Cisco Subscriber Edge Services Manager Administration and Configuration Guide

SESM 3.3

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5366-01

CONTENTS

APPENDIX A

About This Guide

This preface introduces *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*. The preface contains the following sections:

Document Objectives

This guide provides information about the post installation configuration and management of Cisco Subscriber Edge Services Manager (SESM).

Audience

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

Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	Configuring and Managing SESM	Introduces the post installation configuration and management of SESM.
Chapter 2	Configuring RADIUS Servers to Work With SESM	Provides information on how to configure the RADIUS servers in your deployment for use with SESM.
Chapter 3	Configuring a Jetty Container for SESM	Describes how to configure a Jetty container for SESM web applications.
Chapter 4	Configuring Captive Portal	Describes how to configure SESM Captive Portal.
Chapter 5	Configuring SESM Plug and Play	Provides information on how to configure the SESM Plug and Play features.
Chapter 6	Configuring Location Awareness and Whitelist URLs	Describes how to configure and update SESM location awareness features, and location-specific whitelists.
Chapter 7	Configuring SESM for iPass Support	Provides information about SESM support for iPass users.
Chapter 8	Configuring Miscellaneous SESM Features	Describes how to configure various SESM features.
Chapter 9	Running SESM Components	Provides information on how to run SESM components after they have been installed.
Chapter 10	Using Application Manager	Provides information on how to use the SESM Application Manager.
Appendix A	SESM MBeans	Provides information on configuring SESM using MBeans.
Appendix B	SESM Security	Describes the security mechanisms used in a SESM deployment.
Appendix C	Configuring a Tomcat Container for SESM	Provides instructions to configure a Tomcat container for SESM.

Chapter	Title	Description
Appendix D	AR Basic Script for iPass Configuration	Provides the Cisco Access Registrar (AR) extension script to facilitate iPass support.
Appendix E	Generating SSL Certificates for Testing	Provides instructions to generate self-signed SSL certificates for testing environments.
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*
- *Cisco Subscriber Edge Services Manager Installation Guide*
- *Cisco Subscriber Edge Services Manager Administration and Configuration Guide*
- *Cisco Subscriber Edge Services Manager Web Portals Guide*
- *Cisco Subscriber Edge Services Manager Profile Management Guide*
- *Cisco Subscriber Edge Services Manager Web Services Gateways Guide*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Subscriber Edge Services Manager SDK Programmer Guide*
- *Cisco Subscriber Edge Services Manager Troubleshooting Guide*

Documentation for SESM is online at:

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

Documentation for the Cisco SSG is online at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/

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

- *Cisco IOS Security Configuration Guide:*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/sec_vcg.htm
- *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:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm

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:

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

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:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

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:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

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:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- 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:

http://tools.cisco.com/RPF/register/register.do

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:

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

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 applications, 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:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- 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:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

  http://www.cisco.com/en/US/learning/index.html

Configuring and Managing SESM

This chapter introduces the post installation configuration and management of Cisco Subscriber Edge Services Manager (SESM). The chapter contains the following topics:

SESM Configuration Management

After installing SESM (described in the *Cisco Subscriber Edge Services Manager Installation Guide*), you can perform some additional configuration of the SESM applications using the procedures described in this manual.

SESM application configurations are stored in XML configuration files. SESM uses the Java Management Extensions (JMX) specification and its related JMX MBean standards for application configuration. The following is a summary of JMX terminology and its relationship to SESM application management:

- JMX manageable resources—Java objects instrumented to allow spontaneous management by any JMX compliant agent. Each SESM application contains JMX manageable resources.
- JMX agent— A management entity implemented in accordance with the JMX Agent Specification. For SESM, the agent is the Cisco ConfigAgent.
- Managed beans (MBeans)—Java objects that represent a JMX manageable resource. MBeans for each SESM application are specified in XML files installed in the application's config directory under the SESM installation directory.
- JMX server (also called the MBean server)—A registry for objects that are exposed to management operations by an agent. Any object that is registered with the JMX server becomes visible to the agent. In SESM applications, MBeans are registered by the ConfigAgent or by other MBeans.

For descriptions of JMX MBean standards, see http://java.sun.com/products/JavaManagement

Administrators can change SESM application configuration by changing the attribute values in MBeans, in any of the following ways:

Using Application Manager

Application Manager (AM) is a web application that remotely manages SESM applications. It can manage multiple instances of SESM web portal and Captive Portal applications, RDP, Cisco Distributed Application Tool (CDAT), WSG, and other Application Manager instances. These applications can be installed on the same or different systems from Application Manager.

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

Two types of management windows are available:

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

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

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

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

For more information about the Application Manager, see Chapter 10, “Using Application Manager.”

Editing Application Configuration Files

The following topics describe the format of the configuration files that contain SESM MBeans, and how to manually edit the configuration files:

Application Configuration Files

The MBean configuration files are XML files, which set configurable attributes that are used to configure SESM applications. The SESM installation program assigns values for all the key attributes in these files, using a combination of default values and values you provide during the install.

Application XML configuration files are located in the application's config directory (for example, nwsp/config/nwsp.xml). If you use this method, you must stop and restart the application for the changes to take effect.

Restarting Applications after Editing

If you change configuration values by directly editing the configuration files, you must stop and restart the SESM application and its Jetty server for the changes to take effect. In a SESM SPE installation, you must also stop and restart RDP.

Note When you update location and whitelist configurations using the SESM file poller, you do not need to restart the applications. For information about the file poller, see Chapter 6, "Configuring Location Awareness and Whitelist URLs."

Application Configuration File Format

This section summarizes the application configuration file format. The structure and elements of the application XML configuration files are defined in xmlconfig.dtd, a Cisco DTD. The purpose of this summary is to provide enough information to enable you to easily edit the configuration files.

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

```
<XmlConfig>

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

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

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

 <!-- ================================================================ -->
  <Configure jmxname="com.cisco.sesm:name=Logger">
    <Set name="debug" type="boolean">false</Set>
    <Set name="debugPatterns"></Set>
    <Set name="debugThreads"></Set>
    <Set name="debugVerbosity">LOW</Set>
    <Set name="logDateFormat">yyyyMMdd:HHmmss.SSS</Set>
    <Set name="logFile"><Property name="application.home"
default="."/>/logs/yyyy_mm_dd.application.log</Set>
    <Set name="logFrame"  type="boolean">false</Set>
    <Set name="logThread" type="boolean">false</Set>
    <Set name="logStack"  type="boolean">false</Set>
    <Set name="logToErr"  type="boolean">false</Set>
```

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


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

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

The following guidelines explain the basic format of the application configuration files.

- The application configuration file contains a single <XmlConfig> element containing one or more <Instantiate>, <Configure>, and <Action> elements.
- An <Instantiate order = *x*> element causes the ConfigAgent to construct and initialize the named MBean or class of MBeans.

  The value assigned to the order attribute controls the order in which objects are initialized by the ConfigAgent. The lowest value is initialized first and the highest value is initialized last. For example, in the nwsp.xml file, the logger MBean uses the value 1, to ensure that it is initialized first.

  After being initialized, an MBean registers itself with the MBean server. When ConfigAgent detects the newly registered object, it configures the object.
- An <Action> element calls methods on an MBean.
- Each <Configure> element describes the configuration for either:
  - A single MBean, identified with the name attribute
  - A class of MBeans, identified with the class attribute

  ConfigAgent can match a registered MBean by either class or name.
- The <Set> tag within a <Configure> element identifies an MBean attribute. The format for the <Set> tag is:

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

  Where:

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

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

value is the attribute value. You can edit the value, making sure that the value you provide conforms to the data type specified.

- The <Call> tag calls a method defined within the class or the object's class. If the method expects arguments, they are specified within the call tag as well.

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

- The <Arg> tag inside a call tag can be set to any of the following:
  - Literal values.
  - Objects that are created by a New element or returned by a Call element. Call and New elements might contain Set, Put, Call, Array, or Map elements nested in any Arg element. These nested elements are applied to the created or returned object.
- The <Action> tag calls a method defined within the class.
- A <SystemProperty> or <Property> tag might appear inside a <Set> or <Call> tag.

Note If a value is assigned in the start script, it is used in preference to the corresponding default value assigned in these tags. To ensure that the default values in the configuration files are used, remove any use of the corresponding settings in the appropriate startup scripts. See SystemProperty and Property Tags in Configuration Files, page 1-6 for more information.

Cisco ConfigAgent enables you to perform the following management functions for MBeans.

- Construct and initialize an MBean—ConfigAgent uses the <Instantiate> tag to construct and initialize an MBean. Most MBeans are initialized by other objects (for example, other MBeans) and not by ConfigAgent.

  After initialization, an MBean registers with the JMX server.
- Configure an MBean—ConfigAgent uses <Configure> tag to configure an MBean.

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

SystemProperty and Property Tags in Configuration Files

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

- SystemProperty tags—The property value applies to the Java Virtual Machine (JVM). All applications running in the same container must be configured to use the same value.
- Property tags—The property value applies to the name space of an application. Multiple applications running in the same JVM can use properties of the same name but configured with different values.

Note If you use the Store button in the SESM remote management tool to persist a change to an MBean attribute, any <SystemProperty> and <Property> tags in that MBean are overwritten. The Store button saves the currently defined values of all attributes in the MBean, regardless of how those values were derived. The application management tool cannot be aware of properties defined in the configuration file, nor can it be aware of values assigned using the startup scripts.

The value of a property can be set in one of the following ways:

- You can specify a value on the command line at run time. The command line value overrides all other values. The -D argument to the java command defines the value of a property. For example:

  ```
  startNWSP.sh -jvm -DpropertyName=value
  ```

  Note It is not recommended to use the -jvm option in the command line to set application port numbers.

- You can specify a value in the start script using the -D option to the java command. For example, the following lines from the installed start script (START.sh or START.cmd) assigns values to some properties.

  ```
  $JAVA $SERVER -Xms64m -Xmx64m \
    -classpath $CLASSPATH \
    -Dinstall.root=$INSTALLDIR \
    -Djetty.home=$JETTYDIR \
    -Dapplication.home=$APPDIR \
  ```

- If a value is not specified by either of the above methods at application run time, the application uses a default value specified in the application configuration file, in the <SystemProperty> or <Property> tag.

SESM Agent View

SESM Agent View is a web-based view of managed resources and associated MBeans. The Agent View is an adaptation of the Management Console provided by the HTML adaptor server, which is included with the Sun example JMX server. The Cisco adaptations add persistence features to the server.

For more information, see Using Agent View to Configure MBeans, page A-62.

SESM File Poller

Some SESM configurations, for example, locations and whitelist URLs, are based on verbose configuration, which cannot easily be configured through the SESM management screens. In previous releases of SESM, to change the verbose configuration of a module, all the files that contained the configuration clauses had to be modified manually, and the applications had to be stopped and then restarted to apply the changes.

This release of SESM provides a file poller mechanism that updates location and whitelist URL definitions without interrupting the user experience. It can also be used to share a configuration file among several applications, so that a configuration that is contained in several applications needs to be maintained only in a single file.

The file poller polls specified XML configuration files at defined intervals to check whether they have been modified. If a file has been modified, the file poller updates the configuration of the appropriate MBeans.

For more information, see Using the File Poller to Update Locations and Whitelist Configurations, page 6-13.

Configuration Tasks for Managing SESM

Note Before installing SESM, you should have configured the following:

- Configure the SSG to work with SESM.
- For a SESM SPE installation, configure your LDAP server.

If you have not configured these, you must configure them before configuring SESM. See the *Cisco Subscriber Edge Services Manager Installation Guide* for configuration information.

The following are the main configuration tasks for managing SESM:

- If you have installed a web portal application, perform any configuration or customization required using the procedures given in the *Cisco Subscriber Edge Services Manager Web Portals Guide*.
- Configure the RADIUS servers in your SESM deployment using procedures given in Chapter 2, "Configuring RADIUS Servers to Work With SESM."
- Configure the Jetty container for SESM web applications using the procedures given in Chapter 3, "Configuring a Jetty Container for SESM."

  Note To create WAR files for containers other than Jetty, and to configure a Tomcat container, see Appendix C, "Configuring a Tomcat Container for SESM."

- Configure the Captive Portal application using the procedures given in Chapter 4, "Configuring Captive Portal."
- If required, configure the Plug and Play functionality using the procedures given in Chapter 5, "Configuring SESM Plug and Play."
- If required, configure location awareness features and whitelist support using the procedures given in Chapter 6, "Configuring Location Awareness and Whitelist URLs."

- If required, configure the iPass support functionality using the procedures given in Chapter 7, "Configuring SESM for iPass Support."
- If required in a SESM SPE installation, configure the Radius Data Proxy (RDP) application using the information provided in the *Cisco Subscriber Edge Services Manager Profile Management Guide*.
- In a SESM SPE installation, configure profile management using the CDAT application. See the *Cisco Subscriber Edge Services Manager Profile Management Guide* for further details.

For information about memory requirements for SESM applications and optimizing performance, see the *Cisco Subscriber Edge Services Manager Installation Guide*.

Configuring RADIUS Servers to Work With SESM

This section describes the configuration requirements for RADIUS servers in Cisco Subscriber Edge Services Manager (SESM) deployments. This section contains the following topics:

Overview

SESM works with any RADIUS server that accepts vendor-specific attributes (VSAs). Cisco VSAs define the subscriber and service profile information required for use with SESM.

Typically, you use a RADIUS server with SESM because you do not require the self-care features provided by the SPE.

Note Cisco Access Registrar is a carrier class RADIUS platform that is fully tested with SESM. For the link to information on configuring Cisco Access Registrar to work with SESM, see Related Documentation, page xiii.

The RADIUS protocol is based on a client-server model. This protocol uses a RADIUS server, and multiple dial-in Network Access Server (NAS) devices are the clients. Before communication can occur, you must configure each client on the RADIUS server. See Configuring a SESM AAA RADIUS Client List, page 2-2 for more information.

General Procedure for Configuring RADIUS Servers

To configure RADIUS servers in your deployment to work with SESM:

Step 1 Configure the RADIUS clients in your deployment using the information given in Configuring a SESM AAA RADIUS Client List, page 2-2.

Step 2 Define any RADIUS attributes as required using the information given in Defining RADIUS Attributes, page 2-3.

Step 3 Configure the RADIUS accounting feature using the information given in Configuring the RADIUS Accounting Feature, page 2-7.

Step 4 If required, configure the Cisco Access Registrar. For the link to information on configuring Cisco Access Registrar to work with SESM, see Related Documentation, page xiii.

Note Note for information on RADIUS profiles, please refer to RADIUS Profiles for SESM Deployments, page 2-7.

Configuring a SESM AAA RADIUS Client List

SESM deployments require that you configure the following RADIUS clients on the RADIUS server:

- The SSG host—This is the Cisco device on which SSG is running, such as the Cisco 7200, Cisco 7400, or a node route processor (NRP) on the Cisco 56. The RADIUS server must recognize each SSG host as a client.
- The SESM web portal—This might be NWSP or your customized SESM web portal. SESM web portals query the RADIUS server directly for service information. The RADIUS server must recognize the SESM web portal as a client.

Table 2-1 summarizes the information that might be required to define a NAS client on the RADIUS server. See your RADIUS server vendor documentation for more specific requirements, syntax, and procedures.

Table 2-1 NAS Client Configuration

Property	Description
Name or IP Address	Identifies the client. Use either IP address or hostname.
Shared Secret	Must match a shared secret value configured on the client. If the shared secrets do not match, the RADIUS server issues an access-reject message. A shared secret is a value that is configured on both the client and the server. It is never sent over the network. The shared secret is used for MD5 encryption of the profile password.
Type	For SSG—Cisco:NAS For SESM—RAD_RFC

To configure a SESM (authentication, authorization, and accounting) AAA RADIUS client:

Step 1 Using a suitable text editor, open the AAA configuration file, aaa.xml from the following location:

<SESM>/tools/config/aaa.xml

Step 2 Uncomment the CLIENT LIST section of the aaa.xml file, to make the client list active.

```
<!-- CLIENT LIST
- Uncomment and customize this section to define a
- client list and/or per client secrets
<Set name="allowedClients">
<Array class="java.lang.String">
<Item>localhost:localsecret</Item>
<Item>10.0.0.1</Item>
</Array>
</Set>
-->
```

Note Once active, SESM AAA responds only to requests from the clients in the list.

Step 3 Within the aaa.xml file, edit the client list to include your SSGs and SESM servers as follows:

Original lines:

```
<Item>localhost:localsecret</Item>
<Item>10.0.0.1</Item>
```

Modify lines to:

```
<Item>SSG_IP_ADDRESS:SSG_RADIUS_SECRET</Item>
<Item>SESM_IP_ADDRESS:SESM_RADIUS_SECRET</Item>
```

Step 4 Restart the SESM AAA server for changes to take effect.

Defining RADIUS Attributes

RADIUS servers use an attribute dictionary to define the attributes that can appear in profiles. An attribute dictionary contains:

- Standard RADIUS attributes as defined by RFC 2138.
- Vendor-specific attributes (VSAs) that extend the standard attributes. VSAs add new capabilities, supported by specific vendors, to the RADIUS server. The value of a VSA can be one or more subattributes whose meanings depend on the vendor's definition.

This section contains the following topics:

Using Predefined RADIUS Attributes in SESM Applications

SESM applications, including RADIUS Data Proxy (RDP), Cisco Distributed Administration Tool (CDAT), and the web portal applications, internally predefine the standard RADIUS attributes and the Cisco SSG VSAs. You can use these predefined attributes in RADIUS and SPE profiles whether or not they are defined in an attribute dictionary.

Table 2-2 lists the standard RADIUS attribute names that are predefined in SESM applications. Table 2-3 shows the Cisco SSG VSAs that are predefined in SESM applications.

Table 2-2 Standard RADIUS Attributes Predefined in SESM Applications

RADIUS Attribute Names[1]		
USER_NAME	SESSION_TIMEOUT	ACCT_LINK_COUNT
USER_PASSWORD	IDLE_TIMEOUT	ACCT_INPUT_GIGAWORDS
CHAP_PASSWORD	TERMINATION_ACTION	ACCT_OUTPUT_GIGAWORDS
NAS_IP_ADDRESS	CALLED_STATION_ID	EVENT_TIMESTAMP
NAS_PORT	CALLING_STATION_ID	CHAP_CHALLENGE
SERVICE_TYPE	NAS_IDENTIFIER	NAS_PORT_TYPE
FRAMED_PROTOCOL	PROXY_STATE	PORT_LIMIT
FRAMED_IP_ADDRESS	LOGIN_LAT_SERVICE	LOGIN_LAT_PORT
FRAMED_IP_NETMASK	LOGIN_LAT_NODE	ARAP_PASSWORD
FRAMED_ROUTING	LOGIN_LAT_GROUP	ARAP_FEATURES
FILTER_ID	FRAMED_APPLETALK_LINK	ARAP_ZONE_ACCESS
FRAMED_MTU	FRAMED_APPLETALK_NETWORK	ARAP_SECURITY
FRAMED_COMPRESSION	FRAMED_APPLETALK_ZONE	ARAP_SECURITY_DATA
LOGIN_IP_HOST	ACCT_STATUS_TYPE	PASSWORD_RETRY
LOGIN_SERVICE	ACCT_DELAY_TIME	PROMPT
LOGIN_TCP_PORT	ACCT_INPUT_OCTETS	CONNECT_INFO
REPLY_MESSAGE	ACCT_OUTPUT_OCTETS	CONFIGURATION_TOKEN
CALLBACK_NUMBER	ACCT_SESSION_ID	EAP_MESSAGE
CALLBACK_ID	ACCT_AUTHENTIC	MESSAGE_AUTHENTICATOR
FRAMED_ROUTE	ACCT_SESSION_TIME	ARAP_CHALLENGE_RESPONSE
FRAMED_IPX_NETWORK	ACCT_INPUT_PACKET	ACCT_INTERIM_INTERVAL
STATE	ACCT_OUTPUT_PACKETS	NAS_PORT_ID
CLASS	ACCT_TERMINATE_CAUSE	FRAMED_POOL
VENDOR	ACCT_MULTI_SESSION_ID	

1. A hyphen (-) can replace the underbar (_) in RADIUS attribute names. The attribute names are not case-sensitive.

Table 2-3 Cisco VSAs Predefined in SESM Applications

RADIUS Attribute	Vendor ID	Subattribute	Name[1]	Type
26	9	1	Cisco-Av	String
26	9	250	Account-Info	String
26	9	251	Service-Info	String
26	9	252	Command-Code	BINARY
26	9	253	Control-Info	String

1. The hyphen (-) and underbar (_) are interchangeable in RADIUS attribute names. The attribute names are not case-sensitive.

Defining New Attributes

To define additional attributes to use in profiles, such as Cisco VSAs not predefined in the SESM code and non-Cisco VSAs, use the following methods:

- In a SESM RADIUS installation, define the attribute in the RADIUS server attribute dictionary. See your RADIUS server vendor's documentation for instructions and syntax. If you are using the bundled SESM RADIUS server, use the RADIUSDictionary MBean used by the bundled SESM RADIUS server.
- In a SESM SPE installation, you can define new RADIUS attributes in the RADIUSDictionary MBean used by the RDP application.

For an explanation of the RADIUSDictionary MBean, see Appendix A, "SESM MBeans." SESM Application Manager (AM) provides a scenario for editing the RADIUSDictionary MBean for a selected application.

Dynamically Defining New Attributes for Testing and Development

SESM allows you to dynamically define a new attribute when you first use it in a profile. This feature is intended only for testing, demonstration, and development purposes. Use the dynamic attribute feature only in the following circumstances:

- The SESM portal is running in a Demo installation.
- The SESM portal is running in a SESM RADIUS installation, and the RADIUS server you are using is the bundled SESM RADIUS server.
- The SESM portal is running in a SESM SPE installation in a testing or development environment.

Dynamic attributes are defined as new subattributes under the standard RADIUS VSA number 26.

Valid formats are:

[*attributeName*](*radiusAttributeId, vendorId*, *vendorSubattribute*, *datatype*)

Note If you omit *attributeName*, the parentheses surrounding the attribute definition are optional, but recommended.

Where *attributeName* is the name of the new attribute.

This field is optional. If you use it, subsequent profiles can use just the *attributeName*, without the attribute definition. However, be sure that the profile containing the attribute definition gets used before any other profiles that use only the *attributeName*.

Note To successfully use the attribute by name in a different profile, the user whose profile contains the attribute definition must log onto the portal before any user whose profile contains only the new attribute name without the definition.

If you do not use *attributeName*, use only the attribute definition in the profiles.

- *radiusAttributeId*—Use attribute value 26, the VSA.
- *vendorId*—A RADIUS vendor ID.
- *vendorSubattribute*— A unique number that distinguishes this attribute from other VSAs for the same vendor.
- *datatype*—One of the following values: BINARY, STRING, INTEGER, IPADDRESS. When datatype is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string.

An example follows:

demoVSA(26, 1, 1, BINARY)

Another valid syntax is:

name([[type=]26],[vendorId=]*vendorId*,[vendorType=]*vendorType*,[dataType=]*dataType*)

Merit File Examples

In a Merit file, define a new attribute and assign a value in the following format:

[*attributeName*](*attributeDefinition*) = "*attributeValue*"

MY_ATTRIBUTE(type=26, vendorId=9, vendorType=55, dataType=INTEGER) = "34"

BINARY_ATTRIBUTE(type=26, vendorId=9, vendorType=56, dataType=BINARY) = "0x3F45"

(26,9557,IPADDRESS) = "34.43.54.240"

CDAT Examples

In CDAT, define a new attribute and assign a value in the Local RADIUS attributes field as follows:

[*attributeName*](*attributeDefinition*):*attributeValue*

For example:

MY_ATTRIBUTE(type=26, vendorId=9, vendorType=55, dataType=INTEGER):34

BINARY_ATTRIBUTE(type=26, vendorId=9, vendorType=56, dataType=BINARY) :"0x3F45"

(26,9,557,IPADDRESS):34.43.54.240

Configuring the RADIUS Accounting Feature

If you configure a RADIUS accounting port, SSG generates accounting records and forwards them to the RADIUS server. To configure a RADIUS server for accounting only, you must perform the following configuration steps:

- Configure the NAS clients as described in Overview, page 2-1.
- Add the Cisco VSAs to the RADIUS server attribute dictionary, as described in Defining RADIUS Attributes, page 2-3.
- Configure an accounting port on the SSG, as described in *Cisco Subscriber Edge Services Manager Installation Guide*.

Note You do not need to provide service and subscriber profiles if you are using the RADIUS server solely for accounting purposes.

The subscriber actions that cause SSG to generate a RADIUS accounting record are:

- Subscriber logs in.
- Subscriber logs off.
- Subscriber accesses a service.
- Subscriber terminates a service.

Use the following references for more information:

- SSG documentation—Describes the attributes contained in the accounting records.
- RADIUS server vendor documentation—Describes RADIUS accounting capabilities.

RADIUS Profiles for SESM Deployments

This section describes the RADIUS profiles and attributes used in SESM RADIUS installations. The section describes the Cisco VSAs and their subcodes supported in SESM and SSG solutions.

Note For profile descriptions for SESM SPE installations, see the *Cisco Subscriber Edge Services Manager Profile Management Guide*.

This section contains the following topics:

For sample profiles and explanations, see the aaa.properties file in nwsp/config/ in the SESM installation directory.

Service Profiles

Service profiles define the services that subscribers can select from SESM web portals. You must configure a service profile for each service that can be accessed through the SESM web portal.

Table 2-4 describes the attributes in a RADIUS service profile. Use the following references for more information:

- If you are using the Cisco Access Registrar, see the Cisco Access Registrar documentation for service profile examples and syntax. Otherwise, see your RADIUS server vendor documentation for the syntax of a service profile
- For sample SESM service profiles that can be used in SESM RADIUS installations, see the aaa.properties file located in the NWSP config directory (for example, nwsp/config/ aaa.properties). This file is installed whether or not you choose the demo option. It shows service and subscriber profiles in Merit RADIUS format.
- The SSG documentation describes service profile attributes and provides examples of their use. See Related Documentation, page xiii for a link to online SSG documentation.

Table 2-4 Attributes in Service Profiles

Attribute	Description
Service profile name	An identifying name for a service profile. Each profile name must be unique. Service profile names are used in the subscriber profiles to indicate that a subscriber is subscribed to the service.
Password	Must match the service password on the RADIUS server. SESM obtains the service password directly from the RADIUS server. In SESM, configure this password in the servicePassword attribute in the AAA MBean.
Service-Type	Standard RADIUS attribute number 6. The value must be “outbound.”
Session-Timeout	Standard RADIUS attribute number 27. Specifies the maximum length of time, in seconds, that this service (the service object on SSG) can remain active in a session at any one time. When the time expires, SSG deletes the service object, which disconnects subscribers from the service. If the host key feature is enabled on the SSG, the SSG signals the state change to the SESM web portal. **Note** The NWSP application does not relay this state change to the subscriber. If Session-Timeout is not set, there is no limit on how long subscribers can use the service. In a dial-up networking or bridged (non-PPP) network environment, subscribers can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, which can be a problem if the IP address is obtained by another user. You can use the Session-Timeout and the Idle-Timeout attributes to prevent this problem.
Idle-Timeout	Standard RADIUS attribute number 28. Specifies the maximum length of time, in seconds, that a service connection can remain idle before it is disconnected. See the explanation of the Session-Timeout attribute, above, for more information about setting this attribute.

Table 2-4 Attributes in Service Profiles (continued)

Attribute	Description
Service-Info	A VSA (attribute number 26), vendor 9, subattribute 251. Valid values for Service-Info attributes are: • **A***authenType*—Specifies whether SSG uses the CHAP or PAP protocol to authenticate users for proxy services. • **I***description*—Service description. Optional. Describes the service. • **T***type*—Type of service. Optional. Valid values for *type* are: – P—Passthrough. This is the default. – T—Tunnel. – X—Proxy. Indicates that the SSG performs proxy service. • **M***mode*—Service mode. Optional. Valid values for *mode* are: – S—Sequential mode. Prevents the subscriber from accessing any other services while connected to this service. – C—Concurrent mode. This is the default. Allows the subscriber to simultaneously log onto this service while connected to other services. • **R***ip_address;mask*—Service route (destination). Required. Specifies the network or the host where the service resides. Multiple instances of this attribute can exist within a single service profile, to specify multiple service destinations. An Internet service is typically specified as "R0.0.0.0;0.0.0.0". • **D***ip_address_1[;ip_address_2]*—DNS Server Address. Optional. Specifies the IP addresses for the primary and secondary DNS servers to use for the domains that are defined using the O option. • **O***name1[name2]...[;nameX]*—Domain names. Optional. • **S***RadiusServerAddress;authPort;acctPort;secret*[;*retrans*;*timeout*;]—Remote server information. Required when type of service (T) is Proxy (X); not applicable for other service types. Specifies the remote RADIUS server that will perform authentication, authorization, and accounting for this service. • **G***key*—Service next hop gateway. Specifies the next hop key for this service. Each SSG uses its own next hop gateway table that associates this key with a valid IP address. See Next Hop Gateway Profiles, page 2-16 for information about creating a next hop gateway table. • **U***url* or **H***url*—These attributes specify the URL that is displayed in the HTTP address field when the service opens. If the SESM web portal is designed to use HTML frames, then these options also specify whether the service is displayed in a new browser window or in a frame in the current (SESM) window, as follows: – **U***url*—URL for a service displayed in its own browser window. – **H***url*—URL for a service displayed in a frame in the SESM portal window. **Note** In a frameless application, both U and H cause a new browser window to open for the service. The NWSP and SP applications are frameless applications. • **B***size*—The PPP maximum transmission unit (MTU) for SSG as a LAC. By default, the PPP MTU size is1500 bytes.

Table 2-4 Attributes in Service Profiles (continued)

Attribute	Description
Service-Info (*continued*)	• **X**—Indicates that the RADIUS authentication and accounting requests use the full username (for example, user@service). • **QU**;*upstream-token-rate*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-token-rate*;*downstream-normal-burst*;[*downstream-excess-burst*]—Indicates the hierarchical policing policies, also known as quality of service (QOS) for this service. • **V***string*—Service-defined cookie. Optional. Specifies any information that you wish to include in RADIUS authentication and accounting requests. SSG does not parse or interpret *string*. You must configure the proxy RADIUS server to interpret this attribute. SSG supports only one service-defined cookie per service profile. Use this attribute to add fields to accounting records. • **Z**—The service requires service authorization with the SSG prepaid feature.
Cisco-AVpair	A VSA(attribute number 26), vendor 9, subattribute 1. Valid values for the Cisco-AVpair attribute in a service profile are: • **"ip:inacl**[**#***number*]={*standardACL* | *extendedACL*}**"**—Upstream access control list (ACL). Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to upstream traffic coming from the subscriber. • **"ip:outacl**[**#***number*]={*standardACL* | *extendedACL*}**"**—Downstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to downstream traffic going to the subscriber. – *number*—Identifies the access list. If a profile includes multiple inacl or outacl attributes, the attributes are downloaded and run according to the order implied by *number*. – *standardACL*—A Cisco IOS standard ACL. – *extendedACL*—A Cisco IOS extended ACL. **Note** A profile can include multiple instances of inacl attributes and multiple instances of outacl attributes. Use one attribute for each ACL statement. You can use multiple attributes for the same ACL. • **"vpdn:ip-addresses=***address1*[<*delimiter*>*address2*][<*delimiter*>*address3*]...**"**—Virtual private dial-up network (VPDN) IP address. Specifies the IP addresses of the home gateways (LNSs) to receive the L2TP connections. – *address*—IP address of the home gateway. – <*delimiter*>—A comma (,) or a space ( ) indicates that the SSG selects load sharing among IP addresses. A slash (/) indicates that the SSG considers IP addresses on the left side of the slash a higher priority than those on the right side of the slash. • **"vpdn:tunnel-id=***name***"**—VPDN tunnel ID. Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group. • **"vpdn:tunnel-password=***secret***"**—L2TP tunnel password. Specifies the secret (password) used for L2TP tunnel authentication. • **"vpdn:12tp-hello-interval=***interval***"**—L2TP hello interval. Specifies the number of seconds for the hello keepalive interval.

Service Group Profiles

Service group profiles contain a list of services. Table 2-5 describes the attributes in a RADIUS service group profile.

Table 2-5 Attributes in Service Group Profiles

Attribute	Description
Password	The password required to obtain the profile.
Service-Type	Standard RADIUS attribute number 6. The level of service. Must be outbound.
Account-Info	A vendor-specific attribute (attribute number 26), vendor 9, subattribute 250. Valid values for Account-Info attributes are: • **"I***description***"**—Describes the service group. If this field is omitted, the service group profile name is used. • **"G***Name***"**—Service group name. Lists the service groups that belong to this service group. Service groups can be nested. • **"N***name***"**—Lists the services that belong to the group. • **"TE"**—Indicates that this is a mutually exclusive service group.

Subscriber Profiles

Subscriber profiles define SESM logon names and passwords, ACLs associated with each logon, and subscribed services for each logon.

In SESM RADIUS installations, you must define a subscriber profile for each subscriber that will sign onto the portal from a web browser.

Table 2-6 describes the attributes in a RADIUS subscriber profile. Use the following references for more information:

- If you are using the Cisco Access Registrar, see the Cisco Access Registrar documentation for subscriber profile examples and syntax. Otherwise, see your RADIUS server vendor documentation for the syntax of a subscriber profile
- For sample SESM subscriber profiles, see the aaa.properties file located in the NWSP config directory (for example, nwsp/config/ aaa.properties). This file is installed whether or not you choose the demo option. It shows service and subscriber profiles in Merit RADIUS format.
- The SSG documentation describes subscriber profile attributes and provides examples of their use. See Related Documentation, page xiii for a link to online SSG documentation.

Table 2-6 Attributes in Subscriber Profiles

Attribute	Description
User-Name	Standard RADIUS attribute number 1. The subscriber name used for authentication.
User-Password	Standard RADIUS attribute number 2. The subscriber password used for authentication.
Called-Station_Id	Standard RADIUS attribute number 30. The access point name (APN), which can optionally be used for authentication.
Calling-Station_Id	Standard RADIUS attribute number 31. The mobile station ISDN (MSISDN), which can optionally be used for authentication.

Table 2-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
NAS-Identifier	Standard RADIUS attribute number 32. The NAS identifier, which can optionally be used for authentication.
Session-Timeout	Standard RADIUS attribute number 27. Specifies the maximum length of time, in seconds, that this subscriber session (the edge session on SSG) can remain active at any one time. When the time expires, SSG ends the session. If the host key feature is enabled on the SSG, the SSG signals the state change to the SESM web portal. **Note** The NWSP application does not relay this state change to the subscriber. If Session-Timeout is not set, there is no limit on how long the session lasts. In a dial-up networking or bridged (non-PPP) network environment, a subscriber can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, which can be a problem if the IP address is obtained by another user. You can use the Session-Timeout and the Idle-Timeout attributes to prevent this problem.
Idle-Timeout	Standard RADIUS attribute number 28. Specifies the maximum length of time, in seconds, that a subscriber session can remain idle before it is disconnected. See the explanation of the Session-Timeout attribute, above, for more information about setting this attribute.

Table 2-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
Account-Info	**Note** In SSG Release 12.2.4(B) or later, if a PPP subscriber profile does not include any VSAs, the SSG does not create a host object for the subscriber and therefore, the SSG does not apply any control over the subscriber's access. The fact that the PPP link is established and the SSG is not applying any control means that the subscriber has unrestricted access to any downstream connections defined in the subscriber's profile or by the Cisco IOS configuration on the SSG host device. If it is important to avoid this situation, make sure that all PPP clients are subscribed to at least one service or define any other Cisco SSG VSA in the profile, such as a **U***url* or **H***url* attribute. A VSA (attribute number 26), vendor 9, subattribute 250. Valid values for Account-Info attributes are: • **"N***serviceName***"**—Service name. Subscribes the subscriber to the specified service and includes the service in the service list that the SESM web portal presents to the subscriber. The *serviceProfileName* must be defined in a service profile. There can be multiple instances of this attribute within a subscriber profile. • **"G***serviceGroupProfileName***"**—Service group. Creates a folder for the service group on the subscriber's SESM web portal. The *serviceGroupProfileName* must be defined in a service group profile. There can be multiple instances of this attribute within a subscriber profile. • **"A***autoConnectServiceName*[;*username*;*password*]**"**—Automatic connection. Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon. By default, autoconnect services are hidden; that is, they are not included on the SESM service list. The username and password attributes are required for proxy services. **Note** The SESM service list does not include A entries. It only shows N entries. To display an autoconnect service on the service list, include both an A and an N entry for the service in the profile. See Example Subscriber Profile for Autoconnect Services, page 2-17. • **"U***url* or **H***url***"**—These attributes specify the URL for the subscriber's preferred Internet home page. If the SESM web portal is designed to use HTML frames, then these options also specify whether the home page is displayed in a new browser window or in a frame in the current (SESM) window, as follows: – **U***url*—URL for the home page displayed in its own browser window. – **H***url*—URL for the home page displayed in a frame in the SESM browser window. **Note** In a frameless application, both U and H cause a new browser window to open for the home page. The NWSP and SP applications are frameless applications. • **"RI***group*;*duration*[;*service*]**"**—Overrides the TCP redirect configuration on the SSG for initial logon redirections. The *group* is the Captive Portal group to use for initial logon redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The *duration* is the duration of the captivation (in seconds). If you specify the optional *service* field, initial logon redirection occurs only when the subscriber requests connection to the named service. • **"RA***group*;*duration*;*frequency*[;*service*]**"**—Overrides the TCP redirect configuration on the SSG for advertisement redirections. The *group* is the Captive Portal group to use for advertisement redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The *duration* is the duration of the captivation (in seconds). The frequency is the approximate interval between redirections (in seconds). If you specify the optional *service* field, redirection occurs only when the subscriber requests connection to the named service.

Table 2-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
Account-Info *(continued)*	• **"RS"**—Gives the subscriber has SMTP forwarding capability. • **"QU**;*upstream-token-rate*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-token-rate*;*downstream-normal-burst*;[*downstream-excess-burst*]**"**—Indicates hierarchical policing policies, also known as quality of service (QOS) for this subscriber. **Note** The **$** in a subattribute code indicates that the subattribute is used only by SESM, not by SSG or other Cisco network devices. **Note** Deployers might see **$** subcodes in access accept messages from SSG that are not documented below. SSG uses **$** subcodes to identify information about the subscriber that it passes along for SESM use, such as MAC address, virtual path identifier/virtual circuit identifier (VPI/VCI), MSISDN number, and other connection information. Those codes are not documented in this guide because they are not used in subscriber profiles. • **"$PE***permission***"—**Meaningful in a Demo installation only, to demonstrate the SESM SPE self-management, self-subscription, and subaccount creation features. Use this attribute to assign specific permissions to subscribers for use in a demonstration. The *permission* is one of the following: – Service Selection—The permission to select services and disconnect from services is implied and does not have to be explicitly coded in the profile. – Self Manage—Use this string to demonstrate the SESM SPE feature that allows subscribers to update their own account attributes, such as name, address, email, and hobbies. – Subaccount Manage—Use this string to demonstrate the SESM SPE feature that allows subscribers to create, delete, and manage subaccounts. The Demo installation does not create an actual subaccount; you must define the supporting subaccount profile in the aaa.properties file and use the $**FA** attribute. – Service Subscription—Use this string to demonstrate the SESM SPE feature that allows subscribers to subscribe and unsubscribe to services and service groups. • **"$SA***service***"**—Meaningful in a Demo installation only, to demonstrate the SESM SPE self-subscription feature. Use this attribute to list services to which subscribers can self-subscribe. The *service* must be defined in a service profile. • **"$GA***serviceGroupName***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE self-subscription feature. Use this attribute to list service groups to which subscribers can self-subscribe. The *serviceGroupName* must be defined in a service group profile. • **"$UG***userGroupName***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE user group features, including user group branding. This subcode adds users to user groups. The *userGroupName* can be any value. (User groups are a SESM SPE concept. RADIUS profiles do not provide a way to define valid user group names.) The NWSP application running in a Demo installation demonstrates brand awareness by displaying different branded pages based on the user group values of bronze, silver, and gold. See the aaa.properties file.

Table 2-6 Attributes in Subscriber Profiles (continued)

Attribute	Description

Account-Info *(continued)*	• **"$AA***accountAttributeName;type;attributeValue***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE account self-care features. Use this attribute to specify the initial values that will appear in the fields on the My Account page in the NWSP application running in a Demo installation. Use a separate attribute line for each field.
	
	The *accountAttributeName* is a name for a field on the My Account page in the NWSP application. These are X.500 fields. See *Cisco Subscriber Edge Services Manager Profile Management Guide* for a list of the X.500 names. You can add more fields to the demo if you change the NWSP application to display more fields, as described in *Cisco Subscriber Edge Services Manager Web Developer Guide*.
	
	The *type* indicates a type for *attributeValue* and is one of the following:
	– S—*attributeValue* is a simple string.
	– V—*attributeValue* is an array of strings.
	
	The *attributeValue* indicates the value to be displayed in the field in NWSP. If type is V, surround *attributeValue* with braces ({}) and delimit each element in the array with a semicolon.
	
	For example:
	`"$AAgivenName;S;James"`
	`"$AAhobbies;V;{sports;news;travel}"`
	
	• **"$FA***parent***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE subaccount features. This subcode identifies this subscriber as a subaccount. The *parent* is the username of the parent account and must be defined in a subscriber profile.
	
	The NWSP application running in a Demo installation demonstrates subaccounts. In the aaa.properties file, subgolduser is defined as a subaccount to golduser.
	
	• **"$SB***serviceBlocked***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE subaccount features. In a subaccount profile, this subcode identifies a service that is blocked (not available) to the subaccount. The parent account can unblock a service and make it available for subscription. The *service Blocked* must be defined in a service profile.
	
	• **"$GB***serviceGroupBlocked***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE subaccount features. In a subaccount profile, this subcode identifies a service group that is blocked (not available) to the subaccount. The parent account can unblock a service group and make it available for subscription. The *serviceGroupBlocked* must be defined in a service group profile.
	
	• **"$SL***subaccountLimit***"**—Meaningful in a Demo installation only to demonstrate the SESM SPE subaccount features. In a parent account profile, this subcode defines the number of subaccounts that the parent can create. If this subcode is not included in the profile, no limit is enforced. The *subaccountLimit* is an integer value from 0 to any limit imposed by the deployer.
	
	• **"$SO***singleSignOn***"**—Meaningful in a Demo installation only. Allows you to disable single sign-on for individual users when the SESM global sign-on is in effect. If this attribute is not defined, the default value 1 is used. Values are
	– 0—Single sign-on is not permitted for this subscriber.
	– 1 (the default)—Single sign-on is permitted for this subscriber.

