CONTENTS

About This Guide vii
Document Objectives vii
Audience vii
Document Organization viii
Document Conventions viii
Related Documentation viii
Obtaining Documentation ix
Cisco.com ix
Documentation CD-ROM x
Ordering Documentation x
Documentation Feedback x
Obtaining Technical Assistance x
Cisco TAC Website xi
Opening a TAC Case xi
TAC Case Priority Definitions xi
Cisco Developer Support Program xii
Program Benefits xii
Contacting Cisco Developer Support xii
Obtaining Additional Publications and Information xii

CHAPTER 1 1-1

Introduction to SESM Web Portals 1-1
Web Portal Features 1-1
Sample Web Portals 1-2
Service Selection from SESM Web Portals 1-2
Service Authentication and Authorization 1-3
Automatic Connections and Hidden Services 1-3
Subscriber Sessions 1-3
Service Status 1-3
Mutually Exclusive Service Selection 1-4
Service Selection by Bandwidth 1-4
Supported Service Types 1-5
Developing and Customizing Web Portal Applications 1-5
J2EE Web Applications 1-5
Example Web Portal Site Map 1-6
Sample Portal Pages 1-6

**CHAPTER 2**

Configuring and Running SESM Web Portals 2-1
Location of Web Portal Applications 2-1
Configuring Web Portals for Proxied Users 2-2
Configuring Customized SESM Web Portals 2-3
  J2EE Development Platform 2-3
  Changing web.xml and webdefault.xml 2-3
  Importance of the Web Portal Application Name 2-4
  Creating Configuration Files and Startup Scripts 2-5
Logging On to SESM Web Portals 2-5

**CHAPTER 3**

Location Awareness and Branding in Web Portals 3-1
Location Awareness and Web Portals 3-1
  Using Location to Control the Look and Feel of Portal Pages 3-2
  Location Names 3-2
Demonstrating Location Awareness 3-2
  Demonstrating Location Awareness Using Complete ID Attributes 3-3
  Demonstrating Location Awareness Using Subnet Entries 3-4

**CHAPTER 4**

Displaying RADIUS Reply Messages in NWSP 4-1
  Overview of RADIUS Reply Message Display in NWSP 4-1
  Configuring RADIUS Reply Message Display in NWSP 4-2

**CHAPTER 5**

Configuring Miscellaneous SESM Features 5-1
Automatic Connections 5-1
  Configuring a Service for Automatic Connection by SSG 5-1
  Configuring SESM to Request Automatic Connections in an SPE Deployment 5-2
Configuring Hidden Services 5-2
Subscriber Experiences with Automatic Connections 5-3
  Connection Status for Autoconnect Services 5-3
  Pop-Up Window for Autoconnect Services 5-3
  Disconnecting Autoconnect Services 5-3
Multikey Authentication 5-4
Arbitrary Attributes 5-5
  Configuring Arbitrary Attributes 5-5
  Demonstrating Arbitrary Attribute Assignments in Subscriber Portal 5-6
About This Guide

This preface introduces the *Cisco Subscriber Edge Services Manager Web Portals Guide*. The preface contains the following sections:

- Document Objectives
- Audience
- Document Organization
- Document Conventions
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

**Document Objectives**

This guide describes how to configure and run the Cisco Subscriber Edge Services Manager (SESM) web portal applications. The guide also describes how to configure specific SESM portal features. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their end users (subscribers) with a single web interface for accessing multiple Internet Protocol (IP) services and value-added features.

**Audience**

This guide is intended for administrators and others responsible for installing, configuring, and running SESM portal applications.
Document Organization

This guide includes the chapters shown in the following table:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Introduction</td>
<td>Describes the software in the SESM installation packages.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Configuring and Running SESM Web Portals</td>
<td>Summarizes procedures for configuring and running the web portals.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Location Awareness and Branding in Web Portals</td>
<td>Describes how to configure and use the SESM branding and location awareness features for web portals.</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Displaying RADIUS Reply Messages in NWSP</td>
<td>Describes how to configure the display of RADIUS reply messages in NWSP.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Configuring Miscellaneous SESM Features</td>
<td>Describes how to configure and use the following SESM features: arbitrary attributes, automatic connection, and multikey authentication.</td>
</tr>
<tr>
<td>Appendix A</td>
<td>PDA Considerations</td>
<td>Describes how some characteristics of PDA devices might impact subscriber experiences when accessing the SESM portal.</td>
</tr>
</tbody>
</table>

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 SESM 3.3 includes:

- **Release Notes for Cisco Subscriber Edge Services Manager 3.3(1)**
- **Cisco Subscriber Edge Services Manager Introduction Guide**
About This Guide

Obtaining Documentation

Documentation for SESM is online at:

Documentation for the Cisco SSG is online at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/

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

- Cisco IOS Security Configuration Guide:
- Cisco IOS Security Command Reference

If you are including the Cisco Access Registrar (a RADIUS server) in your SESM deployment, see the documentation for Cisco Access Registrar (AR) online at:

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:
http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:
http://www.cisco.com

International Cisco websites can be accessed from this URL:
Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:


All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:


You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
  

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click Feedback at the top of the page.

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

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.
Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:
Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.
Cisco Developer Support Program

The Developer Support Program was developed to provide formalized support for Cisco interfaces to accelerate the delivery of compatible solutions to Cisco customers. The program web site at http://www.cisco.com/go/developersupport provides a central resource point for all your development needs.

