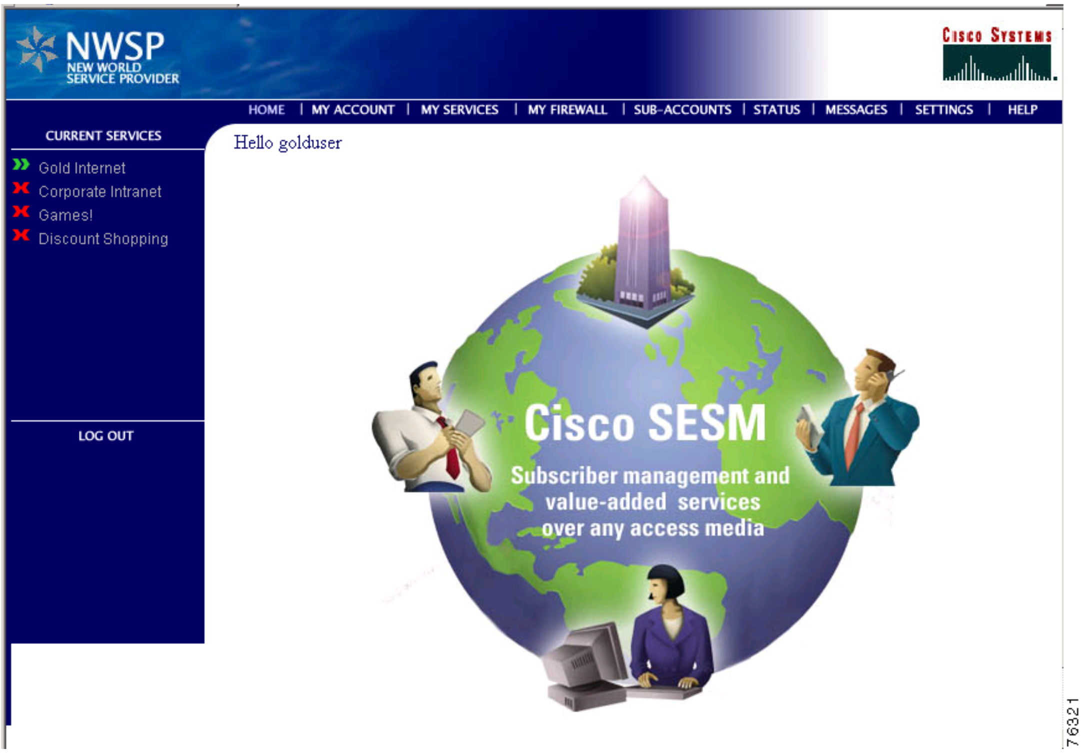
Step 4 Log on using user IDs and passwords from Table 3-5. These values are the user IDs and passwords defined in the profiles in the installed demo data file for the NWSP application (demo.txt).

Table 3-5 Logon Names and Passwords in demo.txt

To demonstrate RADIUS Mode features...	To demonstrate SPE mode features...
User ID: radiususer Password: cisco	User ID: golduser Password: cisco
Other valid users for RADIUS mode demos are user1, user2, and so on, up to user45.	User ID: subgolduser Password: cisco **Note** subgolduser is a subaccount to golduser.

The NWSP home page appears. Figure 3-4 shows the home page for SPE mode. In RADIUS mode, the **MY ACCOUNT**, **MY SERVICES**, and **SUBACCOUNTS** tabs do not appear.

Figure 3-4 NWSP Home Page


NWSP
NEW WORLD SERVICE PROVIDER
CISCO SYSTEMS
HOME | MY ACCOUNT | MY SERVICES | MY FIREWALL | SUB-ACCOUNTS | STATUS | MESSAGES | SETTINGS | HELP
CURRENT SERVICES
» Gold Internet
✗ Corporate Intranet
✗ Games!
✗ Discount Shopping
LOG OUT
Hello golduser
Cisco SESM
Subscriber management and value-added services over any access media
76321

The service selection list (the column on the left side of the window) shows all of the subscribed services for the logged-on user. The icons indicate:

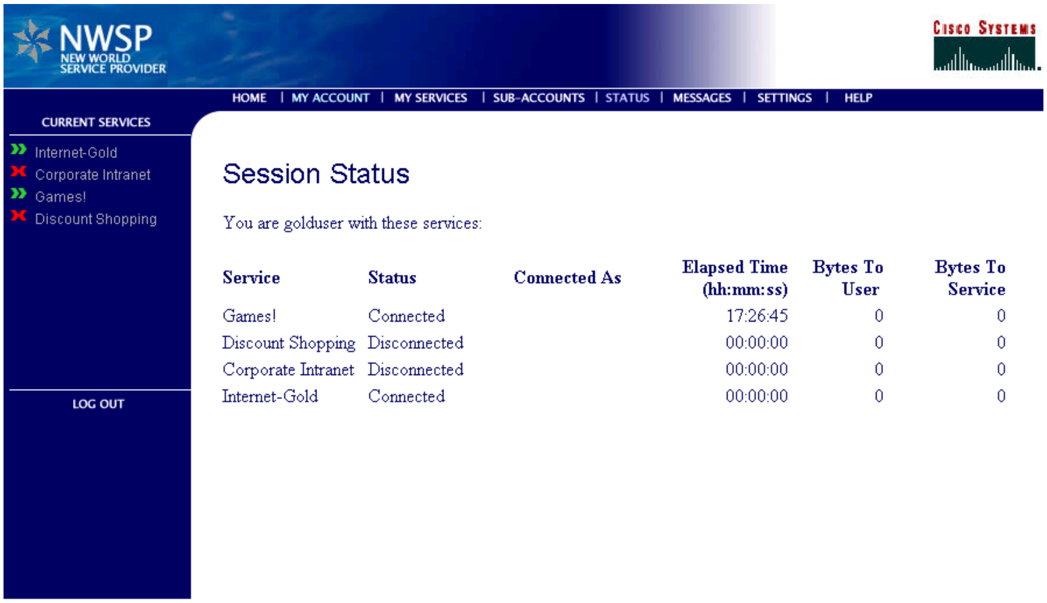
- Green arrow—Connected service. In the radiususer and golduser profiles, the Internet service is marked as an automatically connected service; hence the green arrow icon indicating connection immediately after signing on.
- Red X—Unconnected service.

Step 5 Click on other services in the list to demonstrate service selection and connection. In particular, click on **Corporate Intranet** to show a service logon page for a service that requires authentication.

Because the profiles in data.txt do not include service names and passwords, you cannot demonstrate service logon. If you are demonstrating an LDAP deployment, click the **MY SERVICES** tab, and enter any username and password next to the service.

Step 6 Click the **STATUS** tab to show status information about services for the current SESM session. Figure 3-5 shows the NWSP status page.