Table 2-6 Attributes in Subscriber Profiles (continued)

Attribute	Description
Cisco-AVpair	A VSA (attribute number 26), vendor 9, subattribute 1. Valid values for the Cisco-AVpair attribute in a subscriber profile are: • **"ip:inacl**[**#***number*]={*standardACL* | *extendedACL*}**"**—Upstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to upstream traffic coming from the subscriber. • **"ip:outacl**[**#***number*]={*standardACL* | *extendedACL*}**"**—Downstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to downstream traffic going to the subscriber. – *number*—Identifies the ACL. If a profile includes multiple inacl or outacl attributes, the attributes are downloaded and run according to the order implied by *number*. – *standardACL*—A Cisco IOS standard ACL. – *extendedACL*—A Cisco IOS extended ACL. **Note** A profile can include multiple instances of inacl attributes and multiple instances of outacl attributes. Use one attribute for each ACL statement. Multiple attributes can be used for the same ACL.

Next Hop Gateway Profiles

Next hop gateway profiles associate next hop gateway keys with IP addresses. Because multiple SSGs might access services from different networks, service profiles can specify next hop keys. (See the service-info G attribute in Table 2-4 on page 2-8.) If this is the case, you must configure a next hop gateway pseudo-service profile to resolve the keys to valid IP addresses.

An example next hop gateway pseudo-service profile is shown in Example Next Hop Gateway Profile, page 2-18:

Example RADIUS profiles

Example Service Profiles

The service configuration examples in this section use a Merit RADIUS format.

Example Service Profile for Passthrough Service

```
internet Password = "servicecisco", Service-Type = Outbound
    Service-Info = "IInternet",
    Service-Info = "R153.153.153.0;255.255.255.0",
    Service-Info = "MC",
    Service-Info = "TP"
```

Example Service Profile for Proxy Service

```
corporate Password = "servicecisco", Service-Type = Outbound
    Service-Info = "ICorporate Intranet (proxy)",
    Service-Info = "R154.154.154.0;255.255.255.0",
    Service-Info = "S10.3.3.101;1812;1813;cisco",
    Service-Info = "MC",
    Service-Info = "TX"
```

Example Service Profile Using Timeout Values

```
iptv Password = "servicecisco", Service-Type = Outbound
    Service-Info = "IIP/TV",
    Service-Info = "R160.160.160.0;255.255.255.0",
    Service-Info = "MC",
    Service-Info = "TP"
    Idle-Timeout = 60,
    Session-Timeout = 60
```

Example Service Group Profiles

The service group configuration examples in this section use a Merit RADIUS format.

Example Service Group Profile

```
SvcGroup1 Password = "servicecisco", Service-Type = Outbound
    Account-Info = "Nvidconf",
    Account-Info = "Ndistlearn",
    Account-Info = "Ncorporate",
    Account-Info = "Nbanking"
        Account-Info = "GSvcGroup2”
```

Example Service Group Profile for a Mutex Group

```
MutexGrp1 Password = "groupcisco", Service-Type = Outbound
    Account-Info = "IBandwidth-QoS",
    Account-Info = "Nbw-gold",
    Account-Info = "Nbw-silver",
    Account-Info = "Nbw-bronze",
    Account-Info = "TE"
```

This example defines a set of mutual exclusive connections services. Users can switch between services in the Mutex group, by simply choosing a new service without disconnecting from the existing service.

Example Subscriber Profiles

The subscriber profile examples in this section are in a Merit RADIUS format.

Example Subscriber Profile for Autoconnect Services

```
user1 Password = "cisco"
    Service-Type = Framed-User,
    Account-Info = "Ainternet”,      (hidden on the subscriber’s service list)
    Account-Info = ”Ninternet"       (makes it visible)
```

Note The first Account-Info line specifies automatic connection to the service. If you do not include the second line, the autoconnect service does not appear in the service list.

Example Subscriber Profile for Demo Installation

```
golduser Password = "cisco"
    Service-Type = Framed-User,
    Account-Info = "$UGgold",
    Account-Info = "Ainternet_gold",
    Account-Info = "Ninternet_gold",
    Account-Info = "Ncorporate",
    Account-Info = "Ngames",
    Account-Info = "Ndiscount_shopping",
```

```
    Account-Info = "Hhttp://www.spiderbait.com",
    Account-Info = "$PESelf Manage",
    Account-Info = "$PESubaccount Manage",
    Account-Info = "$PEService Subscription",
    Account-Info = "$SAbanking",
    Account-Info = "$GAnewsgroup",
    Account-Info = "$AAinitials;V;{A}",
    Account-Info = "$AAgender;S;female",
    Account-Info = "$AAsurname;S;Goodbody",
    Account-Info = "$AAtitle;S;Miss",
    Account-Info = "$AAgivenName;S;Felicity",
    Account-Info = "$AAhobbies;V;{science;news;travel}"
```

More RADIUS Profile Examples

SESM includes sample RADIUS profiles in Merit flat file formats. The SESM web portal applications running in a Demo installation use the profiles in these Merit files. The installation includes a separate Merit file for each of the web portal applications. The files are located in the config directory under each web portal application directory, for example, nwsp/config/aaa.properties.

Example Next Hop Gateway Profile

```
ssg-next-hop Password = "xssg-key"
    Control-Info = "Gl2tp-net7;192.168.1.101",
    Control-Info = "Gl2tp-net40;192.168.1.102",
    Control-Info = "Gweb-key;192.168.1.101",
    Control-Info = "Gproxy-radius-key;192.168.1.101",
    Control-Info = "Gxint-24;192.168.1.101"
```

Configuring the Bundled SESM RADIUS Server

This section describes how to use the bundled RADIUS server in a SESM RADIUS installation. All requests are satisfied using profiles in a referenced flat file in Merit format. Topics are:

Bundled SESM RADIUS Server Installed Location

The bundled SESM RADIUS server is installed by default in both SESM RADIUS and SESM SPE installations. None of the SESM installation parameters affects the default configuration of the bundled SESM RADIUS server.

The installed location of configuration files and start scripts that support the bundled SESM RADIUS server is the tools directory under your SESM installation directory:

```
tools
    bin
        startAAA
    config
        aaa.xml
        erp.xml
        aaa.properties
```

The aaa.xml and erp.xml files are MBean configuration files for the bundled SESM RADIUS server. The aaa.properties file is a sample profile file.

Profile File Requirements

The bundled SESM RADIUS server requires a profile file in Merit format.

The default configuration points to the aaa.properties file, a sample Merit file installed with RDP. You can change this to point to a different file by changing the aaaFilename attribute in the AAA MBean. For example, you could point to the aaa.properties file in the NWSP directory.

The bundled SESM RADIUS server loads the contents of the profile file during startup. You must restart the RADIUS server if:

- You change the aaaFilename attribute to point to a different file.
- You make any changes to the profiles in the referenced file.

Starting the Bundled SESM RADIUS Server

The bundled SESM RADIUS server is ready to run immediately after installation. To start it, run the start script with a port number, as follows:

- On Solaris and Linux:

  installDir/tools/bin/startAAA.sh *portNumber*

- On Windows:

  installDir\tools\bin\startAAA.cmd *portNumber*

Note You can edit the start script, inserting a default port number. In that case, you do not need to specify *portNumber* on the command line.

Defining New Attributes to the Bundled SESM RADIUS Server

All SESM applications, including the bundled SESM RADIUS server, internally predefine the standard RADIUS attributes and the Cisco VSAs listed in SESM MBeans, page A-1.

To define additional attributes, such as Cisco VSAs not included in the previously referenced tables or other vendor VSAs, define the new attribute in the RADIUSProxy MBean. New attributes defined in this MBean can be used in your profiles.

Define the new attribute in the profile itself, as described in Dynamically Defining New Attributes for Testing and Development, page 2-5.

Configuring the RADIUS Proxy Server

This section describes how to use RDP as a RADIUS proxy server in a SESM RADIUS installation. All requests are proxied to other configured RADIUS servers. Topics are:

RDP Proxy Server Installed Location

The RDP proxy server is installed by default in both SESM RADIUS and SESM SPE installations. None of the SESM installation parameters affect the default configuration of the bundled SESM RADIUS server.

The installed location of configuration files and start scripts that support the RDP proxy server is the tools directory under your SESM installation directory:

```
tools
    bin
        startProxy
    config
        proxy.xml
        erp.xml
        aaa.properties
```

The proxy.xml and erp.xml files are MBean configuration files for the RDP Proxy Server. The aaa.properties file is a sample profile file.

Starting the RDP Proxy Server

Before running the RDP proxy server the first time, you must edit the proxy.xml file to specify the RADIUS servers that you want to proxy to.

To start the RDP proxy server, run the start script with a port number:

- On Solaris and Linux:

  installDir/tools/bin/startProxy.sh *portNumber*

- On Windows:

  installDir\tools\bin\startProxy.cmd *portNumber*

Note You can edit the start script, inserting a default port number. In that case, you do not need to specify *portNumber* on the command line.

Configuring SESM RADIUS Server to Return Messages Using Attribute 18

RADIUS messages contain a field numbered 18. This field is also known as the Reply Message field. This field is commonly used to return information from the RADIUS server to the caller. Both Access accept and Access reject responses can contain an attribute 18 message if required. A common example is in the case of a failed authentication. The response might contain an attribute 18 field with a message stating why authentication failed.

SESM is supplied with a RADIUS filter that can be applied to RADIUS responses and configured to add attributes and values when these responses contain a particular response code (for example, 3 in the case of Access reject). This filter is not used by the SESM RADIUS server by default but can be configured for use.

When configured, the reply message appears by default in the SESM NWSP web portal after login.

Note RADIUS concatenates the attribute 18 messages. To display these messages separately, you can define a delimiter that SESM uses to separate the concatenated messages.

To disable and enable message display, see *Cisco Subscriber Edge Services Manager Web Portals Guide*.

You can also use SESM to customize the message reply text. SESM uses the message catalog to facilitate internationalization and localization of the attribute 18 message. For information about customizing message text in SESM, see *Cisco Subscriber Edge Services Manager Web Developer Guide*.

To configure the SESM RADIUS server to return the attribute 18 messages defined by the RADIUS server:

Step 1 Using a suitable text editor, open the aaa.xml configuration file using the following command:

```
Open <install-dir>\tools\config\aaa.xml in a suitable text editor
```

Step 2 Within the aaa.xml configuration file, locate the following section:

```
<Set name="handlers">
<Array class="com.cisco.sesm.erp.ERPHandler">
  <Item>
    <New class="com.cisco.sesm.erp.radius.AaaHandler">
      <Set name="name">AAA</Set>
      <Set name="aaaFilename"><SystemProperty name="application.home"
default="."/>/config/aaa.properties</Set>
    </New>
  </Item>
```

Step 3 Within the section of the file specified in step 2, add two handlers, for reject messages and accept messages, by editing the segment of the file below the </Item> tag as follows:

Handler for rejects:

```
<Item>
  <New class="com.cisco.sesm.erp.radius.AddAVsFilter">
    <Set name="name">AVFilterReject</Set>
    <Set name="nextHandler">AVFilterAccept</Set>
    <Set name="responseCodes">
      <Array class="java.lang.Integer">
        <Item type="int">3</Item>
      </Array>
    </Set>
    <Set name="AVs">
      <Array class="java.lang.String">
        <Item>Reply-Message:attr18.reject.message</Item>
      </Array>
    </Set>
  </New>
</Item>
```

Handler for Accepts:

```
<Item>
  <New class="com.cisco.sesm.erp.radius.AddAVsFilter">
    <Set name="name">AVFilterAccept</Set>
    <Set name="nextHandler">AAA</Set>
    <Set name="responseCodes">
      <Array class="java.lang.Integer">
        <Item type="int">2</Item>
      </Array>
    </Set>
    <Set name="AVs">
      <Array class="java.lang.String">
        <Item>Reply-Message:attr18.accept.message</Item>
      </Array>
    </Set>
  </New>
</Item>
```

Step 4 Within the sections of the aaa.xml file shown in Step 3, edit the default attribute 18 reject message and the default attribute 18 accept message, as required.

Step 5 Locate the following section in the aaa.xml file:

```
<Set name="listeners">
  <Array class="com.cisco.sesm.erp.ERPListener">
    <Item>
      <New class="com.cisco.sesm.erp.radius.RADIUSListener">
        <Set name="handler">AAA</Set>
      </New>
    </Item>
  </Array>
</Set>
```

Step 6 Change the `<Set name="handler">AAA</Set>` line to:

```
<Set name="handler">AVFilterReject</Set>
```

Step 7 Locate the following section in the aaa.xml file and change the `RADIUSListener=AAA` entry to the first handler AVFilterReject:

```
<Configure
jmxname="com.cisco.sesm:name=AAA,RADIUSListener=AVFilterReject,component=ThreadPool">
```

Step 8 Locate the following section in the aaa.xml file and change the `RADIUSListener=AAA` entry to the first handler AVFilterReject:

```
<Configure
jmxname="com.cisco.sesm:name=AAA,RADIUSListener=AVFilterReject,component=RADIUSServerSocke
t">
```

The procedure for configuring SESM RADIUS server to return messages using attribute 18 is now complete.

Configuring a Jetty Container for SESM

This chapter contains the following topics:

Note If your solution does not require the port-bundle host key(PBHK) feature on the Service Selection Gateway (SSG), you can create a web archive (WAR) file from the installation directory and deploy SESM web applications in other containers. See Appendix C, "Configuring a Tomcat Container for SESM."

Jetty Containers

SESM web applications are Java 2 Enterprise Edition (J2EE) web applications. They must run in a J2EE web server. The web server is the *container* for the applications that run in it. The SESM installation program installs and configures Jetty servers as the containers for the SESM web applications. Jetty version 4.2.23 is included with this release of SESM.

The Jetty server is currently the only J2EE-compliant server that can support PBHK without requiring further changes. For solutions that use SSG, we recommend enabling PBHK.

PBHK uses a software token (or key) that *uniquely* identifies each subscriber on the host SSG that is currently logged on to a SESM web portal, even when multiple subscribers are using the same IP address. PBHK also provides an SSG IP address in the key.

PBHK provides the following advantages to the SESM web portal:

- It allows SESM web portals to handle overlapping IP addresses, non-routable IP addresses, and dynamically assigned IP addresses in a robust manner.
- It eliminates the need to explicitly map subscriber subnets to SSGs.

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

The SSG makes the port number available, but the J2EE server must access this information and pass it along to the SESM web portal. To do this, the Jetty server uses the PortBundleHandler, an extension that allows access to the request handling part of the server API and thus get the remote port number.

The PortBundleHandler is added to the Jetty container by the following file under the SESM application directory (nwsp, for example), nwsp/webapp/WEB-INF/web-jetty.xml.

Configuring a Jetty Container

The Jetty container software comes bundled with all SESM installation packages. Jetty is installed whenever you install the SESM Web Applications component. The SESM installation process performs all required configurations for running the applications in Jetty containers. Read this section if you want to change or fine-tune the Jetty container configuration after installation.

MBean Definition

SESM uses MBeans to manage attributes for the Jetty container. MBeans are Java classes that follow a model described in the Java Management Extension (JMX) standards. An MBean represents the management interface for a resource. The management interface is the set of all necessary information and controls that a management application needs to operate on the resource.

SESM uses MBeans to:

- Configure components and the communication connections between those components.

  Read-write attributes in the SESM MBeans allow deployers to configure the application. For example, the SESM MBean configures the SESM web portal features and options, the SSG MBean configures communication between SSG and the SESM web applications, the AAA MBean configures communication between RADIUS servers and the SESM web applications, and so on. Container-specific parameters are also defined as MBeans. For example, Cisco created a logging MBean for the Jetty server.

- Provide metrics about a running application.

Changing MBean Attributes

Use either of the following methods to change the attribute values in SESM MBeans:

- Use SESM Application Management (AM)—You can change the value of most MBean attributes while the SESM application is running using AM. These changes take effect immediately on the running application. You can optionally store the changes in the MBean configuration file so that they persist over application restarts.
- Directly edit the MBean configuration file—You can change the value of some attributes by directly editing the appropriate MBean configuration file. These changes take effect the next time you start the application.

  Each application has its own Jetty container configuration file, in the jetty directory under the SESM installation directory, for example, for NWSP, jetty/config/nwsp.jetty.xml.

Configuring a Jetty to Receive Prepaid User Redirections

Captive Portal can redirect prepaid users whose quota has finished, to a Recharge page in the web portal. You must configure the Jetty container to receive prepaid user directions.

You must configure Jetty to open another socket when it starts Captive Portal, so that the application can receive and handle these requests.

To configure an additional socket in Captive Portal:

Step 1 Open the following file:

```
<SESM>/jetty/config/captiveportal.jetty.xml
```

Step 2 Add another SESMSocketListener to the file. You can copy and paste an existing section into this section of the configuration file:

```
<Call name="addListener">
<Arg><New class="com.cisco.sesm.jetty.SESMSocketListener"></New></Arg>
</Call>
```

Step 3 Configure the new SESMSocketListener. Copy an existing configuration section, as in the following example.

In this example, SESMSocketListener number 8 is configured to be called “genericRedirect2”, and the port to be opened is 8097.

```
<Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,SESMSocketListener=8">
    <Set name="port" type="int"><SystemProperty name="genericRedirect2.port"
    default="8097"/></Set>
    <Set name="minThreads" type="int">50</Set>
    <Set name="maxThreads" type="int">255</Set>
    <Set name="maxIdleTimeMs" type="int">60000</Set>
</Configure>
```

Jetty Container MBean Descriptions

A Jetty container uses the following MBeans:

Log MBean

The Log MBean enables the Jetty server debugging and logging mechanisms and configures the information that appears in the Jetty log file. Table 3-1 describes the attributes in the Log MBean.

Table 3-1 Jetty Container—Log MBean

Attribute Name	Explanation
logTimezone	Installed default: empty
logDateFormat	Controls the format of the date stamp in the log messages. Installed default: yyyyMMdd:HHmmss.SSS
logLabels	Controls whether the log messages include frame details. Installed default: false
logOneLine	Installed default: false
logStackSize	Controls whether the log messages include an indication of stack depth. Installed default: false
logStackTrace	Controls whether the log messages include trace information. Installed default: false
logTags	Installed default: true
logTimeStamps	Installed default: true
append	Indicates if messages overwrite existing contents (false) or are appended to the existing file (true). Installed default: true
retainDays	Indicates the number of days to keep an old log file before deleting it. Installed default: 31
filename	Specifies the log filename and path, as follows: *application.home*/logs/*yyyy_mm_dd*.jetty.log Where: *application.home*—A property whose value is set in the SESM start script. See Table 9-2 on page 9-4. logs—A constant. All log files appear in the logs subdirectory under the application directory. *yyyy_mm_dd*—The year, month, and day that the file was created. .jetty.log—A constant identifying the Jetty log files.

Debug MBean

The Debug MBean enables or disables the Jetty server debugging mechanism. Table 3-2 describes the attributes in the DebugMBean.

Table 3-2 Jetty Container—Debug MBean

Attribute Name	Explanation
debug	Controls whether debugging messages are produced. Installed default: false
debugPatterns	By specifying one or more patterns, you turn on a filtering mechanism that excludes any message that does not match the pattern. The patterns are file, class, or method names. Pattern matching is based on substring matches. For example, if you specify the pattern RADIUS, the software focuses on RADIUS messages. To specify multiple patterns, separate the patterns using a comma. Installed default: empty
verbose	Specifies the level of detail reported in debugging messages. The range of allowed values is 0 (no details) to 255 (all details). Installed default: 0
suppressStack	Controls whether stack information is included in debug messages. Installed default: false
suppressWarnings	Controls whether warning messages are included in debug messages. Installed default: false

Server MBean

The Server MBean configures a request log, which records all incoming HTTP requests. Table 3-3 describes the attributes in the Server MBean.

Table 3-3 Jetty Container—Server MBean

Attribute Name	Explanation
RequestLog	Creates a new class with one argument, which specifies the name and location of the request log. The installed value is: *application.home*/logs/*yyyy_mm_dd*.request.log Where: • *application.home*—A property whose value is set in the SESM start script. See Table 9-2 on page 9-4. • logs—A constant. All log files appear in the logs subdirectory under the application directory. • *yyyy_mm_dd*—The year, month, and day that the file was created. The installation program uses the appropriate path name delimiter for the installation platform. • .request.log—A constant identifying an HTTP request file.
retainDays	Indicates the number of days to keep a log file before deleting it. Installed default: 90
append	Indicates whether or not to append messages to an existing file or to create a new file for each application instance. Installed default: true
<Call addWebApplication>	Adds the SESM web portal to run on the web server. It uses five positional arguments: 1. The first positional argument specifies the virtual hostname for the web server application. 2. The second positional argument specifies the context path for locating the web server application. For example, / or /pathname/*. 3. The third positional argument identifies the location of the application. The value is: *application.home*/webapp Where *application.home* is a system property whose value is set in the start script. 4. The fourth positional argument identifies the location of the webdefault.xml file for this application. The value is: *jetty.home*/config/webdefault.xml Where *jetty.home* is a system property whose value is set in the start script. 5. The fifth positional argument specifies whether WAR files are used. Valid values are true and false. The first three arguments define the location of the web server application. `host/context/application` The SESM start script derives the values for *application.home* and *jetty.home* from an expected (installed) directory structure. To change these values, edit the start script.

SESMSocketListener MBean

The SESMSocketListener MBean configures the port that the Jetty server listens on for HTTP requests from subscribers. Table 3-4 describes the attributes in the SESMSocketListener MBean.

Table 3-4 Jetty Container—SESMSocketListener MBean

Attribute Name	Explanation
port	Sets the port number that the web server listens on. The installed value is a Java system property named *application*.portno. **Note** The start script sets this system property. Unless you change the start script, the default value in the MBean configuration file is ignored during application startup. To change the value of *application*.portno, edit the application-specific start script. Default: 8080 Installed value: The SESM installation program sets *application*.portno in the start script to the application port that you provided during the installation process.
minThreads	Sets the minimum number of threads that this listener maintains during periods of low load. This listener always has system resources allocated for this number of threads. Installed default: 50
maxThreads	Sets the maximum number of threads that this listener can allocate resources for, even during peak loads. This listener can have up to this number of threads. Installed default: 255
maxIdleTimeMs	Specifies the length of time a thread can be idle (not used) before the listener deallocates it. The unit is milliseconds. Installed default: 60000

SESMSSLListener MBean

The SESMSSLListener MBean configures the port that the Jetty server listens on for requests from subscribers on the Secure Sockets Layer (SSL). Table 3-5 describes the attributes in the SESMSSLListener MBean.

Table 3-5 Jetty Container—SESMSSLListener MBean

Attribute Name	Explanation
port	Sets the port that the secure socket layer (SSL) listener uses. The installed value is a Java system property named *application*.ssl.portno **Note** The start script sets this system property. Unless you change the start script, the default value in the MBean configuration file is ignored during application startup. The generic start script derives a value for *application*.ssl.portno based on the value of *application*.portno, as follows: *application*.ssl.portno = *application*.portno - 80 + 443 To change the value of *application*.ssl.portno, edit the generic start script.
MinThreads	Sets the minimum number of threads that this listener maintains during periods of low load. The listener always has system resources allocated for this number of threads. Installed default: 50
MaxThreads	Sets the maximum number of threads that this listener can allocate resources for, even during peak loads. The listener can allocate up to this number of threads. Installed default: 255
MaxIdleTimeMs	Specifies the length of time a thread can be idle (not used) before the listener deallocates it. The unit is milliseconds. Installed default: 50000
Keystore	Sets the pathname of the SSL keystore file. The keystore file is a binary file created by keytool. Sample keystore files are included in the installation for each portal. For example: *jetty.home*/config/nwspkeystore Where: *jetty.home*—A system property. The NWSP start script derives the value of *jetty.home* from an expected (installed) directory structure. To change the value of *jetty.home*, edit the start script. Unless you alter the start script, the default value for *jetty.home* specified in this MBean configuration file is ignored at run time. **Caution** A keystore file is required for deployments that use HTTPS. HTTPS does not function without a valid keystore file. The nwspkeystore file included with the SESM installation works, but you should replace it with a keystore valid for your specific deployment. See Using HTTPS in SESM Portals, page B-1 for more information.
Password	Must match the value in the keystore file referenced above.
KeyPassword	Must match the value in the keystore file referenced above.

Configuring Captive Portal

This chapter describes how to configure the SESM Captive Portal. The topics are:

Note

- For a general description of redirection and captivation, see *Cisco Subscriber Edge Services Manager Introduction Guide*.
- To demonstrate the complete capabilities of Captive Portal, you need to run it with a fully configured SSG. To configure the SSG TCP redirect features to work with the configuration parameters that you installed on the SESM side, see *Cisco Subscriber Edge Services Manager Installation Guide*.

Introduction to Captive Portal

SESM Captive Portal (CP) acts as a gateway for all of the different redirections coming from the SSG. Captive Portal does not provide any content to subscribers. Its main purpose is to determine how to redirect the subscriber browser. It can also preserve and pass along information from the original subscriber request to the content applications.

Captive Portal performs the following functions:

- Determines the URL to redirect to, based on configuration attributes in captiveportal.xml.
- Preserves information from the subscriber's original HTTP request.
- Issues an HTTP redirection. The HTTP redirect includes the preserved information from the original subscriber, in the form of parameters appended to the redirection URL.

For details about how message durations are specified and how the specifications interact, see Summary of Message Duration Parameters, page 4-13.

For details of the parameters that Captive Portal captures and forwards to content applications, see Parameters Appended to URLs in HTTP Redirections, page 4-6. The names of these parameters can be configured.

Captive Portal Solution Components

The Captive Portal solution consists of the following SSG and SESM components:

- SSG TCP redirect feature—This component is one of the SSG features offered within the Cisco IOS software. The SSG TCP redirect feature intercepts TCP packets and reroutes them to server groups, which are usually SESM captive portal applications. The SSG modifies the IP address and the port in the TCP packet to cause the redirection. The types of redirection and the redirected destinations are configured on the SSG using Cisco IOS commands. For information about the SSG TCP Redirect features, see the *Cisco Subscriber Edge Services Manager Installation Guide*.
- SESM Captive Portal—This SESM application acts as a gateway for all of the different redirections coming from the SSG. Captive Portal does not provide any content to subscribers. Its main purpose is to apply business logic that determines what will happen next. Captive Portal is extensible. The installed sample preserves and passes along information from the original subscriber request to the content applications.
- Content applications—These applications provide the SESM browser pages that the subscriber sees. Content applications can be SESM web portal applications or compatible third-party web applications. For information about SESM web portal applications, see *Cisco Subscriber Edge Services Manager Web Portals Guide*.

Captive Portal and SESM Plug and Play

The SESM Plug and Play solution allows ISPs to provide Internet access and subscriber services to nomadic users of PWLANs, regardless of how their web proxy or DNS settings are configured.

To enable the Plug and Play web proxy handling feature, additional configuration of Captive Portal is required.

For more information on the role of Captive Portal in the SESM Plug and Play solution, see Chapter 5, “Configuring SESM Plug and Play.”

Captive Portal and SESM Whitelists

SESM provides support of location-specific whitelists to both proxy and non-proxy users using SESM Plug and Play. This enables both proxy and non-proxy users to access free access destinations depending on location.

To configure whitelist URLs you must configure the Captive Portal configuration file. For more information on configuring whitelists in Captive Portal, see Chapter 6, “Configuring Location Awareness and Whitelist URLs.”

Captive Portal and SESM iPass Support

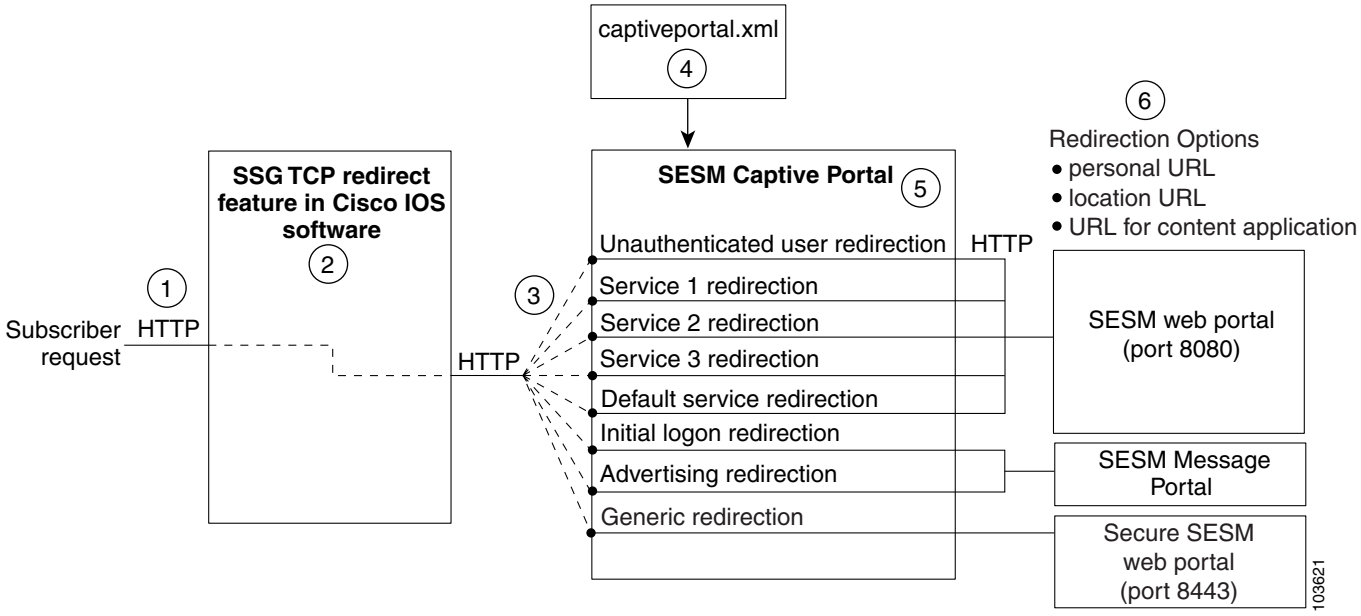
SESM’s roaming access support allows iPass users to connect to the Internet using the iPass smart client. To enable iPass support, you must add User-Agent based redirection in Captive Portal.

For more information on configuring the captive portal to enable iPass support, see Chapter 7, “Configuring SESM for iPass Support.”

How Captive Portal Components Work Together

Figure 4-1 illustrates how Captive Portal components work together to provide appropriate content to the subscriber. Figure 4-1 shows this implementation as it would be configured using all the default values provided by the SESM installation program. There are many possible variations of this default deployment.

Figure 4-1 SESM Captive Portal Application



1	Incoming HTTP requests from subscribers pass through the SSG.
2	When a packet qualifies for redirection, the SSG changes the destination IP address and port in the TCP packet. Cisco IOS software configuration commands issued on the SSG host device define which packets qualify for redirection and the redirected destinations.
3	Captive Portal requires the following configurations on the SSG for the TCP redirected destinations: • IP address—The IP address must identify a web server running Captive Portal. All types of redirection can use the same web server (the same IP address). • Outgoing port—On the SSG, you configure an outgoing port value for each type of SSG TCP redirection. The port number identifies the type of redirection to Captive Portal. To configure Captive Portal to distinguish among the TCP redirect types and handle each one differently in a way appropriate to the TCP redirect type, assign a different outgoing port value to each TCP redirect type. You can also assign any, some, or all TCP redirect types to a generic port. Captive Portal does not distinguish the type of redirection on the generic port; it redirects all requests arriving on the generic port in the same way. The generic redirection provides flexibility and fulfills any requirements that the default installation does not fulfill. In the sample configuration, the generic port is the SESM web portal SSL port.
4	The captiveportal.xml file specifies how requests on each incoming port number should be redirected. The options for each port are: redirect to a content application; redirect to the subscriber's personal URL recorded in the subscriber profile, or redirect to a URL determined from the subscriber's location.

5	Captive Portal determines the redirection URL based on configuration attributes. It issues an HTTP redirect that redirects the subscriber's browser to the appropriate URL. The redirect request can include information from the original HTTP request, in the form of query parameters appended to the HTTP redirect URL.
6	Captive Portal redirects the browser to another configured location. The options are: • Specify a page in another web portal application, such as SESM NWSP or Message Portal. • Use the personalURL keyword, which indicates redirection to a URL specified in the subscriber profile with the H attribute. • Use the locationURL keyword, which indicates redirection to a location-specific URL configured in the SESM Location MBean. In the example solution installed with SESM, Captive Portal is configured as follows: • Redirects unauthenticated user redirections and service redirections to NWSP. • Redirects initial login and advertising redirections to the SESM Message Portal.

Captive Portal Redirection Options

This section describes Captive Portal redirection options:

Redirect to personalURL

The personalURL keyword provides the capability for personalized redirections. Captive Portal redirects to the home URL specified in the subscriber profile.

To add a home URL attribute to subscriber profiles:

- In a SESM RADIUS installation, use the H subattribute code in the Account-Info VSA in the subscriber profile. For example, a Merit RADIUS profile would contain this line:

  ```
  Account-Info = "Hhttp://www.cisco.com"
  ```

- In a SESM SPE installation, use the CDAT interface to specify home URLs for individual users or for user groups.

Redirect to locationURL

The locationURL keyword provides the capability for location-based redirections. If you use the locationURL keyword as the value for any of the attributes in the captiveportal.xml file, then you must include the Location MBean in the captiveportal.xml file. Copy the MBean from the nwsp.xml file and paste it into captiveportal.xml. See Appendix A, "SESM MBeans" for information about this MBean.

Redirect to Content Applications

Content applications provide the SESM browser pages that the subscriber sees. Content applications can be SESM web portal applications or compatible third-party web applications. This guide assumes that you use a SESM web portal:

- NWSP, page 4-5
- Message Portal, page 4-5

NWSP

In the SESM example Captive Portal solution, unauthenticated user redirections and unconnected service redirections are configured to redirect the browsers to NWSP, as follows:

- For unauthenticated user redirections—The default configuration sends browsers to the NWSP login page so the subscriber can authenticate.
- For attempted access to unconnected services:
  - NWSP presents a service login page for the service and coordinates with the SSG to authenticate to the service and then connect to the service.
  - You can configure various contingency pages to handle situations when connection is not possible. For example, suppose the service does not exist or the subscriber is not subscribed to the service. Attributes in the nwsp.xml file configure these situations.
  - In a SESM SPE installation, when a subscriber is not subscribed to a service, the default configuration directs the subscriber to a self-subscription page.
- For the default service redirections (access to services other than the specifically configured ones):
  - If Captive Portal is configured so that it does not pass a service name in the query string for this type of redirection, NWSP uses the serviceNotGivenURI attribute to determine a redirection destination.
  - The default configuration of the sample solution references the NWSP status page.

See Parameters Appended to URLs in HTTP Redirections, page 4-6 for a description of the parameters that Captive Portal forwards to NWSP.

Message Portal

In the SESM example Captive Portal solution, Message Portal provides the message pages for initial and advertisement captivation. Message Portal contains:

- A greetings page for initial captivation redirections
- An advertising page for advertising captivation redirections
- In a SESM SPE installation, Message Portal displays an advertisement page that matches the first subscriber interest item in the subscriber profile.

Message Portal also provides a timing mechanism to control the duration of the displays. Timing starts when the page is displayed and ends when the duration time elapses. When the duration time elapses, Message Portal can optionally redirect to the URL in the subscriber's original HTTP request. Otherwise, the message remains displayed until the subscriber enters another URL.

See Parameters Appended to URLs in HTTP Redirections, page 4-6 for a description of the parameters that Captive Portal forwards to Message Portal.

Parameters Appended to URLs in HTTP Redirections

Table 4-1 shows the parameters that Captive Portal captures and forwards to content applications. The names of these parameters are configurable in the captiveportal.xml file.

Table 4-1 Parameters Appended to URLs in HTTP Redirections

Type of SSG TCP Redirection	Parameter Name in SESM Captive Portal HTTP Redirect	Explanation and Usage by the Content Applications
Unauthenticated user redirection	CPURL	The URL in the subscriber's original request. NWSP uses this value to redirect the browser to this original request after successful authentication.
Service redirection	service	The service name that was requested in the original request. NWSP uses this value to log on to the service.
	username	The username that the subscriber used for SESM authentication. NWSP does not use this value, but it is available for use in customizations.
	serviceURL	The URL to the service that was requested in the original request. The NWSP uses this value to display a popup window after service connection. It overrides the URL that NWSP would normally use after service connection, which is the URL in the service profile.
Initial login and advertising redirections	CPURL	The URL in the subscriber's original request. Message Portal optionally redirects to this URL after the message duration time elapses. If the redirect feature is turned off in the messageportal.xml file, the message portal application ignores this parameter.
	CPDURATION	The message duration obtained from the captiveportal.xml file. Message Portal waits this amount of time before attempting to redirect to the CPURL. Duration attributes exist for both the SSG and SESM Message Portal. See Summary of Message Duration Parameters, page 4-13.
	CPSUBSCRIBER	The subscriber name as obtained from the subscriber profile.

Generic Redirections

The generic redirection feature provides another way to configure redirections. Instead of using a type of redirection in Captive Portal that matches the type of redirection configured on the SSG, you can use a generic redirection in Captive Portal.

For example, you can configure the SSG to do per-user and per-service initial or advertising captivation. However, Captive Portal allows only one default initial and one default advertising captivation to be configured. In such a case, you can configure generic redirections. See the description of the defineGenericRedirection attribute in the captiveportal MBean for more information about configuring generic redirections.

Restricting Captive Portal Redirections

This section explains how redirection for different types of user agents and MIME types can be restricted.

By default, Captive Portal performs TCP redirection for:

- All user agents.
- The following MIME types: text/plain, text/html, and text/xml.

We recommend that Captive Portal acts only on requests from specified MIME types and user agents. If all requests are redirected, the web portal will suffer from performance degradation. You can avoid this by specifying the user agents and MIME types that you want Captive Portal to accept.

Configuring Accepted User Agents

The capturedUserAgents section of the captiveportal.xml file contains a list of the accepted user agents. If a user agent is not declared in this list, a 503 error is generated when a request is made. If the list in the capturedUserAgents attribute is empty, all user agents are allowed.

In the following example, both Microsoft Internet Explorer and Netscape browsers are configured as acceptable user agents.

```
<Set name="capturedUserAgents">
<Array class="java.lang.String">
<Item>msie</Item> //i.e. Microsoft Internet Explorer
<Item>mozilla</Item> //i.e. Netscape and other Mozilla based browsers
</Array>
</Set>
```

Configuring Accepted MIME Types

The capturedMimeTypes section of the captiveportal.xml file contains a list of the accepted MIME types.

If a MIME type is not declared in this list and is known, a 503 error is generated when a request is made. If the list in the capturedMimeTypes attribute is empty, all MIME types are allowed.

Note When you use Jetty, you can determine the default mime properties by looking at the mime.properties file in jetty/lib/org.mortbay.jetty.jar.

A MIME type is known either by default or by adding a mapping to web.xml. For example:

```
<mime-mapping>
<extension>cab</extension>
<mime-type>application/x-cabinet</mime-type>
</mime-mapping>
```

In the following example, text/vnd.wap.wml is configured as an acceptable MIME type, in addition to the default values of text/plain, text/html and text/xml.

```
<Set name="capturedMimeTypes">
<Array class="java.lang.String">
<Item>text/plain</Item>
<Item>text/html</Item>
<Item>text/xml</Item>
<Item>text/vnd.wap.wml</Item>
</Array>
</Set>
```

General Procedure for Working with Captive Portal

After you install SESM and perform preliminary configuration of Captive Portal as required using the SESM installation wizard, use the following procedures to work with Captive Portal.

Step 1 Change the destination URL for services using the procedures given in Configuring Unique Service Login Pages for Service Redirections, page 4-8.

Step 2 Configure the way that subscribers are redirected to a predefined URL after they are authenticated using the information given in Configuring Redirection to a Predefined URL After Authentication, page 4-9.

Step 3 Run the Captive Portal application using the procedures given in Running Captive Portal, page 4-12.

Step 4 If required, demonstrate the features in the captive portal solution by loading some appropriate sample profiles into the RADIUS or Lightweight Directory Access Protocol (LDAP) database using the procedures given in Loading Sample Profiles for Captive Portal, page 4-13.

Step 5 If required, enable the Plug and Play web proxy handling feature, using the procedures given in Chapter 5, “Configuring SESM Plug and Play”.

Configuring Unique Service Login Pages for Service Redirections

The SESM installation program configures three specific service redirections and a default service redirection. However, the installation program asks for only one destination URL for services. It configures all of the service redirections to use this URL. The default value provided by the installation program is the service login page in the NWSP web portal.

You might want to change the configuration so that each service redirection is assigned a unique redirection destination. To change a destination URL for service redirections:

Step 1 Using a suitable text editor, open the captiveportal.xml file from the following location captiveportal/config/captiveportal.xml.

Step 2 Locate the service redirect definition. For example:

```
<Call name="defineServiceRedirect">
    <Arg><SystemProperty name="serviceRedirect1.port" default="8094"/></Arg>
    <Arg><SystemProperty name="serviceRedirect1.URL" default=""/></Arg>
    <Arg><SystemProperty name="serviceRedirect1.service" default="service1"/></Arg>
</Call>
```

Step 3 Change the URL in the second argument in the service redirection definition to the desired service URL, for example:

```
<Arg><SystemProperty name="serviceRedirect1.URL" default="http://www.myweb.com"/></Arg>
```

Note The URL for www.myweb.com needs to be accessible when the subscriber does not have their service activated. Typically, this would be either a SESM web portal page or an open garden service.

Configuring Redirection to a Predefined URL After Authentication

This section describes ways to redirect subscribers to a predefined URL after they are authenticated. For example, service providers might want to redirect all users to the service provider's URL:

Redirecting all Subscribers to the Same Predefined URL

You can change the value of MBean attributes used by Captive Portal to redirect all subscribers to the same predefined URL.

Step 1 Using a suitable text editor, open the captiveportal.xml file from the following location, captiveportal/config/captiveportal.xml.

Step 2 In the captiveportal MBean, change the userRedirectURL attribute to:

```
<Set name="userRedirectURL">urlSP?CPURL=urlRedirect</Set>
```

Where:

- *urlNWSP* is the URL of the NWSP web portal (or the URL of your customized web portal).
- *urlRedirect* is the redirected URL, encoded. For example, the colon (:) is replaced with the value %3A and the slash (/) is replaced with the value %2F. An example of an encoded attribute value is:

```
<Set
name="userRedirectURL">http://10.52.199.82:8080?CPURL=http%3A%2F%2Fwww.cisco.com
</Set>
```

Step 3 Change the userRedirectURLParam attribute to null. The installed default value is CPURL.

In the captiveportal.xml configuration file, change the attribute to null by removing the value. For example, change:

```
<Set name="userRedirectURLParam">CPURL</Set>
```

to:

```
<Set name="userRedirectURLParam"></Set>
```

Step 4 Restart Captive Portal.

Note For more information about SESM MBeans, see SESM MBeans, page A-1.

Adding a Home URL to the Subscriber Profile

You can add a home URL attribute to subscriber profiles and configure your web portal to redirect to the URL in this attribute. With this method, different subscribers or groups of subscribers can be redirected to different URLs.

