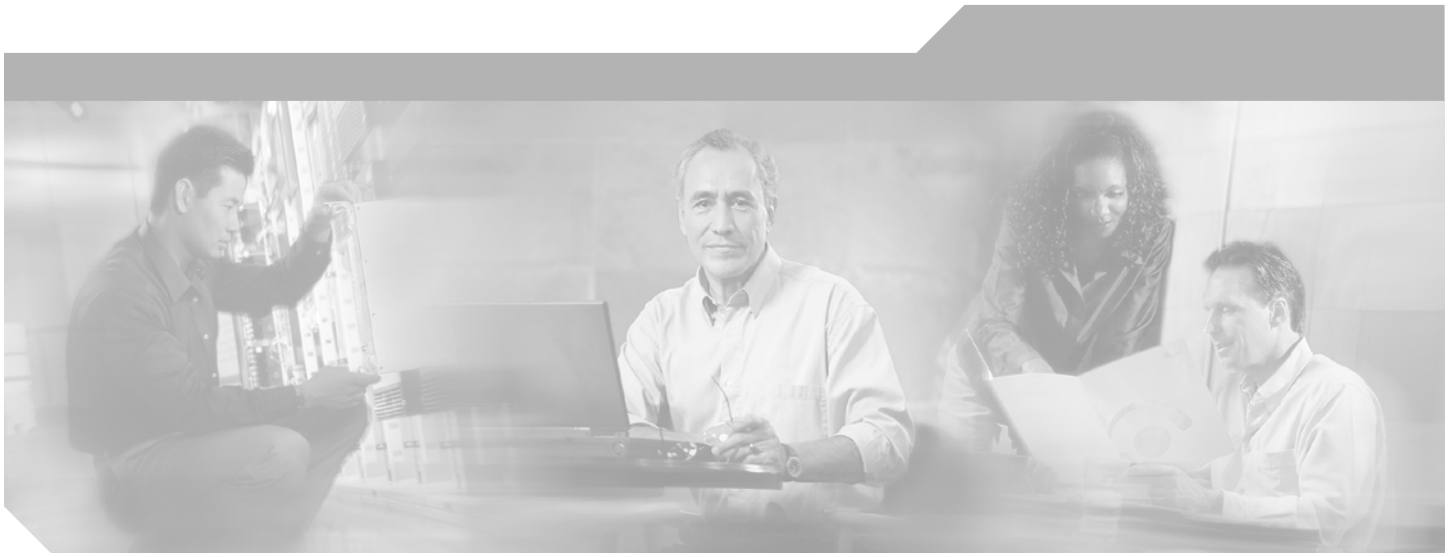


Cisco Subscriber Edge Services Manager Captive Portal Guide

SESM Release 3.2
December 2003

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

Text Part Number: OL-3886-02

CONTENTS

About This Guide

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

Document Objectives

This guide explains the Cisco Subscriber Edge Services Manager (Cisco SESM) captive portal features and how to configure them. The captive portal features, combined with the TCP redirect features on the Service Selection Gateway (SSG), provide value-added services to SESM solutions, such as messaging, advertising, and redirection for the purpose of authentication.

Audience

This guide is intended for anyone responsible for developing, configuring, and deploying SESM solutions that include captive portal features.

Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	Introduction to SESM	Describes the role of the captive portal solution in a SESM deployment.
Chapter 2	Captive Portal Description	Describes the SESM captive portal features and components.
Chapter 3	Installing the Captive Portal Solution	Describes installation prerequisites and procedures for the captive portal solution.
Chapter 4	Configuring the Captive Portal Solution	Describes captive portal configuration tasks.
Chapter 5	Running the Sample Captive Portal Solution	Describes how to start and stop the applications in the captive portal solution.
Chapter 6	MBeans in the Captive Portal Solution	Describes the JMX MBean attributes in the captive portal solution.
Chapter 7	Configuring the SSG TCP Redirect Features	Describes how to configure the Cisco IOS software TCP redirect features on the SSG platform.
Chapter 8	Troubleshooting Captive Portal Configurations	Describes some potential problems and solutions with captive portal installation and configuration.
Appendix A	Captive Portal Demo	Describes how to demo captive portal features using the sample data included with the SESM installation.
Appendix B	Captive Portal Sequence Diagrams	Contains sequence diagrams for the captive portal redirection scenarios.
Index		

Document Conventions

The following conventions are used in this guide:

- *Italic* font is used for parameters for which you supply a value, emphasis, and to introduce new terms.
- **Bold** font is used for user entry and command names.
- `Computer` font is used for examples.

