CHAPTER 1

Product Introduction

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

Introduction to Cisco SESM

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

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

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

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

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

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

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

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

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

SESM Deployment Options

Two SESM deployment options are available:

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

SESM Application Suite

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

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

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

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

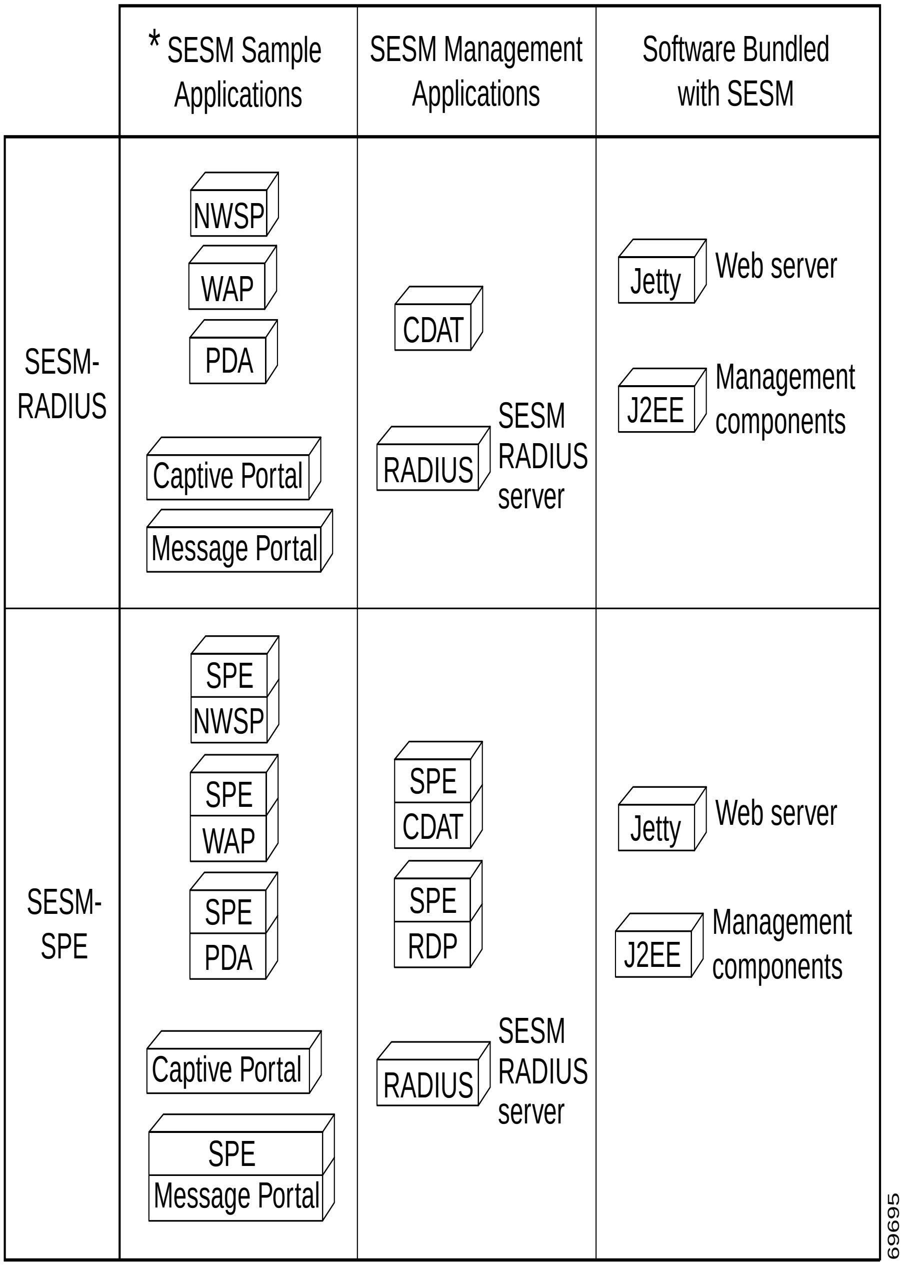
- Captive Portal application—A gateway application between the SSG and other applications in a captive portal solution. The default configuration for this application redirects subscriber browsers to either the Message Portal application or the NWSP application.
- Message Portal application—Produces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

SESM-SPE includes two additional supporting applications:

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

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

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



* Includes SESM platform development kit

Introduction to Cisco SPE

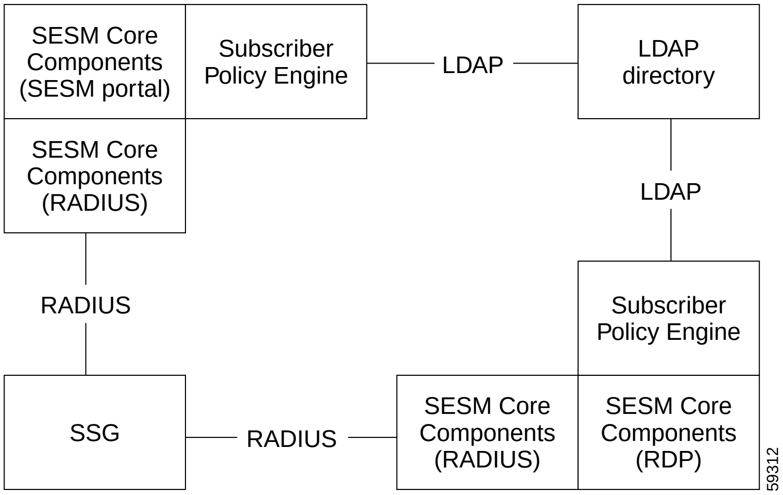
The Cisco Subscriber Policy Engine (SPE) Version 1.01 is a policy server specifically customized to provide granular subscriber service policy. SPE combines role-based access control (RBAC) functionality with an open policy server. Service providers can create differentiated subscriber groups. Service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

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

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

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

Figure 1-2 SESM Components in LDAP Mode


SESM 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

SESM Deployment Modes

You can deploy SESM portal applications in these modes:

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

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

RADIUS Mode—SESM Using an External RADIUS Server

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

See the "SESM in RADIUS Mode" section on page 2-4 for more information about the components and data flow in a RADIUS mode deployment.

LDAP Mode—SESM Integrated with SPE

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

See the "SESM in LDAP Mode" section on page 2-6 for more information about the components and data flow in an LDAP mode deployment.

Demo Mode

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

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

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

Sample Applications versus Demo Mode

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

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

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

SESM Applications

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

- Web Development Kit, page 1-6
- Sample Web Portal Applications, page 1-6
- Sample Captive Portal Solution, page 1-7
- RDP Server, page 1-7
- CDAT Application, page 1-8

Web Development Kit

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

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

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

Sample Web Portal Applications

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

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

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

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

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

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

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

Sample Captive Portal Solution

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

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

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

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

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

RDP Server

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

You can configure the RDP to run in two modes:

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

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

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

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

This guide describes how to install and configure RDP. RDP is intended to be used as installed but it is extensible for special purpose deployments. For information, see Appendix E, "RDP Packet Handlers."

CDAT Application

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

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

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

Software Bundled with SESM

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

- SPE for LDAP Mode, page 1-8
- J2EE Components, page 1-9

SPE for LDAP Mode

When you install the SPE component from the SESM installation package, the installation includes the following items:

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

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

J2EE Components

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

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

  http://jetty.mortbay.com/

- JSP engine—Jetty includes a Java Server Pages (JSP) package, which is currently the Jasper JSP engine from Apache Software Foundation.
- Sun example Java Management Extensions (JMX) server—This is a fully functional JMX server from Sun Microsystems. SESM depends on the JMX server for internal object configuration. For more information about JMX technology and its related JMX MBean standards, see:

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

The sample SESM portal applications and CDAT are installed with configuration files and startup scripts that are ready to run using the Jetty web server and the Sun example JMX server. RDP is installed with configuration files and a startup script that is ready to run using the JMX server. However, SESM is designed to allow the use of any J2EE web server and any JMX-compliant server.

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

J2EE Server

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

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

JMX Server

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

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

Required Network Components

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

- Cisco Service Selection Gateway, page 1-10
- Cisco Access Registrar or Third-Party RADIUS Server, page 1-11
- LDAP Directory, page 1-11

Cisco Service Selection Gateway

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

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

Required Cisco IOS Release

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

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

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

Communication Protocol

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

Port-Bundle Host Key Feature on SSG

The port-bundle host key is an important feature on the SSG that is used for communication between SSG and the SESM portal application. The port-bundle host key feature uses a software token (or key) that *uniquely* identifies each subscriber on the host SSG that is currently logged on to an SESM portal, even when multiple subscribers are using the same IP address. The port-bundle host key feature also provides an SSG IP address in the key.

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

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

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

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

Cisco Access Registrar or Third-Party RADIUS Server

The following scenarios require a RADIUS server:

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

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

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

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

LDAP Directory

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

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

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

Supported Hardware Platforms

An SESM deployment includes the following hardware platforms:

- SSG Devices, page 1-12
- SESM Application Server Devices, page 1-12
- Subscriber Browser Devices, page 1-13

SSG Devices

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

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

SESM Application Server Devices

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

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

Solaris

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

Windows NT

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

Windows 2000

- Pentium III (or equivalent) processor

Linux

- Red Hat Linux Version 7.1
- SuSE Linux

Subscriber Browser Devices

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

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

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

Table 1-1 Browsers for the SESM Sample Portal Applications

SESM Portal Application	Device	Other Requirements
NWSP Message Portal	• 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	