Step 1 Add a home URL attribute to the subscriber profiles:

- For a SESM RADIUS installation, use the H subattribute code in the Account-Info VSA in the subscriber profile. For example, a Merit RADIUS profile would contain this line:

  ```
  Account-Info = "Hhttp://www.cisco.com"
  ```

- In a SESM SPE installation, use the CDAT interface to specify home URLs for individual users or for user groups.

Step 2 Define the order of precedence for redirection URLs. This step requires that you change and recompile the web portal application code.

The order of precedence for redirection is defined in the initUser.jsp file located in nwsp/webapp/decorators.

By default, it is defined as follows:

```
if (capturedURL != null)
     chosenURL = capturedURL;
else if (locationURL != null)
     chosenURL = locationURL;
else if (personalURL != null)
     chosenURL = personalURL;
```

Change the above code so that personalURL is before capturedURL.

For more information, see *Cisco Subscriber Edge Services Manager Web Developer Guide*.

Redirecting Outside the Default Network or Open Gardens

You can configure Captive Portal to redirect all users to a specific URL when they are subject to initial captivation.

Step 1 Using a suitable text editor, open the captiveportal.xml file from the following location, captiveportal/config/captiveportal.xml.

Step 2 Within the following section of the captiveportal.xml file, edit the default field to point to the required URL. For example, news.bbc.co.uk.

```
<Set name="initialCaptivateURL">http://<SystemProperty name="messageportal.host"
default="news.bbc.co.uk"/>:<SystemProperty name="messageportal.port" default="80"/>/</Set>
```

Step 3 To redirect a user to the Home URL in the user-profile, replace the initialCaptivateURL parameter with the **personalURL** keyword, for example:

```
<Set name="initialCaptivateURL">personalURL</Set>
```

This will redirect the user to their personal URL when they are subject to initial captivation.

Step 4 To redirect a user to the location URL for the user's given location, replace the initialCaptivateURL parameter with the **locationURL** keyword, for example:

```
<Set name="initialCaptivateURL">locationURL</Set>
```

This will redirect the user to the location URL when they are subject to initial captivation.

Step 5 If required, configure Captive Portal to achieve redirections outside the default network or open gardens. To do this, Captive Portal must introduce a delay before performing the initial redirection, so that the captivation duration has expired on the SSG. Activate this delay by editing the following line:

```
<Set name="initialCaptivateDelay" type="int">0</Set>
```

The value of this delay should just exceed the duration on the SSG. Because the Captive Portal delay is measured in milliseconds, you can set this to:

```
<Set name="initialCaptivateDelay" type="int">1100</Set>
```

Configuring Prepaid User Redirection

Subscribers who have prepaid Internet access, will be able to access the Internet as long as they have not finished their quota on the billing server. When the quota runs out, the SSG can either disconnect the service immediately or subject the subscriber to prepaid user direct.

Note In order for the SSG to invoke prepaid user redirection, the billing server must respond with an Idle-Timeout value that is greater than zero in the authorization response that it sends to the SSG when the subscriber's quota has run out.

When a subscriber's quota runs out, and an idle-timeout is included in the RADIUS response to the SSG, the SSG redirects traffic for the prepaid service to the configured server-group in the TCP-redirect configuration in SSG for the duration of the idle-timeout, without disconnecting the service. This server group redirects these users to Captive Portal, which HTTP-redirects the users to the SESM web portal, where a recharge page is displayed to the subscriber.

To use prepaid user direction:

- Configure Prepaid User Redirect in the SSG—See *Cisco Subscriber Edge Services Manager Installation Guide* for information.
- Configure the Jetty container to receive prepaid user redirections—See Configuring a Jetty to Receive Prepaid User Redirections, page 3-3.
- Configure Captive Portal for prepaid user redirections as described in the following procedure.

The default Captive Portal configuration does not have a port configured to receive the prepaid user redirections that the SSG can send to it.

To add a generic redirection in the Captive Portal configuration file that uses this new port to handle prepaid user redirection:

Step 1 Using a suitable text editor, open the captiveportal.xml file from the following location, captiveportal/config/captiveportal.xml.

Step 2 Add a generic redirection to HTTP-redirect the prepaid redirect users to the example Recharge page in the SESM web portal:

```
<Call name="defineGenericRedirect">
<Arg>8097</Arg>
<Arg>http://sesm:8080/recharge</Arg>
<Arg>CPURL=capturedURL</Arg>
</Call>
```

Running Captive Portal

This section contains the start and stop scripts that are installed for use with the example Captive Portal solution. You can copy and change these scripts if you develop customized applications.

For information about the contents of these scripts and how to change them, see Chapter 9, "Running SESM Components."

The following table shows the script names for starting and stopping applications in the captive portal application. It also shows the script names for installing the applications as services on the Windows platforms.

Task	Platform	Method or Script Name

Startup	Solaris and Linux	`jetty/bin/startCAPTIVEPORTAL.sh`
		`jetty/bin/startMESSAGEPORTAL.sh`
		`jetty/bin/startNWSP.sh`

	Windows	`jetty\bin\startCAPTIVEPORTAL.cmd`
		`jetty\bin\startMESSAGEPORTAL.cmd`
		`jetty\bin\startNWSP.cmd`
		
		Alternatively, use the Services window accessed from the Windows control panel.

Stop	Solaris and Linux	`jetty/bin/stopCAPTIVEPORTAL.sh` `jetty/bin/stopMESSAGEPORTAL.sh`
	Windows	Use one the following methods: • Task Manager • Services window accessed from the Windows control panel

Add Services	Windows	`jetty\bin\nwspsvc.cmd`
		`jetty\bin\captiveportalsvc.cmd`
		`jetty\bin\messageportalsvc.cmd`

Loading Sample Profiles for Captive Portal

To demonstrate Captive Portal features, you must load some appropriate sample profiles into the RADIUS or LDAP database. To fully demonstrate all of the capabilities of the solution, your sample profiles must conform to the following criteria:

- Service profiles must have service names that match the service names used in the captiveportal.xml file. Matching service names are required to demonstrate service redirections that pass a service name to NWSP for connection.
- Service profiles must have service routes that match exactly the destination networks of the service redirections configured in the SSG TCP redirect commands.
- Subscriber profiles must include subscriptions to the above services.
- For a SESM SPE installation, subscriber profiles must include hobbies if you want to show the Message Portal's capability to display messages tailored to the first hobby listed in the subscriber profile.

In a SESM SPE installation, create some basic subscriber profiles using CDAT. You can then use the NWSP account management feature to modify interests (hobbies) or add subscriptions. The aaa.properties file in each SESM config directory contains many profile examples.

Summary of Message Duration Parameters

This section describes how message durations are specified and how the specifications interact. In summary:

- The SSG duration specifies the minimum amount of time that a message is displayed.
- The SESM duration specifies the maximum amount of time that the message is displayed before an automatic redirect occurs to the originally requested page. (If the automatic redirect feature is turned off, the greeting or message page is displayed until the subscriber enters another URL.)

SESM duration must be equal to or greater than the SSG duration. Otherwise, redirections that SESM tries to perform are too early and do not take place.

Durations on the SSG Side

On the SSG side, the message duration controls the length of time the SSG holds the browser to the message page before allowing the browser to display any other URL. If the subscriber or any web application (such as the SESM message portal application) attempts to redirect the browser before the SSG duration time elapses, the attempt fails. On the SSG side, duration is specified as follows:

- In the following SSG TCP redirect commands:

  ssg tcp-redirect redirect captivate initial default group *group-name* **duration** *seconds*
  ssg tcp-redirect redirect captivate advertising default group *group-name*
  duration *seconds* **frequency** *seconds*

- In the subscriber profile—The duration attributes are optional in a subscriber profile. If provided, they override the values specified in the SSG TCP commands. The subattribute codes and related syntax in the subscriber profile are:
  - **RI***group*;*duration*[;*service*]—Overrides the TCP redirect configuration for initial login redirections.
  - **RA***group*;*duration;frequency*[;*service*]—Overrides the TCP redirect configuration for advertisement redirections.

Durations on the SESM Side

On the SESM side, the message duration controls how long the content application waits before attempting to redirect the browser from the message page to the subscriber's originally intended URL or to a default URL. (If the redirect feature is turned off in the messageportal.xml file, then the SESM duration attributes are ignored.) On the SESM side, duration is specified as follows:

- In the captiveportal.xml file.

  The duration values in the captiveportal.xml file are forwarded to the content application. One set of attributes applies to all messaging applications. Captive Portal forwards this value to the content application, using the CPDURATION parameter in the query string of the HTTP redirect.

  The duration attributes in the captiveportal.xml file are:

  - initialCaptivateDuration
  - advertisingCaptivateDuration

- In the messageportal.xml file.

  The defaultDuration attribute in the messageportal.xml file is a default value used if Captive Portal does not forward a duration attribute.

Demonstrating Captive Portal Features

This section describes how to show captive portal features. The topics are:

- Assumptions, page 4-14
- Demo Procedures, page 4-14

Assumptions

The procedures in this section make the following assumptions:

- You have a fully configured SESM RADIUS installation, or SESM SPE installation, including verified communication with an SSG.
- You completed the configuration of the Captive Portal solution, described in this chapter.

Demo Procedures

To demonstrate Captive Portal features:

Step 1 Start all the applications in the Captive Portal solution by running their start scripts.

```
jetty
    bin
        startNWSP
        startCAPTIVEPORTAL
        startMESSAGEPORTAL
```

Step 2 Open a web browser from a network configured as an incoming network on the SSG. Enter a URL, such as www.yahoo.com, or allow the browser to try to display a home page setting.

Unauthenticated user redirection causes the NWSP login page to appear.

Step 3 Sign on using a user ID and password from the subscriber profiles you created specifically for this demonstration. After successful authentication, the following occurs:

a. The NWSP home page appears in the main window.

b. A popup window appears, intended for the originally requested URL (www.yahoo.com).

c. Initial login redirection causes the greetings page from Message Portal to appear in the pop-up window.

d. After the length of time specified by the duration parameter, the next action depends on how the redirectOn configuration parameter for Message Portal is set:

- True—Message Portal redirects the browser to the originally requested URL (www.yahoo.com). The service is subjected to service redirections.
- False—The greetings page continues to be displayed until you enter another URL. Enter the URL after the duration time expires.

e. In response to a service redirection, NWSP displays one of the following in the main window:

- If the service requires credentials, NWSP displays a service login page.
- If the subscriber is not subscribed to the service, NWSP displays the subscription page.
- If NWSP does not find the service, the home page appears.
- Otherwise, NWSP tries to start the service. It brings the service pop-up window to the foreground.

Step 4 If the service redirection did not work, check the following configurations. To demonstrate service redirection for a service named yahoo, all of the following configurations must be set:

- A service profile must exist whose service name is yahoo and the service URL is www.yahoo.com.
- A specific service redirection must be configured. The service name yahoo must be specified in the service definition in captiveportal.xml.
- The subscriber name that you used during login must be subscribed to the service named yahoo. Check the subscriber profile.

Step 5 To demonstrate a default service redirection, select a service from the NWSP service selection list with an IP address outside the destination networks of all the specific service redirections. It does not matter whether the subscriber is subscribed to the service.

Default service redirection is usually configured so that a service name is not passed to NWSP, which causes NWSP to display the page specified in the serviceNotGivenURI attribute in nwsp.xml. In the default configuration suggested during installation, the serviceNotGivenURI attribute points to the NWSP session status page. You can change this value to point to a different page, such as the NWSP subscription page or home page.

Step 6 To demonstrate an advertising redirection:

1. Wait until the configured TCP advertising interval time has elapsed. (The default time interval used during installation is 60 seconds.)
2. Perform some action on the SESM web page, such as selecting another service or requesting the status page. The SSG intercepts the request with an advertising redirection. An advertisement page from Message Portal appears.

Step 7 To demonstrate the captivation feature, enter another URL before the TCP advertising duration elapses. (The default duration time configured in the sample ssgconfig.txt file is 10 seconds.) The newly entered URL is not honored, and the advertisement page from Message Portal redisplays.

Configuring SESM Plug and Play

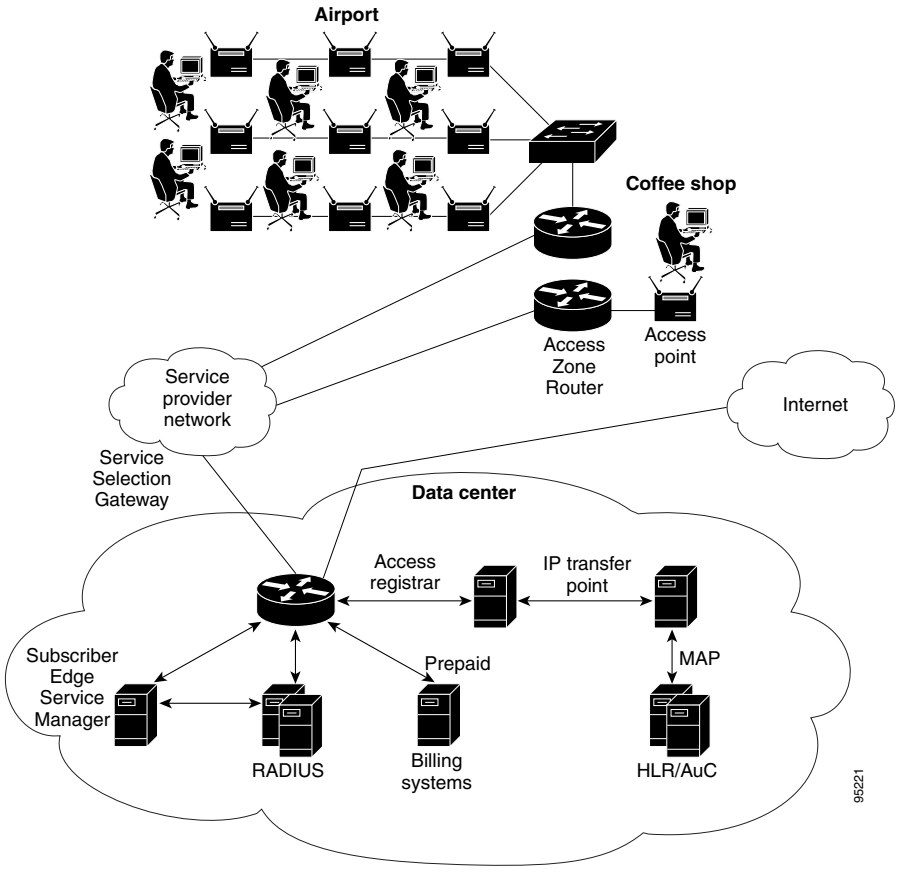
This chapter provides information on how to configure the SESM Plug and Play features. The chapter contains the following topics:

Note For information about configuring whitelists, see Configuring Location-Specific Whitelists, page 6-8.

Plug and Play Overview

The SESM Plug and Play solution allows Internet Service Providers (ISP)s to provide Internet access and subscriber services to nomadic users of Public Wireless LANs (PWLANs), regardless of how their web proxy or DNS settings are configured. As shown in Figure 5-1, the Plug and Play network components consist of wireless access points (APs) connected to Access Zone Routers (AZRs) at wireless hotspot venues such as an airport or coffee shop.

Figure 5-1 Typical PWLAN Network



Note Subscribers who are proxy users should use Internet Explorer 6.0 or higher to access the SESM web portal. There are known problems with earlier versions of Internet Explorer, which might result in unexpected results for subscribers.

Plug and Play Configuration Scenarios

At present, SESM requires additional configuration to provide Plug and Play connectivity for certain client configurations. Additional configuration is needed to handle the following scenarios:

- Clients with a web proxy configured on their PC.
- Clients with unresolved DNS names configured on their PC. This applies to subscribers with DNS names configured on their PC that are only resolvable within private networks.

This section describes how to configure SESM to provide Plug and Play access for both these scenarios.

- Configuring SESM for Subscribers Using a Web Proxy, page 5-5 describes how to configure SESM to provide Plug and Play access to unauthenticated users accessing the web using a web proxy on their PC.
- Configuring SESM for Subscribers with Unresolvable DNS Names, page 5-6 describes how to configure SESM to allow subscribers with unresolvable DNS names on their PC to access the web via the SESM web portal.

Subscribers Using a Web Proxy

Figure 5-2 shows a SESM plug and play scenario using the SESM web proxy:

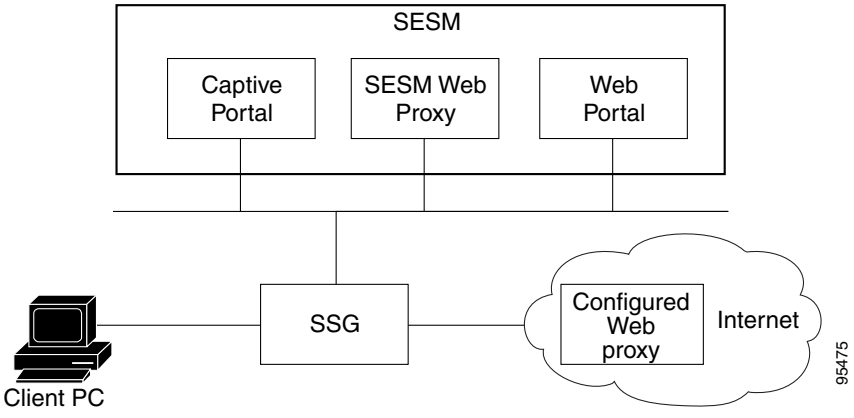
- Captive Portal proxies requests from unauthorized users. Users can be unauthenticated, or authenticated without an active service allowing access to the Internet. Proxy requests are allowed to the SESM web portal or to hosts in the configured whitelists.

  Unauthorized users are TCP-redirected by SSG to Captive Portal. This is either to port 8090 due to unauthenticated user redirection or unauthenticated permanent HTTP redirection, or to port 8101 due to authenticated permanent HTTP redirection.

- The SESM web proxy proxies requests from authorized users. By default, the SESM web proxy is configured to proxy all requests to the Internet.

  Authorized users are TCP-redirected by SSG to the SESM web proxy on port 8102 by the Service-Info="KW<servergroup>" attribute in the profile for the service, which is typically an auto-logon or a prepaid service. See nwsp/config/aaa.properties for an example Internet service profile.

Figure 5-2 SESM Plug and Play Web Proxy Scenario



Note The configured web proxy in the Internet cloud is the web proxy configured for use in the client's browser.

Plug and Play access for subscribers with a web proxy is configured as follows:

- Installing SESM using the Typical installation option, or the Custom option with the Captive Portal feature selected.
- Configuring the Captive Portal captiveportal.xml file with the servers to which unauthorized subscribers will be allowed access. These include Captive Portal and open garden servers.
- Configuring the web proxy webproxy.xml file for authorized subscribers to gain access to the Internet.
- Configuring the web portal web-jetty.xml file.

Subscribers who use a web proxy to attempt to access unauthorized servers are then presented with the standard web portal login screen on startup.

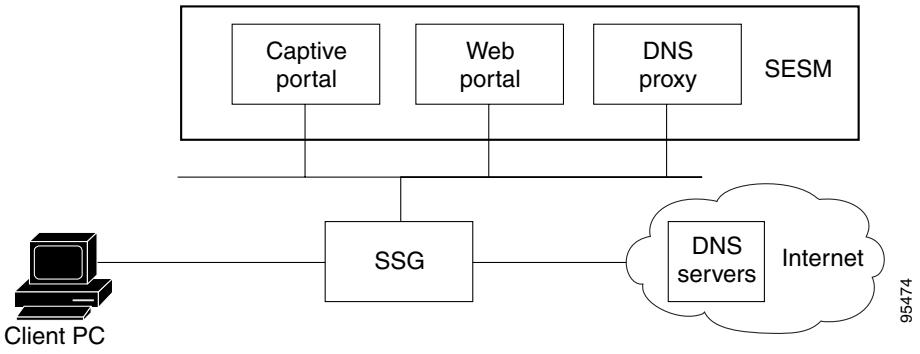
The complete configuration procedure is described in Configuring SESM for Subscribers Using a Web Proxy, page 5-5.

For further information on the call flow sequences used in this scenario, see Redirection of Subscribers Using Web Proxy, page 5-9.

Note This solution supports secure authentication (https) for subscribers using a web proxy.

Subscribers with Unresolvable DNS Names

Figure 5-3 SESM Plug and Play Unresolvable DNS Names Scenario



SESM Plug and Play handles subscribers who have DNS names configured on their PC that are resolvable only within private networks.

For example:

A subscriber starts their web browser in a PWLAN hotspot, and the browser attempts to find http://www.privatedomain.com. This is a private DNS name that corresponds to a server within a corporate network.

The ISP attempts to resolve the DNS name to an IP address to enable contact with the web server. The resolution fails, and as a result the browser fails to request any web page and displays an error. For example, Internet Explorer 6 would display the message “Cannot find server or DNS error”.

Instead of failing to resolve the IP address, the SESM Plug and Play solution simulates a successful DNS response by inserting an upstream IP address so that the client can request a web page. As a result, the client is redirected to the SESM login page.

Plug and Play access for subscribers with unresolvable DNS names is configured as follows:

- Installing SESM using the Typical installation option, or using the Custom installation option with the tools option selected.
- Configuring the dns.xml file with a list of DNS servers that the DNSProxy application will use when it performs a DNS lookup.
- Adding the DNS substitute IP address. This is the IP address with which the DNSProxy application will respond when a client performs a DNS lookup in which the name is not resolvable.

Subscribers with unresolvable DNS names are then presented with the standard web portal login screen on startup.

The complete configuration procedure is described in Configuring SESM for Subscribers with Unresolvable DNS Names, page 5-6.

For further information on the call flow sequences used in this scenario, see Subscribers Requesting an Unresolvable DNS Name, page 5-10.

Configuring SESM for Subscribers Using a Web Proxy

This section describes how to configure SESM for users who have a web proxy configured on their PC.

Note For more information about providing Public Wireless LAN (PWLAN) access to unauthenticated users, and configuration of whitelists, see Chapter 6, “Configuring Location Awareness and Whitelist URLs.”

To configure SESM to provide Plug and Play access for users who have a web proxy configured on their PC, see the following topics:

1. Configuring IP ranges as locations in Captive Portal—see Configuring Location Awareness, page 6-1.
2. Setting the accountWebProxy attribute and the sesmSessionEnabled attribute—see Configuring Whitelists, page 6-9.
3. Editing the Pre-Authentication Whitelists in Captive Portal—see Configuring Whitelists, page 6-9.
4. Editing the Web Portal Host List, page 5-6.

Editing the Web Portal Host List

To configure the web portal host list in the webproxy.xml file:

Step 1 Using a text editor, open the webproxy.xml file from <SESM>/webproxy/config/webproxy.xml.

Step 2 Edit the following section, to ensure that sesmHostList contains all public DNS names and IP addresses by which a user may access a SESM web portal. The installation program automatically adds the web portal host as specified during the installation, but others might need to be added.

```
<Set name="sesmHostList">
    <Array type="java.lang.String">
    <Item>127.0.0.1</Item>
        <Item>localhost</Item>
        <Item>nwsp</Item>
        <Item>captiveportal</Item>
    </Array>
</Set>
```

Step 3 Save the modified webproxy.xml file.

The web proxy configuration is now complete. Subscribers with browsers configured to use web proxy servers are now able to access open garden sites and are redirected to the Web Portal when attempting to access a site outside the open garden. These users can enter their credentials to gain access to services using the standard login page as shown in Figure 5-4.

Note For more details about using SESM web portals, see *Cisco Subscriber Edge Services Manager Web Portals Guide*.

Configuring SESM for Subscribers with Unresolvable DNS Names

This section describes how to configure the Cisco Subscriber Edge Services Manager (SESM) to provide Public Wireless LAN (PWLAN) access to unauthenticated users who have unresolvable DNS names configured on their PC.

To configure SESM to handle subscribers who have unresolvable DNS names configured on their PC, proceed as follows:

Step 1 Install SESM using the procedures described in the *Cisco Subscriber Edge Services Manager Installation Guide*.

Step 2 During the installation process, select the **Custom Install** option.

Step 3 When you reach the product installation screen, select the **Tools** option.

Step 4 Complete the installation process.

Step 5 Using a text editor, open the file <SESM>/tools/config/dns.xml.

The dns.xml file contains a list of DNS servers that the DNSProxy application will use when it performs a DNS lookup.

Step 6 Within the section of the dns.xml file shown below, enter the IP addresses of the DNS servers you want to add, represented by *XXX* and *YYY*.

```
<!-- Configure the RESOLVER with IPs and Port of real DNS --> <Item> <New
class="com.cisco.sesm.erp.dns.DNSDelegationHandler">
<Set name="name">RESOLVER</Set>
<Set name="port">53</Set>
<Set name="servers">
<Array class="java.lang.String">
<Item>XXX.XXX.XXX.XXX</Item>
<Item>YYY.YYY.YYY.YYY</Item>
</Array>
</Set>
<Set name="timeout">5000</Set>
</New>
</Item>
</Array>
</Set>
</Configure>
```

Step 7 Within the section of the dns.xml file shown below, replace the entry marked *ZZZ* with any upstream IP address, such as the one provided. This forces redirection of unauthenticated proxy users to Captive Portal.

```
<!-- Configure substituteIP handler with IP and TTL of unresolved requests --> <New
class="com.cisco.sesm.erp.dns.DNSSubstituteIPHandler">
<Set name="name">DNS</Set>
<Set name="ResolverHandlerName">RESOLVER</Set>
<Set name="substituteIP Address">ZZZ.ZZZ.ZZZ.ZZZ</Set>
<Set name="timeToLive">30</Set>
<Set name="dump">true</Set>
</New>
</Item>
```

Step 8 Start the DNSProxy application using the start script <SESM>/tools/bin/startDNS.sh.

Now the DNS proxy will force all names to resolve so that clients configured with private DNS names can access the open garden and receive the Web Portal to log in.

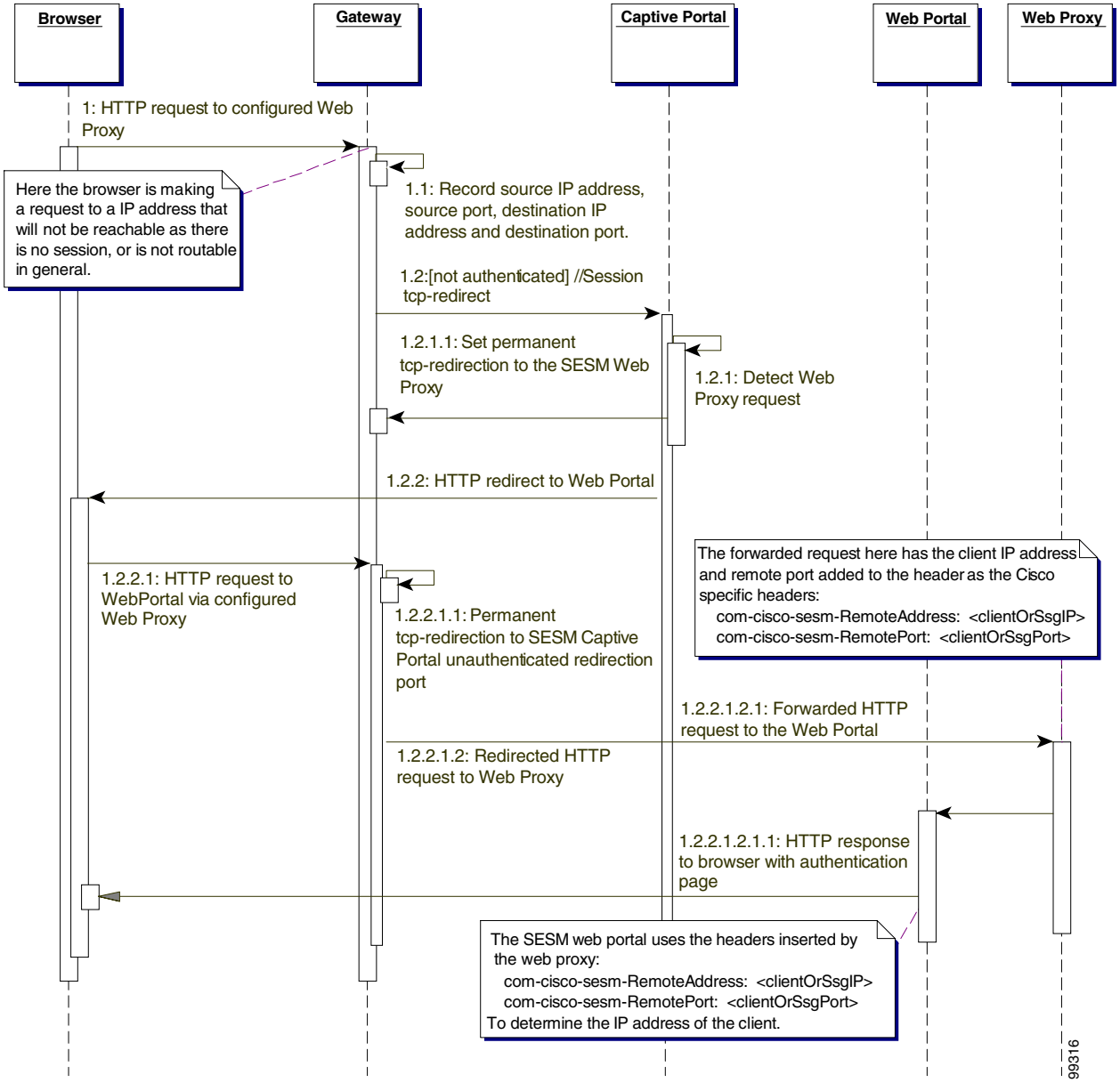
Note For more details about using SESM web portals, see *Cisco Subscriber Edge Services Manager Web Portals Guide*.

Figure 5-4 Web Portal Login Screen

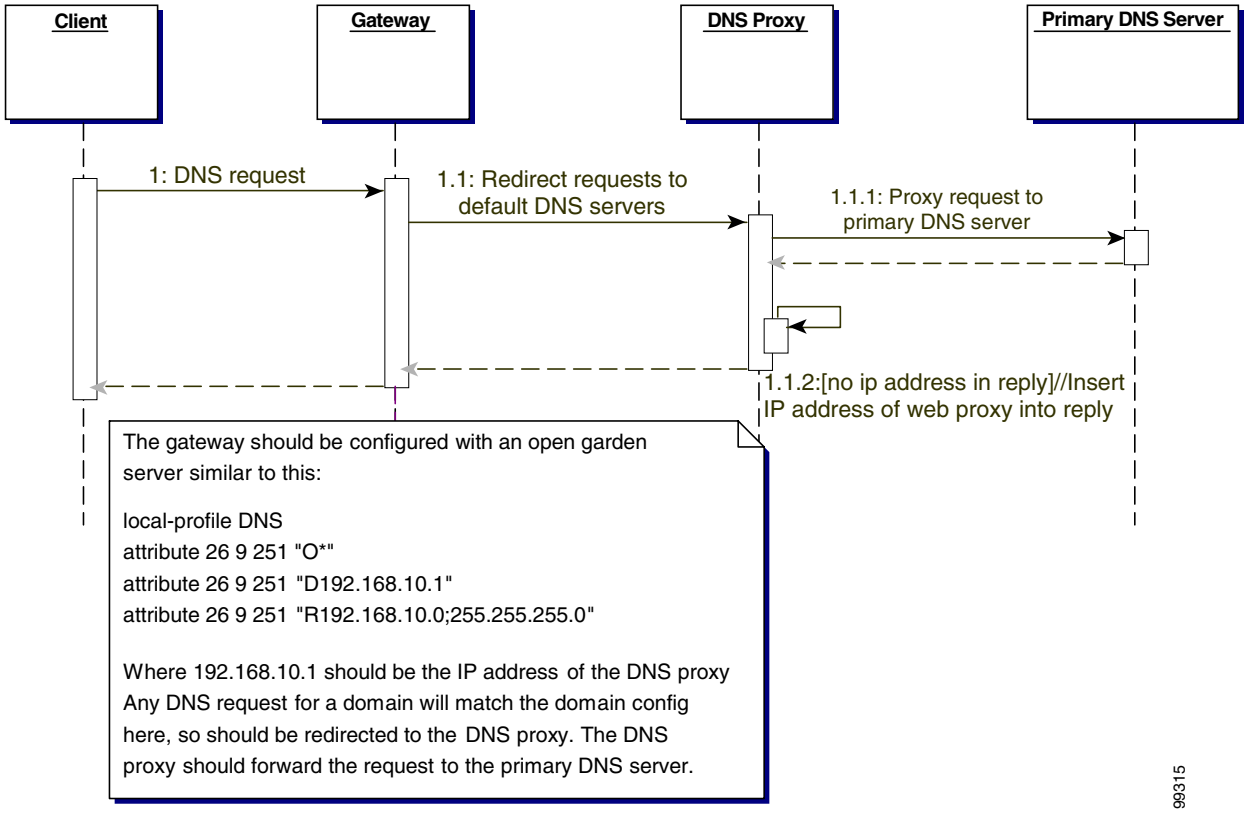
Plug and Play Call Flow Sequence Diagrams

This appendix contains sequence diagrams for the following scenarios:

Redirection of Subscribers Using Web Proxy



Subscribers Requesting an Unresolvable DNS Name



Configuring Location Awareness and Whitelist URLs

This chapter describes how to configure and update the SESM location awareness features and location-specific whitelists. The chapter contains the following topics:

Configuring Location Awareness

This section describes SESM's locations awareness feature. It contains the following topics:

Overview of Location Awareness

The SESM location awareness feature relies on the physical location characteristics of an edge session. SESM obtains this location information from the Service Selection Gateway (SSG) as part of the session's initial connection request. The specific attributes used to determine the location can be configured. The location attributes can consist of the client IP address, virtual path identifier (VPI), virtual connection identifier (VCI), and SSG subinterface, depending on the network deployment, and are valid even before the session authenticates.

The SESM location awareness feature can be used for the following:

- Location branding in SESM web portals—A SESM web portal can use location awareness for location branding to control the look and feel of portal pages. See *Cisco Subscriber Edge Services Manager Web Portals Guide* for more information about web portal branding.
- Provisioning free services using location-based whitelists—SESM supports the creation of location-specific whitelists, which enables you to define a different list of free access destinations per location. Access to these destinations does not require identification and/or authentication of the user. This feature is required in many public wireless LAN (PWLAN) solutions. For more information, see Configuring Location-Specific Whitelists, page 6-8.

SESM offers two ways to configure location awareness. Table 6-1 describes these two methods.

Table 6-1 Location Configuration Methods

Feature	MBean	Attributes That Determine Location	Restrictions
Location awareness using complete ID attributes **Note** This is the recommended method for defining location awareness.	Location MBean	One of the following attributes or a combination of attributes: • A single subscriber IP address range. • Multiple subscriber IP address ranges. • VPI range. • SSG subinterface, such as an Ethernet interface. More attributes might be added in future releases.	Requires the SSG complete ID feature, available from the following Cisco IOS releases: • Release 12.3(4)T. • Release 12.2(16)B.
Location awareness using IP subnets	SSG MBean	Subscriber IP address subnetwork ranges.	Does not work if load balancing is implemented. Does not work if you use the port-bundle host key feature (PBHK). Will be phased out in future releases.

If you configure both of the above location awareness methods for the same SESM web application, 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 web application examines the complete ID criteria in the Location MBean.

The following SESM web applications can use both location features:

- Captive Portal.
- Web portal applications—NWSP, PDA, SP, WAP.
- Web Proxy.
- Web Services Gateway (WSG).

In previous releases of SESM, the location configuration was part of the XML configuration file that configured an entire web application (for example, captiveportal.xml, nwsp.xml, and so on). Location configuration based on complete ID was static, and the relevant web application had to be restarted to reread a modified location configuration. This release of SESM includes the SESM file poller to simplify the task of editing location configurations and to dynamically update location and whitelist information without requiring an application restart.

Note Dynamic update of locations does not affect active sessions. Users with an open session who were already associated with a location, continue with the same location as long as their session is active. The locations are updated only for new sessions after their current session times out. To force an update on users with an open session, clear all sessions in Agent View.

You can use the file poller to share one location configuration among different web applications. For more information about dynamically updating information using the SESM file poller, see Using the File Poller to Update Locations and Whitelist Configurations, page 6-13.

Note Both location awareness features are shipped with an example configuration block in the *application*.xml file (captiveportal.xml, nwsp.xml, and so on). These blocks are commented out. You can uncomment and modify these configuration blocks in the application xml file according to the location settings in its deployment.

To enable these configurations to be dynamically updated by the SESM file poller, cut the configuration blocks from the *application*.xml file and paste them into a polled file. For more information, see Using the File Poller to Update Locations and Whitelist Configurations, page 6-13.

The following sections describe how to configure location awareness in SESM web applications:

- Configuring Location Awareness Based on Complete ID Attributes, page 6-3
- Configuring Location Awareness Based on IP Address Subnets, page 6-7

Configuring Location Awareness Based on Complete ID Attributes

The complete ID is the complete set of identifying attributes available about an edge session. The SSG makes this set of attributes available to SESM. The SESM location awareness feature uses a subset of the complete ID attributes. The complete ID attributes that are currently supported for location awareness are listed in Table 6-1.

Note To use location awareness based on complete ID, your SSG platforms must be running Cisco IOS Release 12.3(4)T or Release 12.2(16)B and later.

Use the Location MBean to define location names and the attributes that are associated with each location. The procedure in this section describes how to configure locations in Captive Portal. To share the same location definitions with other web applications, and to dynamically update location configurations, use the SESM file poller. See Using the File Poller to Update Locations and Whitelist Configurations, page 6-13 for more information about the SESM file poller.

Using Multiple Attributes for the Same Location

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

An attribute definition in a location can include multiple IP ranges, but it is restricted to one value for VPI range and one value for interface. However, you can define more than one location with the same name using the same attributes, but with different attribute values. For example, you can define two “london” locations, each one using a different VPI range.

Using Duplicate, Overlapping, and Nested Attributes for Different Locations

A session's attributes can match the criteria for more than one location. SESM offers two ways to resolve the location in these cases:

- Identify the first matching location—The portal associates the first location whose configured attributes match all of the attributes of the edge session. By default, SESM applications implement location awareness this way using the getLocation method.

  The order of locations in the configuration file is important, as shown in the examples below for overlapping and nested location definitions.

- Identify all matching locations—This feature provides a way to return all matching locations for nesting and overlapping locations. The portal must be customized to use the getLocations method. This method returns an iterator over all of the locations that match the attributes for the session. The iterator ordering is based on the order of the locations in the configuration file.

Overlapping Locations

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

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

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

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

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

Applications that return a single location return the first match. In the examples above, this is location A. Use the order of the location configurations to determine the best location match.

Nested Locations

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

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

The SESM web portals use a single location, which is the location returned by the first match. With nested interfaces, usually you want to define the smallest location first. In the example above, this is location A. The smaller nested locations are effectively hidden if they are not placed in the configuration file before the larger locations that encompass them.

Captive Portal and the SESM web proxy use the locations returned by all matches found in the whitelists; therefore, the order in which nested locations are defined is irrelevant.

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

Procedure to Configure Locations using Complete ID Attributes in Captive Portal

Step 1 Using a text editor, open the captiveportal.xml file from <SESM>/captiveportal/config.

Step 2 Within the captiveportal.xml file, uncomment the following Location MBean instantiation clause:

```
<Instantiate order="50"
         class="com.cisco.sesm.core.location.LocationMBean"
         jmxname="com.cisco.sesm:name=Location"/>
```

Step 3 Within the captiveportal.xml file, edit the Location MBean configuration.

Note If you want to use the file poller, define the location configuration in a separate file (for example, location.xml) from which the file poller can access it.

The following examples define three locations, london, paris, and newyork.

This section of the file is the opening configuration clause for all locations:

```
<Configure jmxname="com.cisco.sesm:name=Location">
  <!-- Defines the class that provides location service implementation -->
  <Set name="locationService">com.cisco.sesm.spis.location.LocationImpl
  </Set>
    <!-- This defines a set of locations and their parameters -->
    <Set name="locations">
      <Array class="com.cisco.sesm.core.location.Location">
```

This section of the file defines parameters for london, using multiple IP ranges:

```
        <Item>
          <New class="com.cisco.sesm.core.location.Location">
            <!-- The "london" Location applies to all sessions with a client
                 IP address in one of the following ranges:
                 10.0.0.0 - 10.9.0.0 or 10.20.0.0 - 10.29.0.0 or
                 20.0.0.0 - 20.9.0.0. This is done with the new
                 multiple IP range parameter -->
            <Set name="name">london</Set>
            <Set name="parameters">
              <Array class="com.cisco.sesm.core.location.LocationParameter">
                <Item>
                  <New class=
                    "com.cisco.sesm.core.location.MultipleIPRangeParam">
                    <set name="subnetRanges">
                      <Array class= "java.lang.String">
                        <Item>10.0.0.0, 10.9.0.0</Item>
                        <Item>10.20.0.0, 10.29.0.0</Item>
                        <Item>20.0.0.0, 20.9.0.0</Item>
                      </Array>
                    </Set>
                  </New>
                </Item>
              </Array>
            </Set>
          </New>
        </Item> <!-- close the item clause of location "london" -->
```

This section of the file defines parameters for the newyork location, using a single IP range:

```
<Item>
   <New class="com.cisco.sesm.core.location.Location">
     <!-- The "newyork" Location applies to all sessions with a client
    IP address in one range of IPs: 30.0.0.0 - 30.0.10.0. Using the single IP
      range parameter -->
     <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">30.0.0.0</set>
             <set name="end" type="String">30.0.10.0</set>
          </New>
         </Item>
       </Array>
     </Set>
   </New>
 </Item> <!-- close the item clause of location "newyork" -->
```

This section of the file is used to define parameters for the paris location, using the VPI and subinterface attributes:

```
<Item>
   <New class="com.cisco.sesm.core.location.Location">
     <!-- The "paris" Location applies to all sessions with a VPI
          range from 1 to 3 on the sub-interface "ATM3/0". Both
          requirements must match for the location to apply to a
          session. -->
     <Set name="name">paris</Set>
     <Set name="parameters">
       <Array class="com.cisco.sesm.core.location.LocationParameter">
         <Item>
           <New class="com.cisco.sesm.core.location.VPIRangeParam">
             <Set name="start" type="int">1</Set>
             <Set name="end" type="int">3</Set>
           </New>
         </Item>
         <Item>
           <New class=
             "com.cisco.sesm.core.location.SubInterfaceParam">
             <Set name="subInterface" type="String">ATM3/0</Set>
           </New>
         </Item>
       </Array>
     </Set>
   </New>
 </Item> <!-- close the item clause of location "paris" -->
</Array>
</Set>
</Configure>
```

Step 4 Save the modified captiveportal.xml file.

Configuring Location Awareness Based on IP Address Subnets

To configure locations based on IP address subnets, use the SSG MBean. Use setSubnetAttribute entries with the SESSION_LOCATION argument. See Appendix A, "SESM MBeans" for more information about the MBean attributes.

Note You cannot use the SSG MBean to configure location awareness if you are using PBHK.