Program Benefits

- Product and document downloads
- Bug reports
- Sample scripts
- Frequently Asked Questions
- Access to Developer Support Engineers

Many of the product and document downloads are accessible with a Cisco.com guest level login. However, as a member of the program, you will get access to all the program benefits listed above to promote your development efforts. The subscription also provides the ability to open support cases using the same infrastructure and processes used by Cisco Technical Assistance Center (TAC).

Our Subscription membership is fee-based. The Developer Support Agreement, with the subscription fees and list of supported interfaces, is available on the Developer Support Web site.

Note

The Cisco TAC does NOT provide support for this API/interface under standard hardware or software support agreements. All technical support for this API/interface, from initial development assistance through API troubleshooting/bugs in final production apps, is provided by Cisco Developer Support and requires a separate Developer Support contract. When opening cases, a Developer Support contract number must be provided in order to receive support.

Contacting Cisco Developer Support

You can contact Cisco Developer Support using the following:

- Email: developer-support@cisco.com
- Web: http://www.cisco.com/go/developersupport

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *The Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

http://www.ciscopress.com

Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/go/packet

iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:


Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

Introduction

This chapter introduces the SESM web portals. The chapter contains the following topics:

- Introduction to SESM Web Portals, page 1-1
- Sample Portal Pages, page 1-6

**Introduction to SESM Web Portals**

SESM web portals interact with a Cisco edge device to enable value added services for both deployers and subscribers. SESM provides a set of sample web portal applications. The following topics provide an introduction to the SESM web portal applications:

- Web Portal Features, page 1-1
- Sample Web Portals, page 1-2
- Service Selection from SESM Web Portals, page 1-2
- Developing and Customizing Web Portal Applications, page 1-5
- J2EE Web Applications, page 1-5
- Example Web Portal Site Map, page 1-6

**Web Portal Features**

The main features of SESM web portals are:

- User logon and logoff.
- Service selection from personalized service lists.
- Personalized web pages—A single SESM web portal can support multiple locales, devices, brands, and other dimensions of the subscriber experience.
- Service connection and disconnection requests.
- User session status and messages—You can customize the RADIUS Attribute 18 reply messages for successful and unsuccessful logon.
- Advertising and messaging.
In a SESM Security Policy Engine (SPE) installation, the following additional features are available to SESM web portals:

- Self-registration.
- Account self-management.
- Service self-subscription.
- Subaccount creation.
- Personal firewall provisioning.
- Always-on connectivity using the SESM Trusted ID Authentication feature.

**Sample Web Portals**

SESM includes the following sample web portals that you can install and configure for demonstration purposes or as a starting point for customization:

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

**Note**

SESM provides a demonstration WAP portal based on Wireless Markup Language (WML) 1.3, but there is no intrinsic limitation in SESM as to the version of WML that can be used.

This guide describes how to configure and run these applications.

**Service Selection from SESM Web Portals**

After a subscriber authenticates, SESM web portals present 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. The web developer controls the format of the service list and how to portray service groups.

You can:

- Select one or more services for connection—The web 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 from 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.

This section describes the following features:

- Service Authentication and Authorization, page 1-3
- Automatic Connections and Hidden Services, page 1-3
Chapter 1      Introduction

Service Authentication and Authorization

A preliminary level of service authorization is implied by the service selection list presented to a subscriber. The SESM web portal presents for selection only those services to which a subscriber is subscribed, according to the subscriber profile. 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 username 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 Administration and Configuration 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.

For more information, see Automatic Connections, page 5-1.

Subscriber Sessions

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

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

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 the NWSP web portal 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 NWSP web portal uses the following images next to the items in the service list:

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

**Mutually Exclusive Service Selection**

Mutually exclusive service selection restricts a subscriber’s access to 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 1-4.

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 SSG.

Note

Service type is known as service class in CDAT.

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

- **Passthrough**—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 username and password. After authentication, the service is accessible until the subscriber 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.

Developing and Customizing Web Portal Applications

The SESM application programming interface (API) is used to develop and customize web portal applications in either a SESM RADIUS installation or a SESM SPE installation. The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes how to create applications for both SESM RADIUS and SESM SPE installations.

J2EE Web Applications

SESM web portals are Java 2 Platform, Enterprise Edition (J2EE) web applications that run in a J2EE-compliant web application server (servlet container). The web server is the *container* for the applications that run in it. The SESM installation program installs and configures Jetty servers as the containers for the SESM web portals. You can create a web application archive (WAR) file from the installation directory and deploy SESM web portals in other containers. For information about configuring the Jetty container, or using other web servers, see *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*. 
Example Web Portal Site Map

Figure 1-1 shows a typical example of how features are implemented in a sample Web Portal, in this case NWSP.

Sample Portal Pages

This section shows some example portal pages from some of the SESM applications.
The page shown in Figure 1-2 is from the NWSP Portal. This page is the Messages page, accessed from the Messages option at the top of the window. Successful authentication messages are automatically displayed in the Message page (unsuccessful authentication messages are displayed on the logon page).
RADIUS Attribute 18 messages can also be displayed. The RADIUS Attribute 18 message shown was customized in NWSP. SESM support of RADIUS Attribute 18 message display also supports internationalization and localization.

