SESM Introduction

This chapter introduces the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(5). The chapter includes the following topics:

- SESM Overview, page 1-1
- SESM Component Descriptions, page 1-4
- Portal Modes, page 1-8
- Related Software, page 1-8
- Supported Platforms, page 1-13

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 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 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 Release 3.1(5) includes the following applications:

- Cisco Distributed Administration Tool (CDAT)—A web-based tool from which administrators can perform the following management functions:
  - Remotely manage and monitor SESM applications
  - 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 LDAP format 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.

SESM solutions work in conjunction with additional network software components. Depending on the goals of the solution, SESM deployments might require one or more of the following components:

- Cisco Security Policy Engine (SPE)
- Cisco Service Selection Gateway (SSG)
- RADIUS Server
- LDAP directory

The "Related Software" section on page 1-8 describes these components.

SESM Packages

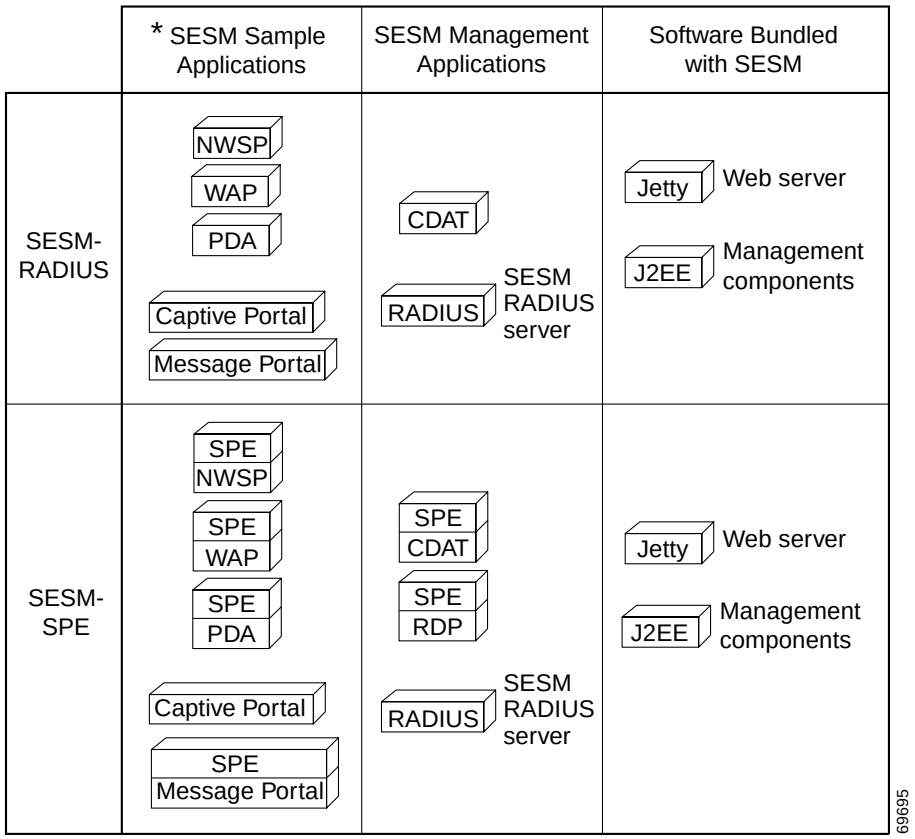
The SESM applications are available in the following packages:

- SESM-RADIUS—This package installs SESM to obtain subscriber and service profile information from a RADIUS server.
- SESM-SPE—This package integrates the Cisco Subscriber Policy Engine (SPE) 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.

Figure 1-1 shows the software included in the SESM packages. Each package is available in versions appropriate for the Sun Solaris, Linux, or Windows platforms.