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this guide.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for the Cisco SESM includes:

- *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.2*
- *Cisco Subscriber Edge Services Manager Solutions Guide*
- *Cisco Subscriber Edge Services Manager Quick Start Guide*
- *Cisco Subscriber Edge Services Manager Installation Guide*
- *Cisco Subscriber Edge Services Manager Deployment Guide*
- *Cisco Subscriber Edge Services Manager Web Portal Guide*
- *Cisco Subscriber Edge Services Manager RADIUS Data Proxy Guide*
- *Cisco Subscriber Edge Services Manager Application Management Guide*
- *Cisco Subscriber Edge Services Manager Troubleshooting Guide*
- *Cisco Distributed Administration Tool Guide*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Subscriber Edge Services Manager SDK Programmer Guide*
- *Cisco Subscriber Edge Services Manager Plug and Play Guide*
- *Cisco Subscriber Edge Services Manager Web Services Gateways Guide*

The Cisco SESM documentation is online at:

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

Documentation for the Cisco SSG is online at:

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

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

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

If you are including the Cisco Access Registrar (a RADIUS server) in your SESM deployment, see the following documents:

- *Release Notes for the Cisco Access Registrar 1.6*
- *Cisco Access Registrar User Guide*

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

Introduction to SESM

This chapter describes the role of the Cisco Subscriber Edge Services Manager (SESM) captive portal solution in a SESM deployment. The chapter contains the following topics:

SESM Captive Portal Overview

The SESM captive portal features, combined with the TCP redirect features on the Service Selection Gateway (SSG), can provide the following benefits for subscribers and deployers:

- Direct subscribers to the SESM web portal application even if they do not know the URL to the web server.
- Force subscribers to authenticate before accessing the network or specific services.
- Direct subscribers to appropriate service logon pages or default service connection page when they attempt to use a service before they are connected to the service.
- Ensure that subscribers are shown a specific message for a defined period while attempting to access services.
- Display advertising messages at specified intervals during the SESM session.
- Display advertising messages based on specific subscriber characteristics, such as hobbies.
- Display an explanation page when connection is denied based on the SSG prepaid feature.

All of the above mentioned uses of captive portal are demonstrated in the sample captive portal solution, which is available for installation as an optional component from any of the SESM packages. The captive portal solution consists of the following suite of applications:

- Captive portal application
- Message portal application
- Captive portal features in the NWSP application

With some customized programming and development, the following additional features could be achieved using the SESM captive portal solution:

- Direct all incoming requests destined to a specific network to a specific URL.
- Direct all requests destined to a specific port to a specialized advertising page that shows new services.
- Direct subscribers to a billing server application that provides account status information or account payment opportunities.

SESM Installation Images

The installation images for SESM are available from the product CD-ROM or from the Cisco web site. SESM images are available for the Sun Solaris, Linux, and Windows platforms.

Table 1-1 shows the names of the compressed and executable files (Note that "x.x.x" is used to denote version number).

Table 1-1 Installation Image Filenames

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

The procedures for obtaining the installation images are detailed in the *Cisco Subscriber Edge Services Manager Installation Guide*.