For information about displaying RADIUS Attribute 18 messages, see Chapter 4, “Displaying RADIUS Reply Messages in NWSP.”

**Figure 1-2 Messages Page with Successful Authentication Message**

![Messages Page with Successful Authentication Message](image)
The page shown in Figure 1-3 is from SP. This page is the home page and is displayed after the subscriber logs on successfully.

Note the following about this page:

- The list of services in the middle of the window is personalized for the current subscriber. It shows one connected service and three services available for connection (subscribed services). The subscriber can click the subscribed services to request a connection.
- The subscriber can view other portal pages by clicking the options at the top of the window.
- The message in the center of the window illustrates messaging and advertising possibilities.
- The logo in the banner shows an example of branding. See Chapter 3, “Location Awareness and Branding in Web Portals,” for additional information.

For information about customizing the look and feel of the portal page, see Cisco Subscriber Edge Services Manager Web Developer Guide.

Figure 1-3 Home Page with Personalized Service List
The page shown in Figure 1-4 is from the SP. This page uses mutually exclusive (Mutex) connection services to enable subscribers to change bandwidth with one mouse click. This feature is called the Fast Blast feature.

To change services, subscribers usually need to disconnect from one service, and then connect to another service. However, you can define a group of mutually exclusive services, which enables subscribers to switch between services without explicitly disconnecting from one service before connecting to a new one. For information about defining Mutex services see Cisco Subscriber Edge Services Manager Administration and Configuration Guide.

Note
You must be a member of the SuperUserGroup to use the Fast Blast feature.

Figure 1-4   Fast Blast Page (service level selection)
The page shown in Figure 1-5 is from SP. You can preview and download movies from this page.

**Figure 1-5  Movies Page**
The page shown in Figure 1-6 is from the WAP web portal. The WAP portal returns pages that are sized specifically for mobile phone display areas. The NWSP application, which uses device type as one of the dimensions of user shape, can also return WAP-sized pages.

Figure 1-6  WAP Home Page
Configuring and Running SESM Web Portals

This chapter summarizes procedures for configuring and running the sample web portals. The chapter contains the following topics:

- Location of Web Portal Applications, page 2-1
- Configuring Web Portals for Proxied Users, page 2-2
- Configuring Customized SESM Web Portals, page 2-3
- Logging On to SESM Web Portals, page 2-5

Note This chapter and following chapters use the NWSP web portal as an example to illustrate procedures. Similar procedures can be followed for each of the sample portals provided with SESM.

Location of Web Portal Applications

Each web portal application has its own subdirectory under the SESM installation directory. For example:

```
 nwsp
  config
   aaa.properties /* Sample RADIUS profiles
   nwsp.xml /* XML configuration file
   docs /* javadoc for the SESM libraries
   webapp /* application code and supporting files, such as images for the JSPs

da
  config
  docs
  webapp

wap
  config
  docs
  webapp
```
Chapter 2  Configuring and Running SESM Web Portals

Configuring Web Portals for Proxied Users

The mechanism used for proxying requests by the proxy server (captive portal for unauthenticated users, web proxy server for authenticated users) to the web portal requires additional configuration before running the web portal.

The sesmProxyList in the configuration file webapp/WEB-INF/web-jetty.xml lists the hostname or IP address of hosts that have SESM-aware proxies. This list must include the Captive Portal and Web Proxy hosts (hostname or IP address), as shown in the following example; otherwise, proxied users will not be able to see the web portal home page.

```xml
<!-- The sesmProxyList is a list of host and IP addresses that have SESM aware proxies. Requests proxied from these hosts should have the remote client connection details sent either inband for http request or out-of-band in Proxy meta data for https requests -->
<Set name="sesmProxyList">
  <Array type="java.lang.String">
    <Item>captivePortalHost</Item>
    <Item>webProxyHost</Item>
    <Item>127.0.0.1</Item>
    <Item>localhost</Item>
  </Array>
</Set>
```

For a full description about starting SESM applications, see Cisco Subscriber Edge Services Manager Administration and Configuration Guide.
Chapter 2 Configuring and Running SESM Web Portals

Configuring Customized SESM Web Portals

Application developers might make changes to the delivered sample applications, producing a customized application. Customized applications require their own set of configuration files, although the files might be very similar to those provided for the sample application. This section describes how to configure your customized application.

For information about customizing web applications, see Cisco Subscriber Edge Services Manager Web Developer Guide.

J2EE Development Platform

SESM provides components for creating specialized J2EE web server applications. J2EE provides a framework for using various Java-based components to develop multi-tiered applications. The multi-tiered application (as opposed to the two-tiered client-server application) provides many opportunities for isolating and controlling functional pieces of a large application. For more information about the J2EE development platform, see the Java development website on the Sun Microsystems website.

Changing web.xml and webdefault.xml

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

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

Table 2-1 shows the J2EE configuration files used to configure SESM web portals.