Figure 3-5 NWSP Status Page



Session Status

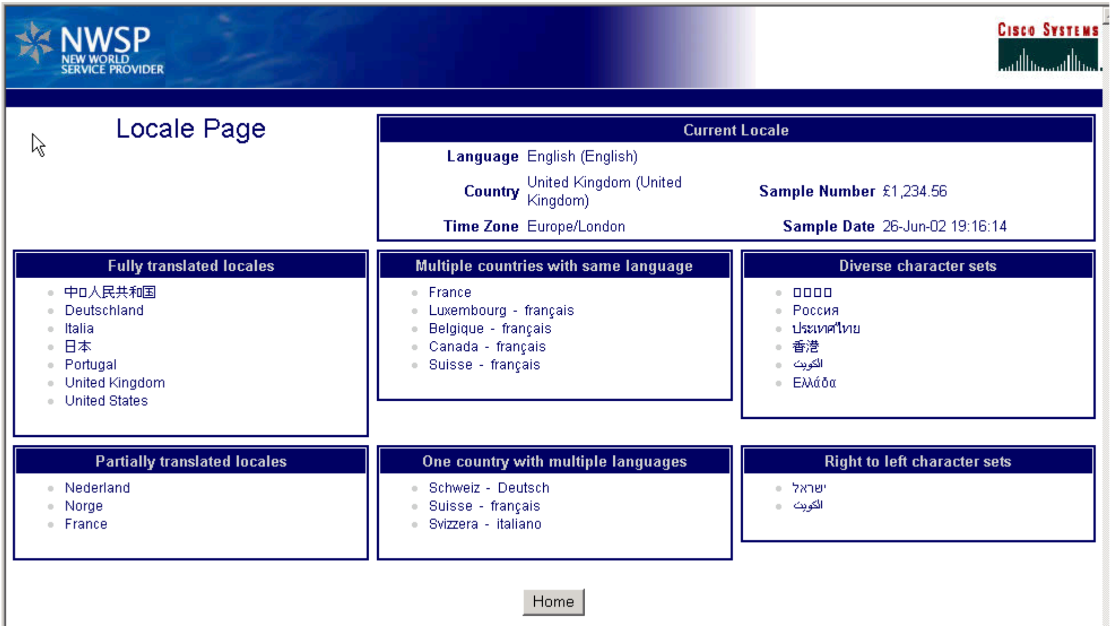
You are golduser with these services:

Service	Status	Connected As	Elapsed Time (hh:mm:ss)	Bytes To User	Bytes To Service
Games!	Connected		17:26:45	0	0
Discount Shopping	Disconnected		00:00:00	0	0
Corporate Intranet	Disconnected		00:00:00	0	0
Internet-Gold	Connected		00:00:00	0	0

Step 7 Demonstrate service disconnection by clicking on the green arrow icon next to a connected service.

Step 8 Click the **SETTINGS** tab to show possibilities for localization and internationalization in the SESM portal. Figure 3-6 shows the NWSP Settings page.

Figure 3-6 NWSP Settings Page



Locale Page

Current Locale

Language English (English)

Country United Kingdom (United Kingdom) **Sample Number** £1,234.56

Time Zone Europe/London **Sample Date** 26-Jun-02 19:16:14

Fully translated locales
- 中□人民共和国
- Deutschland
- Italia
- 日本
- Portugal
- United Kingdom
- United States

Multiple countries with same language
- France
- Luxembourg - français
- Belgique - français
- Canada - français
- Suisse - français

Diverse character sets
- □□□□
- Россия
- ประเทศไทย
- 香港
- الكويت
- Ελλάδα

Partially translated locales
- Nederland
- Norge
- France

One country with multiple languages
- Schweiz - Deutsch
- Suisse - français
- Svizzera - italiano

Right to left character sets
- ישראל
- الكويت

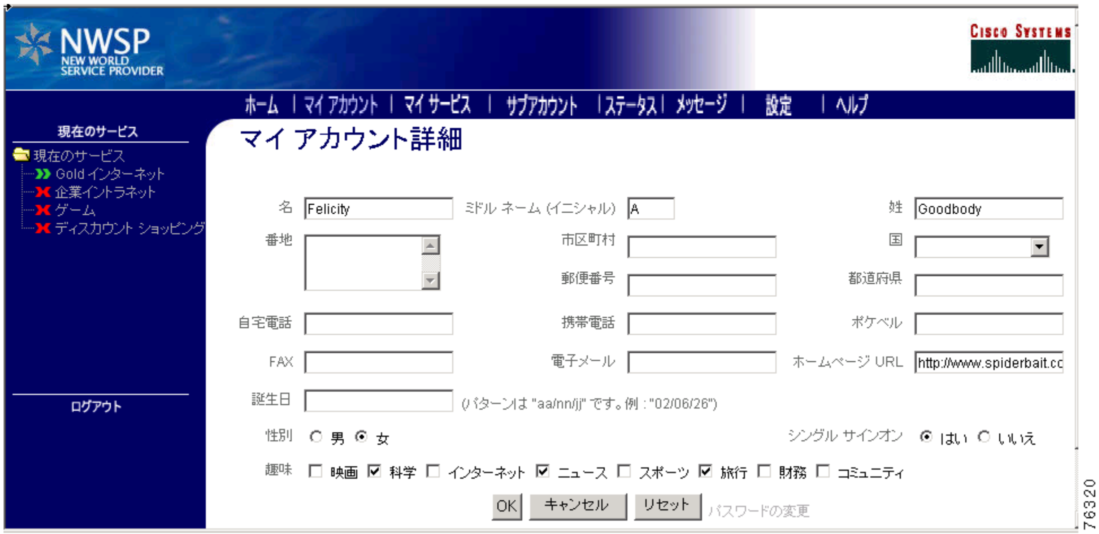
Step 9 To demonstrate translated resources:

1. From the Settings page, in the Fully translated locales box, click **Deutschland**.
2. Click the **HOME** button at the bottom of the window.
3. On the Home page, pass the cursor over the tabs to show tips in German.
4. Click the **STATUS** tab to show a status page containing German.

Step 10 To demonstrate text in resource bundles and images using the Japanese character set:

1. From the Settings page, in the Fully translated locales box, click the first bulleted item.
2. Click the **HOME** button at the bottom of the window.
3. Click any tab to show pages with Japanese resource bundles and images. Figure 3-7 shows the My Account page using the Japanese character set in the button and tab images and in translated resource bundles.

Figure 3-7 NWSP My Account Page Using Japanese Resources



マイ アカウント詳細

名 Felicity ミドル ネーム (イニシャル) A 姓 Goodbody

番地 市区町村 国

郵便番号 都道府県

自宅電話 携帯電話 ポケベル

FAX 電子メール ホームページ URL http://www.spiderbait.cc

誕生日 (パターンは "aa/nn/jj" です。例 : "02/06/26")

性別 ○ 男 ● 女 シングル サインオン ● はい ○ いいえ

趣味 □ 映画 ☑ 科学 □ インターネット ☑ ニュース □ スポーツ ☑ 旅行 □ 財務 □ コミュニティ

If your browser does not display Japanese characters in text fields, download the Japanese font from one of the following web sites:

- For the Microsoft Internet Explorer browser, go to:

  http://www.microsoft.com/japan/

- For the Netscape browser, go to:

  http://wp.netscape.com/eng/intl/

Note For UTF-8 support, use Netscape Version 6 or later.

Step 11 To return to the Settings page, click the tab that is second from the right.