Subscriber and Service Profiles

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

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

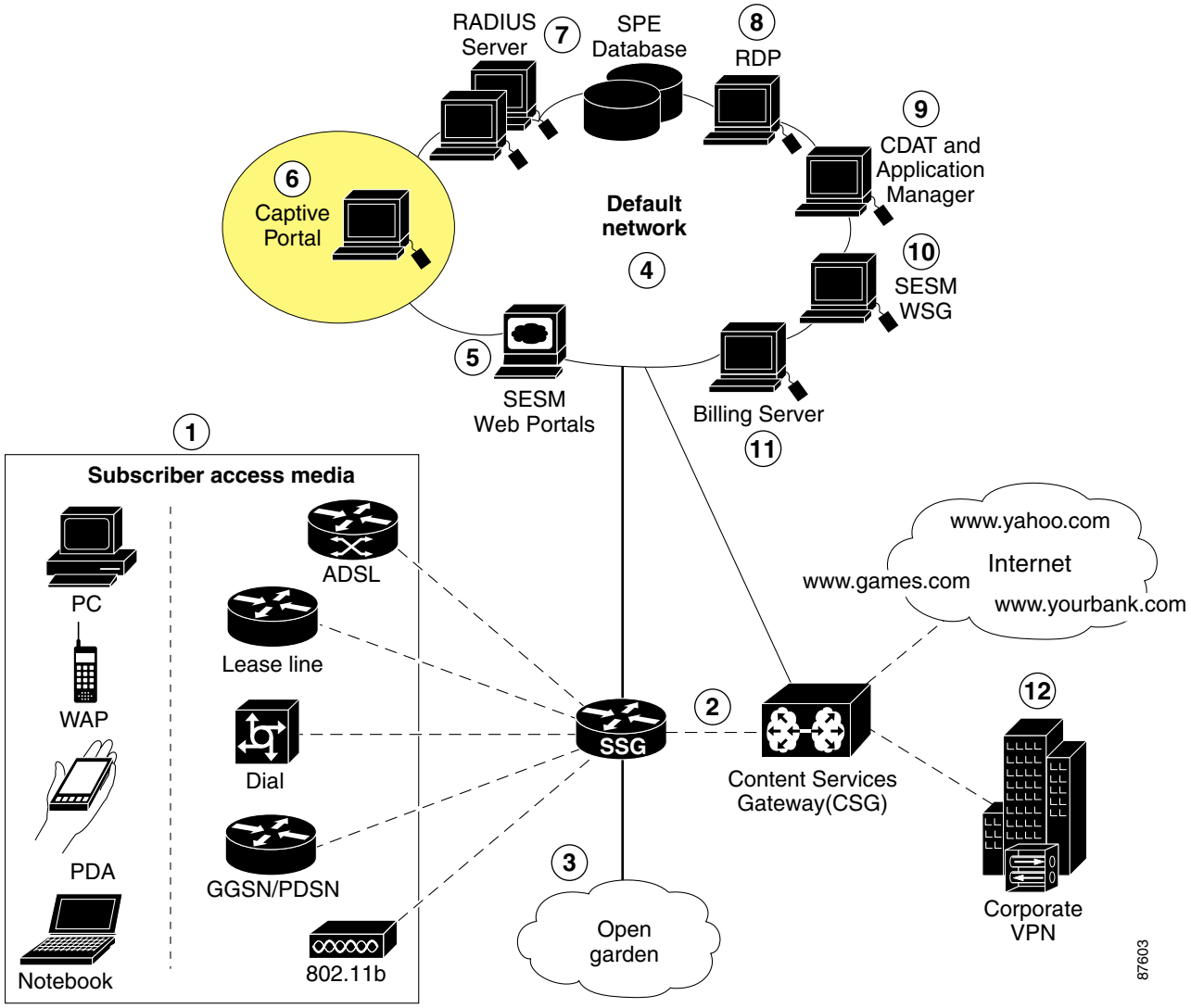
The SESM solution integrates with any one or a combination of the following options to obtain subscriber and service data:

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

SESM Reference Network Diagram

The following figure shows SESM applications in a hypothetical deployment. Actual deployments might not use all of the components shown. The item number 6 is the subject of this guide.

Figure 1-1 SESM Network Diagram



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

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

SESM Application Management

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

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

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

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

Administrators can change SESM application configuration by changing the attribute values in MBeans. In SESM Release 3.2, use any of these ways to change MBean attribute values:

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

Note The Application Manager replaces the SESM Agent View. The Agent View is included in SESM Release 3.2 to provide convenience and continuity during migrations from previous releases.