<table>
<thead>
<tr>
<th>Component</th>
<th>File Path and Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container (Jetty)</td>
<td>jetty/config/webdefault.xml</td>
<td>This file sets attributes that determine how Jetty handles HTTP requests and how those requests map to servlets and Java Server Pages (JSPs).</td>
</tr>
</tbody>
</table>
### Importance of the Web Portal Application Name

The SESM application name that you use for a customized application is arbitrary, but it must match in all of the following locations:

- The name of the application-specific subdirectory under the installation directory. For example, the directory that holds all application specific information for the NWSP application is:

  ```
  <installDir>
  nwsp
  ```

- Application parameter inside the application startup script. In the installed scripts, the application name is hard-coded on the line that calls the generic start script. For example, for the NWSP application on Windows, the call line in startNWSP.cmd is:

  ```
  call "%SCRIPTDIR%start.cmd" nwsp %PORTNO%
  ```

  For NWSP on UNIX/Linux, the startNWSP.sh sets the application name in the line:

  ```
  APP=nwsp
  ```

- Name of the application configuration file in the `<APP>/config` directory. For example, for the NWSP application, the configuration filename in nwsp/config is:

  ```
  nwsp.xml
  ```

- Name of the application’s configuration file in the jetty/config subdirectory. For example, for the NWSP application, the configuration filename is:

  ```
  nwsp.jetty.xml
  ```

An application name in the startup script tells the ConfigAgent which configuration file to open. The application name is passed to ConfigAgent by the application startup scripts. The application name might also be used in other ways. For example, you can configure the parameter that defines the Jetty Server log filename to incorporate the application name in the log filename.

### Table 2-1 Summary of J2EE Configuration Files (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>File Path and Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESM application</td>
<td><code>applicationName</code></td>
<td>This file defines J2EE parameters of a specific web application, including parameters related to JSPs. Each web application contains its own <code>web.xml</code> file.</td>
</tr>
<tr>
<td></td>
<td><code>webapp</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>WEB-INF</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>web.xml</code></td>
<td></td>
</tr>
<tr>
<td>SESM application</td>
<td><code>applicationName</code></td>
<td>This file is required for the port-bundle host key feature. See <em>Cisco Subscriber Edge Services Manager Administration and Configuration Guide</em> for more information.</td>
</tr>
<tr>
<td></td>
<td><code>webapp</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>WEB-INF</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>web-jetty.xml</code></td>
<td></td>
</tr>
</tbody>
</table>
Creating Configuration Files and Startup Scripts

To create the required configuration files and startup scripts for a customized SESM application that will run in a Jetty server:

**Step 1** Create a configuration file for the new application in the container’s config directory. You can copy the nwsp.jetty.xml file and appropriately rename it. For example:

```
jetty
  config
    newApplication.jetty.xml
```

**Step 2** Edit the new file.

**Step 3** Create a startup script for the new application by copying the startNWSP script and appropriately renaming the copy. For example:

```
jetty
  bin
    startNewApplication
```

**Step 4** Edit the new file, changing the application name and the port number parameters.

**Step 5** Copy the nwsp directory structure, and rename the nwsp objects appropriately. For example, copy:

```
 nwsp
   config
     nwsp.xml
 docs
 webapp
```

**Step 6** See *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about customizing the JSPs, images, and other components. That guide also describes how to update the webapp folder, recompile affected components, and edit the web.xml file.

Logging On to SESM Web Portals

To access SESM web portals:

**Step 1** Start the SESM portal application using its startup script.

**Step 2** Start a web browser on a device (such as a desktop computer, a WAP phone, or a PDA) that has network access to the server on which the SESM portal application is running.

**Step 3** Make sure the web browser has Javascript enabled.

**Step 4** Go to the URL of the SESM portal application:

```
http://host:port
```

The URL is the host and port number that you specified during the SESM installation process. Default values used during SESM installation are:

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

To override the installed port value, change the application-specific startup script. An example portal application URL is: http://server1:80
### Step 5

When the SESM portal application’s logon page appears, log in using a valid subscriber ID and password defined in a subscriber profile:

- In a SESM RADIUS installation, the subscriber profile must exist in the RADIUS server database. See the *Cisco Subscriber Edge Services Manager Administration and Configuration Guide* for more information.

- In a SESM SPE installation:
  - If RDP is configured in Proxy mode, the subscriber profile must exist in the RADIUS server database to which the RDP is proxying.
  - If RDP is configured in normal (non-Proxy) mode, the subscriber profile must exist in the LDAP directory in the SPE-specified format. See the *Cisco Distributed Administration Tool Guide* for more information.

- To log in as an iPass user, enter:
  
  `IPASS/ipassusername@ipass.com`

If logon fails, a logon failure message will appear. If logon succeeds, the portal home page is displayed. A Welcome message is available in the Messages page.

Both the logon failure and the Welcome message are RADIUS Attribute 18 messages that have been customized in the web portal.
Location Awareness and Branding in Web Portals

This chapter describes how to use the SESM branding and location awareness features in SESM web portals. The chapter contains the following topics:

- Location Awareness and Web Portals, page 3-1
- Demonstrating Location Awareness, page 3-2

Note

For a complete description of configuring location awareness features, and dynamic update of locations, see Cisco Subscriber Edge Services Manager Administration and Configuration Guide.

Location Awareness and Web Portals

The SESM location awareness feature relies on the physical location characteristics of an edge session. Some examples of using location information in customized SESM portals are:

- Location-based branding—Brand the portal pages and offer free or different services accordingly.
- Personalized portals—Tailor 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.

SESM offers two ways to configure location awareness:

- Location awareness using complete ID attributes —This is the recommended method for defining location awareness.
- Location awareness using IP subnets.