Step 12 To end the current session:

1. Click the **HOME** button.

2. Click the **LOG OUT** button.

SESM Solutions for Subscriber Self-Care

This chapter describes SESM features that support subscriber self-care solutions. It includes the following topics:

Subscriber Self-Care Solution Description

This section describes the common characteristics of SESM self-care solutions. Topics are:

Subscriber Experiences in Self-Care Solutions

The SESM self-care solutions allow subscribers to make on-demand updates to their personal information at any time and see those changes take effect within minutes of submitting the change, with no involvement from the deployer. Subscribers can submit updates using the SESM portal. The self-care portal pages can be branded, personalized, and customized using any SESM web development features.

The NWSP portal contains pages that illustrate the following types of self-care activities:

- Updating personal account information
- Creating and provisioning subaccounts

- Building personal firewalls
- Subscribing and unsubscribing to services

See the "Supported Data Fields in a Self-Care Solution" section on page 4-4 for ways to extend the self-care examples shown in NWSP.

Security in Self-Care Solutions

The following features provide security in SESM self-care solutions:

- User authentication—A subscriber must successfully log in to the SESM portal before gaining access to any account information. The SSG performs authentication services for the SESM portal, based on subscriber profile information obtained by the RADIUS Data Proxy (RDP).
- User permissions—A subscriber must be assigned permissions that allow self-care updates. The provider administrator assigns permissions using CDAT. Permissions can be assigned to individual subscribers or to groups of users.
- Subaccount permissions—When subaccounts exist, the parent account can assign permissions to the subaccount that are more restrictive than the parent account permissions.
- Secure Socket Layer (SSL) mode—The default SESM portal configuration allows the subscriber to choose whether or not to use the SSL port. Providers can change this configuration so that the SESM web server uses only SSL listeners.

Deployment Requirements for Self-Care Solutions

This section lists the required components for self-care solutions.

Cisco Service Selection Gateway

The Cisco Service Selection Gateway (SSG) is required in the self-care solutions described in this chapter. These solutions require SSG for the following services:

- Requesting authentication—The SESM portal initiates authentication by sending an access request to SSG, which in turn sends a RADIUS access request to the RDP.
- Obtaining the subscriber profile—If the RDP reply is an access-accept, the reply includes the subscriber profile. SSG includes the subscriber profile in its reply to the SESM portal.

SSG configuration details for self-care solutions are the same as those for service selection and connection solutions. The SESM portal and RDP must be running on the SSG default network and configured to communicate with the SSG. For more information about how SESM, SSG, and RDP work together, see the "Request Processing in SESM SPE Mode Deployments" section on page 3-11.

SESM Portal

The SESM self-care solutions require that SESM portals are deployed in LDAP mode.

RADIUS Data Proxy

The RADIUS Data Proxy (RDP) is a required component in self-care solutions.

The RDP cache refresh time is directly related to the length of time subscribers must wait to see their updates take effect. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time. The installed default for cache refresh is 10 minutes.

LDAP Directory

The profile data that you want subscribers to update must reside in profiles on an LDAP directory. The LDAP protocol provides the features that allow for on-demand updates to profile data.

We recommend deploying a primary and a secondary directory and using the LDAP directory failover features.

Cisco Distributed Administration Tool

The Cisco Distributed Administration Tool (CDAT) is the tool for administrators to use in adding and maintaining subscriber profiles in the LDAP directory.

CDAT must have access to the LDAP directory. Multiple instances of CDAT can be installed on different systems, giving distributed administrative access to the directory.

Portal Customizations for Self-Care Solutions

The SESM portal is the subscriber interface to self-care activity. You can integrate a self-care solution with a service selection and connection solution or deploy it as a standalone solution. The NWSP application illustrates several self-care solutions as different pages in the same application:

- My Account Page
- My Firewall Page
- My Services Page
- Subaccounts Page

Service provider developers can use the SESM web developer kit to customize the portal page on which subscribers can enter or update the account information. Customizations related to self-care features might include:

- Adding or deleting self-care fields on the pages. See the "Supported Data Fields in a Self-Care Solution" section on page 4-4.
- Implementing the provider's business rules when validating the subscriber-submitted account information.

Supported Data Fields in a Self-Care Solution

SESM 3.1(5) supports the following categories of data in a subscriber profile. Developers can add any field from these categories to an SESM portal page and optionally provide access to them for on-demand updates by subscribers:

- Generic RADIUS attributes. For a list of supported attributes, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*. The online link to the list of generic RADIUS attribute fields that are predefined in the SESM core model is:

  http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_315/instconf/cradius.htm#xtocid5

- SPE attributes. SPE supports many of the fields in the X.500 standard user schema developed for use with LDAP. Some of the fields supported include date of birth, various address and telephone number fields, e-mail, gender, and hobbies. For a list of SPE-supported attributes, see the *Cisco Distributed Administration Tool Guide.* The online link to the SPE DESS/AUTH schema extensions is:

  http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_313/toolguid/appb_sch.htm#xtocid0

Subscriber Profile Requirements for Self-Care Solutions

The following requirements apply to subscriber profiles in SESM self-care solutions:

- The profile data that you want the subscriber to maintain must reside on an LDAP directory.
- The service provider must create the initial profile for each subscriber.

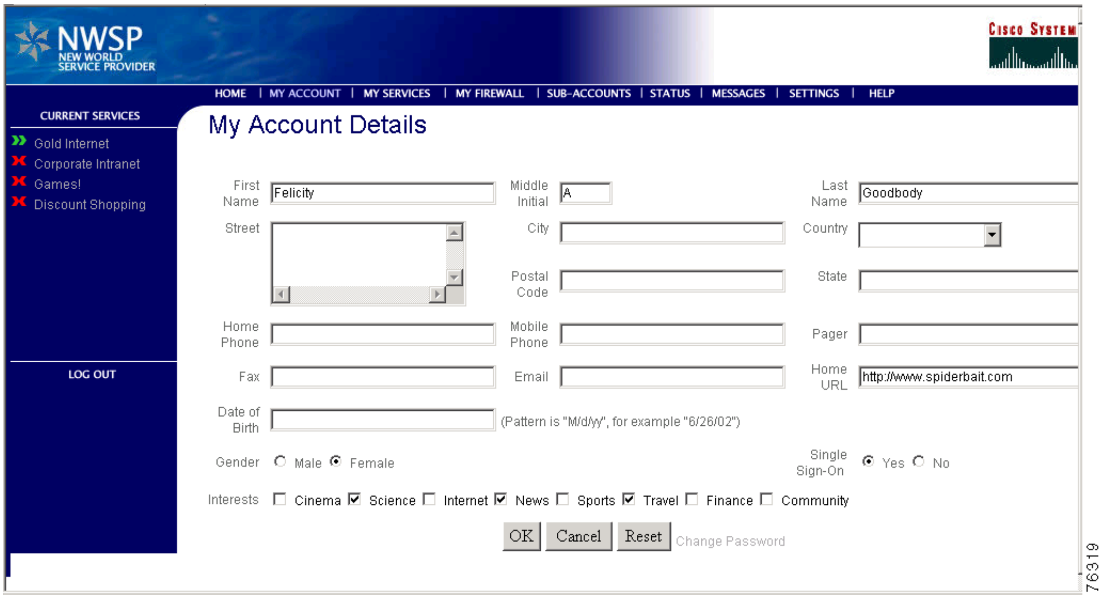
Service provider administrators use the Cisco Distributed Administration Tool (CDAT) to add subscriber profiles to the LDAP directory. Administrators use CDAT to:

- Add a new subscriber.
- Enter subscriber profile information. Required information includes an initial SESM user name and password for logging into the SESM portal. Other optional information can be entered by the administrator in CDAT, or left to the subscriber to fill in later using the self-care features in the SESM portal.
- Assign permissions that allow the subscriber to perform self-care activities. Permissions can be inherited from roles that are assigned to groups of users. User groups, roles, and permissions are Security Policy Engine (SPE) concepts and are explained in the *Cisco Distributed Administration Tool Guide*.