The following example from nwsp.xml shows the attributes required for location awareness:

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

- *ipAddress* and *mask* indicate one of the following:
  - A range of subscriber IP addresses (a subnet)—Use the IP address and Mask fields to indicate a subnet of IP addresses to associate with the same location.
  - A specific IP address—The IP address of the client.
- *location* is the location you want to associate with *ipAddress.* Any value is acceptable, but it must match your intended uses. See *Cisco Subscriber Edge Services Manager Web Portals Guide* for examples of location name usage.

Note To use the SESM file poller to dynamically update locations or share the location configuration among applications, define the location configuration in a separate file (for example, location.xml), from which the file poller can access it. See Using the File Poller to Update Locations and Whitelist Configurations, page 6-13 for more information about the SESM file poller.

Example 1—Location Associated with Subscriber IP Addresses

The following example associates locations with subscriber subnets. The example associates a different subscriber network with different locations. In the NWSP application, when subscribers from the 144.0.0.0 network point their browsers to the NWSP URL, the words New York appear under the NWSP logo.

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

Example 2—Location defined with Multiple Ranges

You can define multiple ranges for a location by including more than one set of attribute definitions for a single location. In the following example, clients in subnets 100.0.0.0 and 200.0.0.0 are both mapped to location london.

```
<Call name="setSubnetAttribute">
  <Arg>100.0.0.0</Arg><Arg>255.0.0.0</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>london</Arg>
</Call>
<Call name="setSubnetAttribute">
  <Arg>200.0.0.0</Arg><Arg>255.0.0.0</Arg>
  <Arg>SESSION_LOCATION</Arg><Arg>london</Arg>
</Call>
```

Configuring Location-Specific Whitelists

This section describes SESM's support of location-specific whitelists to enable users free access destinations depending on their location. This section contains the following topics:

Whitelist Overview

An open garden service (in SSG terminology) is a set of Internet destinations that can be accessed free of charge without subscriber identification/authentication or authorization. The previous release of SESM supported the creation of location-specific whitelists to provide web proxy users with different free access destinations depending on location. This release of SESM extends the support of location-specific whitelists to non-proxy users. Locations can be defined by multiple, noncontiguous client IP address ranges.

Users can access whitelist URLs before authentication (pre-authentication) and after authentication (post-authentication). For non-proxy users post-authentication, authorized access to the whitelist URL (when the whitelist URL destination is part of the provisioned service) is directly through the SSG with no SESM involvement.

For both proxy and non-proxy users, access to whitelist URL sites before authentication is allowed and is free, while access to those sites after authentication is allowed but not always free. When a whitelist URL site is included in one of the services that are activated for the session, access to this site is billed according to the specific service policy.

Note Support for non-proxy users is based on the solution for proxy users. Proxy for non-proxy users is called transparent proxy. A limitation of any solution for transparent proxying is that HTTPS is not supported. It is not possible to seamlessly proxy such requests; otherwise, this would mean that HTTPS is susceptible to "man-in-the-middle" intercept attacks. A certificate mismatch occurs when an HTTPS request is proxied. If the user decides to accept the mismatch, then the user will be successfully proxied.

SESM has been tested to support up to 5000 locations, with 100 IP ranges and 100 hosts per location.

Whitelist Management

Whitelist management can use the location definitions configured with either complete ID attributes or ID address subnets. For more information, see Configuring Location Awareness, page 6-1.

Whitelists can be updated dynamically with the SESM file poller. You do not need to restart the SESM application. See Using the File Poller to Update Locations and Whitelist Configurations, page 6-13 for more information.

Other whitelist management features:

- All attributes for whitelist configuration are accessible via an MBean. You can add and remove elements from any collection of MBeans. See Configuring Whitelists, page 6-9 for a list of the MBeans that can be configured.

- In addition to be being able specify a host using the exact hostname or IP address, you can add domains using partial string matching. For example, if you add **.cisco.com** to a whitelist, this will include all hosts in the cisco.com domain.
- Multiple and overlapping locations are supported. For example if a client IP is included in the IP address ranges for two different locations, then the whitelists for both locations apply.
- You can group by hosts:
  - SESM uses explicit grouping by hosts.
  - Group names are used nonrecursively, meaning a name referred to from within a group will be assumed to be a host name, and will not be checked for being a group name first.

Whitelists are constructed at configuration time rather than during use, to minimize any performance impact of this feature.

Configuring Whitelists

You can configure whitelists before starting the application by modifying the XML file. After Captive Portal or Web Proxy is started it is recommended to configure the MBeans using Agent View. (You cannot configure whitelists using the Application Manager.)

You configure whitelists by configuring the MBeans listed in Table 6-2.

Table 6-2 MBeans for Configuring Whitelists

MBean	Application	Location in Agent View
CPProxyHandler MBean	Captive Portal	Under org.mortbay.jetty name=Jetty,Server=0,WebApplicationContext=0, context=/,CPProxyHandler=0
AccountWebProxyHandler MBean	Web Proxy	Under org.mortbay.jetty name=Jetty,Server=0,WebApplicationContext=0, context=/,AccountWebProxyHandler=0

See Appendix A, "SESM MBeans" for information about the attributes of these MBeans.

The following configuration relates to proxy handling in Captive Portal for proxy users and also for non-proxy users, if configured. This provides access to hosts in the whitelists, regardless of whether the user is authenticated or not.

Note The SESM web proxy is used for proxying requests from authorized proxy users. By default, the SESM web proxy is configured to proxy all requests to the Internet. The SESM web proxy can be configured in the same way as Captive Portal to use locations, whitelists and blacklists, as described in Step 5 and Step 6 in the following procedure. Typically, these would not be configured in web proxy. However, you can use multiple SESM web proxy servers, each with different blacklists, to emulate the use of multiple services. These lists can therefore be considered to be postauthorization blacklists.

Note If you want to use the SESM file poller to dynamically update whitelists, or share the whitelist configuration among applications, define the whitelist configuration clauses in a separate file (for example, whitelist.xml), where it can be accessed by the file poller. See Using the File Poller to Update Locations and Whitelist Configurations, page 6-13 for more information about the SESM file poller.

To configure whitelists in Captive Portal:

Step 1 Using a text editor, open the captiveportal.xml file from <SESM>/captiveportal/config/.

Step 2 Set the accountWebProxy attribute to true, as shown in the following example, to enable full web proxy handling if your SSG supports permanent TCP redirection for web proxy users.

```
<!-- Enable the SSG Account Web Proxy feature so as to use white or
               black lists. This requires SSG 12.3(3)B or 12.3(8)T onwards.-->
          <Set name="accountWebProxy" type="boolean">true</Set>
```

Step 3 Set the sesmSessionEnabled attribute to true, as shown in the following example, only if you need location-based whitelists in Captive Portal (default is disabled).

```
<!-- Set this to true if require location-based white/black lists.-->
          <Set name="sesmSessionEnabled" type="boolean">true</Set>
```

Note Captive Portal also requires a SESMSession when *accountWebProxy* is set to true. In this case, the SESMSession is cached and reused if the following conditions are met:

- The request is from a proxy user, and the request is for a SESM host.
- The request is for a MIME-type that is in the list of handled MIME-types, or, if no such list is defined, has a MIME-type extension that is not in the exclusion list, such as for images or style sheets.

Step 4 If required, edit the following section to define groups of hosts:

```
<!-- Set groups of hosts that can be used in other lists by
               referring to their key (e.g. 'freeservices').
               The keys for groups are not resolved recursively.  -->
          <!--
          <Set name="hostGroups">
            <New class="java.util.HashMap">
               <Put name="freeservices">
                 <Array class="java.lang.String">
                   <Item>.google.com</Item>
                   <Item>.google.nl</Item>
                   <Item>192.168.1.1</Item>
                 </Array>
               </Put>
             </New>
           </Set>
            -->
```

Step 5 If required, edit the following section to define the global and location-specific whitelists for allowed proxy hosts, IP addresses, and domains.

Add maps of keys to arrays of hosts to proxyHostsWhiteLists or proxyHostsBlackLists to permit or deny access. The keys are case-insensitive:

- *"default"* or *""* for the default list. This list is global, it is not location specific.

- <*location*> for a location-specific list.
- <*listener port*> for a redirection-specific list.

The hosts for the arrays are hostnames, IP addresses, partial domain names (such as .cisco.com) or names of non-recursively used groups from hostGroups. String matching is used to determine whether the host is allowed.

```
<!-- Set the white lists for allowed proxy hosts/IPs/domains.
               If no white lists have been set, then no hosts are allowed.
               The hosts in the 'default' list are accessible regardless of
               the keys provided, if they are not blocked in a black list.
               These white lists do not need to contain any SESM web portals,
               as hosts in the 'sesmHostList' are always allowed if
               'sesmHostsAllowed' is true.  Either way, it is important to
               include all possible aliases and IP addresses for SESM hosts,
               otherwise a looping condition will arise.
               Additional hosts can be added to location-specific white lists.
               A list including "*" will allow all hosts for that key. -->
     <!--
          <Set name="proxyHostsWhiteLists">
            <New class="java.util.HashMap">
              <Put name="default">
                <Array class="java.lang.String">
                  <Item>.cisco.com</Item>
                </Array>
              </Put>

              <Put name="london">
                <Array class="java.lang.String">
                  <Item>www.visitlondon.com</Item>
                  <Item>freeservices</Item>
                </Array>
              </Put>
            </New>
          </Set>
           -->
```

Step 6 If required, edit the following section to define blacklists of disallowed proxy hosts, IP addresses, or domains:

```
<!-- Set black lists of disallowed proxy hosts/IPs/domains.
               Additional hosts can be added to location-specific black lists.
           -->
     <!--
          <Set name="proxyHostsBlackLists">
            <New class="java.util.HashMap">
              <Put name="default">
                <Array class="java.lang.String">
                  <Item>.microsoft.com</Item>
                </Array>
              </Put>
              <Put name="london">
                <Array class="java.lang.String">
                  <Item>www.manchester.com</Item>
                </Array>
              </Put>
            </New>
          </Set>
           -->
```

Step 7 Edit the following section to ensure that the sesmHostList attribute contains all possible hostnames and IP addresses by which a user may access a SESM web portal. The installation program automatically adds the web portal host as specified during the installation, but you might need to add others.

Note This attribute is not relevant for transparent proxying of non-proxy requests. Non-proxy requests to SESM hosts are not redirected by the gateway to Captive Portal, as these hosts are in the default network.

```
<!-- The sesmHostList is a list of hosts/IPs/domains that host SESM
                services. Requests proxied to these hosts need the remote
                client connection details sent either inband for http request
                or out-of-band in Proxy meta data for https requests.
                Requests to hosts in this list are always allowed if
                'sesmHostsAllowed' is true. Note that non-proxy requests-->
               to SESM hosts are not redirected by the gateway to Captive Portal,
               as these hosts are in the default network. So this list is
               not relevant for transparent proxying of non-proxy requests.
               -->
          <Set name="sesmHostList">
            <Array class="java.lang.String">
              <Item>nwsp</Item>
            </Array>
          </Set>

          <!-- SESM hosts as defined in sesmHostList are always proxied to,
               regardless of the white/black lists. -->
          <Set name="sesmHostsAllowed" type="boolean">true</Set>
```

Step 8 If required, in the following section, uncomment proxyPorts to allow transparent proxying of non-proxy requests on specific listener ports. (The installation program updates these ports if they are different from the default values.) By default Captive Portal proxies only proxy requests.

For example, in Agent View, to add transparent proxying for unauthenticated user redirection and default unauthorized service redirection on the default listener ports of 8090 and 8093, add **8090** and **8093** respectively.

```
<!-- The listener ports where transparent proxying will
                occur for non-proxy users according to the white/black lists.
                Uncomment the example below to allow this type of proxying
                for unauthenticated user redirection and
                default unauthorized service redirection. -->
          <!--
          <Set name="proxyPorts">
            <Array class="java.lang.String">
              <Item>8090</Item>
              <Item>8093</Item>
            </Array>
          </Set>
           -->
```

Step 9 Edit the following section. This indicates the web portal port to use for out-of-band standard requests sent to the web portal. These requests enable the web portal to determine the host key for secure proxied requests, where it is not possible during proxying to modify the request to add the remote IP address and port to the request header.

```
<!-- The port to use to send proxy meta data to a SESM host -->
          <Set name="proxyMetaDataPort" type="int">8080</Set>
```

Step 10 Save the modified file, captiveportal.xml, or other file that the file poller will poll.

Step 11 Configure the Jetty container for whitelists. Ensure that the captive portal hostname or IP address is added to the Jetty container for the web application in *webapp/WEB-INF/web-jetty.xml*.

For example, for NWSP, check that sesmProxyList in *nwsp/webapp/WEB-INF/web-jetty.xml* contains the Captive Portal and Web Proxy hosts (hostname or IP address). The installation program automatically adds the Captive Portal host as specified during the installation, but it might be necessary for you to add the Web Proxy host if this is on a different server. Note that this attribute cannot be accessed through Agent View. If you update this XML file, you must restart the application.

```
<!-- 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>
```

Using the File Poller to Update Locations and Whitelist Configurations

This section describes how to configure and use the SESM file poller to dynamically update location and whitelist configurations. This section contains the following topics:

Overview of File Poller for Dynamic Updating

Configuration of locations and whitelist URLs are based on verbose configuration, which cannot easily be configured through the SESM management screens. In previous releases of SESM, to change the verbose configuration of a module, all the files that contained the configuration clauses had to be modified manually, and the applications had to be stopped and then restarted to apply the changes.

Some configurations are contained in several applications, such as Captive Portal or NWSP. For example, each application could contain a separate yet identical copy of the location configuration clause in its configuration file.

This release of SESM provides a file poller mechanism that updates location and whitelist URL definitions without interrupting the user experience. It can also be used to share a configuration file among several applications, so that a configuration that is contained in several applications needs to be maintained only in a single file.

The file poller polls specified XML files at defined intervals to check whether they have been modified. These XML files contain the verbose configurations for locations and/or whitelists. If a file has been modified, the file poller updates the configuration of the appropriate MBeans. The polled files might contain the configuration for a specific application, or they might hold a configuration that is shared by several applications.

Typically, all the applications have the same location configuration; therefore, it is recommended to use a single shared file deployment (for example, location.xml). In the case of the whitelist URLs, different servers might require different settings, with each application carrying its own whitelist configuration. Another scenario is that one type of application, such as Captive Portal, would share one whitelist URL configuration, while another group of applications, such as the web proxies, would share another whitelist URL configuration. In this case, you can deploy two shared configuration files, for example, cp_whitelist.xml and wp_whitelist.xml, setting Captive Portal to poll the first file and the web proxies to poll the second file.

Which Configurations Can Be Polled?

The clauses that configure the MBeans of the various modules are located in the application's configuration file. For example, the captiveportal.xml file contains configuration clauses for the Logger MBean, SESM MBean, SSG MBean, Location MBean, and others. Of these, the SSG MBean and the Location MBean have verbose configurations for location awareness, which can be polled.

To use the file poller to update location information, cut and paste the relevant configuration clauses into a separate file, for example, location.xml.

Any XML based configuration in SESM is characterized by three types of clauses—instantiation, configuration, and activation:

- Instantiation clause—Designated by its <Instantiate … /> tag, determines the binding connection between an MBean class and its JMX name, as required by the MBean server. This clause should be invoked only once in an application lifetime during application startup. Therefore the instantiation clause of an MBean should stay in the original application configuration file (for example, in captiveportal.xml). This ensures exactly one registration of this MBean to the MBean server.
- Configuration clause—Designated by its <Configure … /> tag, carries out the module configuration by invoking the setter methods of the appropriate MBean. This is the clause that needs to be polled. You should cut this clause from the application's configuration file (for example, from captiveportal.xml) and paste it into another file (for example, location.xml), which the file poller will poll.
- Activation clause—Designated by its <Action … /> tag, activates methods that were defined in the MBean. If these methods should be invoked automatically each time the configuration has changed, you should add these actions to the polled file along with the configuration clause. However, if these methods are not necessarily interlinked with configuration changes, leave their activation clause in the application configuration file.

Tip To simplify management of the MBeans you want to update, keep the configuration block of each MBean that you want to poll in a separate file (one MBean per file, and one file per MBean).

Important Notes about the File Poller

- Do not update the same MBean using the file poller and Application Manager (or Agent View) simultaneously. The Store operation in Application Manager (and Agent View) removes any call sentence from the configuration block of the MBean.

- Do not poll instantiation clauses. The instantiation clause of any MBean (polled or not) should be in the application's configuration file (for example, captiveportal.xml). This avoids potential problems with the MBean registration and race conditions.
- Do not poll the poller. The instantiation, configuration, and activation blocks of the file poller configuration should be retained in the application configuration file (and not cut out into any polled file). The application's configuration file itself should not be polled.
- Do not split the configuration of a single MBean over several files (including the application configuration file). The file poller will update the configurations correctly, but it would be extremely confusing. In addition, if you use the Store operation on a configuration that is split over several files, it will store the entire configuration in the last file that was polled, which contained a configuration clause of the MBean (although this file may have originally contained only one fragment of the configuration).

  If you use the file poller to update locations configured with IP subnets in the SSG MBean, we recommend that you *do* split up the SSG MBean configuration. You should put only the location configuration clause in the file to be polled, and leave the other configuration clauses in the application configuration file.
- Be aware that different MBeans and attributes might behave differently under dynamic updates. With single value attributes (int, string, and so on), the updated value typically *replaces* the previous value; while with multiple value attributes (map, array, and so on), the new updated values are typically *added* to the list of existing attribute values.

Configuring the File Poller

The file poller configuration is located in the application configuration file of any application that runs the file poller, for example, *captiveportal/config/captiveportal.xml*.

You can configure the application XML file, or you can configure the FilePoller MBean through Agent View or the Application Manager advanced windows.

By default, the file poller configuration in the application configuration file is commented out. To initiate the file poller, uncomment the file poller configuration before you start the application.

You can configure the following:

- Polling Interval—This attribute determines the length of the polling cycle in seconds. The minimum value is 1 minute (60 seconds).
- Polled Files—This attribute contains a list of filenames to be polled, held in a string array.
- Force Polling Now—This method behaves as follows:
  - The first time it is invoked, it initiates the polling cycle.
  - Any subsequent time that the method is invoked, it forces the file poller to poll with no further delay.

The following example sets the initial polling intervals to 1 hour (3600 seconds), lists two files for polling (“/etc/sesm/location.xml” and “/opt/cisco/sesm/captiveportal/config/whitelist.xml”) and finally, invokes the poller by calling the force polling now method.

```
<!-- Instantiation clause of the file poller -->
<Instantiate order="10" class="com.cisco.sesm.jmx.FilePollerMBean"
  jmxname="com.cisco.sesm.jmx:name=FilePoller"/>

<!-- Configuration clause for the polling interval and files -->
<Configure jmxname="com.cisco.sesm.jmx:name=FilePoller">
  <!-- Polling interval (in seconds!) -->
```

```
  <Set name="pollingInterval" type="int">3600</Set>
  <!-- List of files to be polled -->
  <Set name="polledFiles">
    <Array class= "java.lang.String">
      <Item>/etc/sesm/location.xml </Item>
      <Item>/opt/cisco/sesm/captiveportal/config/whitelist.xml </Item>
    </Array>
  </Set>
</Configure>

<!-- Activation clause to initiate poller -->
<Action jmxname="com.cisco.sesm.jmx:name=FilePoller">
  <Call name="forcePollingNow"/>
</Action>
```

Deleting Locations Defined Using IP Subnets

When you use the file poller to update a location configuration that you defined using IP subnets, the new updated values are added to the list of existing attribute values; therefore you must explicitly remove the previous location configuration.

Use the removeNamedSubnetAttributes parameter to remove the previous location configuration. The configuration of removeNamedSubnetAttributes must precede the location definition.

The following example shows the configuration used to update a location defined using IP subnets in the polled file, for example, location.xml. The configuration includes removeNamedSubnetAttributes to remove the previous location definition, and setSubnetAttribute to define the updated configuration.

```
…
<Configure jmxname="com.cisco.sesm:name=SSG">
  …
  <!-- removes previous location configuration from SSGMBean -->
  <call name="removeNamedSubnetAttributes">
    <Arg>SESSION_LOCATION</Arg>
  </call>
  <!-- adds locations to SSGMBean -->
  <Call name="setSubnetAttribute">
    <Arg>110.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg>
    <Arg>london</Arg>
  </Call>
    …
</Configure>
…
```

Deleting Whitelist Configurations Using the File Poller

To delete whitelist configurations using the file poller, change the configuration in the whitelist configuration file, and then update the configuration using the file poller.

- To remove items within a whitelist, remove the entries from the whitelist configuration file, and then update the configuration using the file poller.
- To remove an entire whitelist, remove the entire whitelist configuration from the whitelist configuration file, and then update the configuration using the file poller.

- To remove the entire whitelist configuration, meaning all existing whitelists in the file, change the following section in the whitelist configuration file, and then update the configuration using the file poller.

  Change:

```
<Set name="proxyHostsWhiteLists">
     <New class="java.util.HashMap">
    ......existing whitelist configuration......
      </New>
   </Set>
```

  to

```
<Set name="proxyHostsWhiteLists">
 <New class="java.util.HashMap">
</New>
</Set>
```

Configuring SESM for iPass Support

This chapter provides information about SESM support for iPass users. This chapter contains the following topics:

Overview of SESM iPass Support

SESM support for roaming users enables iPass users to connect to the Internet from public hotspots using their iPass accounts. iPass is a software-enabled virtual network operator (VNO) that provides enterprise connectivity services permitting secure access to information and applications on corporate networks.

SESM enables iPass account holders to:

- Connect to the Internet using the iPass Smart Client—When iPass users connect to the Internet using the iPass Smart Client, the requests are redirected through Captive Portal to NWSP for authentication:
  - Captive Portal identifies the client as an iPass client based on the existence of the iPass identifier ("*iPassConnect*") in the user agent field of the HTTP header.
  - Based on this identification, Captive Portal sends an HTTP redirect to the client, which redirects the client to the NWSP iPass servlet.
  - The NWSP iPass servlets handle the authentication and disconnect flows for iPass clients.

  iPass users can disconnect from the SESM session from the iPass icon in the tray bar.
- Connect to the Internet through a browser—When iPass users try to connect to the Internet through a browser, they are redirected by Captive Portal to the NWSP Login page. iPass users can be recognized by logging on with their iPass username and the iPass prefix. he iPass prefix at the beginning of the username attribute in AAA requests, for example, *IPASS/username@domain,* is used by NWSP and the AAA server to identify the user as a roaming user.

  Note You can customize the NWSP login page, so that iPass users do not need to know of the prefix. See *Cisco Subscriber Edge Services Manager Web Developer Guide* for details.

  iPass users can disconnect by clicking Logout in the NWSP window.

Note

- iPass users do not have access to self-care features or service selection in the SESM web portals.
- Users with HTTP proxy settings in their browsers must first open their browser and be redirected by Captive Portal. After redirection, they can use their iPass account to connect to the Internet. (This workflow is required so that Plug and Play features and SESM iPass support features can be used together.)
- iPass users who want to use free access URLs (open garden or whitelist URLs) before authentication should open a web browser and not the iPass client. The hotspot operator should inform visiting users about the capability of using iPass with open gardens. The Selection Service Gateway (SSG) and SESM cannot notify iPass users about the open garden.
- SESM iPass Smart Client support is limited to a single Generic Interface Specification (GIS) flow, the Proxy Reply flow. For example, the GIS flow, Polling Authentication flow, is not supported.

iPass is supported by any AAA server that recognizes RADIUS requests issued for iPass clients and proxies them to the iPass defined AAA server. The RADIUS requests for iPass clients contain a defined iPass prefix in the username attribute, for example, IPASS/.

Both the SESM RADIUS Data Proxy (RDP) and Cisco Access Registrar (AR) can proxy based on the iPass prefix; hence, both SESM SPE installations and SESM RADIUS installations can support iPass users.

Note

- A Cisco AR extension script is provided to facilitate the iPass support in a SESM RADIUS installation. For details, see Appendix D, "AR Basic Script for iPass Configuration."
- In a SESM SPE installation, iPass is supported through the RDP, and there is no need to install another AAA proxy. The RDP proxies the iPass request to the iPass AAA and proxies all other requests to the SPE LDAP directory.

The AAA server proxies requests to the iPass AAA server for authentication and, after receiving an access-accept, adds the iPass service. This is a vendor-specific attribute (VSA) that authorizes an SSG auto-login service for Internet access.

For authentication requests, you can configure NWSP to provide location information for iPass users by concatenating the location name to the username (Attribute 1), with a defined delimiter that serves as a location separator.

For accounting requests, SSG uses the username and location, which the AAA server uses when proxying accounting messages to the iPass AAA server. Based on GIS, the AAA server uses the RADIUS attribute, called-station-ID (#30) to send the location information to the iPass AAA server.

Note An iPass client might match multiple locations. However, SESM is configured to send the first-match location that is found. The service provider must organize the location definition in such a way that the appropriate location will be the first match.

SESM support for iPass requires configuring:

- Captive Portal.
- NWSP web portal.
- The AAA proxy server (RDP, AR, or other third party AAA server).

Configuring iPass Support

SESM iPass support is disabled by default, and can be enabled if required.

Note When iPass support is enabled, the SSG open garden must not include the iPass client arbitrary URL (this is usually www.yahoo.com).

The following topics describe how to configure iPass support:

- Configuring iPass Support in Captive Portal, page 7-3—Add user-agent based redirection using the CaptivePortal MBean.
- Configuring iPass Support in NWSP, page 7-4—Enable iPass using the SESM MBean and the iPass MBean.
- Configuring iPass Support in RDP, page 7-5—If you are using RDP as the AAA server in a SESM SPE installation, configure the handlers.
- A Cisco AR extension script is provided to facilitate the iPass support in a SESM RADIUS installation, if you are using AR as the AAA server. For details, see Appendix D, "AR Basic Script for iPass Configuration."

Configuring iPass Support in Captive Portal

To configure iPass support in the Captive Portal to identify the iPass client, you must add User-Agent based redirection using the CaptivePortal MBean. Requests from iPass-enabled user-agent software are redirected to the URL served by the SESM application. The list entries for IPASS redirect must always specify redirect to a servlet path ending with "/ipass/redirect".

Step 1 Open the *captiveportal.xml* file from the following location:

```
captiveportal/config/captiveportal.xml
```

Step 2 If required, edit the section for user agent redirection.

The following example shows the default configuration for user agent redirection after installation, where nwsp:8080 is provided during installation. If the values configured by the installation program are correct, no further configuration should be required.

```
<Configure jmxname="com.cisco.sesm:name=captiveportal">
<Set name="agentRedirects">
    <Array class="com.cisco.sesm.jetty.UserAgentRedirect">
    <Item>
        <New class="com.cisco.sesm.jetty.UserAgentRedirect">
        <Set name="agentName" type="String">iPassConnect.*</Set>
        <Set name="redirectUrl" type="String">http://nwsp:8080/ipass/redirect</Set>
        <Set name="instant" type="boolean">true</Set>
        </New>
    </Item>
    </Array>
</Set>
```

* regular expression

Configuring iPass Support in NWSP

Note A Secure Sockets Layer (SSL) certificate signed by a trusted authority must be installed in NWSP for the iPass client. For testing purposes only, you can use self-generated SSL certificates. See Appendix E, "Generating SSL Certificates for Testing" for more information.

To enable iPass in NWSP, configure the following attributes in the SESM MBean and in the iPass MBean in nwsp/config/nwsp.xml:

SESM MBean

- ipassOn—Set to true if iPass functionality is allowed for the NWSP portal. The default value is false.
- ipassProxyIdentity—The prefix to use for login to NWSP. The default is **IPASS/**. This attribute is also used to identify iPass users and assign a different authorization procedure and permissions for them.

Note Although the SESM MBean is used in other applications, these attributes are relevant *only* for the NWSP application.

iPass MBean

- ipassLogonURL—The URL (which must be secure) to post users' principal/credentials. NWSP must provide an SSL certificate signed by a well-known certificate authority to the iPass client before user credentials are posted. This attribute is set automatically during SESM installation.
- ipassLogoffURL—The URL to process user end-session requests. This attribute is set automatically during SESM installation.
- ipassAddLocationToUserName—Set to true to append the user's location to the user credential before authentication. If you are using a RADIUS server different from RDP or CAR, set this parameter to false unless you are sure that the RADIUS server can extract the location from the username in the same way as RDP and CAR.
- ipassLocationSeparator—The character sequence used to delimit the iPass username and domain from the location name. This delimiter must match the delimiter set in the RADIUS server. The default is ###. (Regular expression characters, for example *, ?, and . are not allowed in the ipassLocationSeparator string.)

  Note If you change the location separator, use characters that are not expected to be used in the username. The username should not include the location separator string.

- ipassDefaultLocationName—The location name that is passed to the iPass AAA server if the SESM location service is prohibited, or fails to resolve the user's location.
- ipassDefaultLocationID—The location ID that is passed to the iPass Smart Client XML reply. This attribute was added for iPass's use and is not used by SESM.
- ipassUseSESMLocation—The default value is true, which allows the SESM location service to resolve the user's location. Set to false to use the ipassDefaultLocationName attribute instead.

Step 1 Open the *nwsp.xml* file from the following location:

```
nwsp/config/nwsp.xml
```

Step 2 Edit the iPass MBean section, as required.

The following example shows the configuration for the iPass MBean in NWSP:

```
<Instantiate order="35"
    class="com.cisco.sesm.ipass.IpassMBean"
    jmxname="com.cisco.sesm:name=ipass"/>
       <Configure jmxname="com.cisco.sesm:name=ipass">
               <Set name="ipassLogonURL">https://theportal/ipass/logon</Set>
               <Set name="ipassLogoffURL">http://theportal//ipass/logoff</Set>
               <Set name="ipassAddLocationToUserName" type="boolean">true</Set>
               <Set name="ipassDefaultLocationName">CiscoNatania</Set>
               <Set name="ipassUseSESMLocation" type="boolean">true</Set>
               <Set name="ipassDefaultLocationID">IL</Set>
               <Set name="ipassLocationSeparator">###</Set>
     </Configure>
```

Step 3 Edit the iPassOn and iPassProxyIdentity lines in the SESM MBean section, as required.

The following example shows the configuration of the iPassOn and iPassProxyIdentity lines in the SESM MBean in NWSP:

```
               <Set name="ipassOn" type="boolean">true</Set>
               <Set name="iPassProxyIdentity">IPASS/</Set>
```

Configuring iPass Support in RDP

The configuration of RDP handlers for iPass support are located in rdp.xml:

- RDP MBean—iPass ERP handlers
- Location delimiter
- iPass AAA server IP and Port
- Location Attribute
- iPass Detection (for example, IPASS/)
- iPass Service

Step 1 Open the *rdp.xml* file from the following location:

```
rdp/config/rdp.xml
```

Step 2 Edit the configuration of the iPass Proxy Handler in the RDP MBean, as required.

The following example shows the configuration of iPass Proxy Handler in RDP MBean:

```
<Configure jmxname="com.cisco.sesm:name=RDP,IPASSPROXY=ProxyHandler,
component=RADIUSClientSocket">
    <Set name="throttle" type="int">256</Set>
    <Set name="timeOut" type="int">4000</Set>
    <Set name="maxRetries" type="int">3</Set>
    <Set name="primaryIP">127.0.0.1</Set>
    <Set name="primaryPort" type="int">1816</Set>
    <Set id="IPASSSecret" name="secret">cisco</Set>
    <Set name="secondaryIP">127.0.0.1</Set>
```

```
    <Set name="secondaryPort" type="int">1816</Set>
    <Set name="accountingPortOffset" type="int">1</Set>
</Configure>
```

Step 3 Edit the configuration of the iPass Detection Handler in the RDP MBean, as required.

The following example shows the configuration of iPass Detection Handler in RDP MBean:

```
<Item> <New class="com.cisco.sesm.rdp.IPassDetectionHandler">
    <Set name="name">IPASS</Set>
    <Set name="attribute">USER_NAME</Set>
    <Set name="pattern">IPASS/.*</Set>
    regular expression
    <Set name="noniPassHandler">AAA</Set>
    <Set name="iPassHandler">LOCEXTRACT</Set>
</New> </Item>
<Item><New class="com.cisco.sesm.rdp.LocationExtractionHandler">
    <Set name="name">LOCEXTRACT</Set>
    <Set name="nextHandler">SERVADD</Set>
    <Set name="separator">###</Set>
</New></Item>
<Item> <New class="com.cisco.sesm.rdp.ServiceAddFilter">
    <Set name="name">SERVADD</Set>
    <Set name="nextHandler">IPASSPROXY</Set>
    <Set name="serviceName">iPassService</Set>
    <Set name="serviceUser"></Set>
    <Set name="servicePassword"></Set>
</New></Item>
<Item><New class="com.cisco.sesm.erp.radius.ProxyHandler">
    <Set name="name">IPASSPROXY</Set>
</New></Item>
```

Step 4 Configure the Accounting RADIUS listener to handle iPass requests.

In the last line of the following section of the rdp.xml file, change the handler of the Accounting RADIUS listener from AAA to IPASS:

```
<!-- ACCOUNTING radius Listener -->
<New class="com.cisco.sesm.erp.radius.RADIUSListener">
<Set name="name">ACCOUNTING</Set>
<!-- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ -->
<!-- Set the accounting request handler.  This can be set to:
AAA         - handle the request locally by logging.
PROXY       - proxy the request to another server.
DOMAINPROXY - proxy the request to another server selected
by domain name.
IPASS       - Handle iPass requests                          -->
<!-- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ -->
<Set name="handler">AAA</Set>
```

Step 5 Configure the main RDP handler to handle iPass requests.

In the last line of the following section of the rdp.xml file, change the AAA request handler from AAA to IPASS:

```
<!-- Define and configure the main RDP handler                      -->
<!-- The RDP handler divides handling of AAA and PROFILE requests.  -->
<Item>
<New class="com.cisco.sesm.rdp.RDPHandler">
<Set name="name">RDP</Set>
<!-- Set the name of the AAA request handler
To handle iPass requests, change this to IPASS -->
<Set name="aaaHandler">AAA</Set>
```

CHAPTER 8

Configuring Miscellaneous SESM Features

This chapter describes how to configure the following SESM features:

Quality of Service

Quality of Service (QoS) features control IP traffic transmission rates. You implement QoS features in SESM deployments using SSG hierarchical policing features. See the SSG documentation for information about enabling and configuring hierarchical policing. See Related Documentation, page xiii for the URL to the online location of SSG documents.

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

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

In subscriber or service profiles, the subattribute code Q indicates QOS values. The format is:

QU;*upstream-token-rate*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-token-rate*;*downstream-normal-burst*;[*downstream-excess-burst*]

Profile Examples

In a RADIUS deployment, a subscriber profile in Merit format might include the following QoS attribute values:

```
Account-Info = QU;16000;8000;16000;D;24000;12000;24000
```

A service profile in Merit format might include the following values:

```
Service-Info = QU;16000;8000;16000;D;24000;12000;24000
```

In a SESM SPE installation, use Cisco Distributed Administration Tool (CDAT) to enter the values described above into the Local RADIUS Attributes field of the subscriber or service profile. The format of the Local RADIUS Attributes field is:

attributeName:*value*

For example, in a subscriber profile, enter the following in the Local RADIUS attributes field:

```
Account-Info:QU;16000;8000;16000;D;24000;12000;24000
```

In a service profile, enter the following in the Local RADIUS attributes field:

```
Service-Info:QU;16000;8000;16000;D;24000;12000;24000
```

Configuring Multiple SSGs to work with SESM

The SESM installation program configures communication between SESM applications and a single SSG. This section describes how to configure communication with more than one SSG and how to associate specific SSGs to subscriber subnets. It contains the following topics:

Global and Subnet Configuration Entries in the SSG MBean

SESM uses an SSG MBean to configure communication between the SESM web applications and SSGs. The attributes in the SSG MBean include shared secrets, ports, and IP addresses, and the attributes can also assign specific SSGs to handle requests from specific subscriber subnets.

You can set these attributes globally, by client subnet, or for a specific client IP address, as follows:

- Global attribute elements—A global setting applies to all SSGs. For example, a global shared secret setting means that all SSGs are configured using the same secret. The global attributes are: PORT, SECRET, MASK, and BUNDLE_LENGTH.
- Subnet attribute elements—The subnet attributes apply to a specific subnet and override the global attribute value. The subnet attributes are optional; if any of them are not specifically coded, the global attribute value is used. Subnet attributes that you can supply are: PORT, SECRET, MASK, BUNDLE_LENGTH, and IP. The IP attribute is the IP address of the SSG for a specified subnet.

  You can also specify some optional session information in a subnet entry, using the SESSION_LOCATION and SESSION_BRAND attributes.
- A specific client IP address can be specified in a subnet element.

Note For details of MBeans, see Appendix A, "SESM MBeans."

Subscriber Edge Sessions on SSG

SSG creates and manages per-subscriber sessions, known as edge sessions. SSG creates an edge session when a subscriber logs into SESM. The session ends when the subscriber logs out of SESM or if a timeout occurs. SESM obtains all session status information from SSG.

The SSG edge session provides the following features to SESM deployments:

- Statelessness for SESM web applications—SESM deployers can start and stop SESM web applications without interrupting subscriber activity. Multiple web portals can start up at any time to handle peak loads. Any SESM web portal can handle any request for easy and effective load balancing.

- Session continuity for the subscriber— The edge session remains active if the subscriber closes the browser or points away from the SESM web portal web site.
- Subscriber status information and connection information—The SESM web portal can request session and service status information from the SSG for display to the subscriber.

Multiple SSGs

A typical SESM deployment consists of multiple SSGs. To maintain per-subscriber edge sessions, the same SSG must always handle traffic for the same subscriber. There are two ways to ensure subscriber-to-SSG associations:

- Automatic Associations Using Port-Bundle Host Key Feature
- Manually Mapping Client Subnets to SSGs

Automatic Subscriber-to-SSG Associations

The easiest way to associate a specific SSG with each subscriber is to use the port-bundle host key feature on all SSGs, and configure certain attributes identically on all of the SSG hosts. We recommend using the port-bundle host key feature unless you require backward compatibility with SSD Release 2.5(1).

Note To use the port-bundle host key feature, the SSG device must be running Cisco IOS Release 12.2(2)B or later and the SSG port-bundle host key feature must be configured appropriately.

When the port-bundle host key feature is enabled on an SSG, the SSG replaces the subscriber IP address in the request with a software token (or key) when it forwards the request to SESM. The SESM application uses this key in its responses to SSG, and the SSG does an internal translation to an actual edge session.

The key is a unique combination of an SSG IP address from a range of IP addresses and a port number from a range of port numbers, as follows:

IP_address:*port*

The IP address and port ranges are configured on each SSG. The key uniquely identifies each subscriber currently logged on to SESM, even when multiple subscribers are using the same IP address.

Procedure for Configuring Port-Bundle Host Key on Multiple SSGs

To use the port-bundle host key feature to associate specific SSGs to clients, follow these procedures:

Step 1 Enable and configure the port-bundle host key feature on all of the SSGs, as described in the *Cisco Subscriber Edge Services Manager Installation Guide*.

Step 2 Configure the same values on all of the SSG hosts for the following attributes:

- Port—The SSG port on the SSG host. Specify the port that SSG uses to listen for RADIUS requests from a SESM application. Configure this value on the SSG device using the following command:

  ```
  ssg radius-helper authenticationPort
  ```

- Shared secret—The shared secret used for communication between SSG and a SESM application. Configure this value on the SSG device with the following command:

  ```
  ssg radius-helper key
  ```

- Port bundle length—The number of bits that SSG uses for port bundling when the port-bundle host key feature is enabled. This value must be 0 or 4. Configure this value on the SSG device with the following command

  ```
  ssg port-map length
  ```

Step 3 When the SESM installation program prompts you, enter the globally-configured values in Step 2. These values are saved as global elements in the SSG MBean, as the following example illustrates.

Example SSG MBean for Port-Bundle Host Key

When the port-bundle host key feature is enabled and all of the SSGs use the same port, secret, and port bundle length, the attributes in the SSG MBean are all global settings.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
</Configure>
```

In this example, all SSGs are configured to use a port of 1812 and a shared RADIUS secret of cisco. The BUNDLE_LENGTH of 4 indicates that port-bundle host key is configured on all SSGs.

The MASK attribute specifies the mask that SESM applies to the client (source) IP address in a received message to determine the client's subnet, and, from that, the SSG IP address. However, when a host key is used, the client (source) IP address is the SSG IP address. The SESM installation program provides the default mask of 255.255.255.255.

Example Using Port-bundle Host Key with One Noncomplying SSG

If port-bundle host key is enabled on all SSGs, but some are configured differently, you can configure the global case and then specifically configure exceptions. For example, if all but one SSG is assigned the same shared secret, you can configure the shared secret attribute globally, and then add one subnet entry to configure the different secret for the single SSG.

The installation program lets you provide one set of SSG global attribute values and one subnet entry. It records these attribute values in the <Configure name="SSG"> section of the application MBean configuration file.

In this example, port-bundle host key is enabled on all SSGs. In addition, all SSGs are using the same port, secret, and client IP address mask, except that one SSG uses a different port. In this case, you can set all parameters globally, and then use one subnet entry to define:

- The client subnet being serviced by the SSG that uses the nonconforming port.
- The port value that overrides the globally-set port value.

In this example, the SSG that services subnet 10.1.1.0 uses port 1245.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>PORT
</Arg><Arg>1245</Arg></Call>
</Configure>
```

Manually Mapping Subscriber Subnets to SSGs

This section describes how to manually map SSGs to client subnets in the SSG MBean. Use this procedure if the deployment includes multiple SSGs without the port-bundle host key feature.

Each request arriving at the SESM web portal contains a source, or client, IP address. SESM uses this client IP address to determine which SSG should handle each request.

- If the configuration file explicitly provides an SSG IP address for a subnet or a specific client IP address, SESM uses that SSG. You code an explicit IP address in a <subnet> element. The MASK value in the subnet element specifies whether the element applies to a subnet or to a specific subscriber IP address. The <IP> parameter in the subnet element specifies the SSG IP address.

  For example, the following subnet entry explicitly sets the SSG IP address to 10.6.7.1 for subnet 10.2.0.0:

  ```
  <Call name="setSubnetAttribute">
  <Arg>10.2.0.0</Arg><Arg>255.255.0.0</Arg><Arg>IP</Arg><Arg>10.6.7.1</Arg></Call>
  ```

- If an explicit IP address for the SSG is not provided, SESM masks the subscriber's IP address to determine the SSG that should handle the request.

  Use masking as follows:

  - If port-bundle host key is enabled—The port-bundle host key feature replaces the original client IP address with the IP address of the SSG. (The port bundle key appended to the address preserves a unique identity for each subscriber). Since the client IP address is the SSG IP address, a global setting for MASK of 255.255.255.255 correctly results in the client IP address being used as the SSG IP address. (See Recommended Global or Subnet Mask, page 8-5).
  - If the SSG uses the first IP address in a particular set of client subnets—Specify the mask that the SESM web application can apply to the client IP address to derive the SSG IP address. For example, if, for all 10.x.0.0 client subnets, the SSG IP address is 10.x.0.1, you would specify a subnet of 10.0.0.0 and a mask of 255.0.0.0.
  - If the SSG IP is the first IP in all client subnets—You can set a global value for mask. For example, for all subscriber addresses x.y.z.n, if the SSG always has an IP address of x.y.0.1, then use a global mask of 255.255.0.0.