For a complete description of configuring location awareness features, and dynamic update of locations, see Cisco Subscriber Edge Services Manager Administration and Configuration Guide.
Demonstrating Location Awareness

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

Using Location to Control the Look and Feel of Portal Pages

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

- The portal can use the location as a dimension in the user shape to help determine the resources to use in the returned JSPs. NWSP uses this method to determine a location-specific image to use in the NWSP banner.
  
  See Subscriber Edge Services Manager Web Developer Guide for more information about the user shape mechanism, the location attribute in the locationDimension.jsp, and the SESMSession object.

- The portal can associate attributes to a location using the SESM arbitrary attributes feature. See Arbitrary Attributes, page 5-5 for more information.

Location Names

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

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

```plaintext
nwsp
  webapp
    london
    newyork
    paris
```

- NWSP associates arbitrary attributes to locations. The location names in the arbitrary attributes configuration must match the names used in location awareness configuration. For examples, see Arbitrary Attributes, page 5-5.

Demonstrating Location Awareness

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

Note

You cannot use a Demo installation to show location awareness using complete ID attributes.

To demonstrate location awareness based on Complete ID attributes in a SESM RADIUS or SESM SPE installation, use the following procedure:

Step 1
In the application configuration file, for example, nwsp.xml, comment out the location subnet entries in the SSG MBean.

Step 2
Uncomment the Location MBean and edit it to include a specific IP address for the “london” location. Use the IP address of a client machine that is available for the demonstration. The start and end parameters define the IP range that match the location; make sure that the range you configure contains the IP addresses of the clients that you want to associate with this location.

For example:

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

Step 3
Add a new location to the Location MBean for “newyork.” (Use this value because the installed files include a subdirectory and an image for the newyork value.) For example, insert these lines into the locations array:

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

Step 4
Start NWSP using the NWSP startup script.

Step 5
Open a browser on a client that has an IP address that matches the london location, and on a client that has an IP address that matches the newyork location.

Step 6
From each browser, go to the SESM URL. For example, go to http://servername:8080.
Step 7 Notice the images in the banners in each browser. One should say London; the other should say New York.

Step 8 On a third machine, whose IP address does not match either location, repeat step 6. The banner should not include a city name, because the third browser’s IP address is not associated with any location in the configuration file.

---

Demonstrating Location Awareness Using Subnet Entries

To demonstrate location awareness based on subnet entries in a Demo installation, use the following procedure:

Step 1 In the application configuration file, for example, nwsp.xml, uncomment the location subnet entries in the SSG MBean.

Step 2 Edit setSubnetAttribute parameters in the SSG MBean to include specific IP addresses for two different client systems that are available for the demonstration. For example:

```
<Call name="setSubnetAttribute"><Arg>NEED_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
<Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>NEED_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
<Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
```

Step 3 Start NWSP using the NWSP startup script.

Step 4 Open browsers on each of the client systems.

Step 5 From each browser, go to the SESM URL. For example, go to http://serverName:8080.

Step 6 Notice the images in the banners on each browser. One should say London; the other should say Paris.

Step 7 On a third machine, repeat step 5. The banner should not include a city name, because the third browser’s IP address is not associated with any location in the configuration file.

---

Note You cannot configure locations using subnets if you are using the port-bundle host key feature.
Displaying RADIUS Reply Messages in NWSP

This chapter describes how to configure the display of RADIUS reply messages in NWSP:

- Overview of RADIUS Reply Message Display in NWSP, page 4-1
- Configuring RADIUS Reply Message Display in NWSP, page 4-2

Overview of RADIUS Reply Message Display in NWSP

NWSP supports the display of RADIUS attribute 18 messages (also known as RADIUS Reply Message). An attribute 18 message can be returned as a response to an access request, meaning any Access-Accept, Access-Reject, or Access-Challenge that the AAA server sends to the client might include an attribute 18 message.

NWSP extracts the attribute 18 messages from the response and displays them to the user in the appropriate pages. Messages extracted from access-reject responses are displayed in the Login page, while messages extracted from access-accept responses are displayed in the Messages page. See Sample Portal Pages, page 1-6 for an example of a RADIUS reply message display in NWSP.

Note

In previous releases, SESM extracted attribute 18 messages but did not display them.

Attribute 18 message display is enabled by default. You can turn off attribute 18 message display to prevent incompatibility with any message display function that you already implemented.

How does NWSP display attribute 18 messages?

The default SESM catalog file, messages.properties (in nwsp/webapp/WEB-INF/classes,) holds sets of key-value pairs, including the following two attribute 18 related pairs:

attr18.login.success=You have successfully logged on. Welcome to the NWSP.
attr18.login.failure=This is a message from the RADIUS server about why you failed to login.

The key in each case is an attribute 18 message, and the corresponding value is the text that will be displayed in NWSP.

When the AAA server sends a RADIUS reply message, NWSP extracts the message and looks for a match between a key in the catalog and the attribute 18 message:

- If the catalog is not available, NWSP displays the original attribute 18 message as is.
- If a match is not found in the catalog, NWSP displays the original attribute 18 message as is.
- If a match is found, NWSP displays the value message that corresponds to the key.
**Customizing attribute 18 message display**

You can customize any RADIUS reply message by adding more key-value pairs to the catalog. SESM also uses catalog files to implement internationalization and localization. See *Cisco Subscriber Edge Services Manager Web Developer Guide* for details.