SESM Documentation Map

Table 1-2 can help you to locate information in the SESM documentation set. Go to the following URL to access the online version of the SESM documentation:

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

Table 1-2 SESM Documentation Map

To Learn About	Read
SESM Features	*Cisco Subscriber Edge Services Manager Solutions Guide* *Cisco Subscriber Edge Services Manager Web Portal Guide* *Cisco Subscriber Edge Services Manager RADIUS Data Proxy Guide* *Cisco Subscriber Edge Services Manager Captive Portal Guide*
SESM Deployment	*Cisco Subscriber Edge Services Manager Quick Start Guide* *Cisco Subscriber Edge Services Manager Installation Guide* *Cisco Subscriber Edge Services Manager Deployment Guide*
SESM Application Management and Configuration	*Cisco Subscriber Edge Services Manager Application Management Guide* *Cisco Subscriber Edge Services Manager Web Portal Guide* *Cisco Subscriber Edge Services Manager RADIUS Data Proxy Guide* *Cisco Subscriber Edge Services Manager Captive Portal Guide*
Profile Management RADIUS	*Cisco Subscriber Edge Services Manager Deployment Guide*
Profile Management SPE	*Cisco Distributed Administration Tool Guide*
SPE Role Based Access Control (RBAC)	*Cisco Distributed Administration Tool Guide*
Troubleshooting	*Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.2* *Cisco Subscriber Edge Services Manager Troubleshooting Guide*
SESM Portal Development	*Cisco Subscriber Edge Services Manager Web Developer Guide* *JavaDoc (included with the software distribution)*
Web Services Gateway	*Cisco Subscriber Edge Services Manager Web Services Gateways Guide*
SESM Platform SDK	*Cisco Subscriber Edge Services Manager SDK Platform Programmer Guide*
Plug and Play Connectivity	*Cisco Subscriber Edge Services Manager Plug and Play Guide*

Captive Portal Description

This chapter describes the SESM captive portal solution features and components. It contains the following topics:

Captive Portal Components

The SESM captive portal solution consists of the following 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.
- SESM Captive Portal application—This SESM application acts as a gateway for all of the different redirections coming from the SSG. This application does not provide any content to subscribers. Its main purpose is to apply business logic that determines what will happen next. The captive portal application 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. This guide assumes that you use SESM web portal applications. The sample captive portal solution uses the following two content applications:
  - SESM Message Portal—Provides the message pages for initial and advertisement captivation. This application also provides a timing mechanism to control the duration of the displays.
  - NWSP portal—Provides the logon page for unauthenticated user redirections and appropriate (configured) pages for unconnected service redirections.

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, the captive portal must be installed and additional configuration of the web-jetty.xml file is required.

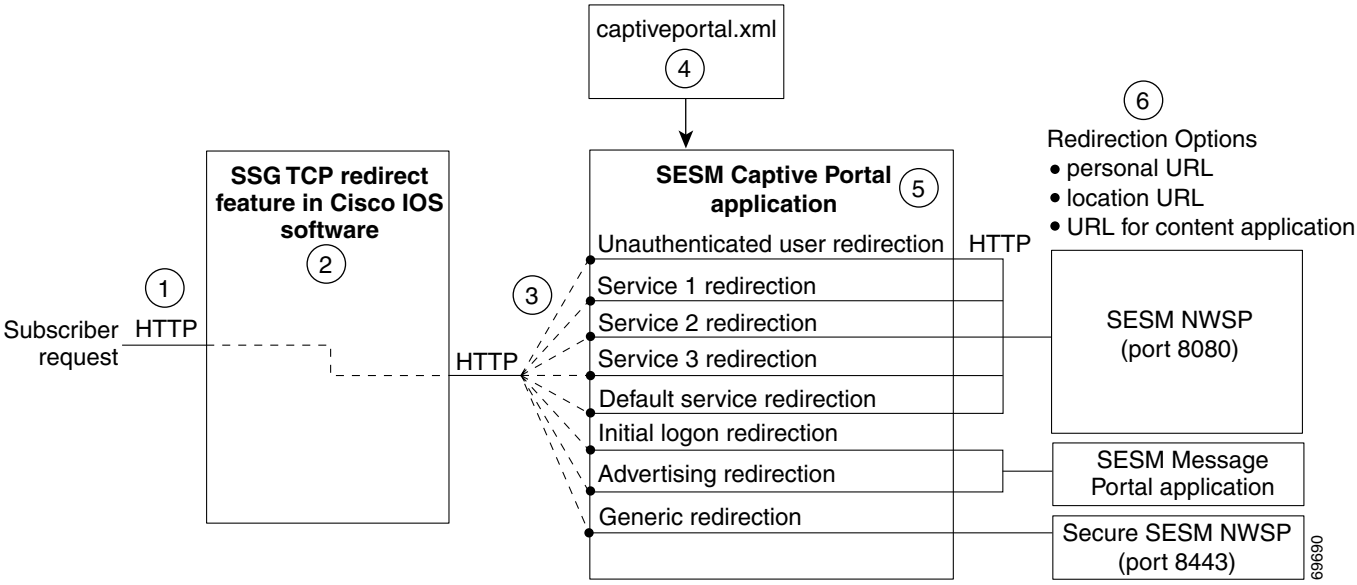
For more information on the role of the captive portal in the SESM Plug and Play solution, see the *Cisco Subscriber Edge Services Manager Plug and Play Guide*.