Recommended Global or Subnet Mask

Set the widest global or subnet mask possible. Each SSG IP address consumes some resources on the machine where the SESM application is running. (Each one uses an open file descriptor.) For example, even when the SSG is using port-bundle host key, a mask of 255.255.255.0 is desirable so that the SESM uses a single SSG IP address rather than 254 different SSG IP addresses. A mask of 255.255.255.255 is the least efficient, but it is the default setup.

Example Mapping Client Subnets to SSGs

In this example, port-bundle host key is not being used. In this case, you must explicitly define the mapping from subscriber subnet to the SSG IP address.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1645</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.1.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.2.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
```

```
</Arg><Arg>10.21.2.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.3.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.3.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.4.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.4.2</Arg></Call>
</Configure>
```

Overriding Buffer Settings

You can change the size of the receive and transmit buffers in RDP. You can also configure the UDP buffer size for communication between a web application and SSG. This applies to all web applications that communicate with SSG via RADIUS.

To change the size of buffers in RDP:

Step 1 Open rdp.xml from the location, <install directory>/rdp/config/rdp.xml.

Step 2 Update rdp.xml by adding the following lines:

```
<Set name="recvBufSize" type="int">4096</Set>
<Set name="sendBufSize" type="int">4096</Set>
```

The following example shows the Auth listener section of the rdp.xml file:

```
<!-- ========================================================= -->
<!-- Configuration for the AUTH radius listener socket -->
<Configure
jmxname="com.cisco.sesm:name=RDP,RADIUSListener=AUTH,component=RADIUSServerSocket">
<Set id="RDPSecret" name="secret">cisco</Set>
<Set name="localIP">0.0.0.0</Set>
<Set name="localPort" type="int"><SystemProperty name="application.portno"
default="1812"/></Set>
<!-- new lines -->
<!-- Desired size of socket receive buffer.
0 = use system default. -->
<Set name="recvBufSize" type="int">4096</Set>
<!-- Desired size of socket transmit buffer.
0 = use system default. -->
<Set name="sendBufSize" type="int">4096</Set>
```

The following example shows the Accounting listener section of the rdp.xml file:

```
<!-- ========================================================= -->
<!-- Configuration for the Accounting radius listener Socket -->
<Configure
jmxname="com.cisco.sesm:name=RDP,RADIUSListener=ACCOUNTING,component=RADIUSServerSocket">
<Set name="secret">cisco</Set>
<Set name="localIP">0.0.0.0</Set>
<Set name="localPort" type="int"><SystemProperty name="accounting.portno"
default="1813"/></Set>
<!-- new lines -->
<!-- Desired size of socket receive buffer.
0 = use system default. -->
<Set name="recvBufSize" type="int">4096</Set>
<!-- Desired size of socket transmit buffer.
0 = use system default. -->
<Set name="sendBufSize" type="int">4096</Set>
```

Important Notes

- If the RDP is set to send proxy requests to another RADIUS server, you can also configure the buffers of the client socket to the RADIUS server as above. Here is an example:

```
<!-- start of RDP acme Proxy Socket configuration
<Configure
jmxname="com.cisco.sesm:name=RDP,acme_PROXY=ProxyHandler,component=RADIUSClientSocket"
>
<Set name="throttle" type="int">256</Set>
<Set name="timeOut" type="int">4000</Set>
<Set name="maxRetries" type="int">3</Set>
<Set name="primaryIP">127.0.0.1</Set>
<Set name="primaryPort" type="int">1812</Set>
<Set name="secret">cisco</Set>
<Set name="secondaryIP">127.0.0.2</Set>
<Set name="secondaryPort" type="int">1812</Set>
<Set name="accountingPortOffset" type="int">1</Set>
<!-- new lines -->
<!-- Desired size of socket receive buffer.
0 = use system default. -->
<Set name="recvBufSize" type="int">32767</Set>
<!-- Desired size of socket transmit buffer.
0 = use system default. -->
<Set name="sendBufSize" type="int">32767</Set>
```

- Other RDP type applications, such as AAA server, and SSG Simulator, also use the RADIUS jar file in libs/radius. If you plan to use such applications, you should add all the changes made to the rdp.xml file to the individual configuration files of the RDP type applications.
- You can use Agent View to change the buffer size while RDP is running. However, there is a known problem with this. Changing a socket setting while the socket is active causes Agent View to freeze until that socket receives a RADIUS packet. This should not be a problem on a live system where the socket is actively dealing with a reasonable volume of requests. However, in a less active system it might be better to change the configuration file manually and restart the application.
- The buffer size setting is actually a request to the operating system. If the requested size lies outside the range of permissible values for the operating system, it does not set the buffer to the size you requested. In the case of RDP sockets and AAA server sockets, you can view the actual buffer size of the socket MBean in Agent View or AM. However, for SSG communication, the SSG socket does not have an MBean. To see the actual buffer size, go to the SSG MBean and select View the values of statistics link for the statistics attribute. This will show you the statistics for all the currently existing SSG sockets. Included are values for the actual receive and send buffer sizes.

To override the buffer settings in a web application:

Step 1 Open the configuration file for the web application located in <install directory>/<application name>/config/<application name>.xml. For example, for the NWSP application, the configuration file would be <install directory>/nwsp/config/nwsp.xml.

Step 2 Find the following line in the config file (inside the SSG MBean):

```
<Call name="setGlobalAttribute"><Arg>THROTTLE</Arg><Arg>20</Arg></Call>
```

Add the following two lines below it:

```
<Call name="setGlobalAttribute"><Arg>RX_BUF_SIZE</Arg><Arg>4096</Arg></Call>
<Call name="setGlobalAttribute"><Arg>TX_BUF_SIZE</Arg><Arg>4096</Arg></Call>
```

You can increase the buffer size (4096) in these lines for the receive and transmit buffers. The recommended size is 32767.

Note The default buffer size after installation is 4096. If this value is overridden with the value 0, the operating system default size is used.

Step 3 Save the configuration file and restart the application.

Note You cannot change the buffer size dynamically on a web application. After you save the configuration, the configuration changes will take effect when the application is restarted.

On Linux systems, the default buffer size is available in the following files:

```
/proc/sys/net/core/rmem_default - default receive window
/proc/sys/net/core/rmem_max - maximum receive window
/proc/sys/net/core/wmem_default - default send window
/proc/sys/net/core/wmem_max - maximum send window
```

On UNIX systems, you can run the following commands to get the default buffer size:

```
ndd /dev/udp udp_recv_hiwat - maximum receive buffer size
ndd /dev/udp udp_xmit_hiwat - Maximum transmit buffer size
```

Note These commands might vary based on the operating system.

To avoid packet loss, increase the receive buffer size to 32767 bytes using one of the following:

- The following line in rdp.xml:

```
<Set name="recvBufSize" type="int">32767</Set>
```

- The following lines in a web application configuration file:

```
<Call name="setGlobalAttribute"><Arg>RX_BUF_SIZE</Arg><Arg>32767</Arg></Call>
<Call name="setGlobalAttribute"><Arg>TX_BUF_SIZE</Arg><Arg>32767</Arg></Call>
```

If you experience packet loss at this setting, increase the buffer size. You can increase it to 65535.

Running SESM Components

This chapter provides information on how to run the Cisco Subscriber Edge Services Manager (SESM) components once they have been installed. The chapter contains the following topics:

Starting SESM Components

To start SESM applications, start an application-specific script, which calls a generic script:

Table 9-1 describes the names and locations of SESM application-specific start scripts.

Table 9-1 SESM Application-Specific Start Scripts

SESM Application	Location	Start Script
Web applications	/jetty/bin	jetty bin startNWSP startWAP startPDA startSP startCAPTIVEPORTAL startMESSAGEPORTAL startCDAT startWSG startAPPMGMT[1] startWebProxy
RDP	/rdp/bin	rdp bin runrdp

Table 9-1 SESM Application-Specific Start Scripts (continued)

SESM Application	Location	Start Script
WSGClient[2]	/wsg/bin	wsg bin wsgClient
Bundled RADIUS servers	/tools/bin	tools bin startAAA startProxy

1. Before you run Application Manager, you must start the RMI Registry (rmiregistry) on each of the SESM application host systems. See Starting Application Manager, page 10-2 for details.
2. WSGclient is provided as a demonstration tool and not as a client for production.

Start Scripts for SESM Web Applications

This section describes the start scripts for SESM web applications:

All the scripts for SESM web applications are located in:

```
jetty
    bin
```

To create start scripts for customized SESM web applications, create an application-specific start script for each new application in this bin directory.

Application-Specific Start Scripts

The application-specific start scripts set the following application-specific variables and call the generic script:

- Application name—Identifies the application name. The generic start script derives path names for configuration files and the docroot subdirectory from the application name. Some applications configure specific settings based on the application name. If you create a customized application, provide the name that identifies your application.
- Port number—Identifies the port that the application's container (the web server) will listen on.

  The installation program updates the application start script with the port number that you provide during installation. To change the port number after installation, edit the start script.

  The port number must be unique on the server. If multiple SESM web applications are running simultaneously on the same server, make sure each one listens on a different port. This caveat applies whether you are running two instances of the same application or two different applications.

Generic Start Script

The generic start script does the following:

- Accepts the variables passed to it from the application start script.
- Sets additional variables, based on the expected (installed) directory structure. For example, it infers the location of the configuration files.
- Checks for a valid Java Virtual Machine (JVM) version and issues appropriate error messages if it finds an incompatible version for the application you want to start. The SESM installation program creates and sets a JDK_HOME variable. The start script checks the version of the JVM that resides in the referenced JDK_HOME variable. If you installed a new Java Runtime Environment (JRE) or Java Development Kit (JDK) after you installed SESM, you can edit the start script to change the value of JDK_HOME. For required JVM versions for the SESM applications, see the prerequisites section in the *Cisco Subscriber Edge Services Manager Installation Guide*.
- Starts a Jetty server instance, which uses configuration attributes in the container MBean configuration file to add applications to run in the container.
- Derives a management console port number as follows:

  ```
  application port + 100
  ```

  For example, if you are using the default application port of 8080 for NWSP, the management console port for NWSP is:

  ```
  8080 + 100 = 8180
  ```

  Note The management console port is used if the application uses the ManagementConsole MBean, which configures the Agent View management tool.

- Derives a secure sockets layer (SSL) port as follows:

  ```
  application port - 80 + 443
  ```

  Starting with the default application port value of 8080, the default SSL port is:

  ```
  8080 - 80 + 433 = 8443
  ```

SystemProperty and Property Assignments in the Start Script

The SESM generic start script assigns values to attributes that are defined with <SystemProperty> and <Property> tags in the installed configuration files. The D option to the Java command makes the assignments, as shown in the following lines from the end of the generic start script:

```
$JAVA $SERVER -Xms64m -Xmx64m \
    -classpath $CLASSPATH \
    -Dinstall.root=$INSTALLDIR \
    -Djetty.home=$JETTYDIR \
    -Dapplication.home=$APPDIR \
    -Dapplication.portno=$PORTNO \
    -Dapplication.ssl.portno=$SSLPORTNO \
    -Dmanagement.portno=$MGMTPORTNO \
```

Table 9-2 describes the properties and how their assigned values are derived.

If a value is not specified by either method at run time, the application uses a default value specified in the MBean configuration file, in the <SystemProperty> or <Property> tag.

Table 9-2 Java System Properties in Start Scripts

System Property and Variable Name	Explanation
jetty.home=$JETTYDIR	jetty.home is the container's directory name. The start script sets $JETTYDIR to the value jetty under the installation directory.
application.home=$APPDIR	application.home is the application's directory name. The start script sets $APPDIR to *applicationName* under the installation directory. The *applicationName* parameter is passed from the application specific start script (for example, startNWSP.sh).
application.portno=$PORTNO	application.portno is the port that the web server listens on for HTTP requests from subscribers. The start script sets $PORTNO to the portNo parameter passed from the application specific start script (for example, startNWSP.sh). $PORTNO is specified during installation. The default is 8080 for the NWSP, WAP, and PDA portal applications. The default is 8081 for CDAT.
application.ssl.portno=$SSLPORTNO	application.ssl.portno is the port that the web server listens on for secure HTTPS requests from subscribers. The start script sets $SSLPORTNO to $PORTNO - 80 + 443.
management.portno=$MGMTPORTNO	management.portno is the console port that displays the current values for all attributes in all of the MBean configuration files. The start script sets $MGMTPORTNO to $PORTNO + 100.

You can specify the value of a property as follows:

- You can specify a value in the start script using the -D option to the java command. For example, the above lines from the installed start script (START.sh or START.cmd) assign values to some properties.
- You can specify a property value on the command line at run time using the -jvm option. The command line value overrides all other values for that property. The -D argument to the java command defines the value of a property.

  For example, you can use the following -jvm option in the command line to run the application in debug mode in a development environment.

```
startNWSP.sh -jvm -Djavac.debug=true
```

Note It is not recommended to use the -jvm option in the command line to set application port numbers.

Determining a JVM at Application Startup

The start scripts determine a JVM for their applications as follows:

- The scripts check for a JDK_HOME environment variable on the system and use the system value if it exists.
- If a JDK_HOME variable is not set on the system, the scripts use the JDK_HOME value set inside the script by the installation program. This value points either to the SESM bundled JRE or the location provided by the user at installation time.
- On Solaris and Linux, the start scripts check the version of the referenced JVM and issue error messages if the version is not supported by the current SESM release.

If you install a JRE or JDK in a different location after running the SESM installation program, you can do one of the following:

- Set a JDK_HOME environment variable on your system. The system environment variable takes precedence over the one in the SESM start scripts.
- Edit the following two scripts:
  - Generic start script—This common script is used for most SESM applications. The location of this script is:

    ```
    jetty
       bin
          start
    ```

  - RDP start script—Because RDP is not a web application, it has its own start script:

    ```
    rdp
       bin
          runrdp
    ```

- Explicitly specify the JVM to use on the command line at startup.

  You can explicitly specify the location of a preinstalled JDK or JRE by starting the installation on a command line and specifying the javahome parameter, as follows:

  ```
  installImageName -is:javahome location
  ```

  Where:

  installImageName is the name of the downloaded SESM image.

  location is the path name for the JRE or JDK directory. For example, /usr/java1.4.2

Stopping SESM Applications

The following topics describe how to stop SESM applications on Solaris, Linux, and Windows platforms:

- Stopping SESM Applications on Solaris and Linux, page 9-6
- Stopping SESM Web Applications on Windows, page 9-6
- Adding and Removing Services on Windows, page 9-6

Stopping SESM Applications on Solaris and Linux

To stop SESM applications on Solaris and Linux, run the stop scripts listed in Table 9-3. These scripts do not accept arguments.

Table 9-3 SESM Stop Scripts on the Solaris and Linux Platforms

Application	Stop Script Path Names (Solaris and Linux platforms only)
SESM web applications	jetty/bin/stopNWSP.sh jetty/bin/stopWAP.sh jetty/bin/stopPDA.sh jetty/bin/stopSP.sh jetty/bin/stopCDAT.sh jetty/bin/stopWSG.sh jetty/bin/stopWebProxy.sh jetty/bin/stopCAPTIVEPORTAL.sh jetty/bin/stopMESSAGEPORTAL.sh jetty/bin/stopAPPMGMT.sh[1]
RDP	rdp/bin/stoprdp.sh
Bundled RADIUS servers	tools/bin/stopAAA.sh tools/bin/stopProxy.sh

1. To stop the RMI Registry (rmiregistry) on each of the SESM application host systems, after you stop Application Manager run the stoprmiregistry.sh script.

Stopping SESM Web Applications on Windows

To stop SESM web applications and their J2EE containers on Windows platforms, you can:

- Open the Task Manager window, select the appropriate task, and click **End Task**. If you are prompted again, click **End Now**.
- If you added the application as an NT service, you can use the Services window to stop the service. Select **Control Panel > Services** or **Control Panel > Administrative Tools > Services** and select the service you want to stop. Use the menu commands in the Services window to stop the selected service.

Adding and Removing Services on Windows

On a Windows platform, you can add your applications to the list of Windows services. When the application is a service, it appears in the Services window accessed from the control panel. You can start and stop any service from this window. Also, you can optionally configure a service to start automatically when you reboot the system.

The SESM installation program provides service scripts with the web portals, CDAT, Application Manager, and RDP applications. The command syntax is the same for all of the service scripts:

- *scriptName* `-i` installs the application as a service so that it can be managed from the Services window
- *scriptName* `-h` displays the command usage
- *scriptName* `-r` removes the application from the Services window

Table 9-4 lists the names and locations of the scripts that add and remove services.

Table 9-4 Scripts for Adding and Removing Services on Windows

Services Script Location and Name	Default Service Name
jetty\bin\nwspsvc.cmd	NWSP Web Application
jetty\bin\wapsvc.cmd	WAP Web Application
jetty\bin\pdasvc.cmd	PDA Web Application
jetty\bin\spsvc.cmd	SP Web Application
jetty\bin\captiveportalsvc.cmd	Captive Portal Web Application
jetty\bin\appmgmtsvc.cmd	Application Manager
jetty\bin\cdatsvc.cmd	CDAT Application
rdp\bin\rdpsvc.cmd	RDP Application

Service Dependencies

If you select the automatic startup option for SESM applications, make sure the dependencies are set correctly.

- On each system that is hosting SESM applications, the RMI Registry must start before the SESM applications.
- The Application Manager, which might or might not be on the same system as other SESM applications, can start before or after the applications it manages. The Application Manager picks up newly started applications whenever you display a new window or refresh the current window, if the configuration files include the newly started application.

CHAPTER 10

Using Application Manager

This chapter provides information on how to use the SESM Application Manager (AM). The chapter includes the following topics:

About SESM Application Manager

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

Note AM uses applets; hence the client machine requires Java Virtual Machine (JVM) to run AM.

The Application Manager can perform the following management tasks:

- Change configuration values for running applications.
- Persist the changes across application restarts.
- View status and metrics for running applications.
- Perform operations on running applications, such as freeing memory in SESM web portals.

Note You cannot clear MBean attributes in AM or in Agent View. To clear an attribute's values, you must configure the appropriate application XML file, and restart the application.

Two types of management windows are available:

- Operational Scenarios—These windows offer convenient access to the subset of attributes that are most likely to require changes during production deployments.

  The scenarios present matrixes of attribute settings by application, enabling administrators to easily compare and change the settings for the same attribute for multiple applications of the same type.

- Advanced Windows—These windows provide access to all attributes in all MBeans used by an application. They include the read-only attributes that provide status and metrics for running applications.

Note You can also update location and whitelist configurations using the SESM file poller. For information about the file poller, see Chapter 6, "Configuring Location Awareness and Whitelist URLs."

Running the Application Manager

This section describes how to start and run the Subscriber Edge Services Manager (SESM) Application Manager. Topics are:

Note On a Windows platform, you can add SESM applications to the list of Windows services. You can start and stop any service in the Services window accessed from the control panel. For more information, see Adding and Removing Services on Windows, page 9-6.

Starting Application Manager

Use the following procedure to start the Application Manager:

Step 1 On each of the SESM application host systems, make sure that the RMI Registry (rmiregistry) is running.

If the rmiregistry process is not running, you can start it with the following script in the SESM installation directory:

```
jetty
    bin
        runrmiregistry
```

Once started, the RMI Registry usually runs continuously until the system reboots.

Step 2 Start the SESM applications on each host system.

Note Applications register with the RMI registry at application startup. The RMI Registry must be running on the system before you start the SESM applications on that system.

Step 3 Start the Application Manager. The startup script is in the SESM installation directory with other SESM web application startup scripts:

```
jetty
    bin
        startAPPMGMT
```

Step 4 Open a web browser.

Step 5 Navigate to the Application Management URL. You can either:

a. Click the Application Management link on the CDAT main page, or

b. Enter the Application Management URL in the browser. For example:

http://localhost:8082

The URL is:

```
http://hostName:portNo
```

Where:

hostName is the IP address or host name of the system where the Application Manager is running

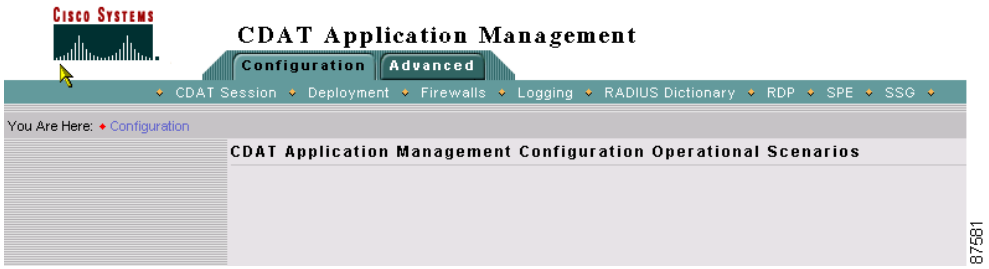
portNo is the Application Management port, specified in the startAPPMGMT startup script.

The Application Management logon page appears.

Step 6 Log in using a valid username and password.

The Application Management main window appears. See Figure 10-1.

Figure 10-1 Application Management Main Window



The tabs at the top of the window control the type of management you can perform.

- Configuration Tab (selected by default)—Accesses the SESM operational scenarios. To enter an operational scenario, click one of the menu items on the second line of the window. For more information, see "Using the Application Manager Advanced Windows" section on page 10-5
- Advanced Tab—Accesses the MBean details for individual applications. For more information, see "Using the Application Manager Advanced Windows" section on page 10-5

Troubleshooting Application Manager Startup

If the main window does not appear:

- Check the Application Manager URL. Make sure the port number in the URL matches the port number used at startup. The startAPPMGMT script sets the port number. ‘
- Check the Application Manager logs in:

```
appmgmt
    logs
```

If applications that you have configured for management do not appear in the operational scenarios, check the following:

- Make sure the RMI Registry is running on the systems that are hosting the SESM applications. See Starting Application Manager, page 10-2 for a description of the rmiregistry script and what it does.
- Make sure the RMI Registry is running before you start the SESM applications that you want to manage.
- Mare sure that the RMI Registry port is correctly specified in the RMIURL attribute in the AdapterFactoryInit.xml file. The default port used by the rmiregistry startup script is 1099. For example:

```
<RMIURL>rmi://server1-w2k01:1099</RMIURL>
```

- Make sure the CLASSPATH environment variable contains the correct path name to the installDir/redist/mx4j/lib/mx4j-tools.jar file in the SESM installation directory. You must change the CLASSPATH variable if you reinstall the product into a different directory. If you have to change the CLASSPATH value, stop and restart the rmiregistry process.
- Make sure the JNDIName attributes in the application rmi.xml files specify a unique names for each application running on a system.

Note The RDP application does not use a separate rmi.xml file. The JNDIName attribute is in the rdp.xml file.

- Make sure the JNDIName attribute values in the application rmi.xml files match the JNDIName attribute values in the AdapterFactoryInit.xml file. The relevant path names are:

```
nwsp (or other application name)
    config
       rmi.xml
appmgmt
    config
       AdapterFactoryInit.xml
```

For example, the following line is extracted from nwsp/config/rmi.xml:

```
<Set name="JNDIName" type="String">webapp_server1-w2k01_8080</Set>
    </Configure>
```

The following lines are extracted from appmgmt/config/AdapterFactoryInit.xml:

```
<AdapterMapping name="webapp_server1-w2k01_8080">
    <Protocol>rmi</Protocol>
    <JNDIName>webapp_server1-w2k01_8080</JNDIName>
    <RMIURL>rmi://server1-w2k01:1099</RMIURL>
</AdapterMapping>
```

Note The name attribute specifies the name displayed in the Application Manager window. It does not have to match the JNDIName, but matching names aids debugging.

Stopping the Application Manager

To stop the Application Manager on Solaris and Linux, run the following script. The script does not accept arguments.

```
jetty/bin/stopAPPMGMT.sh
```

To stop the Application Manager on Windows:

- Open the Task Manager window, select the appropriate task, and click the **End Task** button. If you are prompted again, click the **End Now** button.
- If you added the application as an NT service, you can use the Services window to stop the service. Open **Control Panel > Services** or **Control Panel > Administrative Tools > Services** and select the service you want to stop. Use the menu commands on the Services window to stop the selected service.

Using the Application Manager Advanced Windows

This section describes how to use the Cisco Subscriber Edge Services Manager (SESM) Application Manager Advanced windows. This section contains the following topics:

Introduction

The Application Manager advanced windows display the current value of any attribute in any MBean in the managed applications. The advanced windows display each application separately.

Use the advanced windows to:

- Check the status of managed applications
- Connect to applications that were started after the Application Manager was started
- Connect to applications that were previously unmanageable, but are now available for management
- Change attributes that are not included on the operational scenarios
- View monitoring (read-only) attribute values

The Application Manager advanced windows present an interface very similar to the Agent View remote management tool.

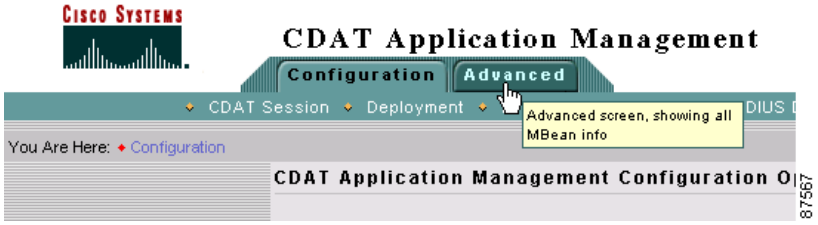
Note Some types of configuration parameters cannot be updated by Advanced windows, for example, Array types.

Accessing the Advanced Windows

To access the advanced window for an application:

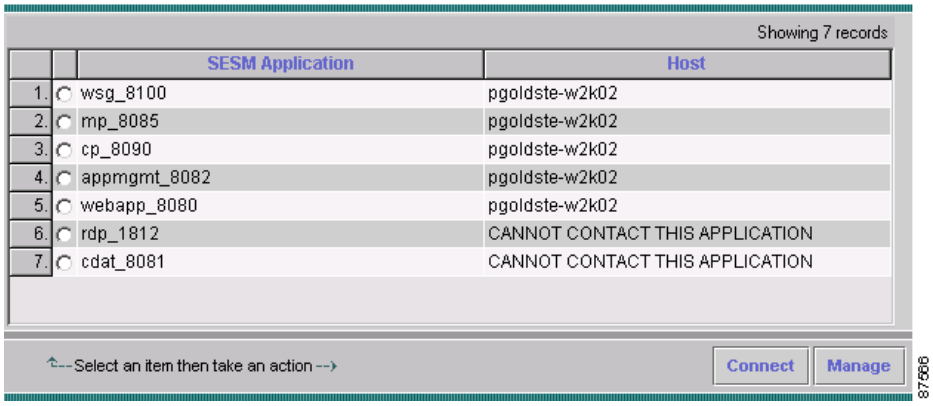
Step 1 Click the Advanced tab on the top line of the SESM Application Manager window. (See Figure 10-2.)

Figure 10-2 Advanced Tab



The next window shows all of the applications that are listed in the AdapterFactoryInit.xml file in the Application Manager's config directory. (See Figure 10-3.)

Figure 10-3 Advanced Window



From this window, you can:

- Determine whether applications are currently manageable.
  - If the host name is listed, the application is currently running and manageable.
  - If the host name is not listed, one of the following conditions exists:

    The application is not running.

    The RMI Registry on the application's host system is not running or was started after the application was started.

    The application was started after the Application Manager was started. In this case, click the Connect button to attempt to connect to the application.

    The application is not properly configured for management. See the "Troubleshooting Application Manager Startup" section on page 10-4 for help.
- Connect to applications that have recently become manageable.
- Manage the application.

Step 2 To connect or manage an application:

- Click the radio button next to an application name to select that application
- Click the Connect or Manage button.
  - If you click Connect, and the connection fails, review the reasons listed in Step 1.
  - If you click Manage, the resulting window shows all of the domains in the application and the MBeans in each domain. See Figure 10-4.

Figure 10-4 Advanced Window List of MBeans

Step 3 Scroll down on the page until you find the MBean whose attributes you want to view.

Step 4 Click the MBean that you want to examine. The MBean names (in the left column) are hypertext links to the MBean details.

The resulting window shows the attributes and operations in the MBean. See Figures 10-5 and 10-6.

Figure 10-5 Directory MBean (1 of 2)

MBean Description

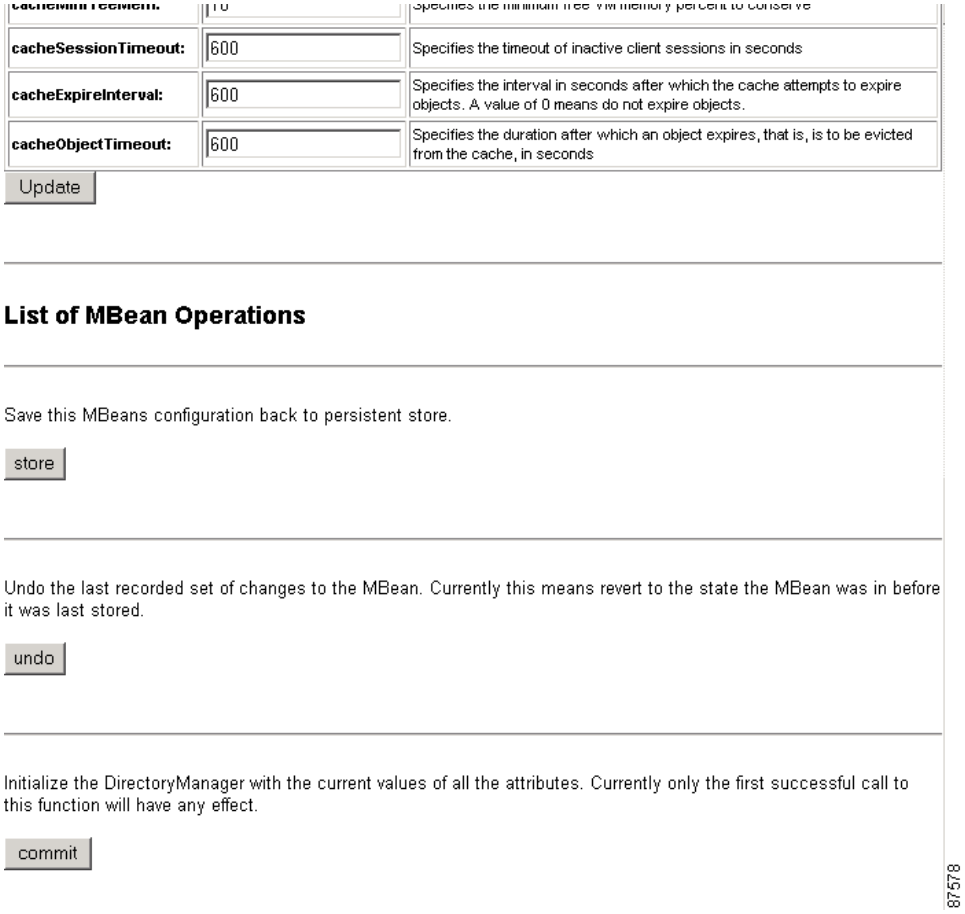
com.cisco.sesm.dessauth.DirectoryMBean

List of MBean Attributes

Property	Value	Description
connectionNameRoot:	com.cisco.sesm:name=	The root name for all of the connection MBeans
DESSPrincipal:	cn=admin,ou=sesm,o=c	The principal used by DESS to perform operations. Must be known to RBAC.
factory:	com.cisco.cns.security.	The full classname of the JNDI connection factory
context:	ou=sesm,o=cisco	The default LDAP context used for LDAP operations
alwaysGetAllAttributes:	false	If set to true then all the attributes of an LDAP entry are returned for every query
traceLevel:	NONE	Should be one of: NONE, ERROR, BRIEF, VERBOSE or DEBUG
traceFileName:	nwsp/logs/dess.log	The name of the Directory log file
printTraceToConsole:	false	If set to true then echo trace messages to the console as well as writing them into the log file.
stackTrace:	false	If set to true, print a stack trace with each trace message.
cacheMaxObjects:	50000	Specifies the max number of objects to hold in the cache
cacheMinFreeMem:	10	Specifies the minimum free VM memory percent to conserve
cacheSessionTimeout:	600	Specifies the timeout of inactive client sessions in seconds

87577

Figure 10-6 Directory MBean (2 of 2)



Step 5 To edit an attribute, click on the attribute value and make the change.

Step 6 To make the change take effect on the running application, click Update.

Step 7 To make the change persist across restarts, click Store. You must click Update the current application before storing the change.

Buttons on the MBean Windows

The buttons on the MBean windows represent methods defined for the class that you are viewing. You can click any button to dynamically call the method and perform the operation on the running application.

- Update—Sends the attribute changes to the running application. The change takes effect immediately on the running application unless you receive an error message stating otherwise.
- Store—Saves the attribute changes in the appropriate configuration file (for example, nwsp.xml). This action persists the changes for future application restarts. The Store button has the following effects on the MBean in the configuration file:
  - Deletes any <SystemProperty> or <Property> tags used in the MBean in the originally-installed configuration file. The Store button saves the currently defined value of all attributes in the MBean, regardless of how those values were derived. The Store operation is not aware of property definitions or values assigned by the startup script.
  - Deletes comments in the MBean.
  - Includes all read-write attributes in the MBean, whereas the installed configuration files might include only the most commonly changed attributes.
  - Deletes a <Call> tag inside a <Configure> tag. If the <Call> element sets an attribute value, the rewritten MBean contains the attribute assignment performed in a different way. However, if the <Call> element is performing an action other than setting an attribute value, the action is lost. The correct way to call methods is to use the <Action> tag
- Undo—Reverts the running application to the state before the last store. You can undo only the last stored action. The Undo operation applies to the running application only. To persist an undo, you must save the Undo action to the configuration files by clicking **Store** after clicking **Undo**. You can reverse a stored undo, if it is the last stored action.
- Additional operations—Some MBeans have additional buttons. In most cases, the buttons represent specialized update methods for an array or mapping element. You can use these buttons to update elements.

Logging and Debugging in SESM Applications

This section describes how to configure the logging and debugging mechanisms for Cisco Subscriber Edge Services Manager (SESM) applications and the Jetty server. Topics are:

Log File Descriptions

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

- Jetty log—Contains logging and debugging messages from Jetty. The logging messages record the startup of the Jetty server and all ongoing activity, such as errors trapped by the Jetty server and HTTP errors. If the SESM application fails to start, look at this log. Make sure you monitor this log file for illegal HTTP requests that might indicate attempts to subvert the web server. If you enable debugging, the log file also includes more detailed debugging messages.
- Jetty HTTP Request log—Contains incoming HTTP requests. You can use this log file to analyze volume and traffic patterns for the web server.
- Application log—Contains logging and debugging messages from the SESM application. The logging tool logs SESM web application activity. The debugging mechanism produces messages useful to developers in debugging applications.

You can configure all three of these logs for the SESM web portal applications, DNS Proxy, and CDAT. RDP uses only the application log.

MBeans for Log File Configuration

Table 10-1 shows the MBeans that configure the log files. The MBeans control the level of verbosity in the logs, message filtering, debugging, file location, and file management.

Table 10-1 Configuring the Log Files

Process	Log Type	MBean Name and Reference to More Information	Attribute that Specifies File Path Name	Default Log Filename
Jetty Server	Jetty log	name=Log, page A-52 Debug=0, page A-52	filename	*date*.jetty.log
	Request log	name=Jetty,Server=0,, page A-54	RequestLog	*date*.request.log
SESM Application	Application log	name=Logger, page A-23	logFile	*date*.application.log

To change the location of a log file, change the value of the attribute listed in Table 10-1. The installed default value for the file path name attributes is the application.home property. The value for the application.home property is set by the start script at run time.

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