**How does SESM handle concatenated RADIUS reply messages?**

SSG concatenates all the RADIUS reply messages in a response into a single string. SESM enables you to separate the messages using a delimiter. The delimiter string is added as a suffix to the reply messages. When SESM gets the concatenated string, it separates the message and displays the individual messages without the delimiter string.

For example, if the original messages were:

```
REPLY-MESSAGE=msg1###
REPLY-MESSAGE=msg2###
```

The message that SESM receives from SSG is concatenated, as follows:

```
REPLY-MESSAGE=msg1###msg2###
```

The delimiter (set to `###`) separates the concatenated string into individual messages:

```
REPLY-MESSAGE=msg1
REPLY-MESSAGE=msg2
```

### Configuring RADIUS Reply Message Display in NWSP

Attribute 18 message display is enabled by default. You can turn attribute 18 message display on and off using the `enableReplyMessageDisplay` attribute in the WebApp MBean.

You can configure the delimiter to separate RADIUS reply messages using the `replyMessageDelimiter` attribute in the WebApp MBean.

**Step 1**

Using a text editor, open the `nwsp.xml` file from the following location:

```xml
<SESM>/nwsp/config/
```

**Step 2**

To enable attribute 18 message display, set the `enableReplyMessageDisplay` to true. To disable attribute 18 message display, set the `enableReplyMessageDisplay` to false. Edit the following section of the WebApp MBean in `nwsp.xml` to change true to false:

```xml
...  <!-- Enable display of RADIUS REPLY_MESSAGE in the web portal-->
  <Set name="enableReplyMessageDisplay" type="boolean">true</Set>
...
```

**Step 3**

To change the RADIUS reply message delimiter, edit the `replyMessageDelimiter` attribute configuration shown below:

```xml
...  <!-- Set the RADIUS REPLY_MESSAGE delimiter in the web portal-->
  <Set name="replyMessageDelimiter" type="String">###</Set>
...  <!-- The delimiter must comply with Java regular expression patterns. -->
```
For more information about RADIUS reply message display, see:

- *Cisco Subscriber Edge Services Manager Web Developer Guide*—Describes how to customize the text that will be displayed for RADIUS reply messages.
- *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*—Describes how to configure the SESM RADIUS server to return attribute 18 messages.
Configuring Miscellaneous SESM Features

This chapter describes how to configure the following SESM features:

- Automatic Connections, page 5-1
- Multikey Authentication, page 5-4
- Arbitrary Attributes, page 5-5

Automatic Connections

This section describes how to configure and use the SESM automatic connection feature.

An autoconnect service is a service that SSG connects immediately after the subscriber authenticates, without requiring the subscriber to explicitly select the service.

In general, if a service is marked as an autoconnect service, the SSG performs the automatic connection after the subscriber authenticates. There is a special case in SESM SPE installations in which SESM is involved with automatic connection. The following sections describe how to configure the general case and then how and when to configure the specific case that involves SESM.

Configuring a Service for Automatic Connection by SSG

A subscriber profile specifies that a service is an autoconnect service.

In a RADIUS deployment, to configure an autoconnect service, use the Account-Info A attribute in the subscriber profile. See Cisco Subscriber Edge Services Manager Administration and Configuration Guide for more information about RADIUS profile formats.

In a SESM SPE installation, to configure an autoconnect service:

- Subscribers can use the web portal’s self-management features to select and deselect the autoconnect feature for a service.
- Administrators can use CDAT to maintain subscriber profiles. See the Cisco Subscriber Edge Services Manager Profile Management Guide for information.
Chapter 5      Configuring Miscellaneous SESM Features

Configuring SESM to Request Automatic Connections in an SPE Deployment

In a SESM SPE installation, a configuration option controls whether the service list is available to the SSG at the time the user authenticates. The SSG performs automatic connections if the service list is available. When the service list is not available to the SSG, a second configuration option can specify that the SESM web portal request the automatic connections.

The RDP Add Services option controls whether the service list is included in authentication replies to SSG. The RDP Add Services option is set to true by default. You can change the setting in the RDP configuration file, rdp.xml. The Add Services option works as follows:

- When the Add Services option is set to true, the RDP returns a service list to SSG.
  
  In this case, the SSG performs automatic connections for autoconnect services specified in the subscriber profile.

  Note   The service information consumes memory on the SSG platform.

- When the Add Services option is set to false, the RDP does not return a service list to SSG. In this case, SSG cannot perform automatic connections. The advantage to this configuration is that it saves memory on the SSG platform. The disadvantage is that the user must log into the SESM web portal to connect their autoconnect services. PPP authenticated users will not have their autoconnect services connected.

  In this case, you can configure the SESM web portal to request automatic connections. The autoConnect attribute in the SESM MBean controls whether the SESM web portal requests automatic connections, as follows:

  - If the autoConnect attribute is true—SESM sends connection requests for autoconnect services in the subscriber profile.
  
  - If the autoConnect attribute is false—SESM does not request automatic connections.

Configuring Hidden Services

A hidden service is an autoconnect service that does not appear in the SESM service list. The subscriber profile controls whether an autoconnect service is hidden.

- Hidden—The subscriber profile identifies the autoconnect service using the A option.

- Not Hidden—The subscriber profile identifies the autoconnect service using both the A and the N options.