Captive Portal Diagram

Figure 2-1 illustrates how the components in the SESM captive portal solution work together to provide appropriate content to the subscriber.

The figure shows the sample solution as it would be configured using all of the default values provided by the SESM installation program. There are many possible variations to this default deployment.

Figure 2-1 Sample SESM Captive Portal Solution



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	The sample SESM captive portal solution requires the following configurations for the TCP redirected destinations: • IP address—The IP address must identify a web server running the SESM Captive Portal application. 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 the SESM Captive Portal application. To configure the SESM Captive Portal application 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. The Captive Portal application 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 more flexibility and is provided to fulfill any requirements that the default installation does not fulfill. In the sample configuration, the generic port is the NWSP 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	The SESM Captive Portal application 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	The captive portal application redirects the browser to another configured location. The options are: • Specify a page in another web portal application, such as the SESM NWSP or Message Portal application • 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, the Captive Portal application is configured as follows: • Redirects unauthenticated user redirections and service redirections to the NWSP application • Redirects initial logon and advertising redirections to the SESM Message Portal application

SSG TCP Redirection Types

Table 2-1 describes the SSG TCP redirection types and how the SESM captive portal solution supports those redirection types. The table describes the role of SESM applications in the sample captive portal solution installed with SESM. In the third column, the following keywords are used:

Table 2-1 Supported Redirection Types

SSG TCP Redirect Type	Role of SSG TCP Redirect Feature	Default Configuration of the SESM Captive Portal Solution
Initial logon redirection—Gives providers a way to deliver messages to subscribers when they first log in.	Redirects all TCP packets destined to a configured list of ports when the edge session is first created. Activates a timing mechanism for a specified duration, during which the subscriber cannot redirect the browser. The configured Captive Portal application (as opposed to SSG) controls what occurs after the duration time elapses.	In the sample solution: 1. The Captive Portal application redirects to the /initial page in the Message Portal application. The /initial page provides message content. 2. After the message duration time elapses, the Message Portal can optionally redirect the browser to the original URL requested.
Unauthenticated user redirection—Handles attempted access to services by subscribers who have not yet authenticated for the session.	Without TCP redirection, the SSG discards packets from unauthenticated users. With TCP redirection, unauthenticated packets are allowed some controlled access to particular services within the SSG, such as access to a captive portal application.	In the sample solution: 1. The Captive Portal application redirects to the /home page in NWSP. The /home page provides a login page. 2. NWSP sends a session start request to SSG using the information from the logon page. 3. SSG removes the TCP redirection. 4. After authentication, NWSP can optionally redirect the browser to the subscriber's original request.
Unconnected service redirection—Handles attempts to access a service when the service is not connected.	Without TCP redirection, the SSG discards packets directed at services for which the subscriber is not connected. With TCP redirections, these packets are redirected to a configured server group. There are two ways to configure service redirection: • Specific services • Default service redirection	In the sample solution: 1. The Captive Portal application redirects to a service page in NWSP. a. For specific service redirections, NWSP presents a logon page specific to the service being requested. b. For default service redirections, NWSP displays a default service selection page. c. In an SPE deployment, NWSP displays a self-subscription page if the subscriber is not already subscribed to the service. 2. NWSP sends a service connection request to SSG in response to subscriber input. 3. SSG removes the TCP redirection.