```
SESMinstallDir
    nwsp
        logs
```

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

SESM MBeans

This appendix provides information on the MBeans used to configure SESM. This appendix contains the following topics:

Guide to MBeans Used for Configuring SESM

Table A-1 lists the MBeans used for configuring the following SESM applications:

Note For details of the MBeans and their associated attributes listed in this section, see SESM MBeans and Their Attributes, page A-6.

Table A-1 SESM Applications and Associated Configuration MBeans

SESM Application	Domain	Associated MBeans used for configuring this application
Application Manager	com.cisco.sesm	agent=configuration, page A-7 name=Login, page A-23 name=Logger, page A-23 name=ManagementConsole, page A-26
	org.mortbay.jetty	Debug=0, page A-52 name=Log, page A-52 name=Jetty,NCSARequestLog=0,Server=0, page A-53 name=Log,OutputStreamLogSink=0, page A-54 name=Jetty,Server=0,, page A-54 name=Jetty,Server=0,WebApplicationContext=0, context=/, page A-56 name=jetty,SESMSSLListener=0,Server=0, page A-57 name=Jetty,SESMSocketListener=0, Server=0, page A-58
Captive Portal	com.cisco.sesm	agent=configuration, page A-7 name=captiveportal, page A-7 name=Directory, page A-13 name=Directory,type=Connection,instance=Primary, page A-14 name=Directory,type=Connection,instance=Secondary, page A-15 name=Extension, page A-19 name=ExtensionSpecification, page A-18 name=firewall, page A-20 name=Location, page A-25 name=Logger, page A-23 name=ManagementConsole, page A-26 name=SESM, page A-46 name=SSG, page A-43 name=Version, page A-49 name=WebApp, page A-49
	org.mortbay.jetty	Debug=0, page A-52 name=Log, page A-52 name=Jetty,NCSARequestLog=0,Server=0, page A-53 name=Log,OutputStreamLogSink=0, page A-54 name=jetty,SESMSSLListener=0,Server=0, page A-57 name=Jetty,SESMSocketListener=0, Server=0, page A-58 name=Jetty,Server=0,, page A-54 name=Jetty,Server=0,WebApplicationContext=0, context=/, page A-56

Table A-1 SESM Applications and Associated Configuration MBeans (continued)

SESM Application	Domain	Associated MBeans used for configuring this application
Web Services Gateway	com.cisco.sesm	agent=configuration, page A-7 name=Directory, page A-13 name=Directory,type=Connection,instance=Primary, page A-14 name=Directory,type=Connection,instance=Secondary, page A-15 name=Extension, page A-19 name=ExtensionSpecification, page A-18 name=firewall, page A-20 name=Location, page A-25 name=Logger, page A-23 name=ManagementConsole, page A-26 name=SESM, page A-46 name=SSG, page A-43 name=Version, page A-49 name=WebApp, page A-49
	org.mortbay.jetty	Debug=0, page A-52 name=Log, page A-52 name=Jetty,NCSARequestLog=0,Server=0, page A-53 name=Log,OutputStreamLogSink=0, page A-54 name=Jetty,Server=0,, page A-54 name=Jetty,Server=0,WebApplicationContext=0, context=/, page A-56 name=jetty,SESMSSLListener=0,Server=0, page A-57
Message Portal	com.cisco.sesm	agent=configuration, page A-7 name=Directory, page A-13 name=Directory,type=Connection,instance=Primary, page A-14 name=Directory,type=Connection,instance=Secondary, page A-15 name=firewall, page A-20 name=Location, page A-25 name=Logger, page A-23 name=ManagementConsole, page A-26 name=messageportal, page A-26 name=SESM, page A-46 name=Version, page A-49
	org.mortbay.jetty	Debug=0, page A-52 name=Log, page A-52 name=Jetty,NCSARequestLog=0,Server=0, page A-53 name=Log,OutputStreamLogSink=0, page A-54 name=Jetty,Server=0,, page A-54 name=Jetty,Server=0,WebApplicationContext=0, context=/, page A-56 name=Jetty,SESMSocketListener=0, Server=0, page A-58

Table A-1 SESM Applications and Associated Configuration MBeans (continued)

SESM Application	Domain	Associated MBeans used for configuring this application
NWSP Portal	com.cisco.sesm	agent=configuration, page A-7 name=DESSMode, page A-15 name=Directory, page A-13 name=Directory,type=Connection,instance=Primary, page A-14 name=Directory,type=Connection,instance=Secondary, page A-15 name=Extension, page A-19 name=ExtensionSpecification, page A-18 name=firewall, page A-20 name=Location, page A-25 name=Logger, page A-23 name=ManagementConsole, page A-26 name=RDPLoginModule, page A-37 name=SESM, page A-46 name=SSG, page A-43 name=Version, page A-49 name=WebApp, page A-49
	org.mortbay.jetty	Debug=0, page A-52 name=Log, page A-52 name=Jetty,NCSARequestLog=0,Server=0, page A-53 name=Log,OutputStreamLogSink=0, page A-54 name=jetty,SESMSSLListener=0,Server=0, page A-57 name=Jetty,Server=0,, page A-54 name=Jetty,Server=0,WebApplicationContext=0, context=/, page A-56 name=Jetty,SESMSocketListener=0, Server=0, page A-58
CDAT	com.cisco.sesm	agent=configuration, page A-7 name=CDAT, page A-12 name=Directory, page A-13 name=Directory,type=Connection,instance=Primary, page A-14 name=Directory,type=Connection,instance=Secondary, page A-15 name=Logger, page A-23 name=MainServlet, page A-28 name=ManagementConsole, page A-26
	org.mortbay.jetty	Debug=0, page A-52 name=Log, page A-52 name=Jetty,NCSARequestLog=0,Server=0, page A-53 name=Log,OutputStreamLogSink=0, page A-54 name=jetty,SESMSSLListener=0,Server=0, page A-57 name=Jetty,Server=0,, page A-54 name=Jetty,Server=0,WebApplicationContext=0, context=/, page A-56 name=Jetty,SESMSocketListener=0, Server=0, page A-58

Table A-1 SESM Applications and Associated Configuration MBeans (continued)

SESM Application	Domain	Associated MBeans used for configuring this application
RDP	com.cisco.sesm	agent=configuration, page A-7 name=Directory, page A-13 name=Directory,type=Connection,instance=Primary, page A-14 name=Directory,type=Connection,instance=Secondary, page A-15 name=Logger, page A-23 name=ManagementConsole, page A-26 name=RDP, page A-29 name=RDP,AAA=AddAVsFilter, page A-35 name=RDP,AUTHENTICATION=DESSAuthenticationHandler, page A-35 name=RDP,AUTHORIZATION=DESSAuthorizationFilter, page A-35 name=RDP,DOMAINPROXY=DomainHandler, page A-36 name=RDP,GROUP-PROFILE=DESSGroupProfileHandler, page A-36 name=RDP,LOCAL=AaaHandler, page A-36 name=RDPLoginModule, page A-37 name=RDP,NEXTHOP-PROFILE=DESSNextHopProfileHandler, page A-38 name=RDP,SERVICE-PROFILE=DESSServiceProfileHandler, page A-38 name=RDP,PROXY=ProxyHandler, page A-39 name=RDP,PROXY=ProxyHandler,component=RADIUSClientSocket, page A-39 name=RDP,RADIUSListener=ACCOUNTING, page A-40 name=RDP,RADIUSListener=ACCOUNTING,component=RADIUSServerSocket, page A-40 name=RDP,RADIUSListener=ACCOUNTING,component=ThreadPool, page A-40 name=RDP,RADIUSListener=AUTH, page A-41 name=RDP,RADIUSListener=AUTH,component=RADIUSServerSocket, page A-41 name=RDP,RADIUSListener=AUTH,component=ThreadPool, page A-42 name=RDP,RDP=RDPHandler, page A-43 name=RDP,PROFILE=DESSProfileHandler, page A-43 RADIUSDictionary=0, page A-28
DNS Proxy	com.cisco.sesm	agent=configuration, page A-7 name=DNSProxy, page A-16 name=DNSProxy,DNS=DNSSubstituteIPhandler, page A-16 name=DNSProxy,RESOLVER=DNSDelegationHandler, page A-17 name=DNSProxy,UDPListener=DNS, page A-17 name=DNSProxy,UDPListener=DNS,component=ThreadPool, page A-18 name=Logger, page A-23 name=ManagementConsole, page A-26

SESM MBeans and Their Attributes

This section provides information about the MBeans used by SESM and includes the following:

Generic MBeans

The MBeans summarized in Table A-2 are used by all SESM applications.

Table A-2 Generic MBeans used by SESM

MBean	Domain	Description
type=MBeanServerDelegate	JMImplementation	Provides information on the management interface of the MBean.
name=ManagementAdaptor	com.cisco.sesm.ignore	Provides a management interface of an agent to Web browser clients.
name=version	com.cisco.sesm.jmx	Gets the package versions of the various system jars.
protocol=JRMP	Adaptor	Provides information on the management interface of the MBean. For example, JRMP is an Adaptor MBean that enables the server to communicate using RMI over JRMP.
interceptor=invoker,protocol=JRMP	Adaptor	Provides information on the management interface of the MBean. For example, created by the JRMP Adaptor MBean.

com.cisco.sesm MBeans

agent=configuration

Configuration agent MBean. This object observes JMX registration events looking for objects known to it. If a known object registers, then the configuration agent attempts to use it's MBean interface to push a configuration at the new MBean.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT, RDP.

Table A-3 Configuration Agent MBean Attributes

Attribute	Explanation
configuration	The configuration files used by the ConfigAgent.
freeMemory	The approximate amount of free memory on the Java heap in bytes.
totalMemory	The total size of the javaheap in bytes.

name=captiveportal

Captive Portal MBean. A Web application to redirect requests due to TCP-redirection from the edge device.

SESM Applications Using this MBean

Captive Portal

Table A-4 Captive Portal MBean Attributes

Attribute Name	Explanation
userRedirectOn initialCaptivateOn advertisingCaptivateOn serviceRedirectOn	These attributes provide a convenient way to switch on and off one or more of the TCP redirection types. Changing these attributes is much easier than reconfiguring the SSG. Valid values are: • true—The captive portal application performs an HTTP redirect to an appropriate content application. • false—The captive portal application does not respond to a particular type of TCP redirection. The subscriber experience is the same as if this type of TCP redirection were not configured.
host	Identifies the captive portal host. The value can be a comma-separated list of aliases or addresses, or a combination of aliases and addresses. The application uses this attribute to detect loops. The captive portal application redirects the browser to the URL in errorURL when both of the following conditions are true: • The host in the request matches this host value, and • The port in the request matches the listener port
In the installed configuration files, the following attributes are assigned values that are Java system properties. You can change the default value of a system property in the XML file, or you can override the default value at run time on the startup script command line.	

Table A-4 Captive Portal MBean Attributes (continued)

Attribute Name	Explanation
userRedirectURL initialCaptivateURL advertisingCaptivateURL	The URL that you want the subscriber's browser to be redirected to after each type of redirection. You can set this value to any of the following: • A URL pointing to a specific web page in the desired content application—Specify the URL in this format: http://*host*:*port/URI* where: – *host* is an IP address or host name of a web server – *port* is the port that the web server is listening on – *URI* is the relative path for the page within the content application that you want the subscriber's browser to be redirected to. • personalURL—This keyword specifies that the final redirection should be to the URL specified in the subscriber profile, in the H attribute. This option is not available for the unauthenticated user redirections (the userRedirectURL attribute) because the subscriber profile is not available at the time of redirection. • locationURL—This keyword specifies that the final redirection should be to the URL specified in the LocationMBean for the subscriber's subnet. If you use this keyword, you must copy the Location MBean from nwsp.xml, paste it into the captiveportal.xml file, and configure the MBean as described in the *Cisco Subscriber Edge Services Manager Subscriber Portal Guide*. Default: The default configuration after installation sets these attributes to URLs that point to pages in NWSP or Message Portal. The URLs are defined using system properties to represent the NWSP and the Message Portal applications. – userRedirectURL—Points to the NWSP logon page http://serviceportal.home:serviceportal.port/home – initialCaptivateURL—Points to the greetings page in the Message Portal application http://messageportal.home:messageportal.port/initial – advertisingCaptivateURL—Points to the advertising page in the Message Portal application http://messageportal.home:messageportal.port/advertising The values for the system properties in the URLs were set during the SESM installation process, in the URL Out fields. To change the system property values, edit the captiveportal.xml file. The default values after installation are: – serviceportal.host—IP address or host name of NWSP – serviceportal.port —8080, the default port used for NWSP – messageportal.host—IP address or host name of the Message Portal application – messageportal.port —8085, the default port used for Message Portal

Table A-4 Captive Portal MBean Attributes (continued)

Attribute Name	Explanation
userRedirectURL initialCaptivateURL advertisingCaptivateURL	The URL that you want the subscriber's browser to be redirected to after each type of redirection. You can set this value to any of the following: • A URL pointing to a specific web page in the desired content application—Specify the URL in this format: http://*host*:*port/URI* where: – *host* is an IP address or host name of a web server – *port* is the port that the web server is listening on – *URI* is the relative path for the page within the content application that you want the subscriber's browser to be redirected to. • personalURL—This keyword specifies that the final redirection should be to the URL specified in the subscriber profile, in the H attribute. This option is not available for the unauthenticated user redirections (the userRedirectURL attribute) because the subscriber profile is not available at the time of redirection. • locationURL—This keyword specifies that the final redirection should be to the URL specified in the LocationMBean for the subscriber's subnet. If you use this keyword, you must copy the Location MBean from nwsp.xml, paste it into the captiveportal.xml file, and configure the MBean as described in the *Cisco Subscriber Edge Services Manager Subscriber Portal Guide*. Default: The default configuration after installation sets these attributes to URLs that point to pages in NWSP or Message Portal. The URLs are defined using system properties to represent the NWSP and the Message Portal applications. – userRedirectURL—Points to the NWSP logon page http://serviceportal.home:serviceportal.port/home – initialCaptivateURL—Points to the greetings page in the Message Portal application http://messageportal.home:messageportal.port/initial – advertisingCaptivateURL—Points to the advertising page in the Message Portal application http://messageportal.home:messageportal.port/advertising The values for the system properties in the URLs were set during the SESM installation process, in the URL Out fields. To change the system property values, edit the captiveportal.xml file. The default values after installation are: – serviceportal.host—IP address or host name of NWSP – serviceportal.port —8080, the default port used for NWSP – messageportal.host—IP address or host name of the Message Portal application – messageportal.port —8085, the default port used for Message Portal

Table A-4 Captive Portal MBean Attributes (continued)

Attribute Name	Explanation
userRedirectPort initialCaptivatePort advertisingCaptivatePort	The port that the web server for the Captive Portal application will listen on for each redirection type coming from the SSG. These attributes are set to the following java system properties: • userRedirect.port—default is 8090 • initialCaptivate.port—default is 8091 • advertisingCaptivate.port—default is 8092 The default values for the system properties are the values you provided during installation in the Port In fields. If you change a port value, you must also change the SSG configuration to send redirections to the same port.
initialCaptivateDuration advertisingCaptivateDuration	This value is passed to the Message Portal application in the CPDURATION parameter. It specifies the length of time that the Message Portal application waits before attempting to perform a redirection to the subscriber's originally requested URL. **Note** The SSG TCP redirect commands also accept a duration attribute. See the "Summary of Message Duration Parameters" section on page 4-13 for more information.
serviceRedirectDefaultURL	The URL that the subscriber's browser is redirected to for any service redirection that does not have a service-specific URL defined in the defineServiceRedirect call, described next.
defineServiceRedirect	defineServiceRedirect is a system call that passes 3 arguments. There is a call for each specific service redirection and one for the default service redirection. 1. Port—The port that the web server for the Captive Portal application will listen on for the service redirections coming from the SSG. Its value is a Java system property whose default value was set during installation in the Port In fields. The default port values assigned by the installation program are: • Default service—8093 • Service1—8094 • Service2—8095 • Service3—8096 If you change a port value, also change the SSG configuration to send the service redirection to the same port. 2. URL (Optional)—The complete URL to the page you want the browser to be redirected to after the service redirection. If blank, the serviceRedirectDefaultURL is used. **Note** The installation program does not prompt for or set these URLs, which means that all service redirections are redirected to the serviceRedirectDefaultURL above. If you want to set service-specific URLs for each service redirection, provide the URLs here. 3. service name (Optional)—If provided, the captive portal application includes the service name in the query parameters appended to the URL that it forwards to the configured content application (for example, NWSP). The NWSP application uses the service name to attempt to connect to the service.

Table A-4 Captive Portal MBean Attributes (continued)

Attribute Name	Explanation

defineGenericRedirect	Configures a generic redirection port. (Multiple TCP redirection types can be assigned to this port.) The attribute has three arguments:
	• *port*—Specify a port value that is different from all other ports used in this configuration file. On the SSG, configure the desired TCP redirection types to go this port.
	• *destination*—Specify the destination of the redirection. Can be any of the following:
	– A specific URL to a page in another web portal application, such as the SESM NWSP or Message Portal application
	– personalURL, a keyword indicating redirection to a URL specified in the subscriber profile with the H attribute
	– locationURL, a keyword indicating redirection to a location-specific URL configured in the SESM Location MBean
	• *parameters*—A query string to be appended to the HTTP redirection request. The values in the query string will be URL-encoded for you. Use the following format:
	`"key1=value1&amp;key2=value2&amp;..."`
	where:
	keyx can be any HTTP standard parameter or any other query parameter that the destination page will understand
	valuex can be any of the following:
	– capturedURL
	– personalURL
	– locationURL
	– subscriberName
	The following example redirects all requests to the NWSP SSL port. It passes the subscriber's originally requested URL as an HTTP query parameter.
	`<Call name="defineGenericRedirect">`
	`<Arg>8099</Arg>`
	`<Arg>http://nwsp:8443</Arg>`
	`<Arg>CPURL=capturedURL</Arg>`
	`</Call>`

Table A-4 Captive Portal MBean Attributes (continued)

Attribute Name	Explanation
errorURL	The URL that the Captive Portal application redirects to if it does not find a URL to redirect to for the given port that the request came in on. The default value set at installation time redirects to the NWSP /home page.
Parameter names: • userRedirectURLParam • serviceRedirectURLParam • serviceRedirectService Param • serviceRedirectSubscriber Param • messageRedirectURL Param • messageRedirect SubscriberParam • messageRedirectDuration Param	These attributes define the parameter names used in the HTTP redirect requests. For example, the parameter name used to identify the subscriber's originally requested URL is CPSUBSCRIBER. You can change this to some other name by changing the value of userRedirectURLParam or MessageRedirectURLParam. These parameter names are visible to the subscriber in the browser's URL field. They appear in the query string appended to the URL.

name=CDAT

CDAT MBean. This class allows various attributes affecting the functioning of CDAT to be configured.

SESM Applications Using this MBean

CDAT.

Table A-5 CDAT MBean Attributes

Attribute	Explanation
maxVariables	The maximum number of page or page instance variables allowed for each CDAT directory management session. This number affects how many pages can be visited before their state is lost, although it is not a one-to-one mapping. If many StateTimedOut errors are occurring, increase this number. Default: 40
naming	The component in distinguished name (dn) that your LDAP directory uses to allow access to the directory. • cn—NDS, for example, uses common name cn. • uid—iPlanet, for example, uses unique identifier (uid).
queryMaxResults	The maximum number of results to return from any one query to the LDAP directory. Changes to this attribute value take immediate effect. A value of zero removes any limits. Default: 500

Table A-5 CDAT MBean Attributes (continued)

Attribute	Explanation
queryTimeout	The timeout (in milliseconds) for queries to the LDAP directory. Changes to this attribute value take immediate effect. A value of zero is an infinite timeout value. Default: 0
sessionTimeout	The maximum period of inactivity allowed after logging into a CDAT directory management session. When this time period elapses with no activity, CDAT logs the user out. Values are in seconds. A negative value prevents the user from ever being logged out. Changes to this attribute value take effect for subsequent logins. Default: 600

name=Directory

Directory MBean. Allows you to configure the directory server.The Directory MBean configures logging and caching attributes for executing classes in the SPE APIs.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT, RDP.

Table A-6 Directory MBean Attributes

Attribute Name	Explanation
connectionNameRoot	Root name of the individual connection MBeans. This MBean searches for other MBeans that begin with this name and assumes that those MBeans are connections to the directory.
factory	Java class used to create a connection to the data store. Do not change the installed value.
context	Default LDAP context. This is the organization and organizational unit that was created to hold the SESM data.
DESSPrincipal	Name used to connect to the SESM organization and organization unit. This user must have permission to create objects in the SESM context.
alwaysGetAllAttributes	If set to true, all the attributes of an LDAP entry are returned for each query.
traceFileName	Name of the directory log file.
traceLevel	Should be one of: NONE, ERROR, BRIEF, VERBOSE, or DEBUG.
printTraceToConsole	If set to true, the application sends trace messages to the console and writes them into the log file.
stackTrace	If set to true, the application prints a stack trace with each trace message.
cacheMaxObjects	Specifies the maximum number of software objects to hold in the cache. Objects represent subscribers, services, privileges, roles, and so on. When the cache contains cacheMaxObjects, old objects are deleted from cache, regardless of available cache space. Set this value high to allow the available cache space to be the determining factor for cache management. Installed default: 50000

Table A-6 Directory MBean Attributes (continued)

Attribute Name	Explanation
cacheMinFreeMem	Specifies the percentage of Java virtual memory that must remain available (that is, not used by the cache) after the application is loaded into memory. You can calculate the specific amount of memory available for the cache as follows: `cacheSize = (JavaVirtualMemory – applCodeSize) * (100% – cacheMinFreeMem)` Where: *JavaVirtualMemory* is the maximum virtual memory size specified at application startup time with the jvm argument. For example, if the installed startup scripts use the following values: • The startNWSP script uses 64 MB • The runrdp script uses 20 MB *applCodeSize* is the application size. The NWSP is approximately 18 MB. *cacheMinFreeMem* is the percentage of JVM that must remain available after the application is loaded into memory. For example, the *cacheSize* for NWSP is 90% of 14 MB, or 12.6 MB: *cacheSize* = (32 MB – 18 MB) * (100% – 10%) Default: 10
cacheSessionTimeout	Specifies the timeout of inactive client sessions in seconds. Default: 600
cacheExpireInterval	Specifies the interval in seconds after which the cache attempts to expire objects. **Note** Do not set this attribute to 0. A value of 0 causes *every* request to go to the directory, bypassing caching and any memory storage from a recent request for the same object. A value of 0 degrades performance substantially. Default: 600
cacheObjectTimeout	Specifies the number of seconds before objects time out. Default: 600

name=Directory,type=Connection,instance=Primary

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

- Connection, instance=Primary
- Connection, instance=Secondary See name=Directory,type=Connection,instance=Secondary

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT, RDP,Message Portal

Table A-7 Connection MBean Attributes

Attribute Name	Explanation
poolSize	Number of active connections allowed to the LDAP server.
URL	URL of the LDAP server.
principal	Name used when connecting to the LDAP server.
credentials	Credentials (such as password) used for connecting to the LDAP server.

name=Directory,type=Connection,instance=Secondary

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

- Connection, instance=Primary. See name=Directory,type=Connection,instance=Primary
- Connection, instance=Secondary

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT, RDP,Message Portal

Table A-8 SPE—Connection MBeans

Attribute Name	Explanation
poolSize	Number of active connections allowed to the LDAP server.
URL	URL of the LDAP server.
principal	Name used when connecting to the LDAP server.
credentials	Credentials (such as password) used for connecting to the LDAP server.

name=DESSMode

DESS mode MBean. Allows you to configure the naming attributes used for the LDAP directory as well as the Token Check Interval. In addition, this MBean allows you to display the current, total and maximum number of sessions.

SESM Applications Using this MBean

NWSP Portal.

Table A-9 DESS Mode MBean Attributes

Attribute	Explanation
currentSessions	The number of SPE sessions currently active.
maxSessions	The maximum number of sessions that were ever active at once.

Table A-9 DESS Mode MBean Attributes (continued)

Attribute	Explanation
naming	The component in distinguished name (dn) that the LDAP directory uses to allow access to the directory. For example: • cn—Indicates the common name (cn) used in an NDS directory • uid—Indicates the unique identifier (uid) used in an iPlanet directory
tokenCheckInterval	The time in seconds between checking the authorization tokens. Default: 300 seconds
tokenMaxAge	The length of time in seconds a token can remain in cache without being used before it is deleted. Default: 600 seconds
totalSessions	The number of sessions that have ever been active.

name=DNSProxy

DNS proxy MBean. Extensible Request Proxy. Provides mapping of ERPlisteners to request handlers in DNSProxy.

SESM Applications Using this MBean

DNS Proxy.

Table A-10 DNSProxy MBean Attributes

Attribute	Explanation
handlerMap	An alternative read-only view of the array of handlers, represented as a map.
handlers	An array of handler objects. DNS packets are passed to each handler in the chain in turn, which perform different operations on the packets.
listeners	An array of listener objects. A listener listens on a port for incoming packets and passes them to the first handler in the chain.
started	True if the DNS proxy is running.

name=DNSProxy,DNS=DNSSubstituteIPhandler

DNS substitute IP handler MBean. A DNS Handler that inserts a substitute IP address into the DNS response in the event of an unresolved request.

SESM Applications Using this MBean

DNS Proxy.

Table A-11 DNS substitute IP handler MBean attributes

Attribute	Explanation
dump	If true, requests and responses are dumped to stderr.
name	The name of this handler.
resolverHandlerName	The name of the ERP handler to try to resolve the DNS requests.

Table A-11 DNS substitute IP handler MBean attributes (continued)

Attribute	Explanation
started	True if this component is started.
substituteIPAddress	The IP address to use if the resolver was unable to resolve the DNS address.
substituteIPMap	SubstituteIP map.
timeToLive	The TTL value for spoofed addresses.

name=DNSProxy,RESOLVER=DNSDelegationHandler

DNS delegation handler MBean. A DNS Handler that delegates requests to other servers.

SESM Applications Using this MBean

DNS Proxy.

Table A-12 DNS delegation handler MBean attributes

Attribute	Explanation
dump	If true, requests and responses are dumped to stderr.
name	The name of this handler.
port	The DNS port to send delegated requests to.
servers	An array of IP addresses for the delegate servers.
started	True if this component started.
timeout	The time to wait for a response.

name=DNSProxy,UDPListener=DNS

UDP listener MBean. A listener for DNS requests.

SESM Applications Using this MBean

DNS Proxy.

Table A-13 UDP listener MBean Attributes

Attribute	Explanation
dump	If true, requests and responses are dumped to stderr.
handler	The name of the handler for requests from this listener.
localPort	The port to listen on.
maxRequestBytes	The max size of a received UDP packet.
name	The name of this listener.
started	True if this component is started.

name=DNSProxy,UDPListener=DNS,component=ThreadPool

ThreadPool MBean. The DNSProxy application ThreadPool.

SESM Applications Using this MBean

DNS Proxy.

Table A-14 ThreadPool MBean Attributes

Attribute	Explanation
daemon	True if running in daemon mode.
destroyed	Has the thread pool been destroyed.
idleThreads	Number of threads sitting idle.
maxIdleThreads	Maximum number of threads ever idle at one time.
maxIdleTimeMs	Maximum time in ms that a thread may be idle before it is reclaimed.
maxThreads	Maximum number of threads in the pool.
maxUsedThreads	Maximum number of threads ever in use at one time.
minThreads	Minimum number of threads in the pool.
name	Name of the running thread.
startTime	Start Time.
started	Has the thread pool been started.
threads	Current size of the threadpool.
usedThreads	Number of threads currently in use.

name=ExtensionSpecification

Extension Specification MBean. Allows you to configure an extension specification holding an extension and, optionally, a provider. Examples of extensions are Authentication, Authorization, ServiceConnection and ServiceProfile. Examples of providers are com.cisco.sesm.spis.demo, com.cisco.sesm.spis.radius and com.cisco.sesm.spis.dess.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, NWSP Portal.

Table A-15 Extension Specification MBean Attributes

Attribute	Explanation
name	Name.
provider	Provider.

name=Extension

Extension MBean. Allows you to configure extension specifications and the default provider.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, NWSP Portal.

Table A-16 Extension MBean attributes

Attribute	Explanation
defaultProvider	The name of the provider package to use if none is defined for a particular extension.
extensions	An array of extension specifications. Each contains the name of the extension and optionally, the provider.

name=FilePoller

FilePoller MBean. Allows you to configure polling interval, and the files to be polled for updating locations and whitelists.

SESM Applications Using this MBean:

Captive Portal, Web Proxy, web portal applications, Message Portal, WSG.

Table A-17 FilePoller MBean attributes

Attribute	Explanation
pollingInterval	An integer to determine the time period that the poller is inactive (asleep) between polling attempts. The minimum value is one minute (60 seconds). Default: 3600 seconds (one hour)
polledFiles	An array of strings containing all the file names to be examined by the poller.
forcePollingNow	Forces the file poller to do file polling without delay. This method behaves as follows: • The first time it is invoked, it initiates the polling cycle. • Any subsequent time that the method is invoked, it forces the file poller to poll with no further delay.

name=firewall

The Firewall MBean configures fields on the NWSP My Firewall page. Table A-18 describes the attributes in the Firewall MBean.

Firewall Protocols and Applications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SESM Applications Using this MBean

NWSP Portal.

Table A-18 Firewall MBean Attributes

Attribute Name	Explanation

customProtocols	Defines additional firewall protocols. Each item in the array consists of two elements:
	• Key—Names the firewall protocol. The name can be anything.
	• Value—The lower layer protocol (OSI Layer 3 or 4 protocol) and an optional port, separated by a comma. The lower layer protocol value must be a protocol that the SSG host is configured to accept.
	For example:
	`<Key>tcp</Key>`
	`<Value>tcp</Value>`
	
	`<Key>ftp</Key>`
	`<Value>tcp, 21</Value>`
	
	See the "Firewall Protocols and Applications" section on page A-20 for a definition and more examples of firewall protocols. Several firewall protocols are predefined in SESM and do not need to be explicitly defined here. The operational scenario shows all defined protocols.

customApplications	Defines additional firewall applications. Each item in the array consists of two elements:
	• Key—Names the firewall application. The name can be anything.
	• Value—A list of firewall protocols that comprise the application, separated by commas. Valid values are the SESM predefined and custom firewall protocols.
	For example:
	`<Key>ftp</Key>`
	`<Value>ftp</Value>`
	
	`<Key>www</Key>`
	`<Value>http,https</Value>`
	
	See the "Firewall Protocols and Applications" section on page A-20 for a definition and more examples of firewall applications. The operational scenario shows all defined applications.

displayApplications	Specifies the firewall applications that appear on the NWSP My Firewall page, in the Applications/Protocols column. Items in this list must be defined as predefined or custom firewall applications. To see a list of all defined applications, use the SESM Application Manager Advanced tab to access the Firewall MBean and click in the value column of the AllApplicationsDescriptions attribute, a read-only attribute. The text that represents the application on the My Firewall page is configured as a resource bundle in the NWSP installation directory. For example, for NWSP, resources are in: nwsp/webapp/WEB-INF/classes/messages[_*locale*].properties. NWSP searches its resource bundles for the resource *firewallAppName*Description, where *firewallAppName* is the application defined in the Firewall MBean. If a matching resource is not found, then *firewallAppName* is displayed on the My Firewall page. For example, consider the following firewall application: www NWSP searches for a resource named wwwDescription, and displays the text in the appropriate language on the My Firewall page. (In the installed files, this is World-Wide-Web for the en locale.) If the wwwDescription resource did not exist, then www would appear on the My Firewall page.

Table A-18 Firewall MBean Attributes (continued)

Attribute Name	Explanation
direction	Specifies direction (in or out) for the default access control direction in the ACLs created by SESM. Possible values for direction are: • in—Upstream, from the subscriber • out—Downstream, to the subscriber All connections have a return path. A block on in also affects traffic traveling in the opposite direction, and vice-versa. For any ACL, the choice of whether to control the in or out direction is a matter of preference.
returnOption	Sets the return option for TCP applications. Recommended values are: permit and default. Default refers to the Permit/Deny All Else button on the My Firewall page. Default: permit **Note** You can alter the My Firewall JSP to add a button allowing the subscriber to choose the TCP return option. The JSP contains commented-out code for an ipPermission button, which you could copy to implement a return TCP permission button.

name=Ipass

Ipass MBean. Allows you to configure support for iPass clients.

SESM Applications Using this MBean

NWSP Portal.

Table A-19 Ipass MBean Attributes

Attribute	Explanation
ipassLogonURL	The URL (must be secure) to post users principal/credentials. NWSP must provide a SSL certificate signed by a well-known certificate authority to the iPass client before the user credential is posted.
ipassLogoffURL	The URL to process user end-session requests.
ipassAddLocationToUserName	Required to append user's location to user credential before authentication
ipassLocationSeparator	The character sequence used to delimit the iPass user name and domain from the location name. The default value is "###". Regular expression characters, for example *, ?, and . are not allowed in the ipassLocationSeparator string. **Note** If you change the location separator, use characters that are not expected to be used in the username. The username should not include location separator characters as part of the name.
ipassDefaultLocationName	The location name that is passed to the iPass AAA server if the SESM location service is prohibited, or fails to resolve the user's location.
ipassDefaultLocationID	The location ID that is passed to the iPass Smart client XML reply. This attribute has been added for iPass's use and is not used by SESM
ipassUseSESMLocation	When set to true, it allows the SESM location service to resolve the user's location. If set to false, ipassDefaultLocationName attribute is used instead. Default value is set to true.

name=JNDI

JNDI naming server MBean. Allows you to perform JNDI naming server configuration for storing and retrieving extensions.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal.

Table A-20 JNDI naming server MBean Attributes

Attribute	Explanation
contextFactory	The initial context factory for creating the naming service context.

name=Login

Login MBean. Allows you to configure login parameters.

SESM Applications Using this MBean

Application Manager.

Table A-21 Login MBean Attributes

Attribute	Explanation
authInfo	The Login MBean holds an array of authInfo objects. Each object holds a user name and password. Users logging in are checked against this array.
authInfoDescription	An easily readable representation of the authInfo array (read-only).

name=Logger

The Logger MBean configures both logging and debugging tools. The logging tool traces business events in the SESM portal. The debugging mechanism produces messages useful to developers in debugging applications. Table A-22 describes the attributes in the Logger MBean.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT, RDP, DNS Proxy

Table A-22 SESM Portal Application—Logger MBean

Attribute Name	Explanation
debug	Turns debugging on or off. That is, it controls whether Log.debug calls executed by the SESM application are displayed in the log file. **Note** Logging remains on regardless of this value. That is, all Log.trace and Log.warning calls executed in the SESM application are written to the log file regardless of the value of the debug attribute. To turn off logging, comment out the entire Logger MBean. Values for this attribute are: • false—The application produces trace messages but not debug messages. The trace messages record business activity performed by the SESM portal. This setting is the normal, recommended setting for production environments. The trace messages provide important information for diagnosing configuration problems. • true—The application produces trace and debug messages. This setting is intended for development environments to debug portal code behavior. The logging of debug messages can affect performance; hence, this setting is not recommended for production environments. The following parameters control the contents of debug messages that the application generates: logFrame, logStack, logThread, debugPatterns, and debugThreads. The following parameters control the types of logging messages produced: trace and warning. Installed default: false
debugPatterns	By specifying one or more patterns, you turn on a filtering mechanism that excludes any message that does not match the pattern. The patterns are file, class, or method names. Pattern matching is based on substring matches. For example, if you specify the pattern RADIUS, the software focuses on RADIUS messages. To specify multiple patterns, separate the patterns using a comma. Installed default: empty, which means that you receive all messages.
debugThreads	Specifies a specific thread name for which to show debugging messages. You can specify multiple thread names, separating them using a comma. For example: 6,13,22. By default, no thread name is specified. Because each user interaction with the SESM web application takes place in a thread named for that user, this parameter can be used to focus the logging trace on a specific user activity. Enter a list of thread names separated by commas. Installed default: empty
debugVerbosity	Specifies the level of detail in debugging messages. When the debug attribute is set to false, this attribute is ignored. Values are MAX, MED, or LOW. Installed default: LOW
logDateFormat	Specifies format of dates in the log file. Installed default: yyyyMMdd:HHmmss.SSS

Table A-22 SESM Portal Application—Logger MBean (continued)

Attribute Name	Explanation
logFile	Specifies the filename and location for the logging (tracing) of business events performed by the SESM application. The installed default is: *application.home*/logs/*yyyy_mm_dd*.application.log Where: • *application.home*—A property whose value is set in the SESM start script. • logs—A constant. All log files appear in the logs subdirectory under the application directory. • *yyyy_mm_dd* —The year, month, and day that the file was created. • application.log—A constant identifying the application log files.
logFrame	Controls whether or not to log the calling member function. Installed default: false
logStack	Controls whether or not to log stack traces. Installed default: false
logThread	Controls whether or not to log thread IDs. Installed default: true
logToErr	Controls whether or not to route log messages to stderr, in addition to the log file. This parameter is useful for monitoring the SESM web application at the command line. Displaying output to stderr is not recommended for production deployments. Installed default: true
trace	Controls whether or not to log trace messages. These messages indicate entry and exit to code points. Installed default: true
warning	Controls whether or not to log warning messages (nonfatal exceptions). Installed default: true

name=Location

Location MBean. Allows you to define a set of Locations. A Location is defined by a set of identifiers: Client IP address, VPI and sub-interface. For example, the application can use the location of a session to change its look and feel.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal.

Table A-23 Location MBean attributes

Attribute	Explanation
locationService	Defines the SESM class containing the logic for location determination. You can change this attribute to point to a customized service provider interface (SPI) class.
locations	Defines an array of location values. **Note** Configure locations by editing the configuration file. For more information, see Chapter 6, "Configuring Location Awareness and Whitelist URLs."

name=ManagementConsole

The ManagementConsole MBean configures the portal's management console port, including valid usernames and passwords for accessing the console.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT, RDP.

Note The installation process does not add a link on the CDAT main window to this Agent View. You can add this link manually. Before creating the link, edit the startAAA script, inserting a port number that you want to consistently use to start the bundled SESM RADIUS server. Then configure the link on the CDAT window to go to the configured RDP port + 100.

Table A-24 ManagementConsole MBean Attributes

Attribute	Explanation
authInfo	Used by the persistence mechanism.
authInfoDescription	A list of the logins configured for this agent view.
port	The port the Agent View HTML Adaptor should run on.

name=messageportal

Message portal MBean. Allows you to configure settings for the Message Portal.

SESM Applications Using this MBean

Message Portal.

Table A-25 messageportal MBean Attributes

Attribute Name	Explanation
defaultPage	For advertisement redirections, specifies the default page to redirect to if: • The subscriber profile does not contain any interests. • The ignoreProfile attribute is set to true. • The interestPages attribute indicates that the default page should be used for a specific interest.
defaultURL	For initial logon and advertisement redirections, specifies a default URL to redirect to after the captivation duration has elapsed, if a CPURL parameter was not included in the query string of the HTTP request from the Captive Portal application. The CPURL parameter specifies the originally requested URL from the subscriber (before redirection).
defaultDuration	Optional. This value is used if the Captive Portal application does not forward a CPDURATION parameter. This attribute applies only if the redirectOn attribute is true. For initial logon and advertisement redirections, it specifies the length of time that the Message Portal application waits before attempting to perform a redirection to the subscriber's originally requested URL. **Note** The SSG TCP redirect commands also accept a duration attribute. See the "Summary of Message Duration Parameters" section on page 4-13 for more information.

Table A-25 messageportal MBean Attributes (continued)

Attribute Name	Explanation
ignoreProfile	For advertisement redirections, indicates whether the interest attribute in the subscriber profile should be used to determine the page to redirect to. Valid values are: • true—Ignore the interest field. Redirect to the page specified in the defaultPage attribute. • false—Redirect to a page based on the first interest in the subscriber profile. **Note** In RADIUS mode, this attribute must be set to true. The interest attribute is not available with RADIUS profiles.
redirectOn	For initial logon and advertisement redirections, indicates action to take after the captivation duration elapses: • true—Issue another redirection to the original page requested before the logon or advertisement redirection occurred. This is the URL specified in CPURL parameter in the query string of the HTTP request from the Captive Portal application. • false—Do not issue another redirection. The message or advertisement page remains displayed until the subscriber enters another URL.

interests	Specifies the interest values that can appear in a subscriber profile. Separate each interest value with a comma. For example:
	`cinema,`
	`science,`
	`internet,`
	`news,`
	`sports,`
	`travel,`
	`finance,`
	`community`
	The interest values must match the options that you allow the subscriber to choose (for example, on an account self management page in NWSP) or that the service provider administrators are allowed to enter into an SPE subscriber profile.

interestPages	Specifies the advertisement page to display for each interest. (The Message Portal application displays the page appropriate to the first interest listed in a subscriber profile.) Separate each interest page with a comma.
	To use the default page for an interest, use any single character in the interestPages list.
	In the following example, subscribers whose profile contains science as the first interest see the default page as an advertisement.
	`cinema.jsp,`
	`.,`
	`internet.jsp,`
	`news.jsp,`
	`sports.jsp,`
	`travel.jsp,`
	`finance.jsp,`
	`community.jsp`

name=MainServlet

MainServlet MBean. This class allows you to configure the links on the main page of CDAT.

SESM Applications Using this MBean

CDAT.

Table A-26 MainServlet MBean Attributes

Attribute	Explanation
linkDescriptions	An array of links in human readable form.

links	Specifies the links to display on the CDAT main window, such as the links to:
	• Logon pages that provide access to LDAP directory maintenance.
	• Remote management of SESM applications.
	The links attribute is an array. For each link, provide the following information:
	• label—The static text that appears on the CDAT window to identify the link.
	• URI—The HTTP address that points to the target page. To point to the management console for a SESM application, use that application's host name and management console port. For example:
	`http://server1:8180/`
	The SESM startup scripts set the management port to application.port + 100. For example, if you installed the Subscriber Portal using the default port value 8080, its Agent View management port is:
	`8080 + 100 = 8180`
	Similarly, if you installed CDAT using the default port value 8081, its Agent View management port is:
	`8081 + 100 = 8181`
	• linkText—The active text that the user clicks to go to the URI. For example, the installed file uses the text Agent View as the active text for the link to the NWSP wep portal management console.

RADIUSDictionary=0

RADIUSDictionary MBean. Allows RADIUS Dictionary style access to the RADIUS attributes. All SESM applications, including this RADIUS server, internally predefine the standard RADIUS attributes and the Cisco SSG vendor-specific attributes (VSAs). You can define additional attributes, such as additional Cisco VSAs or VSAs from other vendors, in the RADIUSDictionary MBean. When you define attributes in this MBean, you can use the defined attribute names in RADIUS profiles.

SESM Applications Using this MBean

RDP.

Table A-27 RADIUSDictionary MBean Attributes

Attribute Name	Explanation
dynamicAttributes	An array of new attribute definitions. To define a new attribute, add a new item to this array. The format for an item is: *name*(*radiusAttributeId, vendorId*, *vendorSubattribute*, *datatype*) Where: • *name*—Is the new attribute name. • *radiusAttributeId*—Use attribute value 26, the vendor-specific attribute. • *vendorId*—A RADIUS vendor ID. • *vendorSubattribute*— A unique number that distinguishes this attribute from other VSAs for the same vendor. • *datatype*—One of the following values: BINARY, STRING, INTEGER, or IPADDRESS. When *datatype* is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string. For example: demoVSA(26, 1, 1, BINARY) Other valid syntax formats are represented below: *name*([[type=]26],[vendorId=]*vendorId*,[vendorType=]*vendorType*,[dataType=]*dataType*) For example: demoVSA(type=26, vendorId=1, vendorType=1,dataType=INTEGER)

name=RDP

Extensible Request Proxy MBean. The RDP MBean configures the RDP listeners and handlers.

SESM Applications Using this MBean

RDP.

Table A-28 RDP MBean Attributes

Attribute Name	Explanation
The following attributes define the listeners. The RDP MBean defines two listeners.	
name	Sets the listener name. The two names are: AUTH and ACC.
handler	Defines the type of listener being configured. The default values are: • RDP for the AUTH listener—Do not change this value. The RDP handler performs the functions described in this manual. • AAA for the ACC listener—The AAA handler responds to accounting requests, but does not process them. You can change this value; for example, you might want to use the DOMAIN or PROXY handlers to proxy accounting to other RADIUS servers.

Table A-28 RDP MBean Attributes (continued)

Attribute Name	Explanation
dump	• true—Displays all RADIUS messages on the console (stderr) • false—Does not display messages Default: false
The following attributes configure the RDP handler. The RDP handler examines requests on the AUTH port, determines whether each request is an authentication request or a request for service information, and calls the configured handler.	
name	The required value is RDP.
aaaHandler	Specifies the next handler for authentication requests. Default: AAA
profileHandler	Specifies the next handler for service profile requests. Default: PROFILE
The AddAVsFilter class in the AAA handler uses the following attribute.	
AVs	Adds a Cisco AVpair to all responses. This field has the following uses: • You can use it to add customized or universal default values for specific fields for all responses. The Cisco AVpair is a RADIUS vendor-specific attribute supported by SSG and RDP. The Cisco AVpair field can contain any number of attribute value pairs, in the following format: attribute:value • The installed configuration uses it to add a service-type attribute with the value OUTBOUND to all responses. This value identifies a response as a service profile, rather than a subscriber profile. It is added to all requests, with the expectation that the OUTBOUND value will be written over with the value FRAMED-USER when authentication is successful. When authentication is not successful, the request continues to be processed by the Profile Handler. When the profile handler cannot handle the request successfully, the returned response is an accept-reject.
The DESSAuthorizationFilter class in the AUTHORIZATION handler uses the following attributes:	
addService addAutoService addGroup	These options control the type of service information that the handler adds to authentication replies. Operational scenario: **RDP**
The DESSAuthenticationHandler class in the AUTHENTICATION handler use the following attribute.	
authAttributes	This attribute specifies the RADIUS attributes to use in subscriber authentication, in addition to the USER_NAME attribute. USER_NAME is always required and should not appear in the list. Any other standard RADIUS attribute can be used for authentication. Typical values are: • USER_PASSWORD • CALLED_STATION_ID (APN) • CALLING_STATION_ID (MSISDN) • NAS_IDENTIFIER Operational scenario: **RDP**

Table A-28 RDP MBean Attributes (continued)

Attribute Name	Explanation
To configure the following handlers, see *Cisco Subscriber Edge Services Manager Profile Management Guide*: • AUTHENTICATION Handler • AUTHORIZATION Handler • PROXY Handler • LOCAL Handler • DOMAIN Handler • PROFILE Handler	
The DESSServiceProfileHandler, DESSGroupProfileHandler, and DESSNextHopProfileHandler classes use the following attributes.	

servicePassword
groupPassword
nextHopPassword
	RDP requires passwords to obtain service, group, and next hop profiles. The SSG sets the password in the request. The values you configure here must match the values configured on the SSG, or, in the case of the groupPassword, in SESM configuration. If the configured password does not match the password in a profile, RDP returns an access-reject message.
	• servicePassword—Requests containing this password value are requests for a single service profile. RDP uses the SPE API to obtain a list of authorized services for a subscriber. This servicePassword must match the password configured on the SSG with the following command:
	`ssg service-password servicePassword`
	• groupPassword—Requests containing this password value are requests for a service group profile. RDP forwards requests to a RADIUS server to obtain a list of authorized services for the group of which the subscriber is a member. Group requests are relevant only when RDP is configured in proxy mode. The groupPassword value must match the password configured on the SESM portal in the serviceGroupPassword attribute in the AAA MBean.
	• nextHopPassword—Requests containing this password value are requests for a next hop table profile. RDP passes authentication requests to the AAAMBean when the RDP is configured in proxy mode, or through SPE to the directory when the RDP is not in proxy mode. On the SSG side, set this password using the following command:
	`ssg next-hop download nextHopTableName password`
	Operational scenario: **RDP**

The following attributes configure the listener threadpools. Each listener has its own settings, identified as follows: • RADIUSListener=AUTH,component=ThreadPool • RADIUSListener=ACC,component=ThreadPool	
minThreads	Sets the minimum number of threads that this listener maintains during periods of low load. This listener always has system resources allocated for this number of threads. Default: 5
maxThreads	Sets the maximum number of threads that this listener can allocate resources for, even during peak loads. This listener can have up to this number of threads. Default: 255

Table A-28 RDP MBean Attributes (continued)

Attribute Name	Explanation
The following attributes configure the listener sockets. Each listener has its own settings, identified as follows: • RADIUSListener=AUTH,component=RADIUSServerSocket • RADIUSListener=ACC,component=RADIUSServerSocket	
secret	The shared secret that must be used in RADIUS protocol messages sent to the bundled SESM RADIUS server. This attribute sets a global shared secret for all clients. To specify different shared secrets for each client, use the allowedClients attribute. Default: cisco
localIP	The IP address of the RDP. Usually set this value to 0.0.0.0. RDP accepts requests containing any destination IP address if this attribute is set to 0.0.0.0. When this attribute is not 0.0.0.0, the destination address in the request must match this configured value exactly, or RDP ignores the request. If RDP is running on a system configured with more than one interface (for example, multiple Ethernet interfaces in multiple networks), the localIP attribute provides a way to restrict access to RDP. In that case, set localIP to match the address of the desired interface—RDP will accept requests addressed to the localIP address and ignore all others. To configure RDP to accept requests from all the system's configured interfaces, set localIP to 0.0.0.0. Default: 0.0.0.0
localPort	The port the RADIUS server listens on. The installed configuration file defines two ports as system properties: • application.portno—Default is 1812 This default is used in both the rdp.xml file and in the runrdp script. To change the application.portno, edit the start script • accounting.portno—Default is 1814. This default is used in the rdp.xml file. To change the accounting.portno, edit the rdp.xml file. The installed start script does not include assignments for accounting.portno.
allowedClients	Configures a list of clients from which the server can accept requests. Also configures shared secrets. Turn this feature on and off as follows: • Allow any client to access the RDP—Comment out the allowedClients attribute in the XML file, or remove all clients from the allowedClients list. • Restrict client access—Uncomment the allowedClients attribute in the XML file. **Note** If the allowedClients attribute does not appear in the Application Management windows, check the configuration file (the XML file). The allowedClients attribute might be commented out. If so, remove the comment characters, save the XML file, and then restart RDP. RDP clients are SSGs. You can add more clients by adding more elements to the allowedClients attribute. An element in the allowedClients attribute has the following format: {hostName | IPAddress}[:localSecret] Where: *hostName* or *IPAddress* identify a client (an SSG, for example) that has access to the RDP. *localSecret* identifies the secret that this client uses for RADIUS communication If the client is an SSG, this value must match the shared secret configured on the SSG device: `radius-server key SharedSecret`

Table A-28 RDP MBean Attributes (continued)

Attribute Name	Explanation
The following attributes configure RADIUSClientSockets for proxy handlers. Use these attributes to define the RADIUS servers to which you want to proxy. Each proxied server has its own settings.	
throttle	The maximum number of simultaneous requests that RDP can send to a RADIUS server. This is a RADIUS protocol attribute. The RADIUS protocol queues additional requests and issues them as the server returns responses or timeout messages for previous requests. Default: 256
timeOut	The number of seconds that RDP waits before timing out RADIUS packets that it sends to the RADIUS server. Default: 4000
maxRetries	The number of times RDP re-sends packets to the RADIUS server if no response is received. Default: 3
primaryIP	The IP address or the host name of the primary RADIUS server.