For more information about subscriber profiles, including some examples, see Cisco Subscriber Edge Services Manager Administration and Configuration Guide.
Subscriber Experiences with Automatic Connections

This section describes the behavior of SESM web portals regarding automatically connected services.

Connection Status for Autoconnect Services

The status page in SESM web portals shows the status for all services, including automatically connected services. Immediately after logging in, the service status for autoconnect services might display as not connected. This happens if the service indicators display before the connection is completed. Proxy and tunnel services, for example, can take a while to connect. If the subscriber refreshes the window or reselects the status window, the autoconnect services display with a connected status.

Pop-Up Window for Autoconnect Services

If the subscriber’s home URL is set to an autoconnect service, the pop-up window for the service might appear before the connection completes. If this occurs, the following message appears in the pop-up window:

Page cannot be displayed.

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

Disconnecting Autoconnect Services

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

When the SESM session expires:

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

We recommend running SESM web portal with single sign-on turned on.
Multikey Authentication

SESM supports multikey authentication (also known as 3-key authentication), which performs authentication using multiple RADIUS attributes.

To implement 3-key authentication:

**Step 1** Add the authentication fields to the web portal logon page.

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

**Note** You cannot use the SESM multikey authentication example if you configure SESM for iPass support.

**Step 2** Change the NWSP logon page to prompt for these keys and process them:

a. Open nwsp/webapp WEB-INF/web.xml for editing.

b. Change the following line:

   `com.cisco.sesm.webapp.control.IpassAccountLogonControl`

   to:

   `com.cisco.sesm.webapp.control.AccountLogon3KeyControl`


   c. Change the following line:

   `<param-value>/pages/accountLogon.jsp</param-value>`

   to:

   `<param-value>/pages/accountLogon3Key.jsp</param-value>`

**Step 3** Ensure that the RADIUS server authenticates against the same fields that are specified on the Login page.

In a SESM SPE installation, you can configure RDP to use additional fields for authentication.

a. Edit the DESSAuthenticationHandler Mbean from the RDP management console, or manually edit rdp.xml.

b. Add items to the AuthAttribute attribute. To configure with the installed example in NWSP that uses three keys, make sure the following items are listed in AuthAttribute, in this order: USER_PASSWORD, CALLING_STATION_ID. (The USER_NAME attribute is always used for authentication and should not appear in the AuthAttribute array.)

See the chapter on configuring RDP in the *Cisco Subscriber Edge Services Manager Profile Management Guide* for more information.

In a SESM RADIUS installation, logic to authenticate with multiple keys must exist in the RADIUS server you are using. If you are using Cisco Access Registrar (AR), add the Calling-Station-Id attribute. For information about configuring AR, see the AR User Guide. See Related Documentation, page viii for the link to the AR documentation.
Step 4 Make sure that the subscriber profiles include the values against which to authenticate. In a SESM SPE installation, in CDAT, configure the local RADIUS attribute CALLING_STATION_ID with the user telephone number, for example CALLING_STATION_ID:1234567. For more information, see the chapter on the CDAT interface in *Cisco Subscriber Edge Services Manager Profile Management Guide*.

### Arbitrary Attributes

The arbitrary attribute feature lets the deployer create any arbitrary attribute and associate it with other known attributes. For example, SP uses arbitrary attributes associated with locations to help determine the initial URL for an Internet service pop-up window.

To use the arbitrary attribute feature, you configure a multidimensional table consisting of:

- Known attribute values
- Arbitrary attributes you want to associate with each of the known values

In SP, to associate URLs with locations, the elements in the multidimensional table are as follows:

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

At run time, SESM constructs a reference table holding all of the configured values. The arbitrary attribute values are available for use by SP to help determine the initial URL for an Internet service pop-up window.

### Configuring Arbitrary Attributes

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

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

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

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

An example from sp.xml is:

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

Where:

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

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

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

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

Demonstrating Arbitrary Attribute Assignments in Subscriber Portal

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

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

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

Step 1
Configure location awareness. You can use either location awareness method: subnets configured in the SSG MBean, or complete ID attributes configured in the Location MBean.

Step 2
Edit the parameters to the addDimension calls in the WebApp MBean. Make sure the second argument in the addDimension call matches exactly the location strings you defined for location awareness. The installed sp.xml file contains the following lines:

```xml
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>london</Arg>
  <Arg>http://www.london.com</Arg>
</Call>
<Call name="addDimension">
  <Arg type="int">1</Arg>
  <Arg>paris</Arg>
  <Arg>http://www.paris-france.org</Arg>
</Call>
```

Step 3
Start SP using the SP startup script.

Step 4
Start a browser on a system whose location was configured in Step 1.

Step 5
Go to the SP URL.
Step 6  Log in using the following values:

- RADIUS deployment demos:
  - User: radiususer
  - Password: cisco
- SPE deployment demos:
  - User: golduser
  - Password: cisco

Step 7  Select the Internet service from the SP service list (if the Internet service was not automatically configured.)

A service pop-up window appears, with the browser pointing to the URL in the addDimension call. For example, the london location points to www.london.com.

Note  If you configured the Captive Portal, the browser’s original request is honored instead of the arbitrary attribute associated with the location.
Arbitrary Attributes
PDA Considerations

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

Some PDA considerations are:

- PDAs use basic IE browsers, which might lose the port number of the request during redirections. This characteristic might not be noticeable with simple configurations, but it is a problem with the SSG TCP redirection feature. It is therefore important to run the server on the default ports (80 for standard connections, 443 for secure connections).