Personal Account Maintenance

Figure 4-1 shows the My Account Page in NWSP. See the "Supported Data Fields in a Self-Care Solution" section on page 4-4 for other supported fields that you might want to add to a personal account maintenance page.

Figure 4-1 NWSP My Account Page



My Account Details

First Name: Felicity
Middle Initial: A
Last Name: Goodbody
Street:
City:
Country:
Postal Code:
State:
Home Phone:
Mobile Phone:
Pager:
Fax:
Email:
Home URL: http://www.spiderbait.com
Date of Birth: (Pattern is "M/d/yy", for example "6/26/02")
Gender ○ Male ● Female
Single Sign-On ● Yes ○ No
Interests ☐ Cinema ☑ Science ☐ Internet ☑ News ☐ Sports ☑ Travel ☐ Finance ☐ Community

The initial display of the My Account Details page reflects the contents of the subscriber profile. After subscribers enter or update their personal details, they can go back to the My Account Details page in about 20 minutes to see the changes. In Demo mode, the changes are *not* recorded in the profile.

Personal Firewalls

The SESM personal firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on a web portal page. The portal page presents a list of applications that are available for firewall protection. The SESM deployer configures the list of applications using the Firewall MBean.

Deployers can also configure firewall controls for subscribers which cannot be changed by the subscriber. Administrators use CDAT to configure these controls.

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

The ACLs are stored in the subscriber profiles as 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:

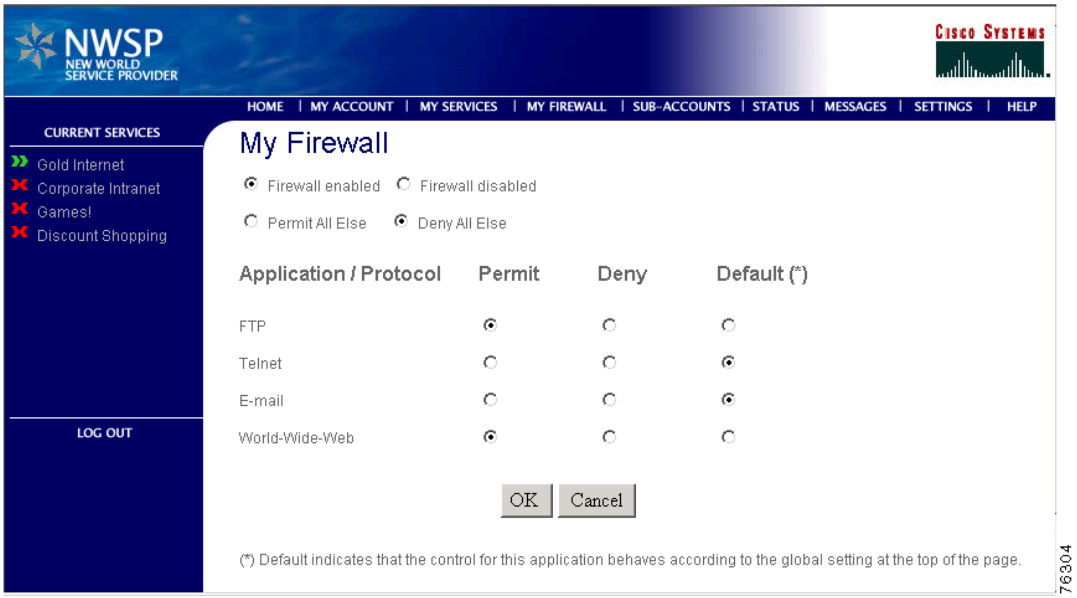
- When a subscriber configures firewall settings from the SESM portal, the portal creates the appropriate ACLs to support the subscriber’s choices. The created ACLs are grouped by application, with one ACL per chosen protocol and control direction (upstream or downstream). The ACLs allow traffic to and from *any* source and destination IP address, for a given protocol and port number. (The subscriber does not have the means to enter specific IP addresses when configuring a personal firewall.)
- In the case of deployer imposed firewall settings, the administrators manually create the correctly formatted ACLs and enter them in CDAT. The ACLs entered in CDAT can use the full range of ACL options as described in the Cisco IOS documentation.

SESM and SSG implement the firewall as follows:

- The subscriber logs into the SESM portal.
- The logon request is accepted by SESM and passes through the SSG to RDP.
- During authentication processing, RDP obtains the subscriber profile from the directory and adds all of the profile information, including the ACLs, in the access-accept reply to the SSG.
- The SSG applies the ACLs against traffic to and from the subscriber’s connection.

Figure 4-2 shows the My Firewall page in NWSP.

Figure 4-2 NWSP My Firewall Page


NWSP
NEW WORLD SERVICE PROVIDER
CISCO SYSTEMS
HOME | MY ACCOUNT | MY SERVICES | MY FIREWALL | SUB-ACCOUNTS | STATUS | MESSAGES | SETTINGS | HELP
CURRENT SERVICES
Gold Internet
Corporate Intranet
Games!
Discount Shopping
LOG OUT
OK
Cancel
76304

My Firewall

● Firewall enabled ○ Firewall disabled

○ Permit All Else ● Deny All Else

Application / Protocol	Permit	Deny	Default (*)
FTP	●	○	○
Telnet	○	○	●
E-mail	○	○	●
World-Wide-Web	●	○	○

(*) Default indicates that the control for this application behaves according to the global setting at the top of the page.

By clicking the Permit, Deny, and Default radio buttons on this page, subscribers can control the upstream and downstream traffic to their IP address.

For each application, the initial displayed state of the Permit, Deny, and Default radio buttons depends upon the ACLs that exist in the subscriber profile. The SESM portal analyzes the ACLs to determine the appropriate settings to display.