Table 2-1 Supported Redirection Types (continued)

SSG TCP Redirect Type	Role of SSG TCP Redirect Feature	Default Configuration of the SESM Captive Portal Solution
Advertising redirection—Gives providers a way to deliver advertising or other messages at timed intervals during an active session.	Redirects all TCP packets destined to a configured list of ports at specified intervals. Activates a session timing mechanism to keep track of the time since the last advertisement redirection. When the configured interval elapses, SSG performs an advertising redirection the next time the subscriber initiates a TCP packet. Activates a message duration timing mechanism as described above for the initial logon redirection.	In the sample solution: 1. The Captive Portal application redirects to the /advertising page in Message Portal. 2. After the advertising duration time elapses, the Message Portal can optionally redirect the browser to the previous URL with no further action required from the subscriber.
SMTP redirection—Forwards SMTP traffic.	Handles all aspects of Simple Mail Transfer Protocol (SMTP) redirection.	This type of redirection does not require a captive portal application.

SESM Captive Portal Application Description

The SESM Captive Portal application acts as a gateway for all of the different redirections coming from the SSG. This application 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.

The SESM Captive Portal application 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.

Table 2-2 shows the parameters that the Captive Portal application captures and forwards to content applications. The names of these parameters are configurable in the captiveportal.xml file.

Table 2-2 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. The NWSP application uses this value to redirect the browser to this original request after successful authentication.

Table 2-2 Parameters Appended to URLs in HTTP Redirections (continued)

Type of SSG TCP Redirection	Parameter Name in SESM Captive Portal HTTP Redirect	Explanation and Usage by the Content Applications
Service redirection	service	The service name that was requested in the original request.The NWSP application uses this value to log on to the service.
	username	The user name 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 NWPS uses this value to display a pop-up 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 logon and advertising redirections	CPURL	The URL in the subscriber's original request. The Message Portal application 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. The Message Portal application waits this amount of time before attempting to redirect to the CPURL. Duration attributes exist on both the SSG side and the SESM side. See the "Summary of Message Duration Parameters" section on page 4-3.
	CPSUBSCRIBER	The subscriber name as obtained from the subscriber profile.

SESM Captive Portal Redirection Options

This section describes the captive portal redirection options, which are:

- Redirect to personalURL, page 2-6
- Redirect to locationURL, page 2-7
- Redirect to Content Applications, page 2-7
- Generic Redirections, page 2-8

Redirect to personalURL

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

To add a home URL attribute to subscriber profiles:

- For RADIUS mode, 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 SPE mode, 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 the *Cisco Subscriber Edge Services Manager Web Portal Guide* 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 SESM web portal applications.

NWSP Application

In the SESM example captive portal solution, unauthenticated user redirections and unconnected service redirections are configured to redirect the browsers to the NWSP application, 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 logon 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 SPE mode, 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 the Captive Portal application 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 Table 2-2 on page 2-5 for a description of the parameters that the Captive Portal application forwards to the NWSP application.

Message Portal Application

In the SESM example captive portal solution, the Message Portal application provides the message pages for initial and advertisement captivation. The Message Portal application contains:

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

This application 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, the message portal application 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 Table 2-2 for a description of the parameters that the Captive Portal application forwards to the Message Portal application.

Generic Redirections

The generic redirection feature provides another way to configure redirections. Rather than using a type of redirection in the captive portal application that matches the type of redirection configured on the SSG, you can instead use a generic redirection in the captive portal application.

For example, you can configure the SSG to do per-user and per-service initial or advertising captivation. However, the captive portal application 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 Table 6-1 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, the captive portal performs TCP redirection for:

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

It is recommended that the captive portal only acts on requests from specified MIME types and user agents. If all requests are redirected then the captive portal will suffer performance degradation. This can be avoided by specifying the user agents and MIME types that you want the captive portal to accept.