- The webapp/decorators/httpSniff.jsp is useful for fine-tuning the recognition of the subscriber device type. This JSP modifies the default behavior of the SESM HttpSniffBean decorator, which influences the shape decoration. See the Cisco Subscriber Edge Services Manager Web Developer Guide for more information about decorators.

- If a PDA device does not have an IP address, it cannot use DNS to resolve a requested URL. The result is a “Page Not Found” error.

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

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

- PDA browsers cache easily. If a subscriber selects a web site that is cached, the cached page might display even though the subscriber is not authenticated. PDA browsers do not have controls for avoiding this behavior.
IN-1

Cisco Subscriber Edge Services Manager Web Portals Guide

OL-3884-03

INDEX

A

Add Services option 5-2
application name, web portal, importance of 2-4
arbitrary attributes 5-5
configuring 5-5
demonstrating in Subscriber Portal 5-6
attribute 18 messages, See RADIUS reply messages
authentication
  for services 1-3
  multikey 5-4
authorization for services 1-3
autoconnect services
  connection status for 5-3
disconnecting 5-3
  pop-up window for 5-3
automatic connections 1-3, 5-1
configuring services for 5-1
in an SPE deployment 5-2
subscriber experiences with 5-3

B

bandwidth, service selection by 1-4
branding 3-1

c

Captive Portal, configuring for proxied users 2-2
complete ID for location awareness 3-3
concatenated RADIUS reply messages 4-2
configuration files 2-5
configuring
  arbitrary attributes 5-5
  automatic connections in an SPE deployment 5-2
  customized web portals 2-3
  hidden services 5-2
  services for automatic connection 5-1
  web portals 2-1
  web portals for proxied users 2-2
connection metrics 1-3
connections, automatic 1-3, 5-1
connection status for autoconnect services 5-3
customized web portals
  configuring 2-3
  startup scripts for 2-5
customizing
  attribute 18 message display 4-2
  web portals 1-5

d

developing web portals 1-5
development platform for J2EE 2-3
disconnecting autoconnect services 5-3
disconnecting from services 1-2
displaying RADIUS reply messages in NWSP 4-1

e

example web portal site map 1-6

H

hidden services 1-3
Index

I

images, in service list 1-4
IP subnets, for location awareness 3-4

J

J2EE
development platform 2-3
web applications 1-5

L

location awareness 3-1
demonstrating 3-2
demonstrating using complete ID 3-3
demonstrating using subnet entries 3-4
location names 3-2
to control look and feel of portal pages 3-2
location dimension 3-2
location of web portal applications 2-1
login to web portals 2-5
logoff from web portals 1-2

M

metrics, status and connection 1-3
multikey authentication 5-4
mutually exclusive service selection 1-4

N

NWSP web portal 1-2
accessing with PDA devices A-1
displaying RADIUS reply messages 4-1
sample pages 1-6

P

passthrough services 1-5
PDA considerations A-1
PDA web portal 1-2
sample pages 1-6
portals, See web portals
port-bundle host key (PBHK)
and location awareness
required configuration files for 2-3
ports
overriding installed value 2-5
used by web portals 2-1
proxied users, configuring web portals for 2-2
proxy services 1-5

R

RADIUS reply messages
concatenated messages 4-2
configuring display in NWSP 4-2
customizing display 4-2
displaying in NWSP 4-1
running web portals 2-1

S

sample portal pages 1-6
sample web portals 1-2
self-care features 1-1
service list images 1-4
services
authentication and authorization 1-3
configuring for automatic connection 5-1
configuring hidden 5-2
connection status for autoconnect 5-3
disconnecting autoconnect 5-3
disconnecting from 1-2
hidden 1-3
pop-up window for autoconnect 5-3
status of 1-3
types 1-5
service selection
by bandwidth 1-4
from web portals 1-2
mutually exclusive 1-4
service types
passthrough 1-5
proxy 1-5
tunnel 1-5
sessions, subscriber 1-3
single sign-on 5-3
site map, web portal example 1-6
SPE, configuring automatic connections 5-2
SSG
automatic connections 5-1
concatenated RADIUS reply messages 4-2
connection features implemented by 1-2
dh sessions 1-3
hierarchical policing 1-4
service types 1-5
startup scripts 2-5
status metrics 1-3
status of services 1-3
subnets, See IP subnets
Subscriber Portal (sp) 1-2
demonstrating arbitrary attributes 5-6
sample pages 1-6
subscriber sessions 1-3

W
WAP web portal 1-2
web.xml and webdefault.xml, changing 2-3
web portals
application name, importance of 2-4
branding and location awareness 3-1
configuring and running 2-1
configuring customized 2-3
configuring for proxied users 2-2
customizing and developing 1-5
demonstrating arbitrary attributes 5-6
example site map 1-6
features 1-1
introduction 1-1
J2EE web applications 1-5
location of applications 2-1
login 2-5
logoff 1-2
ports 2-1
sample pages 1-6
samples supplied by SESM 1-2
self-care features 1-1
service selection 1-2
Web Proxy
customizing for proxied users 2-2

T
tunnel services 1-5

U
user shape 3-2