primaryPort	The port number that the primary RADIUS server listens on. Default: 1812
secret	The shared secret used between the RADIUS server and RDP. The shared secret must be the same for the primary and secondary servers. It must match the secret specified when you configured RDP as a NAS client on the RADIUS server. Default: cisco
secondaryIP	The IP address or host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, reenter the primary server.
secondaryPort	The port number that the secondary RADIUS server listens on. If you are not using a secondary server, reenter the primary server. Default: 1812
accountingPortOffset	The offset applied to the authentication ports to calculate the accounting ports for the proxied servers. Default: 1 (which results in 1813 as the accounting port default)

name=AAA

The AAA MBean configures the AAA listener, including its thread pool and socket (port).Table A-29 describes the configurable attributes in the AAA MBean.

SESM Applications Using this MBean

RDP.

Table A-29 AAA MBean Attributes

Attribute Name	Explanation
throttle	The maximum number of simultaneous requests that NWSP can send to a RADIUS server. This is a RADIUS protocol attribute. The RADIUS protocol queues additional requests and issues them as the server returns responses or timeout messages for previous requests. Installed default: 256
timeOut	The number of seconds the SESM NWSP waits before timing out RADIUS packets that it sends to the AAA server. Installed default: 4
maxRetries	The number of times the SESM NWSP resends packets to the AAA server if no response is received. Installed default: 3
primaryIP	The IP address or the host name of the primary AAA server.
primaryPort	The port number that the primary RADIUS server listens on. Default: 1812
secret	The shared secret used between the RADIUS server and NWSP. The shared secret must be the same for the primary and secondary servers. It must match the secret specified when you configured SESM as a NAS client on the RADIUS server. Default: `cisco`.
secondaryIP	The IP address or host name of the secondary AAA server. If you are not using a secondary RADIUS server, reenter the primary server, this value should match that of the primaryIP.
secondaryPort	The port number that the secondary RADIUS server listens on. If you are not using a secondary server, reenter the primary server, this value should match that of the primaryPort. Default: 1812
servicePassword	The password that NWSP uses to request service profiles from the RADIUS server. It must match the service password values used in the service profiles in the RADIUS database. Default: `servicecisco`
serviceGroupPassword	The password that NWSP uses to request group profiles from the RADIUS server. It must match the service group password values used in the service group profiles in the RADIUS database. Default: `groupcisco`

name=RDP,AAA=AddAVsFilter

ERP filter MBean. Provides an ERPFilter to add RADIUS AVs to a response.

SESM Applications Using this MBean

RDP.

Table A-30 ERP filter MBean Attributes

Attribute	Explanation
AVs	Array of string attribute: value definitions.
name	The name of this handler.
nextHandler	Name of the next handler for this filter.
responseCodes	Array of integer response codes that will activate this filter.
started	True if this component is started.

name=RDP,AUTHENTICATION=DESSAuthenticationHandler

DESSAuthenticationHandler MBean. An AAA Handler using the DESS library for LDAP authentication.

SESM Applications Using this MBean

RDP.

Table A-31 DESSAuthenticationHandler MBean Attributes

Attribute	Explanation
authAttributes	Array of radius attribute definitions that if present in the DESS profile are used to authenticate the radius request.
name	The name of this handler.
started	Array of radius attributes that if present in the DESS profile are used to authenticate the radius request.

name=RDP,AUTHORIZATION=DESSAuthorizationFilter

DESSAuthorizationFilter MBean. Filter to add authorization information using the DESS library.

SESM Applications Using this MBean

RDP.

Table A-32 DESSAuthorizationFilter MBean Attributes

Attribute	Explanation
addAutoService	If true auto service authorizations are added to this response.
addGroup	If true group authorizations are added to this response.
addService	If true authorizations are added to the response.
name	The name of this handler.

Table A-32 DESSAuthorizationFilter MBean Attributes (continued)

Attribute	Explanation
nextHandler	Name of the next handler for this filter.
started	True if this component is started.

name=RDP,DOMAINPROXY=DomainHandler

Generic ERP Handler MBean. Provides configuration of handler for domain based proxying.

SESM Applications Using this MBean

RDP.

Table A-33 Generic ERP Handler MBean Attributes

Attribute	Explanation
domainMap	The domain map.
name	The name of this handler.
started	true if this component is started.

name=RDP,GROUP-PROFILE=DESSGroupProfileHandler

DESSGroupProfileHandler MBean. Handler for Group profile requests backed by DESS.

SESM Applications Using this MBean

RDP.

Table A-34 DESSGroupProfileHandler MBean Attributes

Attribute	Explanation
dontCopyAttributes	Array of attributes not to copy from a request to a response.
groupPassword	The password for group profile requests.
name	The name of this handler.
started	True if this component is started.

name=RDP,LOCAL=AaaHandler

AAA Handler MBean. Provides local flat file handler configuration.

SESM Applications Using this MBean

RDP.

Table A-35 AAA Handler MBean Attributes

Attribute	Explanation
aaaFilename	Filename or resource name of the AAA file in merit format.
name	The name of this handler.
started	True if this component is started.

name=RDPLoginModule

RDPLoginModule MBean. Configures options on the Portal, including:

- Attributes to control the IP Address and the Port of the primary RADIUS Server to authenticate against
- Attributes to control the IP Address and the Port of the secondary RADIUS Server to authenticate against
- Attributes to control the behavior of the RDPLoginModule if it is selected for use in the WebApp MBean/jaasConfigIndex value
- Attributes to control the behavior of the timeout waiting from sending of request to the receiving of the response from the RADIUS Server

SESM Applications Using this MBean

RDP, NWSP Portal.

Table A-36 RDPLoginModule MBean Attributes

Attribute	Explanation
secret	The secret string is used to encrypt the transactions that take place between the RADIUS Client and the RADIUS Server. This value is known to both the client and server in these communications, but is not transmitted. Any change to the secret value on the SESM Portal (which is the client) may result in failed RADIUS Requests as the secret value should be the same at the server side. If this occurs, the server should be modified so that it has the same secret value.
primaryIP	The IP Address of the Primary RADIUS Server.
primaryPort	The port on the Primary RADIUS Server where RADIUS Packets should be sent to.
secondaryIP	If configured, this is the IP Address of the Secondary RADIUS Server. The Secondary RADIUS Server is used when no response is obtained from the Primary RADIUS Server or if request is resent a number of time without any response.
secondaryPort	If configured, this is the port on the Secondary RADIUS Server where RADIUS Packets should be sent to.

Table A-36 RDPLoginModule MBean Attributes (continued)

Attribute	Explanation
shutdownTime	The time, in milliseconds, the RADIUS Client Socket is kept open when a action is requested to reconfigure the RADIUS Client Socket using the existing values for primaryIP/primaryPort and secondaryIP/secondaryPort. This time period is used to allow clients who are using the RADIUS Client Socket to fulfill their requests.
timeout	The time, in milliseconds, the RADIUS Client will wait on the RADIUS Server for a response to its request before timing out. Default values: secret - cisco PrimaryIP - 127.0.0.1 PrimaryPort - 1812 SecondaryIP - 127.0.0.1 SecondaryPort - 1912 ShutdownTime - 120000 Timeout - 5000

name=RDP,NEXTHOP-PROFILE=DESSNextHopProfileHandler

Handler for NextHop profile requests backed by DESS.

SESM Applications Using this MBean

RDP.

Table A-37 Handler for NextHop MBean Attributes

Attribute	Explanation
dontCopyAttributes	Array of attribute not to copy from a request to a response.
name	The name of this handler.
nextHopPassword	The password for next hop profile requests.
started	True if this component is started.

name=RDP,SERVICE-PROFILE=DESSServiceProfileHandler

Handler for Service profile requests backed by DESS.

SESM Applications Using this MBean

RDP.

Table A-38 Handler for Service profile requests MBean Attributes

Attribute	Explanation
dontCopyAttributes	Array of attributes not to copy from a request to a response.
name	The name of this handler.
servicePassword	The password for service profile requests.
started	True if this component is started.

name=RDP,PROXY=ProxyHandler

RADIUS Proxy MBean. Provides configuration of RADIUS Proxy handler.

SESM Applications Using this MBean

RDP.

Table A-39 RADIUS Proxy MBean Attributes

Attribute	Explanation
name	The ERPHandler name of this proxy.
started	True if this component is started.

name=RDP,PROXY=ProxyHandler,component=RADIUSClientSocket

RADIUSClientSocket MBean. Provides the RADIUS Client Socket.

SESM Applications Using this MBean

RDP.

Table A-40 RADIUSClientSocket MBean Attributes

Attribute	Explanation
accountingPortOffset	The offset to add to the destination port when sending accounting requests.
dump	Dump
localIP	String representation of Host or IP address of the local RADIUS socket.
localPort	Port number of the local RADIUS socket.
localPortMax	If the localPort is not set, one will be allocated from within the range of localPortMin to localPortMax.
localPortMin	If the localPort is not set, one will be allocated from within the range of localPortMin to localportMax.
maxRetries	Number of times to try a send before falling back to the secondary, or failing if already on the secondary.
open	If true the socket is open.
primaryIP	String representation of host or IP address of the primary remote RADIUS socket.
primaryPort	Port number of the primary remote RADIUS socket.
secondaryIP	String representation of host or IP address of the secondary remote RADIUS socket.
secondaryPort	Port number of the secondary remote RADIUS socket.
secret	RADIUS shared secret.
statistics	String representation of statistics
throttle	The number of simultaneous requests allowed per RADIUS socket.
timeOut	Timeout in milliseconds for send or receive.

name=RDP,RADIUSListener=ACCOUNTING

ERP listener MBean. Provides an ERPListener for RADIUS requests.

SESM Applications Using this MBean

RDP.

Table A-41 ERP listener MBean Attributes

Attribute	Explanation
dump	If true all packets are dumped to stderr.
handler	The name of the handler for requests from this listener.
name	The name of this listener.
started	True if this component is started.

name=RDP,RADIUSListener=ACCOUNTING,component=RADIUSServerSocket

RADIUSServerSocket MBean. Provides RADIUS Server Socket configuration for accounting.

SESM Applications Using this MBean

RDP.

Table A-42 RADIUSServerSocket MBean Attributes

Attribute	Explanation
allowedClients	Array of hostnames for clients accepted by this server. If empty or null, then all clients are accepted. A per client secret may be specified with a colon separated secret added to the client ip, or name.
dump	Dump
localIP	String representation of Host or IP address of the local RADIUS socket.
localPort	Port number of the local RAIUS socket.
needMessageAuthenticator	If true, all received messages require a valid message authenticator.
open	If true, the socket is open.
secret	RADIUS shared secret.
statistics	String representation of statistics.
timeOut	Timeout in milliseconds for send or receive.
recvBufSize	Desired size of socket receive buffer. Set the value to 0 to use the system default.
sendBufSize	Desired size of socket transmit buffer. Set the value to 0 to use the system default.

name=RDP,RADIUSListener=ACCOUNTING,component=ThreadPool

ThreadPool MBean. Provides the ThreadPool settings for the accounting listener.

SESM Applications Using this MBean

RDP.

Table A-43 ThreadPool MBean Attributes

Attribute	Explanation
daemon	True if running in Daemon mode.
destroyed	Has the thread pool been destroyed?
idleThreads	Number of threads sitting idle.
maxIdleThreads	Maximum number of threads ever idle at one time.
maxIdleTimeMs	Maximum time in ms that a thread may be idle before it is reclaimed.
maxThreads	Maximum number of threads in the pool.
maxUsedThreads	Maximum number of threads ever in use at one time.
minThreads	Minimum number of threads in the pool.
name	Name of the running thread.
startTime	Start time.
started	Has the thread pool been started?
threads	Current size of the thread pool.
usedThreads	Number of threads currently in use.

name=RDP,RADIUSListener=AUTH

ERP listener MBean. Provides an ERPListener for Auth (authentication and authorization) requests.

SESM Applications Using this MBean

RDP.

Table A-44 ERP listener MBean Attributes

Attribute	Explanation
dump	If true all packets are dumped to stderr.
handler	The name of the handler for requests from this listener.
name	The name of this listener.
started	True if this component is started.

name=RDP,RADIUSListener=AUTH,component=RADIUSServerSocket

RADIUSServerSocket MBean. Provides the RADIUS server socket for the auth listener.

SESM Applications Using this MBean

RDP.

Table A-45 RADIUSServerSocket MBean Attributes

Attribute	Explanation
allowedClients	Array of hostnames or IPs for clients accepted by this server. If empty or null, then all clients are accepted. A per client secret may be specified with a colon separated secret added to the client ip or name.
dump	Dump.
localIP	String representation of host or IP address of the local RADIUS socket.
localPort	Port number of the local RADIUS socket.
needMessageAuthenticator	If true all received messages require a valid message authenticator.
open	If true, the socket is open.
secret	RADIUS Shared Secret.
statistics	String representation of statistics.
timeOut	Timeout in milliseconds for send or receive.
recvBufSize	Desired size of socket receive buffer. Set the value to 0 to use the system default.
sendBufSize	Desired size of socket transmit buffer. Set the value to 0 to use the system default.

name=RDP,RADIUSListener=AUTH,component=ThreadPool

ThreadPool MBean. Provides ThreadPool settings for the auth listener.

SESM Applications Using this MBean

RDP.

Table A-46 ThreadPool MBean Attributes

Attribute	Explanation
daemon	True if running in daemon mode.
destroyed	Has the threadpool been destroyed?
idleThreads	Number of threads sitting idle.
maxIdleThreads	Maximum number of threads ever idle at one time.
maxIdleTimeMs	Maximum time in ms that a thread may be idle before it is reclaimed.
maxThreads	Maximum number of threads in the pool.
maxUsedThreads	Maximum number of threads ever in use at one time.
minThreads	Minimum number of threads in the pool.
name	Name of the running thread.
startTime	Start time.
started	Has the threadpool been started?
threads	Current size of the threadpool.
usedThreads	Number of threads currently in use.

name=RDP,RDP=RDPHandler

RDPHandler MBean. Provides the initial ERP handler for the RDP. Select between AAA and Profile requests.

SESM Applications Using this MBean

RDP.

Table A-47 RDPHandler MBean Attributes

Attribute	Explanation
aaaHandler	The name of the ERP handler for AAA requests.
name	The name of this handler.
profileHandler	The name of the ERP handler for Profile requests.
started	True if this component is started.

name=RDP,PROFILE=DESSProfileHandler

DESSProfileHandler MBean. Handler for Profile request backed by DESS. Uses the ObjectClass to select a the actual Profile Handler.

SESM Applications Using this MBean

RDP.

Table A-48 DESSProfileHandler MBean Attributes

Attribute	Explanation
dontCopyAttributes	Array of attributes not to copy from a request to a response.
name	The name of this handler.
password	Password required for all profile requests. This password should only be set if all profile requests have the same password.
profileMap	Map of DESS ObjectCLass name to ERPHandler name used to select the ERPHandler for a particular profile type.
started	True if this component is started.

name=SSG

The SSG MBean configures the SSG connections.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, NWSP Portal.

Table A-49 SSG MBean

Attribute Name	Explanation
ssgippolicyclass	Sets the policy to use for mapping SSGs to subscribers. Installed default: com.cisco.sesm.ssg.DefaultSSGIPPolicy The DefaultSSGIPPolicy is implemented using the attributes described in the rest of this table. Other policies are subsets of DefaultSSGIPPolicy. Deployers might also implement customized policies of their own. See the javadoc for more information.
port	The global value for RADIUS ports on the SSG hosts. This value must match the value configured on the SSG device using the following command: `ssg radius-helper` *`authenticationPort`* You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.
timeoutsecs	The number of seconds NWSP waits before timing out RADIUS packets that it sends to SSG. You cannot override this global value. Installed default: 5
retries	The number of times NWSP resends a RADIUS packet to SSG if no response is received. You cannot override this global value. Installed default: 3
secret	The global value for the RADIUS protocol shared secret used for communication between NWSP and the SSGs. This value must match the value entered on the SSG device using the **ssg radius-helper key** command. You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.
mask	The global value for the mask that NWSP applies to incoming subscriber IP addresses to derive an IP address for the SSG. You can create subnet entries in the MBean configuration file to override this global value for specific subnets.
generateMessage Authenticators	When this attribute is true, NWSP adds the RADIUS Message-Authenticator attribute (attribute number 80) to access requests it sends to SSG. The RADIUS Message-Authenticator attribute resolves the following vulnerabilities in SESM solutions: • Integrity of packets sent between SESM solution components— Message authentication verifies that the contents of packets are not altered during transmission. • Verification of Account-Status-Requests sent in ACCESS-REQUEST packets by SESM to SSG—These requests do not contain a User-Password attribute; therefore, it is not possible to verify that the sender knows the shared secret.

Table A-49 SSG MBean (continued)

Attribute Name	Explanation
send_framed_ip	When this attribute is true, NWSP includes the RADIUS Framed-IP-Address attribute in requests it sends to SSG. Set this attribute to true when SSGs are being load balanced by a RADIUS Load Balancer (RLB). The attribute is required by the RLB to implement the load balancer's stickiness feature. When this attribute is true, SESM sets the Framed-IP-Address to the value of the client IP address. The request is sent through the RLB, and the RLB routes the request and reply to the appropriate SSG. This feature does not work with port-bundle host key, because in that case, the client IP address is obscured and not available for insertion.
throttle	The global value for the maximum number of simultaneous requests that SESM portals can send to an SSG. The RADIUS protocol queues additional requests and issues them as the SSG returns responses or timeout messages for previous requests. If set correctly, this throttle attribute prevents the situation in which the SSG receives requests at a faster rate than it can handle, causing the SESM application to time out waiting for responses. Set the throttle value according to the ability of the SSG device to process access requests from a client. If the SESM portal times out while waiting for responses from the SSG, try adjusting this value lower. Installed default: 255
bundle_length	The global value for the port bundle length that SSGs use when the port-bundle host key feature is enabled. The port bundle length is the number of bits that SSG uses to indicate bundled slots. For example, a value of 4 indicates 16 bundled slots. This value must match the value used in the following command on the SSG host: `ssg port-map` *`length`* Default: You set this value during installation
port_bundle_ host_key_ switch	The global value indicating whether or not the port-bundle host key feature is enabled on the SSGs. If BUNDLE_LENGTH is zero, then the value of this switch is important. • true—The SSGs have port-bundle host key enabled with a 0 bundle length. This is the case for persistent conditions. • false—The SSGs do not have port-bundle host key enabled. • If BUNDLE_LENGTH is non-zero, this switch is ignored, because a nonzero value implies the use of the host key feature.
min_local_port max_local_port	Together, these two attributes specify a range of UDP ports for RADIUS protocol requests from the SESM portal application to the SSG. By using these attributes, you restrict the source ports used by NWSP to only the ports in the specified range. For example, you might want to restrict port usage if a firewall separates SESM from other components. In that case, you can configure the firewall to allow traffic through the specified range of ports. You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.

Table A-49 SSG MBean (continued)

Attribute Name	Explanation
ID_TIMEOUT	The time in milliseconds to wait for a RADIUS ID to become available. A value of 0 indicates that the pool returns immediately with an error if there is no ID available. Default: 0

Subnet entries use positional arguments.	The format for a subnet entry is:
	`<Call name="setSubnetAttribute">`
	`<Arg>`*`subnetAddress`*`</Arg>`
	`<Arg>`*`subnetMask`*`</Arg>`
	`<Arg>`*`argumentName`*`</Arg>`
	`<Arg>`*`argumentValue`*`</Arg>`
	`</Call>`
	The call to setSubnetAttribute has four positional arguments:
	1. *subnetAddress* is the subnet for which you are explicitly setting a value, overriding the globally set value.
	2. *subnetMask* is the mask that can be applied to the subscriber's IP address to derive the subnet.
	3. *argumentName* is the argument that you are explicitly setting:
	– PORT
	– MASK
	– SECRET
	– BUNDLE_LENGTH
	– IP
	– THROTTLE
	– SESSION_LOCATION and SESSION_BRAND
	– MIN_LOCAL_PORT and MAX_LOCAL_PORT
	– ID_TIMEOUT
	4. *argumentValue* is the value for *argumentName*.
	Note SESSION_LOCATION cannot be used if you use PBHK.

RX_BUF_SIZE	Desired size of socket receive buffer. Set the value to 0 to use the system default. The recommended size is 32767.
TX_BUF_SIZE	Desired size of socket transmit buffer. Set the value to 0 to use the system default. The recommended size is 32767.

name=SESM

SESM MBean. Allows you to configure settings and to view statistics for the SESM model.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal.

Table A-50 SESM MBean Attributes.

Attribute	Explanation
activeAuthenticatedSessions	Active authenticated sessions.
activeSessions	The current number of active sessions.
authenticatedSessions	Authenticated sessions
authenticationFailures	Authentication failures
authenticationSPI	AuthenticationSPI classname.
authenticationTime	Authentication time.
authorizationSPI	AuthorizationSPI classname.
authorizationTime	Authorization time.
autoConnect	Specifies if SESM should send connection requests to SSG for the services marked for auto connection in the subscriber's profile. Values are: • false—SESM does not send connection requests to SSG • true—SESM sends connection requests to SSG In RADIUS deployment option, set this attribute to false, because SSG automatically makes the connections immediately after authentication. You do not need SESM to request those connections. In an SPE deployment, the SSG performs automatic connections if it obtains a service list from the RDP. If SSG does not obtain the service list from RDP, you should set this attribute to true.
confirmMutexDisconnect	Controls the action of the SESM portal if a subscriber is currently connected to a service in a mutually exclusive service group and then selects another service in that group. • true—The SESM portal displays an error message to the subscriber stating that the current service must be disconnected before selecting the newly selected service. • false—The SESM portal sends a request to SSG to disconnect the current service before sending the request to connect to the newly selected service. Installed default: false
hardEntries	The current number of sessions in the hard cache.
ipassOn	When true, iPass functionality is allowed for the NWSP portal. The default value is false. **Note** This attribute is relevant *only* for NWSP application.
ipassProxyIdentity	The prefix to be used for logon to NWSP. The default is "IPASS/". This attribute is also used to identify iPass users and assign a different authorization procedure and permissions for them. **Note** This attribute is relevant *only* for NWSP application.
maxSessions	The maximum number of sessions that were ever active at once.
memRequired	This attribute is no longer used and always shows a value of 0.
mode	No longer used.
modeNames	No longer used.
modes	No longer used.

Table A-50 SESM MBean Attributes. (continued)

Attribute	Explanation
profileCachePeriod	The profile timeout period. This is the minimum amount of time in seconds that a service or group object must be idle in the cache before its resources are deallocated from memory. **Note** Setting this parameter to 0 will disable clearing of the cache. Installed default: 30 seconds
serviceConnectionSPI	ServiceConnectionSPI classname.
serviceProfileSPI	ServiceProfileSPI classname.
sessionCachePeriod	The session timeout period in seconds. This is the minimum amount of time that the session can be in memory without being accessed before timeout occurs. If this value is 0 or undefined, the application calculates a value as: profileCachePeriod * 2. The session cache is checked only when the profileCachePeriod elapses. With the default settings of profileCachePeriod and sessionCachePeriod, sessions time out some time between 2 and 3 minutes after no subscriber activity. When using whitelists, it is recommended to increase the value for Captive Portal to 300 (5 minutes). Installed default: 120 (2 minutes)
sessionCacheSize	The size of the hard session cache. Sessions in the hard cache are not removed by garbage collection.
sessions	Descriptions of all the currently active sessions.
singleSignOn	Enables or disables the single sign-on (SSO) feature. • true—Subscribers only need to authenticate during a session. Single sign-on offers the following advantages: – Subscribers can stop the browser or navigate away from NWSP, and then return to the SESM pages later and not be required to reauthenticate. – Subscribers do not need to reauthenticate if SESM automatic memory management clears sessions from the SESM portal. – Point-to-point protocol (PPP) clients do not need to authenticate to the SESM portal. Instead, the SESM portal uses the PPP authenticated identity from SSG. • false—Subscribers are required to reauthenticate for all the cases described above. **Note** When you disable singleSignOn, it will only take effect after the current session expires. Installed default: true
totalSessions	The number of sessions that have ever been active.

name=SESMDemoMode

The SESMDemoMode MBean configures SESM in a demo installation. Table A-51 describes the attributes in the SESMDemoMode MBean.

Table A-51 SESMDemoMode MBean

Attribute Name	Explanation
demoDataFile	Specifies the file that contains data for Demo mode. The installed value is: *application.home*/config/aaa.properties Where: *application.home* is a system property The SESM start script derives the value for application.home from an expected (installed) directory structure. To change the value of application.home, edit the start script.

name=Version

Version MBean. Allows you to get the package version of the jar file for the SESM model.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, Message Portal, NWSP Portal.

Table A-52 Version MBean Attributes.

Attribute	Explanation
modelJarVersion	modelJar version.
verbose	Set this attribute to true for a verbose listing of the package versions.
version	Version.

name=WebApp

Web applications MBean. Allows you to configure different aspects of the behavior of the SESM web applications. Table A-53 explains configuration attributes in the WebAppMBean.

SESM Applications Using this MBean

Captive Portal, Web Services Gateway, NWSP Portal.

Table A-53 WebAppMBean Attributes

Attribute Name	Explanation
Attributes for NWSP	
confirmAtServiceLogon	Controls whether or not NWSP prompts the user for confirmation before it acts on a request to start a service. Default: FALSE

Table A-53 WebAppMBean Attributes (continued)

Attribute Name	Explanation
confirmAtServiceLogoff	Controls whether or not NWSP prompts the user for confirmation before it acts on a request to disconnect a service. Default: TRUE
confirmAtAccountLogoff	Controls whether or not NWSP prompts the user for confirmation before it acts on a request to log off of the SESM application. Default: TRUE
disconnectWhenUnsubscribe	Controls whether SESM requests the SSG to disconnect an existing service connection if the subscriber unsubscribes from that service. Applies to SPE deployments only.
sessionTimeOut	The number of seconds of inactivity allowed before NWSP closes a session. This value overrides the timeout value in the nwsp.jetty.xml file. Default: 7200
usernameMinLength usernameMaxLength passwordMinLength passwordMaxLength	These attributes control the length of usernames and passwords. A value of 0 is valid for usernameMinLength and passwordMinLength. Configuration files from SESM releases earlier than Release 3.1(7) that use the credentialMaxLength attribute are valid. The value in credentialMaxLength sets usernameMaxLength and passwordMaxLength values. Defaults for usernameMinLength and passwordMinLength: 1 Defaults for usernameMaxLength and passwordMaxLength: 30
addDimension entries	You can create arbitrary attributes and associate them with subscriber requests in the manner described in *Cisco Subscriber Edge Services Manager Web Portals Guide*.
showAllowAlwaysOn	When set to true, the NWSP will show the state of the "AllowAlwaysOn" flag (for the Trusted ID authorization feature) in the MyAccount page, and allow the user to change its state. Default: FALSE
enableReplyMessageDisplay	When set to true, RADIUS attribute 18 messages are displayed to the user in the web portal. Default: TRUE
replyMessageDelimiter	Specifies a message delimiter to add as a suffix to RADIUS attribute 18 messages. SSG concatenates multiple reply messages in a RADIUS response. The message delimiter is used to separate multiple attribute 18 messages, and display them separately in the web portal. The delimiter should comply with the Java regular expression format.
Attributes for Captive Portal	
prepaidRedirectionURL	For service redirections when the SSG prepaid feature is enabled, tells NWSP which page to redirect to if the prepaid limit for the requested service is reached. No redirection occurs if this attribute is null or empty. The default value that exists after installation is the NWSP recharge page.
serviceNotGivenURI	For service redirections, tells NWSP which page to redirect to if the HTTP request from the Captive Portal application does not include a service parameter. The default value that exists after installation is the NWSP status page.

Table A-53 WebAppMBean Attributes (continued)

Attribute Name	Explanation
defaultURI	For service redirections, tells NWSP which page to redirect to if: • The service specified in the HTTP request from the Captive Portal application is not available. • The service exists, the subscriber is not subscribed to it, and the subscriber does not have permission to visit the subscription page. • Any other unexpected conditions. The default value that exists after installation is the NWSP home page.
serviceSubscriptionURI	For service redirections, tells NWSP which page to redirect to if the subscriber is not subscribed to the service that is specified in the HTTP request from the Captive Portal application. The default value that exists after installation is: • In a SESM SPE installation, the NWSP subscriptionManage page. • In a SESM RADIUS installation, the NWSP displays the page specified in the defaultURI attribute.
noSubscribePermissionURI	For service redirections, tells NWSP which page to redirect to if the subscriber is not subscribed to the requested service and: • The application is running in a SESM RADIUS installation, or • The application is running in a SESM SPE installation, and the subscriber does not have the permission to self-subscribe to services. The default value that exists after installation is the NWSP home page.
serviceStartURI	For service redirections, tells NWSP which page to redirect to when the service in the HTTP request from the Captive Portal application does not require service logon. The default value that exists after installation is the NWSP serviceStart page.
serviceLogonURI	For service redirections, tells NWSP which page to redirect to when the service in the HTTP request from the Captive Portal application requires service logon credentials. The default value that exists after installation is the NWSP serviceLogon page.
serviceComparator	Tells NWSP how to order a service list. You can order a list in one of two ways: • Alphabetically by description, or • Alphabetically by name The default setting is to leave the service list unordered.

org.mortbay.jetty MBeans

Debug=0

Debugging and Defensive programming support. The Debug MBean enables or disables the Jetty server debugging mechanism. Table A-54 describes the attributes in the DebugMBean.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT.

Table A-54 Jetty Container—Debug MBean

Attribute Name	Explanation
debug	Controls whether or not debugging messages are produced. Installed default: false
debugPatterns	By specifying one or more patterns, you turn on a filtering mechanism that excludes any message that does not match the pattern. The patterns are file, class, or method names. Pattern matching is based on substring matches. For example, if you specify the pattern RADIUS, the software focuses on RADIUS messages. To specify multiple patterns, separate the patterns using a comma. Installed default: empty
verbose	Specifies the level of detail reported in debugging messages. The range of allowed values is 0 (no details) to 255 (all details). Installed default: 0
suppressStack	Controls whether or not stack information is included in debug messages. Installed default: false
suppressWarnings	Controls whether or not warning messages are included in debug messages. Installed default: false

name=Log

The org.mortbay.util.Log logging service. This object allows LogSink instances to be added. MBeans for the LogSinks are created by this object. The Log MBean enables the Jetty server debugging and logging mechanisms and configures the information that appears in the jetty log file. Table A-55 describes the attributes in the Log MBean.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT.

Table A-55 Jetty Container—Log MBean

Attribute Name	Explanation
logTimezone	Installed default: empty
logDateFormat	Controls the format of the date stamp in the log messages. Installed default: yyyyMMdd:HHmmss.SSS

Table A-55 Jetty Container—Log MBean (continued)

Attribute Name	Explanation
logLabels	Controls whether or not the log messages include frame details. Installed default: false
logOneLine	Installed default: false
logStackSize	Controls whether or not the log messages include an indication of stack depth. Installed default: false
logStackTrace	Controls whether or not the log messages include trace information. Installed default: false
logTags	Installed default: true
logTimeStamps	Installed default: true
append	Indicates if messages overwrite existing contents (false) or are appended to the existing file (true). Installed default: true
retainDays	Indicates the number of days to keep an old log file before deleting it. Installed default: 31
filename	Specifies the log filename and path, as follows: *application.home*/logs/*yyyy_mm_dd*.jetty.log Where: • *application.home*—A property whose value is set in the SESM start script. • logs—A constant. All log files appear in the logs subdirectory under the application directory. • *yyyy_mm_dd*—The year, month, and day that the file was created. • .jetty.log—A constant identifying the Jetty log files.

name=Jetty,NCSARequestLog=0,Server=0

http Request logger providing the normal or extended NCSA format.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT.

Table A-56 http Request logger MBean Attributes

Attribute	Explanation
append	If true append to existing log file, else rename them.
datedFilename	The current dated filename in use.
extended	If true, use the extended NCSA format.
filename	File name
logDateFormat	Date format to use in the log.
logTimeZone	Timezone to use for formatting log dates.

Table A-56 http Request logger MBean Attributes (continued)

Attribute	Explanation
retainDays	Days to return old log file. If 0, files are kept forever.
started	True if the instance has been started and is still running.

name=Log,OutputStreamLogSink=0

A LogSink that writes messages to a OutputStream or File.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT.

Table A-57 LogSink MBean Attributes

Attribute	Explanation
append	If true, log existing log files are appended to.
datedFilename	Dated file name.
filename	The filename to log to. If the filename contains the string yyy_mm_dd, then the log is rolled over every midnight to a new file named with the date.
flushOn	If true, the log is flushed on every log entry.
logDateFormat	The SimpleDateFormat string to use for formatting log messages.
logLabels	If true, the Frame details are added when formatting messages.
logOneLine	If true, log messages are formatted onto a single line.
logStackSize	If true an indication of stack depth is added when formatting messages.
logStackTrace	If true, a stack trace is added to every logged message.
logTags	If true, the tag is added when formatting messages.
logTimeStamps	If true, timestamps are added when formatting messages.
logTimezone	The timezone to use for formatting log messages.
retainDays	The number of days to retain old log files before deleting them.
started	True if the instance has been started and is still running.

name=Jetty,Server=0,

Jetty HTTP Server and Servlet container. The Server MBean configures a request log, which records all incoming HTTP requests. Table A-58 describes the attributes in the Server MBean.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT.

Table A-58 Jetty Container—Server MBean

Attribute Name	Explanation
RequestLog	Creates a new class with one argument, which specifies the name and location of the request log. The installed value is: *application.home*/logs/*yyyy_mm_dd*.request.log Where: • *application.home*—A property whose value is set in the SESM start script. • logs—A constant. All log files appear in the logs subdirectory under the application directory. • *yyyy_mm_dd*—The year, month, and day that the file was created. The installation program uses the appropriate path name delimiter for the installation platform. • .request.log—A constant identifying an HTTP request file.
retainDays	Indicates the number of days to keep a log file before deleting it. Installed default: 90
append	Indicates whether or not to append messages to an existing file or to create a new file for each application instance. Installed default: true
<Call addWebApplication>	This call adds the SESM application to run on the web server. It uses five positional arguments: 1. The first positional argument specifies the virtual host name for the web server application. 2. The second positional argument specifies the context path for locating the web server application. For example, / or /pathname/*. 3. The third positional argument identifies the location of the application. The value is: *application.home*/webapp Where *application.home* is a system property whose value is set in the start script. 4. The fourth positional argument identifies the location of the webdefault.xml file for this application. The value is: *jetty.home*/config/webdefault.xml Where *jetty.home* is a system property whose value is set in the start script. 5. The fifth positional argument specifies whether or not web archive (WAR) files are used. Valid values are TRUE and FALSE. The first three arguments define the location of the web server application. `host/context/application` The SESM start script derives the values for *application.home* and *jetty.home* from an expected (installed) directory structure. To change these values, edit the start script.

name=Jetty,Server=0,WebApplicationContext=0, context=/

A J2EE Web application extension of ServletHttpContext. Changes made to this MBean are not persisted.

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, Message Portal, NWSP Portal, CDAT.

Table A-59 J2EE Web application extension MBean Attributes

Attribute	Explanation
WAR	The WAR file or directory as a URL or filename.
classPath	The path to load classes for this context from.
contextPath	The URL prefix of this context.
defaultsDescriptor	The XML resource defining the default configuration for the context.
deploymentDescriptor	The XML resource defining the specific configuration of the context.
displayName	The display name of the web application context.
extractWAR	If true, packed WAR files are extracted to a temp directory.
handlers	HttpHandlers for this context.
hosts	An array of real host aliases that this context will accept requests from. A requests are expected if null or empty.
maxCacheSize	The maximum size in bytes of the resource cache.
maxCachedFileSize	The maximum size in bytes of a file that cab be cached.
mimeMap	Context specific map of file extension to MIME type.
realm	The instance of the security realm for the context.
realmName	The name of the security realm for the context.
redirectNullPath	If true requests to /context path are redirected to /contextpath/
requestLog	The request log for the context.
requests	Number of requests since statsReset() called. Undefined if setStatsOn(false).
requestsActive	Number of requests currently active. Undefined if setStatsOn(false).
requestsActiveMax	Maximum number of active requests since statsReset() called. Undefined if setStatsOn(false).
resourceBase	The file or URL to use as a prefix to all resource lookups within the context.
responses1xx	Number of responses with 1xx status (Informal) since statsReset() called. Undefined if setStatsOn(false).
responses2xx	Number of responses with 2xx status (Success) since statsReset() called. Undefined if setStatsOn(false).
responses3xx	Number of responses with 3xx status (Redirection) since statsReset() called. Undefined if setStatsOn(false).
responses4xx	Number of responses with 4xx status (Client Error) since statsReset() called. Undefined if setStatsOn(false).
responses5xx	Number of responses with 5xx status (Server Error) since statsReset() called. Undefined if setStatsOn(false).
started	True if the instance has been started and is still running.

Table A-59 J2EE Web application extension MBean Attributes (continued)

Attribute	Explanation
statsOn	True if statistics collection is turned on.
statsOnMs	Time in Milliseconds that stats have been collected for.
virtualHosts	An array of virtual host aliases that this context is registered against.
welcomeFiles	Array of welcome file names.

name=jetty,SESMSSLListener=0,Server=0

com.cisco.sesm.jetty.SESMSLListenercom

SESM Applications Using this MBean

Application Manager, Captive Portal, Web Services Gateway, NWSP Portal, CDAT.

Table A-60 SESMSLListener MBean Attributes

Attribute	Explanation
bufferReserve	Buffer reserve.
bufferSize	Buffer size.
confidentialPort	Port to redirect for confidential connections. 0 if not supported.
confidentialScheme	Protocol to use for confidential redirections.
defaultScheme	The protocol expected for connections to this listener.
host	Host or IP listening interface.
idleThreads	Number of idle threads.
integralPort	Port to redirect to for integral connections. 0 if not supported.
integralScheme	Protocol to use for integral redirections.
keyPassword	Key password.
keystore	Name of the Key Store file.
lingerTimeSecs	The maximum time in seconds that a connection lingers during close handshaking.
lowOnResources	True if listener is low on resources.
lowResourcePersistTimeMs	Time in ms to persist idle connections if low on resources.
maxIdleTimeMs	Time in MS that a thread can be idle before it mat expire.
maxThreads	Maximum number of threads allowed.
minThreads	Minimum number of threads allowed.
name	Name of the pool.
needClientAuth	If true, client certificates are requests.
outOfResources	True if listener is out of resources.
password	Password for SSL Key Store.
poolName	Pool name.
port	The listening port number.

Table A-60 SESMSLListener MBean Attributes (continued)

Attribute	Explanation
started	True if the instance has been started and is still running.
threads	Number of thread instances.

name=Jetty,SESMSocketListener=0, Server=0

com.cisco.sesm.jetty.SESMSocketListener

SESM Applications Using this MBean

Application Manager, Captive Portal, Message Portal, CDAT.

Table A-61 SESM Socket Listener MBean Attributes

Attribute	Explanation
bufferReserve	Buffer reserve.
bufferSize	Buffer size.
confidentialPort	Port to redirect to for confidential connections. 0 if not supported.
confidentialScheme	Protocol to use confidential redirections.
defaultScheme	The protocol expected for connections to this listener.
host	Host or IP of listening interface.
idleThreads	Number of idle threads.
integralPort	Port to redirect to for integral connections. 0 if not supported.
integralScheme	Protocol to use for integral redirections.
lingerTimeSecs	The maximum time in seconds that a connection lingers during close handshaking.
lowOnResources	True if listener is low on resources.
lowResourcePersistTimeMs	Time in ms to persist idle connections if low on resources.
maxIdleTimeMs	Time in MS that a thread can be idle before it may expire.
maxThreads	Maximum number of threads allowed.
minThreads	Minimum number of threads allowed.
name	Name of the pool.
outOfResources	True if the listener is out of resources.
poolName	Pool name.
port	The listening port number.
started	True if the instance has been started and is still running.
threads	Number of thread instances.

name=WebProxyHandler, name=SesmWebProxyHandler

Used to configure whitelists and blacklists. The WebProxyHandlerMBean is the parent class for SesmWebProxyHandlerMBean, which in turn is the parent class for CPProxyHandlerMBean (used by Captive Portal) and AccountWebProxyHandlerMBean (used by Web Proxy). The attributes and operations described in Table A-62 are valid for all these MBeans.

SESM Applications Using this MBean

Captive Portal, Web Proxy.

Table A-62 Attributes for the WebProxyHandler MBean and SesmWebProxyHandler MBean

Attribute	Explanation
started	True if the instance has been started and is still running.
hostGroups	Map of names of host groups to arrays of hostnames and IPs.
hostGroupsView	View map of names of host groups to arrays of hostnames and IPs.
proxyHostsWhiteList	Default array of hostnames and IPs that are proxied.
proxyHostsWhiteLists	Map of keys to arrays of hostnames and IPs that are proxied. See the defaultAllowed attribute if the map is empty.
proxyHostsWhiteListsResView	View map of keys to arrays of hostnames and IPs that are proxied. This resolved map is used to look up hosts. It replaces any host group keys found by the corresponding hosts. See the defaultAllowed attribute if the map is empty.
proxyHostsWhiteListsView	View map of keys to arrays of hostnames and IPs that are proxied. This map stores the configured white lists. See the defaultAllowed attribute if the map is empty.
proxyHostsBlackList	Default array of hostnames and IPs that are not proxied.
proxyHostsBlackLists	Map of keys to arrays of hostnames and IPs that are not proxied.
proxyHostsBlackListsResView	View map of keys to arrays of hostnames and IPs that are not proxied. This resolved map is used to look up hosts. It replaces any host group keys found by the hosts for the host group.
proxyHostsBlackListsView	View map of keys to arrays of hostnames and IPs that are not proxied. This map stores the configured black lists.
sesmHostList	Array of known SESM hosts names and IPs. Any hosts in this list are always proxied to if the sesmHostsAllowed attribute is set to true.
sesmHostsAllowed	Set to true if SESM hosts are always proxied to for proxy requests, regardless of white/black lists.
defaultAllowed	If set to true and if there are no white lists, then all hosts are proxied to, as long as they are not blocked by the black lists. This is set to false for Captive Portal and set to true for Web Proxy.
proxyMetaDataPort	The port to send proxy meta data requests.

Table A-62 Attributes for the WebProxyHandler MBean and SesmWebProxyHandler MBean (continued)

Attribute	Explanation
tunnelTimeoutMs	The tunnel timeout in ms for CONNECT request disconnect
start()	Initialize and start the instance.
stop()	Stop the instance.
sesmSessionEnabled	When set to true, handling of SESMSession is enabled.
defaultListKeyIncluded	When set to true, the default list key is always included to look up lists.
locationInvariant	When set to true, the location is cached in the SESMSession. This attribute is set to true by the installation when you use IPHK. This attribute is set to false by the installation when you use PBHK. This gives more accurate location resolution, but might affect performance.
portKeyIncluded	When set to true, the listener port key is always included to look up lists.
handledMimeTypes	Get MIME-types for which there are interactions with the gateway. When using locations and PBHK, these requests result in a combined query to the gateway to check if the location has changed. Also in the case of Captive Portal, handshake with the gateway occurs to indicate a proxy user.
extensionsExclusionList	Get MIME-type extensions for which there are no interactions with the gateway. These exclusions only work if handledMimeTypes is empty. This attribute is deprecated in SESM 3.3(1) and will be removed after the following two releases.
allowedPorts	The allowed ports for the proxy server to proxy to. These are used for: • Secure proxy requests. • All proxy requests to hosts in the SESM host list. • standard proxy requests to remote hosts, but with everything above 1024 allowed. The default http port (80) is always allowed. Allowed ports must include listener ports for web portals and must not include listener ports for Captive Portal or Web Proxy.

name=CPProxyHandler

Table A-63 describes additional attributes and operations for the CPProxyHandler MBean, in addition to those described in Table A-62.

SESM Applications Using this MBean

Captive Portal

Table A-63 Additional attributes and operations for the CPProxyHandler MBean

Attribute	Explanation
accountWebProxy	Is account web proxy on gateway enabled.
resourceMap	A map, which if set, maps path suffixes to resources to serve for all requests with those suffixes.
noProxyResource	If non null, this resource is served for proxy requests where the host is not allowed to be proxied to, according to the whitelists and blacklists.
proxyPorts	Get ports which allow proxy handling for non-proxy users. Proxying is independent of the port for proxy users.
closeConnection	When set to true, the connection is closed for all proxy requests to a host in the SESM host list.
proxyLogging	When set to true, this option enables logging of proxy requests. It logs the remote IP address and port with the proxied URL, or if whitelists are in use, the hostkey for the session. As this option has an impact on performance, it is recommended to use it only when using PBHK. Default: FALSE

name=AccountWebProxyHandler

Table A-64 describes additional attributes and operations for the AccountWebProxyHandler MBean, in addition to those described in Table A-62.

SESM Applications Using this MBean

Web Proxy

Table A-64 Additional attributes and operations for the AccountWebProxyHandler MBean

Attribute	Explanation
noProxyResource	If non null, this resource is served for proxy requests where the host is not allowed to be proxied to, according to the whitelists and blacklists.
closeConnection	When set to true, the connection is closed for all proxy requests to a host in the SESM host list.
proxyLogging	When set to true, this option enables logging of proxy requests. It logs the remote IP address and port with the proxied URL, or if whitelists are in use, the hostkey for the session. As this option has an impact on performance, it is recommended to use it only when using PBHK. Default: FALSE
userLogging	When set to true, this option enables logging usernames for proxy requests. This option can be used only when proxyLogging is set to true, and it has a considerable impact on performance. Before enabling this feature, ensure that you comply with all relevant legislation pertaining to privacy and data protection. Default: FALSE

MBean Configuration Methods

Administrators can change SESM application configuration by changing the attribute values in MBeans. In SESM, you can use the following to change MBean attribute values:

- SESM Application Manager (AM)—A web-based GUI tool. This is the preferred way to manage running SESM applications. For information about the Application Manager, see Chapter 10, "Using Application Manager."
- Manually edit the application XML configuration files —Application XML configuration files are located in the application's config directory (for example, nwsp/config/nwsp.xml). If you use this method, you must stop and restart the application for the changes to take effect. See CHAPTER 1
- SESM Agent View—A web-based view of managed resources and associated MBeans. The Agent View is an adaptation of the Management Console provided by the HTML adaptor server, which is included with the Sun example JMX server. The Cisco adaptations add persistence features to the server. See Using Agent View to Configure MBeans, page A-62.
- SESM file poller—Use the file poller to dynamically update location and whitelist configurations. When you update location and whitelist configurations using the SESM file poller, you do not need to restart the applications. For information about the file poller, see Using the File Poller to Update Locations and Whitelist Configurations, page 6-13.

Using Agent View to Configure MBeans

This section describes how to remotely manage SESM applications using the SESM Agent View tool. Topics in this appendix are:

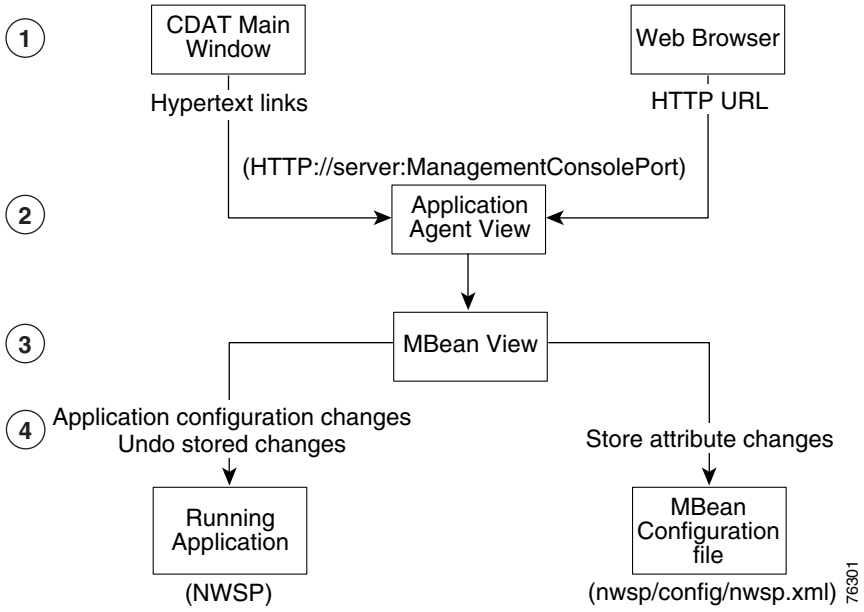
SESM Agent View Overview

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

Note The SESM Agent View is an adaptation of the Management Console provided by the HTML adaptor server, which is included with the Sun JMX server examples. The Cisco adaptations add persistence features to the server.

Figure A-1 summarizes how to access the Agent View for an application (for example, NWSP), and describes the tasks you can perform.

Figure A-1 Agent View Summary



1	Access Agent View—Each SESM application has a management console, known as Agent View. You can access an application's Agent View in two ways: • In CDAT main window—Click a link, if it is configured on the CDAT main window. It is convenient to access the Agent Views for all SESM applications from one list of links. To configure the links to Agent Views, use the CDAT configuration file. • In a browser—Enter the URL for the application's management console in a web browser.
2	Access application MBeans—An application's Agent View lists all the MBeans in the running application. From the Agent View, you can access MBean Views.
3	Access MBean attributes—An MBean View provides access to all the attributes in the MBean.
4	View and configure attributes—From the MBean View, you can perform the following actions on attribute values: • View current attribute values for the running application. • Apply changes to most writable attributes. Applied changes take effect immediately on the running application. • Store changes in the application's configuration file. Stored changes persist for future restarts of the application. • Undo (revert) the running application to the state before the last store. You can undo only the last stored action. The Undo operation applies to the running application only. To persist an undo, you must save the Undo action to the XML configuration files by clicking **Store** after clicking **Undo**. You can reverse a stored undo, if it is the last stored action.

Note You cannot clear MBean attributes in Agent View. To clear an attribute's values, you must configure the appropriate application XML configuration file, and restart the application.

Accessing an Application's Agent View

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

Configuring the ManagementConsole MBean

Each SESM application includes a ManagementConsole MBean, which configures and starts an Agent View for the application. Table A-65 describes the attributes in the ManagementConsole MBean.

Table A-65 SESM Portal Application—ManagementConsole MBean

Attribute Name	Explanation
Port	Specifies the management console port for this application. In the installed configuration files, the port value is a system property named management.portno. All the installed startup scripts set this system property to the value of {application.portno + 100} For example, if the application.portno is 8080, the management.portno is 8180. This runtime setting overrides any value you enter in the configuration file. To change the value of this attribute, edit the start script.
AuthInfo	AuthInfo provides a level of access control on the Management Console. When a user attempts to access the management console port from a web browser, a logon window appears. The user must enter a user ID and password that matches values specified in AuthInfo. Each application has a ManagementConsole MBean that configures the login values for that application's management console. You can configure different user IDs and passwords for each application or use the same values for all applications. You can specify multiple sets of AuthInfo information to allow multiple users access to a management console. The AuthInfo array has two elements: • User ID—Specifies the user ID who has access to the management console. Default: MgmtUser • Password—The password that is required to access the management console. Default: MgmtPassword You can add, change, and delete AuthInfo values in the configuration files or through the management console. **Note** If you use the management console to change or delete the user ID or password that you used to log into the console, the console redisplays the login prompts. You must log in again using the new authentication values.

Starting and Removing the Management Console

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

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

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

URLs for Accessing Agent Views

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

The URL for accessing the Agent View must include the name of the host on which the application is running and the configured management console port number (for example, the value for management.portno). The default URL for the NWSP Agent View, based on default application port 8080, is:

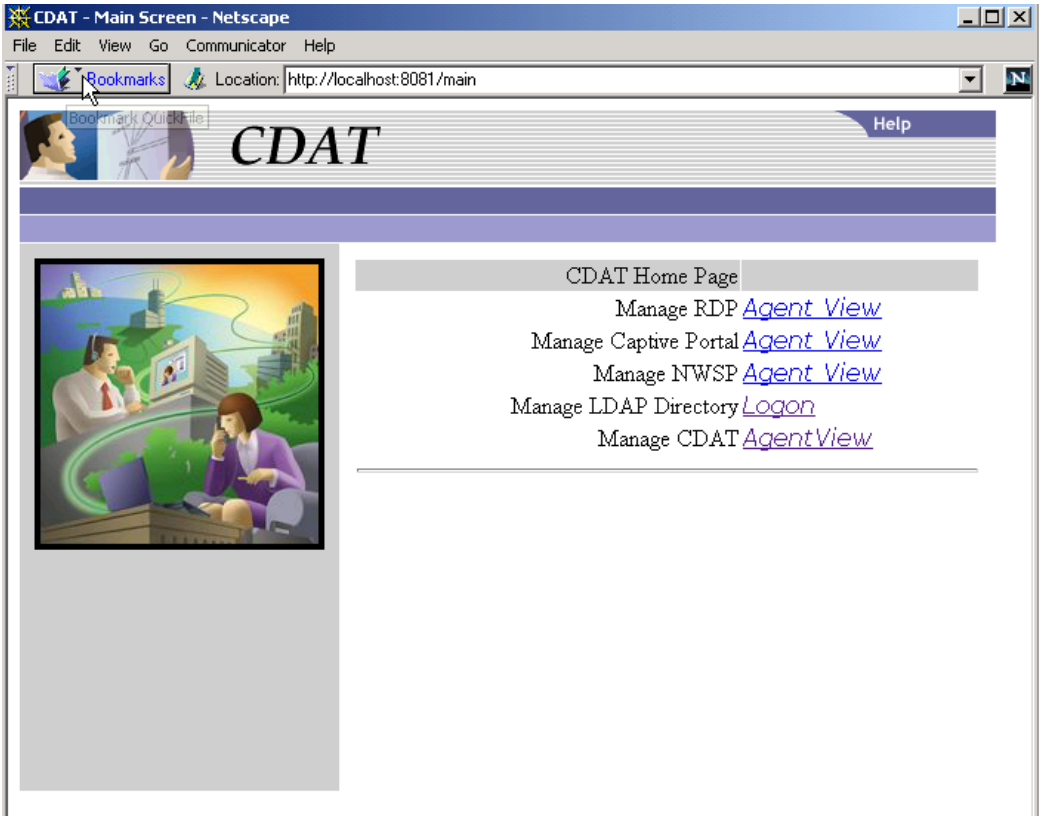
```
http://server1:8180
```

Using the CDAT Main Window to Access Agent Views

The CDAT main window can provide a convenient way to access Agent Views. You can add links to the Agent Views for all the SESM applications that you want to manage. To add links or change the URLs behind the links, edit the links attribute in the MainServlet MBean in the CDAT application's configuration file. See name=MainServlet, page A-28 for details.

Figure A-2 shows an example CDAT main window with links to various Agent View URLs.

Figure A-2 CDAT Main Window



To use the CDAT main window to access an Agent View:

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