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

Figure 1-1 SESM Release 3.1(5) Bundled Packages



* Includes SESM platform development kit

SESM Component Descriptions

This section describes the SESM product. Topics in this section are:

- CDAT Management Application, page 1-4
- RDP Server, page 1-5
- Web Development Kit, page 1-5
- Sample Portal Applications, page 1-6
- Sample Captive Portal Solution, page 1-6
- Bundled SESM RADIUS Server, page 1-7
- Bundled J2EE Components, page 1-7

CDAT Management Application

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:

- Remotely view and change configuration attributes for SESM applications. Configuration changes can be temporary (that is, apply to the currently running instance only) or they can be persistent, in which case the changes are applied to the application's configuration files.
- Remotely monitor SESM application activity and performance.
- 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.

For more information, see:

- The *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*—Contains information about installing and configuring CDAT and using its remote management features to configure SESM applications.
- The *Cisco Distributed Administration Tool Guide*—Contains information about the SPE directory extensions and how to use CDAT to create profiles in 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.

For more information about configuring RDP, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

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.

See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about developing a customized SESM portal application. See the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* to deploy and configure a customized application.

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 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 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.

See the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* for more information about captive portal features and how to install and configure the captive portal solution.

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.

Portal Modes

You can install and run the sample portal applications (NWSP, WAP, and PDA) in any of the SESM deployment modes:

- RADIUS Mode, page 1-8
- LDAP Mode, page 1-8
- Demo Mode, page 1-8

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

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

LDAP Mode

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), which is available from the SESM installation package if your SESM purchase license allows it.

Demo Mode

The Demo deployment mode allows the portal to run without access to other solution components, such as an 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.

Demo mode demonstrates the capabilities of both RADIUS and LDAP modes.

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. The additional software components are:

- J2EE Components, page 1-9
- Cisco Security Policy Engine, page 1-9
- Cisco Service Selection Gateway, page 1-11

- RADIUS Server, page 1-12
- LDAP Directory, page 1-12

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 Installation and Configuration 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

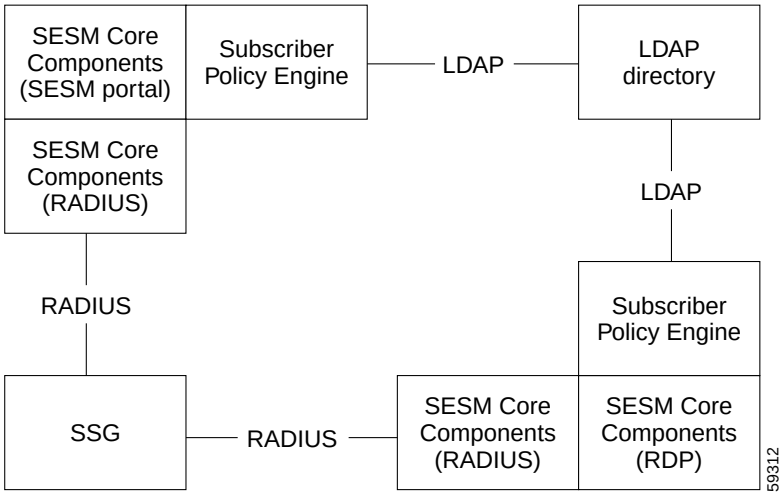
The Cisco Subscriber Policy Engine (SPE) is a policy server specifically customized to provide granular subscriber service policy. SPE combines role-based access control (RBAC) functionality with an open policy server. Service providers can create differentiated subscriber groups. Service and content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

SPE is required when SESM is deployed in 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



SPE Software

The SESM-SPE package includes SPE. When you install applications in LDAP 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.

Further Information about SPE

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

The following SESM deployments require a RADIUS server:

- SESM portals deployed in RADIUS mode—This deployment requires user and service profile information in a RADIUS database.
- SESM portals 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.
- SESM portals 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). 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 Installation and Configuration 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 LDAP mode require access to an LDAP-compliant directory. An LDAP directory allows interactive updates to information stored in the directory. 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.

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 Installation and Configuration 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.l • 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	