The Application/Protocol column is configurable by the deployer:

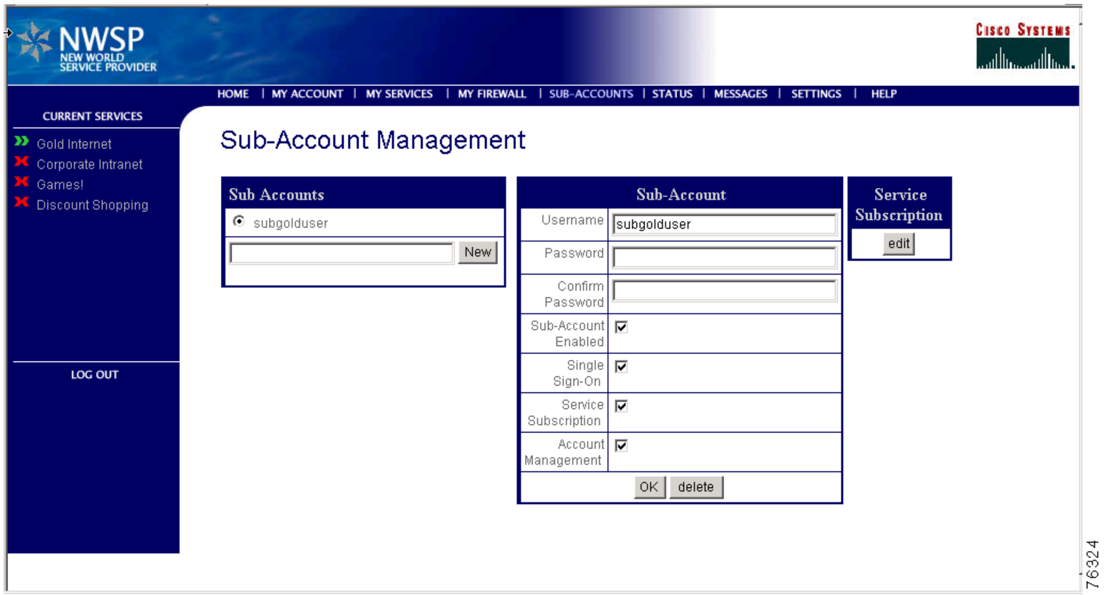
- The contents of the Applications/Protocols list is controlled by configuration attributes.
- The text strings in the Applications/Protocols list are resource bundles. The strings can be anything the deployer wants, and can be localized to match subscriber language preferences.

Subaccount Creation

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

Figure 4-3 shows the NWSP Subaccounts page.

Figure 4-3 NWSP Subaccounts Page



NWSP
NEW WORLD SERVICE PROVIDER
CISCO SYSTEMS
HOME | MY ACCOUNT | MY SERVICES | MY FIREWALL | SUB-ACCOUNTS | STATUS | MESSAGES | SETTINGS | HELP
CURRENT SERVICES
Gold Internet
Corporate Intranet
Games!
Discount Shopping
LOG OUT
76324

Sub-Account Management

Sub Accounts

● subgolduser

[ ] New

Sub-Account

Username	subgolduser
Password	
Confirm Password	
Sub-Account Enabled	☑
Single Sign-On	☑
Service Subscription	☑
Account Management	☑

OK delete

Service Subscription

edit

From this page, a subscriber can:

- Create new subaccounts
- Change passwords for subaccounts
- Change the permissions for subaccounts. For example, give or deny permission for the subaccount to:
  - Self-subscribe to services
  - Perform account self-maintenance
- Change the service subscription information for a subaccount, including:
  - Block services from this subaccount
  - Subscribe and unsubscribe services

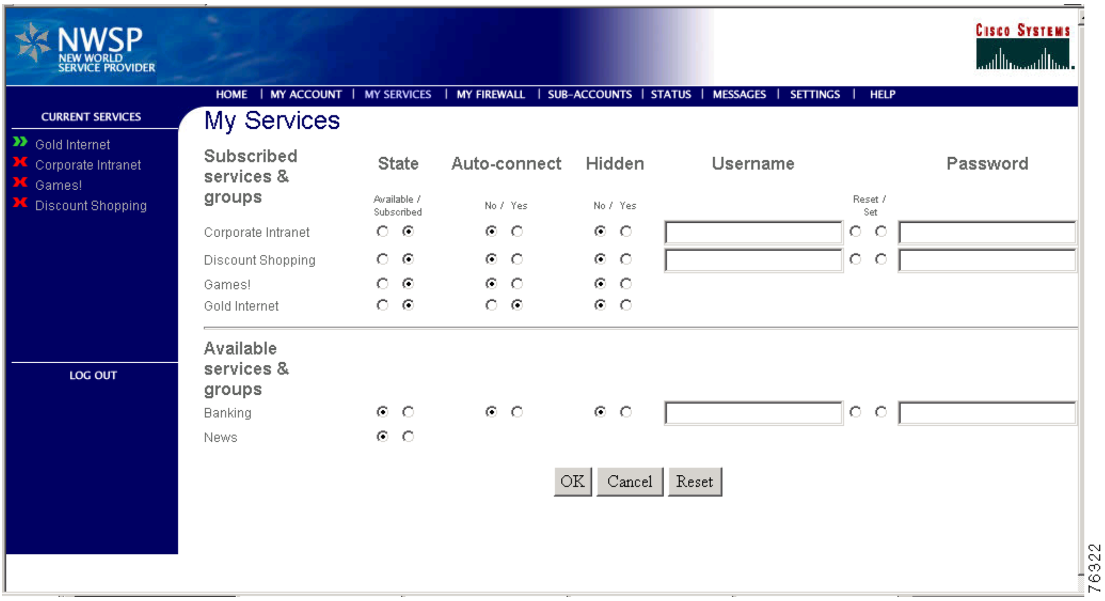
- Mark services as automatically connected and hidden.
- Provide user names and passwords for service authentication

Service Self-Subscription

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

Figure 4-4 shows the My Services page from the NWSP application.

Figure 4-4 NWSP My Services Page


NWSP
NEW WORLD SERVICE PROVIDER
CISCO SYSTEMS
HOME | MY ACCOUNT | MY SERVICES | MY FIREWALL | SUB-ACCOUNTS | STATUS | MESSAGES | SETTINGS | HELP
CURRENT SERVICES
Gold Internet
Corporate Intranet
Games!
Discount Shopping
LOG OUT
OK
Cancel
Reset
76322

My Services

Subscribed services & groups	State Available / Subscribed	Auto-connect No / Yes	Hidden No / Yes	Username	Reset / Set	Password
Corporate Intranet	○ ●	● ○	● ○		○ ○	
Discount Shopping	○ ●	● ○	● ○		○ ○	
Games!	○ ●	● ○	● ○			
Gold Internet	○ ●	○ ●	● ○			
Available services & groups						
Banking	● ○	● ○	● ○		○ ○	
News	● ○					

The page shows:

- Services available for subscription, as listed in the subscriber profile
- Whether or not this subscriber is subscribed to the service
- Whether or not the service is marked for automatic connection upon SESM logon
- Whether or not automatically connected services are hidden (not shown) on the service list
- User name and password for the service, if the service requires a logon

SESM Self-Care Demo

To demonstrate SESM self-care features using Demo mode, follow this procedure:

Step 1 Install NWSP (LDAP evaluation or licensed version) in Demo mode. See the "Quick Start for Installing and Running Portals in Demo Mode" section on page A-2 for instructions.

Step 2 Start NWSP. The start script path name is:

```
jetty
    bin
        startNWSP
```

See the "Starting a Demo" section on page A-5 for more information.

Step 3 Open a web browser and go to the NWSP page.

If the web browser is on the same system where NWSP is running, and you accepted the default port during installation, you can use the following URL:

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

Otherwise, the URL is:

```
http://NWSPhostName:NWSPportNumber
```

Step 4 On the NWSP login page, log in using the following information:

User: golduser

Password: cisco

Note To understand the relationship between values in a subscriber profile and the initial contents of the NWSP pages, examine the golduser profile in the nwsp/config/demo.txt file.