```
jetty
    bin
        startCDAT
```

Step 2 Open a web browser.

Step 3 Direct the browser to the CDAT main window. (See Figure A-2.)

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

```
http://<host>:8081
```

where <host> can be an IP or a hostname.

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

Using the Agent View

The Agent View displays the MBeans in a running application. Figure A-3 shows an example of the Agent View for a NWSP application running in a SESM SPE installation.

Figure A-3 Agent View

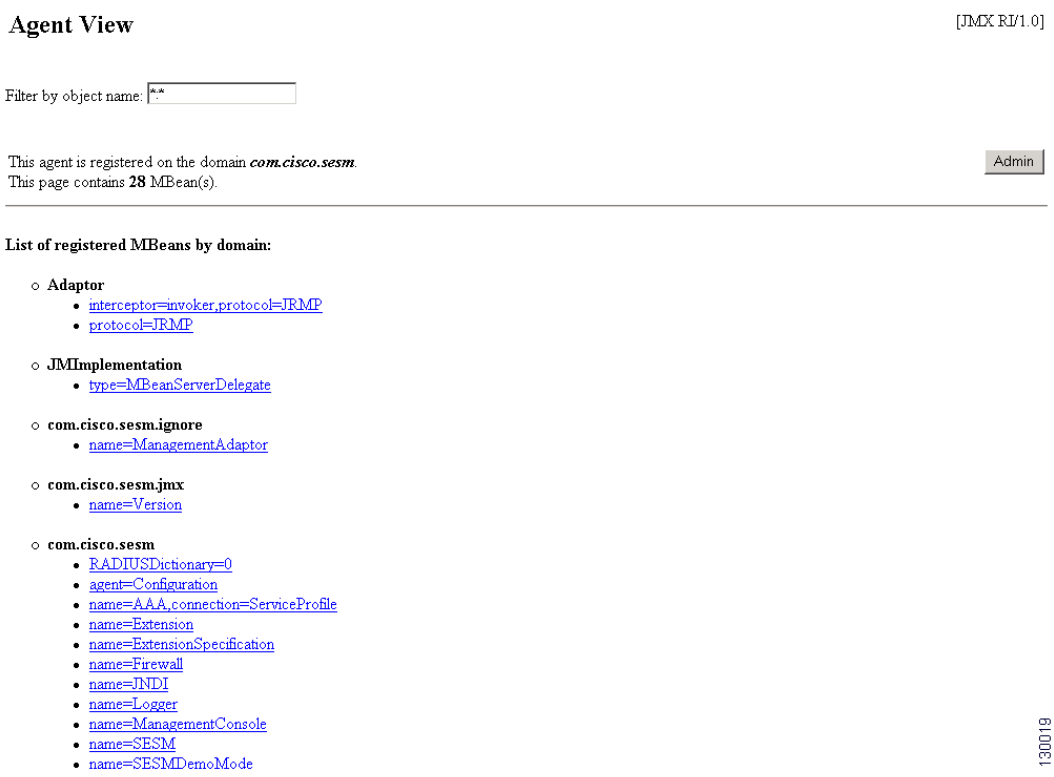


Table A-66 explains the actions you can perform from the Agent View.

Table A-66 Actions from the Agent View

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

Using the MBean View

The MBean View displays the attributes in an MBean. Figure A-4 and Figure A-5 show the MBean View for the WebApp MBean in NWSP. Table A-67, which follows the figures, explains the numbered callouts in these figures.

Figure A-4 MBean View—Top Portion

Figure A-5 MBean View—Bottom Portion

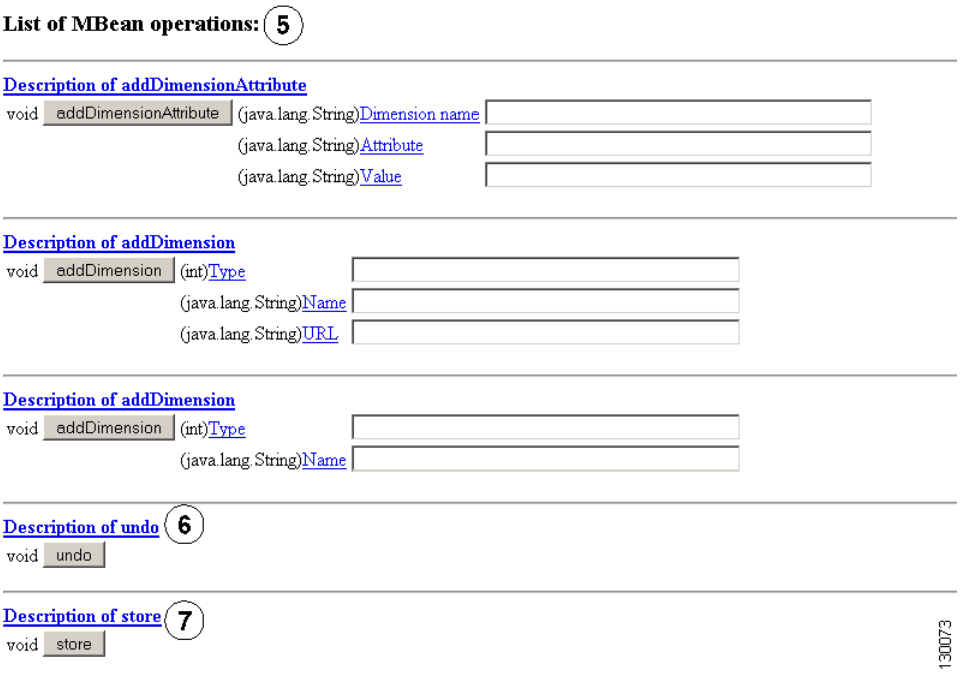


Table A-67 Actions available from the MBean View

Figure Key	Name	Description
1	Reload Period Reload button	A reload obtains new information from the application and reloads the page. • The reload period specifies the number of seconds between automatic page reloads. You can change the reload period here. The change takes effect immediately. • If the reload period is 0 (the default), use the Reload button to manually reload the view.
2	Unregister button	Makes the MBean inaccessible to the running application. Do not use this button.

Table A-67 Actions available from the MBean View (continued)

Figure Key	Name	Description
3	List of MBean attributes	Lists all the attributes in the MBean. From this section, you can: • Display a short description of an attribute—Click the attribute name. • Change the value of read-write attributes • Monitor metrics (read-only attributes) To change an attribute value, do one of the following, depending on the attribute type: • Integers and strings—Type the attribute value in the Value column. • Booleans—Choose the desired radio button. • Arrays: – If the Value column contains the phrase "Type Not Supported"—Choose one of the buttons from the MBean Operations section. – If the Value column contains a hypertext link over the phrase "view the values of *attribute*"—Click the link, which opens another page that lists the array elements and current values. Use the appropriate operation in the MBean Operations section to add or change element values.
4	Apply button	Sends the attribute changes to the running application. The change takes effect immediately on the running application unless you receive an error message stating otherwise.
5	MBean operations	Lists operations that you can perform against the MBean. The list is different for each MBean. However, all MBeans include the Store and Undo operations, described below.
6	Undo button	Reverts the running application to the state before the last store. You can undo only the last stored action. The Undo operation applies to the running application only. To persist an undo, you must save the Undo action to the configuration files by clicking **Store** after clicking **Undo**. You can reverse a stored undo, if it is the last stored action. Table A-68 shows how the Undo operation works.
7	Store button	Saves the attribute changes in the appropriate configuration file (for example, nwsp.xml). This action persists the changes for future application restarts. The Store button has the following effects on the MBean in the configuration file: • Deletes any <SystemProperty> or <Property> tags used in the MBean in the originally-installed configuration file. The Store button saves the currently defined value of all attributes in the MBean, regardless of how those values were derived. The Store operation is not aware of property definitions or values assigned by the startup script. • Deletes comments in the MBean. • Includes all the read-write attributes in the MBean. (The installed configuration files might include only the most commonly modified attributes.) • Deletes a <Call> tag inside a <Configure> tag. If the <Call> element sets an attribute value, the rewritten MBean contains the attribute assignment performed in a different way. However, if the <Call> element performs an action other than setting an attribute value, the action is lost. The correct way to call methods is to use the <Action> tag.

Table A-68 Sequential Store and Undo Operations

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

Monitoring an Application

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

Some useful monitoring features on the MBean View are:

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

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

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

MBean View [JMX RI/1.0]

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

Back to Agent View

Reload Period in seconds: 5 Reload

Unregister

MBean description:

SESM Mode configuration.

List of MBean attributes:

Name	Type	Access	
activeAuthenticatedSessions	int	RO	0
activeSessions	int	RO	0
authenticatedSessions	int	RO	0
authenticationFailures	int	RO	0
authenticationSPI	java.lang.String	RO	com.cisco.sesm.spis.radius.RADIUSAuthe
authenticationTime	long	RO	0
authorizationSPI	java.lang.String	RO	com.cisco.sesm.spis.dess.DESSAuthorizati
authorizationTime	long	RO	0
autoConnect	boolean	RW	○ True ◉ False

76307

SESM Security

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

Java Platform Security References

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

- For Java security software and documentation:

  http://java.sun.com/security/index.html
- For Java authentication and authorization documentation:

  http://java.sun.com/products/jaas/overview.html
- For information related to JDK:

  http://java.sun.com/products/jdk/
- For training:

  http://developer.java.sun.com/developer/onlineTraining/Security/Fundamentals
- For miscellaneous articles:

  http://developer.java.sun.com/developer/technicalArticles/Security/

Using HTTPS in SESM Portals

This section contains the following topics concerning HTTPS:

HTTPS References

HTTPS (Secure Hypertext Transfer Protocol) is HTTP over Secure Sockets Layer (SSL), which are HTTP packets sent as encrypted data. This is the mechanism by which data is securely transmitted over the Internet between a browser client and a server.

SESM implements SSL using the Java Secure Sockets Extension (JSSE). For information about JSSE, go to:

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

The J2EE specifications describe an extension framework for the integration of SSL implementations. For implementations other than JSSE, go to:

http://www.phaos.com/e_security/prod_ssl.html

Keytool and Keystore

The SSL part of HTTPS requires a certificate to generate the encryption key. For the Jetty web server bundled with SESM, the certificate is named keystore and is found in the /etc directory. The keystore file is created by the keytool utility. For detailed instructions on the use of keytool, go to the following URL:

http://java.sun.com/products/jdk/1.3/docs/guide/security/SecurityToolsSummary.html

The sample keystore functions for nonproduction deployments. However, you must obtain a site-specific certificate for production deployments from VeriSign, Inc. at:

http://www.verisign.com

Though certificates are generally the same in concept, they tend to differ in implementation. Therefore, a degree of certificate manipulation is required to obtain a certificate from a given source to work with a given SSL implementation. For JSSE and the Jetty web server, the required steps are described at:

http://jetty.mortbay.com/jetty/doc/SslListener.html

For other implementations, go to:

http://www.openssl.org

The keystore file is a certificate used for secure sockets layer (SSL) encryption. The SSL implementation shipped with SESM is of commercial quality and can use certificates generated by keytool. Keytool resides in the same directory as the JRE.

Caution A keystore is required for deployments that use HTTPS. HTTPS does not function without a valid keystore file. The file included with the installation works, but you should replace it with a keystore valid for your specific deployment.

Configuring NWSP Portal to Run on SSL Ports Only

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

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

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

Note This step applies to the broadband implementation of NWSP Portal only.

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

Step 2 In the Jetty configuration file, comment out or remove the call that starts the standard HTTP listener.

For example, in sp.jetty.xml, surround the Configure tag for the SESMSocketListener for the HTTP port with comment indicators, as shown here:

```
<!-- (start comment)
<Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,SESMSocketListener=0">
    <Set name="port" type="int"><SystemProperty name="application.portno"
        default="8080"/></Set>
    <Set name="minThreads" type="int">50</Set>
    <Set name="maxThreads" type="int">255</Set>
    <Set name="maxIdleTimeMs" type="int">60000</Set>
    <Set name="maxReadTimeMs" type="int">60000</Set>
</Configure>
(end comment) -->
```

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

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

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

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

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

Step 4 If you are running a captive portal solution, change the configured redirections to the NWSP Portal to use the HTTPS protocol and the HTTPS port number for the NWSP Portal.

The HTTPS port will be dynamically calculated based on the PORTNO in the startNWSP.sh script. This is done using the formula:

```
SSLPORTNO = PORTNO - 80 + 443
```

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

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

to

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

Step 5 If you are using the Message Portal application in your captive portal solution, change the configured redirections to NWSP to use the HTTPS protocol and the HTTPS port HTTPS port number for the NWSP Portal.

The HTTPS port will be dynamically calculated based on the PORTNO in the startNWSP.sh script. This is done using the formula:

```
SSLPORTNO = PORTNO - 80 + 443
```

Step 6 In messageportal.xml, change the following lines:

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

to:

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

Configuring a Tomcat Container for SESM

This chapter contains the following topics:

J2EE Containers

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

Container Requirement for the Port-Bundle Host Key Feature

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

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

Creating WAR Files for Containers Other Than Jetty

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

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

For instructions about deploying an application using a WAR file, see the documentation for the container you are using. Also, consider the following points:

- The installed configuration is specific to a Jetty container. If you choose to deploy the SESM web applications in a container other than Jetty, you must make changes to the container MBeans. For example, you must change class or object names. You might need to add MBeans.
- Web containers might use their own JSP engine, so the installed precompiled JSPs for the SESM web applications cannot be used.

Configuring a Tomcat Container

This section describes how to use an installed SESM web application in a Tomcat container from the Apache Software Foundation. Tomcat is the servlet container used in the official reference implementation for the Java servlet and JavaServer Pages technologies, developed by Sun under the Java Community Process. For more information and to obtain the Apache Tomcat software, see:

http://jakarta.apache.org/tomcat/

The recommended release for use is Tomcat 4.1.27.

Note This release of SESM does not work with Tomcat 5.x. SESM uses the Servlet 2.3 and JSP1.2 APIs, while Tomcat 5.x implements the Servlet 2.4 and JSP2.0 specifications.

The following procedure describes configuring a Tomcat container for the NWSP web portal application. You must configure a Tomcat container for each web application required.

Step 1 Install Tomcat from the following location.

```
http://jakarta.apache.org/tomcat
```

Step 2 Install SESM and a JDK, as described in the *Cisco Subscriber Edge Services Manager Installation Guide*.

Step 3 Using the **jar** command from the previously installed JDK, create a ROOT.war file from NWSP.

```
cd $SESM/nwsp/webapp
jar cvf ../ROOT.war *
```

Step 4 Go to the Tomcat home directory.

```
cd $CATALINA_HOME
```

Step 5 Remove (rename) the Tomcat default ROOT directory in webapp.

```
mv webapps/ROOT webapps/ROOTorig
```

Step 6 Make the NWSP the default webapp.

```
cp $SESM/nwsp/ROOT.war webapps
```

Step 7 Make an NWSP home directory for config and logs.

```
mkdir nwsp
```

Step 8 Make a NWSP log directory.

```
mkdir nwsp/logs
```

Step 9 Copy the nwsp configuration directory from the SESM directory into the tomcat directory.

```
cp -r $SESM/nwsp/config nwsp
```

Step 10 Add the permissions required for SESM to run as a ROOT web application.

c. Go to $CATALINA_HOME.

d. Edit the conf/catalina.policy file.

e. Add the following section, which gives permission for SESM applications to run as ROOT web applications.

```
// Permissions required for SESM running as ROOT web application
grant codeBase "file:${catalina.home}/webapps/ROOT/WEB-INF/-" {
//permission java.security.AllPermission;
permission java.net.SocketPermission "*",
"accept,connect,listen,resolve";
permission java.io.FilePermission "/-", "read,write,delete";
};
```

Step 11 Increase the heap sizes reserved for Tomcat. The heap size is taken from the environment variable, so at the terminal, enter:

```
setenv JAVA_OPTS="-Xms64m -Xmx64m"
```

Step 12 Unpack the WAR file:

a. Run Tomcat:

```
bin/startup.sh
```

b. Verify that the ROOT directory has been created in $CATALINA_HOME/webapps

c. Stop Tomcat

```
bin/shutdown.sh
```

Note These instructions assume that the WAR file is unpacked, which is the default setting in a Tomcat installation. To check the setting, find the following lines in conf/server.xml:

```
<!-- Define the default virtual host -->
<Host name="localhost" debug="0" appBase="webapps" unpackWARs="true">
```

Step 13 Add the general and SESM libraries common to all applications (this list can be verified by checking the class path in jetty/bin/start.sh):

```
cp $SESM/libs/jmx/lib/com.cisco.sesm.jmx.jar common/lib
cp $SESM/libs/logging/lib/com.cisco.sesm.logging.jar common/lib
cp $SESM/redist/jaxp/lib/xalan.jar common/lib
cp $SESM/redist/jce/lib/* common/lib
cp $SESM/redist/jmx/lib/* common/lib
cp $SESM/redist/mx4j/lib/* common/lib
```

Step 14 To ensure that the web application uses the same logging library as configured and used by the MBeans, remove the local library:

```
rm $CATALINA_HOME/webapps/ROOT/WEB_INF/lib/com.cisco.sesm.logging.jar
```

Note The NWSP class loader diverges from the default Java 2 delegation model, in accordance with the servlet specification, version 2.3. Unlike Jetty, it is not possible to configure Tomcat to follow the Java 2 or the servlet 2.3 delegation model. So when a request to load a class from the NWSP class loader is processed, this class loader will look in the local repositories first, instead of delegating before looking.

Step 15 In webapps/ROOT/WEB_INF/web.xml, edit the initParam for application.home of MainServlet. The value provided should be the absolute path of the NWSP home directory for config and logs.
For example:

```
<init-param>
<param-name>application.home</param-name>
<param-value>D:\Tomcat4.0.6\nwsp</param-value>
</init-param>
```

Step 16 (Optional) If running Tomcat from $CATALINA_HOME using bin/startup.sh, then the DESS log is placed in $CATALINA_HOME/logs. To change this log file location to be in a different directory, edit nwsp/config/dessauth.xml. Change the relative path for the DESS log to an absolute path. For example, the following change places the log in nwsp\logs under the Tomcat directory:

```
<Set name="traceFileName">D:\Tomcat4.0.6\nwsp\logs\dess.log</Set>
```

Step 17 (Optional) You do not have to install the SESM application into webapps/ROOT. You can change the application's default context by modifying conf/server.xml.

For example, to use webapps/nwsp rather than webapps/ROOT, follow these steps:

a. Edit conf/server.xml.

b. Find this line:

```
<!-- Tomcat Root Context -->
```

and uncomment the following line.

c. Change:

```
<Context path="" docBase="ROOT" debug="0"/>
```

to

<Context path="" docBase="nwsp" debug="0"/>

Step 18 Run Tomcat.

```
bin/startup.sh
```

Note If only nwsp.war exists at this stage, then the nwsp directory structure is unpacked, but an exception occurs because the nwsp directory did not initially exist. In that case, restart Tomcat and the application will run.

This completes configuration for Tomcat 4.0. If you are configuring Tomcat 4.1.x, continue with the following steps.

Note An unmodified Tomcat 4.1 installation does not work with a SESM WAR file.

Step 19 Disable Tomcat 4.1 JMX MBeans support. Edit conf/server.xml, search for the following lines and comment them out (using <!-- and -->):

```
<Listener className="org.apache.catalina.mbeans.ServerLifecycleListener"debug="0"/>
<Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"
debug="0"/>
```

Note Tomcat 4.1 MBeans support should be disabled, as no default domain has been specified. Many SESM MBeans are instantiated using the appropriate tags in the container-independent configuration. However, certain mechanisms such as that for extensions require self-registering MBeans. For these, SESM requires a default domain of "com.cisco.sesm". This is satisfied as long as the MBeanServer is not instantiated by the Tomcat container rather than by the SESM web application.

Step 20 Enable access (request) logs [optional]. Edit conf/server.xml, search for the following tag and uncomment it (by removing <!-- and -->):

```
<Valve className="org.apache.catalina.valves.AccessLogValve "directory="logs"
prefix="localhost_access_log." suffix=".txt" pattern="common" resolveHosts="false"/>
```

Note Tomcat 4.1 has access logging disabled by default.

Step 21 Enable servlet invocation. Edit conf/web.xml, search for the following lines and uncomment them (by removing <!-- and -->):

```
<servlet-mapping>
    <servlet-name>invoker</servlet-name>
    <url-pattern>/servlet/*</url-pattern>
</servlet-mapping>
```

Note Tomcat 4.1 has the mapping for the invoker servlet removed by default.

Step 22 Tomcat 4.1 uses Jasper 2. The precompiled JSPs in NWSP were produced with Jasper 1. The recommended modification is to follow the instructions in the Tomcat 4.1 release note for using Jasper 1. That is, copy the following Tomcat 4.0.6 files into $CATALINA_HOME/common/lib:

```
$TOMCAT40x_HOME/lib/jasper-runtime.jar
$TOMCAT40x_HOME/lib/jasper-compiler.jar
```

Note An alternative approach is to compile the JSPs at run time, as described in the *Cisco Subscriber Edge Services Manager Web Developer Guide*. In summary, copy web.recompile.xml and web.xml, and restart the server.

However, this last approach may require changes to the TLD descriptors in nwsp/webapp/WEB-INF or to the way the tags are used in the JSPs. The TLDs conform to the ordering of tags as given in the DTD for JSP 1.2 Tag Library Descriptors. They do not as yet include any optional information to validate the conformance of the JSP pages to using this tag library (javax.servlet.jsp.tagext.TagLibraryValidator). Jasper 1 in Tomcat 4.0 version does not validate, while Jasper 2 in Tomcat 4.1 does perform validations.

AR Basic Script for iPass Configuration

This appendix provides an example of a Cisco Access Registrar (AR) extension script, which can be used to facilitate the iPass support in a SESM RADIUS installation with AR. AR 3.5.3 includes a similar script file in the AR installation folder, $INSTALL/contrib/ipass.

Note

- *<item_name>* is a placeholder for an item name. Replace the name and the angle brackets (<>) with the required name.
- When you copy/paste the script below from the PDF format file, the line wrapping translates into additional line breaks. Verify where the line breaks should be and delete any additional line breaks.

```
# IPASS.tcl July 1, 2004
# Copyright (c) 2004 by Cisco Systems, Inc. All rights reserved.
#
# This software contains proprietary information which shall not be
# reproduced or transferred to other documents and shall not be disclosed
# to others or used for manufacturing or any other purpose without prior
# permission of Cisco Systems.
#
#
#
######################################################################
#             Script Installation and Configuration                  #
######################################################################
#
# # Create the script file on the AR machine, example assumes IPASS.tcl is used.
#
# # In aregcmd:
# # Disable the session manager, invoke:
# set /Radius/DefaultSessionManager ""
# # Configure the scripts, invoke:
# add /Radius/Scripts/IPASS-request "" tcl /<script_dir>/IPASS.tcl IPASS-request
IPASS-init <location_delimiter>,<ipass_service_name>
# add /Radius/Scripts/IPASS-response "" tcl /<script_dir>IPASS.tcl IPASS-response
IPASS-init <location_delimiter>,<ipass_service_name>
# # Create the configuration to do IPASS proxy:
# add /Radius/Services/ipass "" radius "" IPASS-response
# set /Radius/Services/ipass/RemoteServers/1 ipassServerA
# # Configure the iPass AAA server, invoke:
# add /Radius/RemoteServers/ipassServerA "" radius <iPass_server_IP> <iPass_server_port>
300000 <secret>
# # Set the incoming script for iPass, invoke:
# set /Radius/IncomingScript IPASS-request
```

```
# # Create the configuration to proxy non-ipass requests in case you aren't using the
default AR service, invoke:
# add /Radius/Services/nonipass "" radius "" ""
# set /Radius/Services/nonipass/RemoteServers/1 nonipassServerA
# # Configure the non iPass AAA server in case you aren't using the default AR service,
invoke:
# add /Radius/RemoteServers/nonipassServerA "" radius <non_ipass_server_IP>
<non_ipass_server_port> 300000 <secret>
# # Save and reload, Invoke:
# save
# reload

#########################################################################
#            Controlling the script functionality                       #
#########################################################################
# You can control the script functionality by commenting and uncommenting
# Sections in the script.
# 1) Controlling the AR service to be used for Non iPass users.
#    By default, non ipass users will use the AR default service.
#    If you want to proxy the Non iPass requests to another AAA server
#    Please refer to the else block of the IPASS-request proc (lines 102-114).
#
# 2) Controlling whether the iPass Auto-connect service will be visiable to the end user
#    if NWSP is installled in RADIUS mode.
#    By default, if NWSP is installed in RADIUS mode the iPass service
#    will not be visiable to the user. You can change this functionality
#    by uncommenting the line that appends N${serviceName}" to the response
#    see the end of the IPASS-response proc.
#

#########################################################################
#            Script Code                                                #
#########################################################################
#
# init procedure, assuming the script init arguments are
# <location delimiter>,<iPass service name>.
# Location delimiter will be used to extract location string from the username.
# iPass service name will be added to the user profile as auto-logon service.
#
proc IPASS-init { request response environ } {

   global delimiter
   global serviceName
   set args [ $environ get Arguments ]
   regexp -- "(.+),(.+)$" $args match delimiter serviceName
}

# Handling iPass Request. If the user is iPass user,
# extract location data and place it in Called-Station-Id attribute.
# If the user isn't iPass users, set the Authentication and Authorization
# Services to be nonipass.
#
proc IPASS-request { request response environ } {

  set nai [ $request get User-Name ]

  # Check if user is iPass User.
  if { [ string match IPASS/* $nai ] } {

    # User is iPass user, set Authentication, Authorization
    # and Accounting services to ipass service.
        $environ put Authentication-Service ipass
        $environ put Authorization-Service ipass
        $environ put Accounting-Service ipass
```

```
        # Extract the location out of the username sring
    global delimiter
        if { [ regexp -- "(\[^@\]+@\[^@\]+)${delimiter}(.+)$" $nai match newusername
location ] } {
                $environ put User-Name $newusername
                $request put Called-Station-Id $location
        }
        # Replace the NAS-Port-Type for iPass
        # The value can be either "Ethernet" or "Wireless - IEEE 802.11"
        $request put NAS-Port-Type "Ethernet" REPLACE
  }
# else {
#         # User isn't iPass, set the Authentication and Authorization
#         # to be proxied to nonipass. This assumes accounting stored in AR.
#         # in case accounting needs to be proxy as well you can add
#         # $environ put Accounting-Service nonipass
#         # NOTE that the proxy to the nonipass server isn't the default.
#         # by default the local-users service will be used.
#         # To change this functionality make sure to comment the lines that
#         # set the service to local-users and uncomment the following lines:
#         #
#         #$environ put Authentication-Service nonipass
#         #$environ put Authorization-Service nonipass
# }

}


# Handling iPass Response. If the user is iPass user,
# return the original username. if the response is Access-Accept,
# add the iPass service name to the user profile as auto-logon service.
#

proc IPASS-response { request response environ } {

  set nai [ $response get User-Name ]

  # Check if user is iPass User.
  if { [ string match IPASS/* $nai ] || [ string compare $nai NULL ] } {

    # Return original username
        $response put User-Name [ $request get User-Name ]

        # Check if response is access accept
    if { [ string compare [ $environ get Response-Type ] Access-Accept ] == 0 } {

           # Response is Access-Accept, add the iPass service as Auto-Logon
           global serviceName
           $response put Cisco-SSG-Account-Info "A${serviceName}"
           # To allow service to be seen by user, uncomment the following line.
           # $response put Cisco-SSG-Account-Info "N${serviceName}" APPEND
        }
  }

}
```

Generating SSL Certificates for Testing

This appendix provides instructions on how to generate self signed SSL certificates for testing environments. This procedure is based on the Sun Java Keytool utility. For more information about Keytool, see the Sun Java website.

Note This procedure is only for development, test, and trial environments. It must not be used in a production environment.

Step 1 Generate a self-signed certificate using the Java keytool utility. At the prompt, enter:

```
keytool -genkey -v -dname "cn=<server_name>, ou=<organizational_unit>,
o=<organization_name>, c=<2_ch_country_code>" -alias <certificate_alias>
-keystore "<keystore_filename>" -keypass "<key_password>" -storepass "<store_password>"
```

Note The -dname parameter definition must not contain a line break. You can omit the -dname definition and reply to the prompts at the Keytool console.

Step 2 Use the following command to export the certificate so that it can be added to the iPass or WSG client store:

```
keytool -export -file <certificate_filename> -keypass <key_password>
-keystore <keystore_filename> -storepass <store_password> -alias <certificate_alias>
```

Step 3 On the Jetty web server, modify jetty/config/<*server_application*>.jetty.xml to use the store file defined defined under -keystore <*keystore_filename*>.

For example:

```
 <Configure jmxname="org.mortbay.jetty:name=Jetty,Server=0,SESMSSLListener=0">
     <Set name="keystore"><SystemProperty name="jetty.home"
default="."/>/config/sesm-dev-4-self</Set>
     <Set name="password">mypwd</Set>
     <Set name="keyPassword">mypwd</Set>
  </Configure>
```

Step 4 On the iPass client machine, do the following:

a. Open your IE browser, then select Tools > Internet Options.

b. Select the Content tab.

c. Click the Certificates.. button.

d. Click the Import button, and follow the instructions in the Import wizard.

Note For WSG client, replace Step 4 with the following:

a. Enter the following command to add the certificate to JVM keystore located at <JAVA_HOME>/jre/lib/security/cacerts using the Keytool utility:

```
keytool -import -file <certificate_filename> -alias <certificate_alias> -keystore
<JAVA_HOME>/jre/lib/security/cacerts
```

When prompted for the keystore password, enter the cacerts password (the default is changeit).

b. In the wsgClient start script, update the following parameters to point to your new keystore file and file password:

```
-Djavax.net.ssl.trustStore="<keystore_filename>"
-Djavax.net.ssl.trustStorePassword="<store_password>"
```

The values in <> are taken from Step 1.

When the import completes successfully, a message is displayed informing you that the certificate was added to the store.

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X