Step 5 Close the new browser window that opens as a result of the home URL specified in the profile.

Step 6 On the NWSP main page, click the **MY SERVICES** tab.

The My Services page initially displays information as recorded in the profiles in the demo.txt file.

You can change the service information on the My Services page to demonstrate self-management features. In Demo mode, the changes you make are *not* propagated into the demo.txt file.

Step 7 To demonstrate self-subscription to a new service, click the **Subscribed** radio button for one of the services in the Available list. The available services and service groups are obtained from the subscriber profile.

Note To demonstrate subscription to a service group, subscribe to News.

After a confirmation prompt, the My Services page reappears, showing the new service in the Subscribed list. In Demo mode, the new service is *not* changed to subscribed in the subscriber profile.

Step 8 To demonstrate that the new service in immediately available for connection, click the newly subscribed service in the Current Services list.

The status of the new service changes to active.

Step 9 To demonstrate setting and changing service authentication values:

1. Check the service status to make sure the service is stopped. If not, click on it in the Current Services list to stop it.
2. Click the **Set** button for one of the services, and enter a user name and password of your choice. (The golduser profile in demo.txt does not configure any service authentication values for any of the services.)
3. Click **OK**.
4. Answer **OK** to the confirmation prompt.
5. When the My Services page reappears, click the service in the Current Services list to restart it.
6. To see the Authentication Failed message, enter an invalid user name or password on the authentication page.
7. To complete service authentication, enter the user name and password you just set on the My Services page.

Step 10 To demonstrate unsubscribing to a service, click the **Available** radio button next to the service.

After a confirmation prompt, the My Services page reappears, showing the service in the Available list. If the service was running at the time you unsubscribed, the service is now stopped.

Step 11 Although you can click on the **Auto-connect** and **Hidden** radio buttons in Demo mode, you cannot demonstrate the effects of these buttons because changes are not recorded in the subscriber profile when SESM is running in Demo mode.

Step 12 Click the **MY ACCOUNT** tab to display information recorded in the subscriber profile.

The page initially displays information as recorded in the profile in the demo.txt file. You can change the subscriber information on the My Account page to demonstrate self-management features. In Demo mode, the changes you make are *not* propagated into the demo.txt file.

Step 13 To demonstrate subaccount maintenance, click the **SUB-ACCOUNTS** tab.

The installed demo.txt file contains a profile for one subaccount user (subgolduser) under the main golduser account.

Step 14 To create a new subaccount under golduser:

1. Enter a new user ID in the New field.
2. Click **New**. The new subaccount appears in the subaccount list.
3. Enter a password in the Password field.
4. Click **OK**.
5. Click Service Subscription **Edit**.
6. Select services for the subaccount and decide if they should be automatically connected and hidden.
7. Click **OK**.

In Demo mode, the subaccount profile is not added to the demo.txt file. Therefore, you cannot log in using the new subaccount.

Demonstrating Personal Firewalls

You can use the My Firewall page in Demo mode to simulate firewall changes. To see the effects of the changes, you must use a fully configured system running in LDAP mode. In a fully configured system, the effects of changes made on the My Firewall page are visible in these ways:

- View the subscriber profile in CDAT or on the LDAP directory. The firewall ACLs are visible in the Local Generic Attribute field in CDAT.
- Wait about 20 minutes (the time it takes the RDP to refresh its cache) and then view the My Firewall page again. The initial display reflects the newly created ACLs.
- Try accessing an application or protocol that you have blocked with a Deny firewall. For example, Deny access to FTP and then try to perform an FTP transfer.

APPENDIX A

Establishing a Testing Environment for SESM

This appendix describes the tools for establishing a testing environment for Subscriber Edge Services Manager (SESM) deployments. A testing environment can help with evaluating SESM features, developing customized portals, and testing deployment options. Topics in this chapter are:

SESM Demo Mode

The SESM Demo mode allows a portal to run in a simulated network, without access to other solution components, such as SSG, a RADIUS server, or an LDAP directory. Use Demo mode for the following purposes:

- To demonstrate the capabilities of SESM when other required network components are not available. In Demo mode, you can demonstrate the features of both RADIUS and LDAP deployments.
- To test customizations to JSPs in SESM portal application. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about using Demo mode during application development.

Standalone Demo mode is *only* intended for the above purposes. Demo mode is not in any way representative of SESM performance in an end-to-end solution with actual network components.

You can run any SESM portal (including your own customized portals) in Demo mode. The following characteristics apply to any SESM portal running in Demo mode:

- The portal reads profiles from a flat file in MERIT format. The file path name is configured in the SESMDemoMode MBean.
- The portal does not alter the contents of the demo profile file.

Installation and Run Options

Use one of the following methods to install and run SESM portals in Demo mode:

- Choose Demo mode at installation time—This installation option configures all of the SESM sample portals to run in Demo mode.
- Choose SPE or RADIUS mode at installation time—This installation option configures all of the SESM sample portals to run in the installed mode. You can switch to Demo mode by:
  - Using the *mode* command line option when you execute the application startup script. See the "Starting a Demo" section on page A-5 for more information.
  - Changing the portal configuration file. The run mode for the SESM portal is configured in the SESM MBean. See the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* for more information.

Using the Demo Mode Installation Option

The Demo mode installation is quick. It requires the entry of only a few parameters.

If you install in Demo mode, plan to perform another install before attempting to run an application in RADIUS or SPE mode. Do not expect to switch a Demo installation to SPE or RADIUS modes at run time for the following reasons:

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

Using the SPE or RADIUS Mode Installation Options

You can install and configure SESM to run in SPE or RADIUS mode, and then easily switch to run the application in Demo mode at run time. The switch to Demo mode at run time is easy because:

- When you install SESM in SPE or RADIUS mode, the Demo profile file that supports Demo mode is included in your installation directory.
- The MBean configuration files are set up to point to the Demo profile file when the application is run in Demo mode.
- The NWSP startup scripts accept a run time mode argument to change the mode.

To switch to Demo mode at run time, use the *mode* option on the command line when you start the SESM portal. See the "Starting a Demo" section on page A-5 for the command syntax.

Quick Start for Installing and Running Portals in Demo Mode

This section describes how to install and run SESM portals in Demo mode. It includes the following topics:

- Installing SESM in Demo Mode, page A-3
- Choosing a Browser for a Demo, page A-4
- Downloading International Character Sets, page A-4

- Starting a Demo, page A-5

Installing SESM in Demo Mode

To install SESM in Demo mode, follow this procedure:

Step 1 Log on as a privileged user:

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

Make sure you have write privileges to the directory in which you intend to load the demo.

Step 2 Obtain the installation image from the product CD-ROM or from the Cisco web site. The installation image is a tar or zip file, depending on the platform on which you want to install the demo.

Step 3 Uncompress the tar or zip file to a temporary directory. The result includes an executable .bin or .exe file. Table A-1 shows the names of the compressed and executable files.

Table A-1 Installation Image Filenames

Platform	Compressed Filename	Executable Filename
Solaris	sesm-3.1.5-pkg-sol.tar	sesm_sol.bin
Linux	sesm-3.1.5-pkg-linux.tar	sesm_linux.bin
Windows NT	sesm-3.1.5-pkg-win32.zip	sesm_win.exe

Step 4 Execute the installation image as follows:

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

```
solaris>sesm_sol.bin
```

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

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

Step 5 Follow instructions in Table A-2 to install an evaluation license type in Demo mode.

Table A-2 Instructions for Demo Mode Installation

Input Summary	Explanation
License type	Click the **Evaluation-RADIUS mode** or **Evaluation-SPE mode** button. A Demo installation is the same regardless of which license type you choose here. You do not need a license number.
License agreement	Read the displayed license agreement to ensure that you agree with the terms of the license. You must accept the agreement to proceed with installation.

Table A-2 Instructions for Demo Mode Installation (continued)

Input Summary	Explanation
Installation directory	**Tip** You must have write privileges to the installation directory. You can do any of the following: • Accept the displayed default directory: – On Solaris and Linux:`/opt/cisco/sesm_3.1.3` – On Windows NT: `C:\Program Files\cisco\sesm_3.1.3` • Click **Browse** to choose a location. • Type a directory name in the box.
Type of installation	Click the **Demo** button.
Web Application Port Number	Specify the port on which the J2EE web server for the SESM portal application will listen for HTTP requests. The displayed default value is port 8080. 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 configured to listen on 8080, change this value. 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 startup scripts to ensure that each application uses a different port.

Choosing a Browser for a Demo

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

- Netscape Release 4.x and later.

  SESM uses Unicode Transformation Format Version 8 (UTF-8) character representations. UTF-8 supports both 1-byte and double-byte character sets. To demonstrate support for double-byte character sets on a Netscape browser, use Netscape Version 6 or later.

- Internet Explorer Release 5.x and later

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

Downloading International Character Sets

To support localization, SESM uses Unicode Transformation Format Version 8 (UTF-8) character representations. UTF-8 supports both 1-byte and double-byte character sets. If your browser does not display the characters for the language that you have chosen on the NWSP Settings page, you need to download the character set from the browser vendor’s Internet site. For example, to download the Japanese character set, go to one of the following web sites:

- For the Microsoft Internet Explorer browser, go to:

http://www.microsoft.com/japan/

- For the Netscape browser, go to:

  http://wp.netscape.com/eng/intl/

For instructions on localizing an SESM portal, including how to construct translated resource bundles and images for buttons, see the *Cisco Subscriber Edge Services Manager Web Developer Guide*.

Starting a Demo

To start the NWSP application in Demo mode, follow this procedure:

Step 1 Execute the appropriate startup script as shown in Table A-3.

Table A-3 Starting the Demo

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

Note If you are using a Windows platform, ignore the nonfatal JIT error that appears in the command window upon startup.

Step 2 Open a web browser.

Step 3 Go to the NWSP URL, which is:

http://*host*:*port*

For example:

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

Where:

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

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

Step 4 On the SESM portal log on page, use any username whose profile is defined in the Demo profile file. See the "Logon Names and Passwords for a Demo" section on page A-6.

Logon Names and Passwords for a Demo

Table A-4 shows the user IDs and passwords in the profiles in the installed Demo profile file.

Table A-4 Logon Names and Passwords in demo.txt

To demonstrate RADIUS Mode features...	To demonstrate SPE mode features...	To demonstrate branding based on user groups...
User ID: radiususer Password: cisco	User ID: golduser Password: cisco	User ID: bronzeuser Password: cisco User ID: silveruser Password: cisco User ID: golduser Password: cisco
Other valid users for RADIUS mode demos are user1, user2, and so on, up to user45.	User ID: subgolduser Password: cisco **Note** subgolduser is a subaccount to golduser.	

Demo Profile Files

The Demo profile file contains sample profiles to support the SESM portals running in Demo mode. The SESM Demo mode requires a flat file with profiles in MERIT format.

You might want to examine the Demo profile file to:

- See the services and features associated with each demo user ID.
- See examples of the vendor specific attributes (VSAs) that SESM and SSG require in a RADIUS database.
- Add new profiles or change existing ones to enhance your demonstration.
- You can use the profiles in the Demo profile files as test data for SESM deployments in RADIUS mode.

Installed Path Names of Demo Profile Files

SESM comes with a different demo profile file for each sample portal application. Each demo profile file contains profiles that illustrate specific features of the sample application. The installed Demo profile files are listed in Table A-5.

Table A-5 Demo Profile File Installed Path Names

SESM Portal	Demo Profile File
NWSP	nwsp/config/demo.txt
WAP	wap/config/wapdemo.txt
PDA	pda/config/pdademo.txt

Changing the Location of Demo Profile Files

If you change the name or location of the Demo profile file, you must reflect this change in the demoDataFile attribute in the SESMDemoMode MBean in the portal's XML file.

File Contents and Format

The Demo profile files contain example subscriber profiles, service profiles, and service group profiles that support the SESM sample applications when they are running in Demo mode. The file is in Merit RADIUS flat file format and includes profiles that use the following types of attributes:

- RADIUS standard attributes
- SSG vendor-specific attributes
- SESM demonstration attributes (These are attributes reserved for SESM use; most of these attributes are meaningful in Demo mode only, and are used to simulate features available only in SPE mode.)
- For descriptions of the SSG vendor-specific attributes and SESM demonstration attributes, see the *Cisco Subscriber Edge Services Manager Deployment Guide*.

SESM Bundled RADIUS Server

The SESM bundled RADIUS server is installed by default in both RADIUS and SPE mode installations. This server provides a quick way to establish an actual SESM deployment to test, rather than relying on the Demo mode.

The SESM bundled RADIUS server is ready to run immediately after installation. It uses the following configuration:

- port—1813, on the localhost
- secret—cisco

None of the SESM installation parameters affects the default configuration of the SESM bundled RADIUS server. However, you can edit the aaa.xml file shown below to change the installed configuration. The *Cisco Subscriber Edge Services Manager Deployment Guide* contains more information about the JMX MBeans in the aaa.xml file.

The installed location of configuration files and startup scripts that support the SESM bundled 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 SESM bundled RADIUS server. The aaa.properties file is a sample profile file.

Profile File Requirements

The SESM bundled 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.

Communication with Components in the Deployment

Follow instructions in the *Cisco Subscriber Edge Services Manager Deployment Guide* to configure other components in the deployment to communicate with this RADIUS server.

- In a RADIUS mode deployment, the following components must communicate with the RADIUS server:
  - SESM web portal (NWSP)
  - SSG
- In an SPE mode deployment, you might configure the RDP to proxy to a RADIUS server. The SESM Proxy Server, described in the next section, is the SESM bundled RADIUS server configured to accept proxied requests from the RDP.

SESM SSG Simulator

The SESM SSG Simulator is installed by default in both RADIUS and SPE mode installations. This simulator provides a way to test a SESM deployment with actual authentication and service connection services when a Cisco device that can host a real SSG is not available. You can configure the SSG simulator in SESM RAD IUS or SPE deployments.

None of the SESM installation parameters affects the default configuration of the SESM bundled RADIUS server. However, you can edit the ssgsim.xml file shown below to change the installed configuration.

The installed location of files that support the SSG Simulator is the tools directory under your SESM installation directory:

```
tools
    config
        erp.xml
        ssgsim.xml
```

APPENDIX B

Using the SESM Web Services Gateway

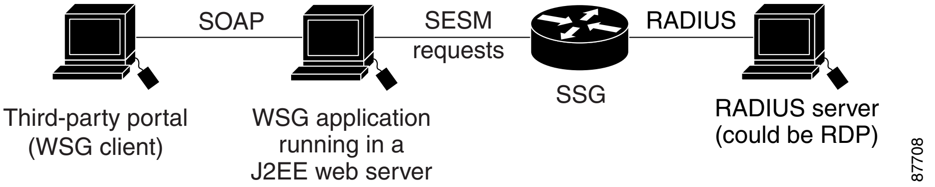
This appendix describes how to install, start, and use the WSG application and sample client. Topics are:

- Web Services Gateway Introduction, page B-1
- Installing WSG, page B-2
- Configuring WSG, page B-2
- Starting and Stopping the WSG Application, page B-2
- Running the Demonstration Client Interface, page B-3

Web Services Gateway Introduction

The Web Services Gateway (WSG) application provides a Simple Objects Access Protocol (SOAP)-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. Any client application can interface with SSG through the WSG using SOAP over HTTP communication. Figure B-1 shows WSG deployment.

Figure B-1 WSG Deployment


SOAP
SESM requests
RADIUS
Third-party portal (WSG client)
WSG application running in a J2EE web server
SSG
RADIUS server (could be RDP)
87708

The WSG installation includes a web application configured to run in a Jetty container and a command-line client script for demonstration purposes. The WSG web application runs in RADIUS and SPE modes. It does not work in Demo mode.

In this first release, the WSG client interface enables access to the SSG for the following activities:

- Authenticating, starting, and ending sessions on the SSG
- Obtaining session status
- Connecting and disconnecting services

This first release of WSG offers a preview of future development efforts. We invite interested parties to contact us through a Cisco account representative to discuss potential uses for WSG and participate in feature planning efforts for future releases.

Installing WSG

To install WSG:

1. In the SESM installation program, choose the custom installation option.
2. Check the WSG box in the list of custom installation options.

WSG is installed in the *install_dir*\wsg directory.

Configuring WSG

WSG is configured by default to run in a Jetty container on port 8100.

To change the Jetty container configuration for the WSG application, edit the following file:

```
jetty
    config
        wsg.jetty.xml
```

To change the WSG application configuration, you can either:

- Access the MBeans through the WSG AgentView (port 8200)
- Manually edit the following MBean configuration files:

```
wsg
    config
        lib.xml
        sesm.xml
        dessauth.xml
```

For explanations of the MBeans, see the *Cisco Subscriber Edge Services Manager Web Portal Guide*. The contents of the sesm.xml file is the same as the contents of nwsp.xml.

Starting and Stopping the WSG Application

The SESM installation process installs and configures the WSG application to run in a Jetty container. To start and stop WSG, run its startup or stop script:

```
jetty
    bin
        WSGstart
        WSGstop
```

This script accepts all of the options and parameters that other SESM web applications use, including the mode option, which allows you to switch between LDAP, RADIUS, and Demo modes at run time. For more information, see the *Cisco Subscriber Edge Services Manager Web Portal Guide*

The installed default port for the WSG is 8100.

Running the Demonstration Client Interface

Note The client interface is intended for demonstration purposes only. It can provide an understanding of the WSG interface and possibilities for development. Contact us through your Cisco account representative to discuss your development goals and deployment requirements regarding a WSG interface.

The demonstration client interface script provides command line access to the WSG using SOAP remote procedure calls (RPC). The script is located in:

```
wsg
    bin
        wsgClient
```

To start the client, enter the following command:

wsgClient [*endpoint*]

Where *endpoint* is always:

http://*WSGhost*:8100/services/SESM

If you do not supply the endpoint, the script provides command usage help. The wsgClient command-line prompt is:

wsg>

At the prompt, enter **help** to display available commands. At subsequent prompts, enter any of the commands.

Examples

The following examples show the WSG client command-line interface and output from various commands.

```
user1> wsgClient.sh http://localhost:8100/services/SESM
wsg/webapp/WEB-INF/lib/auth.jar:wsg/webapp/WEB-INF/lib/authentication.jar:wsg/webapp/WEB-I
NF/lib/axis.jar:wsg/webapp/WEB-INF/lib/com.cisco.sesm.contextlib.jar:wsg/webapp/WEB-INF/li
b/com.cisco.sesm.lib.jar:wsg/webapp/WEB-INF/lib/com.cisco.sesm.wsg.jar:wsg/webapp/WEB-INF/
lib/commons-logging.jar:wsg/webapp/WEB-INF/lib/dess.jar:wsg/webapp/WEB-INF/lib/jaxrpc.jar:
wsg/webapp/WEB-INF/lib/jmxri.jar:wsg/webapp/WEB-INF/lib/jmxtools.jar:wsg/webapp/WEB-INF/li
b/log4j-1.2.4.jar:wsg/webapp/WEB-INF/lib/mail.jar:wsg/webapp/WEB-INF/lib/protect.jar:wsg/w
ebapp/WEB-INF/lib/saaj.jar:wsg/webapp/WEB-INF/lib/sesm.jar:wsg/webapp/WEB-INF/lib/tt-bytec
ode.jar:wsg/webapp/WEB-INF/lib/wsdl4j.jar:lib/lib/com.cisco.sesm.lib.jar:redist/axis/lib/a
xis.jar:redist/axis/lib/commons-logging.jar:redist/axis/lib/jaxrpc.jar:redist/axis/lib/log
4j-1.2.4.jar:redist/axis/lib/mail.jar:redist/axis/lib/saaj.jar:redist/axis/lib/tt-bytecode
.jar:redist/axis/lib/wsdl4j.jar:redist/jaxp/lib/crimson.jar:redist/jaxp/lib/jaxp.jar:redis
t/jaxp/lib/xalan.jar

wsg> help
act[ivateService] svc [user passwd] - Activate service
auth[enticate] user passwd - Authenticate username/password
dea[ctivate] svc - Deactivate service
end[session] - End the session
get[status] - Get status
h[elp] - This summary
host[key] ip[/port][;name=value ..] - Set hostkey
q[uit] - Quit client

wsg> hostkey 121.121.122.3
hostkey=121.121.122.3
```

In the preceding command, 121.121.122.3 is the IP address of the subscriber. The SSG must be able to route this address. It uses the address to bind a downlink interface when it creates the edge session for the subscriber.

```
wsg> authenticate ug1-u1 cisco      // username/password respectively
authenticate=true

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: off
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: off
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> act pt1
activate pt1 = true

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: ON
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: off
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> dea pt1
deactivate pt1

wsg> act tunnelNrp4 cisco cisco   // An example of activating authenticated tunnel service
activate tunnelNrp4 = true

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: off
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: ON
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> deactivate tunnelNrp4
deactivate tunnelNrp4

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: off
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: off
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> end
endSession

wsg> quit
test-user-u10:165>
```

INDEX