Configuring Accepted User Agents

A list of the accepted user agents is contained in the capturedUserAgents section of the captiveportal.xml file. 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, then 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

A list of the accepted MIME types is contained in the capturedMimeTypes section of the captiveportal.xml file.

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, then all MIME types are allowed.

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>
```

Alternative Deployment Options for a Captive Portal Solution

The sample SESM captive portal solution offers one way to implement captivation features. This section describes some alternative deployment options.

Eliminating Redirection Types

You do not need to deploy all of the redirection types. Each type of TCP redirection is independent of the others. To eliminate a redirection type from the captive portal solution, you can do any of the following:

- Turn off the redirection type in the captiveportal.xml file.
  - During captive portal installation, you can uncheck the enable box for any redirection type.
  - After installation, you can set to false the appropriate attribute by editing the captiveportal.xml file.
- Do not configure the redirection type on the SSG.

Eliminating J2EE Listeners

The web server container in which the captive portal application runs is configured with a separate listener for each TCP redirect port you configured. That is, separate listeners exist for user redirections, each service redirection, a default service redirection, initial logon redirections, and advertising redirections. If you do not implement all of the redirection types, you might want to edit the captiveportal.jetty.xml file to disable the unnecessary listeners. This is optional.

Using Customized Content Applications

You can deploy one or many content applications. You might have a single content application that handles all types of redirection, or you might have a different application for each type of redirection, including a different application for each configured service redirection. The content applications do not need to be SESM applications. The SESM Captive Portal application can redirect to any web application.

Using a Customized Captive Portal Application

The SSG TCP redirect feature can accept any web application in the SSG captive portal groups. There is no requirement to use the SESM Captive Portal application. The installed Captive Portal application is extensible.

Altering Captive Portal Deployment

As installed, the Captive Portal application runs in a Jetty container. You can deploy the Captive Portal application in any J2EE container.

There is no requirement to use the 2-tiered approach used by the SESM solution. However, the 2-tiered approach offered by the SESM Captive Portal application has certain advantages:

- It is an efficient, small footprint, application.
- By acting as a gateway to any number of other applications with varying functions, it isolates common functionality into a single application.
- By offering an isolated interface to SSG, you can add and change content applications without changing the Cisco IOS configuration. You add or change configuration parameters in the Captive Portal application configuration file (an XML file) to point to the new content applications. This is much easier than changing the captive portal group configuration on the SSG, which requires that you enter Cisco IOS commands on each SSG platform.

You can configure the TCP redirect feature to redirect directly to an application that provides content to the subscriber. For example:

- You could configure captive portal groups for unauthenticated user redirections as instances of NWSP (or some other appropriate web application), bypassing the SESM Captive Portal application. However, if you want to retain the feature that preserves the originally requested URL from the user, you must customize the NWSP application by adding some code that is currently in the SESM Captive Portal application.
- Similarly, you could configure captive portal groups for initial logon and advertising redirections as instances of a content application similar to the SESM Message Portal application, bypassing the SESM Captive Portal application.

Note If you redirect directly to the delivered SESM Message Portal (bypassing the Captive Portal application), the originally requested URL is not available and no pages based on subscriber profile are presented.

Installing the Captive Portal Solution

This chapter describes installation prerequisites and procedures for the captive portal solution. The topics are:

Important Information about Installing Captive Portal

The sample captive portal applications are available for installation from any of the SESM installation packages.

The following information is important to understand when installing the captive portal solution:

- You must choose **Custom Install** to install the captive portal solution. The captive portal solution is not included in a typical installation.
- The SESM captive portal solution requires the services of a Cisco Service Selection Gateway (SSG). The SSG is a software feature embedded in the Cisco IOS running on a Cisco edge device. Make sure that your deployment environment uses the required Cisco IOS release required for the SSG features you need, as described in the "SSG Software Release Requirements for Captive Portal Compatibility" section on page 3-2.
- Many of the captive portal installation parameters must match values that are configured on the SSG for TCP redirect features. The easiest way to ensure that values match in both places is to:
  - Accept all of the default values presented during SESM captive portal installation.
  - Use the ssgconfig.txt file to configure the TCP redirect features on the SSG. The configuration values in ssgconfig.txt match the default values used in the SESM installation program. See the "Configuring the SSG to Match the Installed Captive Portal Solution" section on page 4-1 for instructions on using ssgconfig.txt.
- If you install the captive portal solution in a separate installation sessions from NWSP, make sure you install both components (NWSP and captive portal) using the same mode (SPE, RADIUS, or Demo). Otherwise, you must override the mode for one of the applications at startup by using the mode argument with the startup script.

SSG Software Release Requirements for Captive Portal Compatibility

The following table shows Cisco IOS software and Cisco SESM release requirements for implementing captivation features.

Captivation Type	Required Cisco IOS Software Release Level (for the SSG feature set)	Required Cisco SESM Release Level
Unauthenticated user redirection	Cisco IOS Release 12.1(5)DC1 or later	SESM Release 3.1(1) or later
Unauthorized service redirection Initial logon redirection Advertising redirection	Cisco IOS Release 12.2(4)B or later	SESM Release 3.1(3) or later

Note The SSG TCP redirect features can redirect to any web server application. There is no requirement to use SESM applications. However, this guide assumes that you are using SESM applications.

Reference to Detailed Installation Instructions

See the *Cisco Subscriber Edge Services Manager Installation Guide* for:

- Installation platform requirements
- Prerequisite steps to perform before running the installation program
- Detailed installation procedures
- Explanations of the configuration attributes presented by the installation program

Installation Results

The captive portal installation procedure adds two directories under your SESM installation directory:

```
captiveportal
    config
      captiveportal.xml
      ssgconfig.txt
    webapp
    docs
messageportal
    config
      messageportal.xml
    webapp
    docs
```

The installation procedure also adds startup scripts and container configuration files for Captive Portal and Message Portal to the jetty directory under your SESM installation directory:

```
jetty
    bin
      startCAPTIVEPORTAL
      startMESSAGEPORTAL
    config
      captiveportal.jetty.xml
      messageportal.jetty.xml
```

Configuring the Captive Portal Solution

This chapter describes how to configure the Cisco Subscriber Edge Services Manager (SESM) captive portal solution. The topics are:

Configuring the SSG to Match the Installed Captive Portal Solution

To demonstrate the complete capabilities of the captive portal solution, 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 just installed on the SESM side, follow these procedures:

Step 1 Make sure the SSG platform is running the appropriate Cisco IOS release, as described in the "SSG Software Release Requirements for Captive Portal Compatibility" section on page 3-2. If not, upgrade the Cisco IOS release before proceeding.

Step 2 Make sure that basic SSG functionality is enabled and configured, as described in the "Basic SSG Configuration" section in the *Cisco Subscriber Edge Services Manager Deployment Guide*.

Step 3 Open the ssgconfig.txt file in a text editor. The file location is:

```
captiveportal
    config
      ssgconfig.txt
```

The ssgconfig.txt file contains all of the Cisco IOS software commands required to configure the four types of TCP redirection that the sample captive portal solution can support and demonstrate. The commands in this file configure SSG to match the default values presented during the captive portal installation. The file includes example IP addresses.

Note The installation displays default inputs for captive portal group names and port numbers. These defaults correspond to values used in the TCP redirect commands in the ssgconfig.txt file. If you change these captive portal group names or port numbers, you must make corresponding changes to the port numbers in the ssgconfig.txt file.

Step 4 Edit ssgconfig.txt as follows:

- You *must* edit the placeholder IP addresses. Change them to the actual network IP addresses you entered during captive portal installation.
- If you changed the displayed defaults for captive portal group names or the incoming port numbers, then you must edit those values in ssgconfig.txt to match the values you entered during captive portal installation.

Step 5 On the SSG host device, enter the contents of ssgconfig.txt to update the Cisco IOS running-config file.

Step 6 Save running-config.

Loading Sample Profiles for Captive Portal Demonstration

To demonstrate the features in the captive portal solution, 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. See the "Redirected Networks Do Not Match Service Routes" section on page 8-3.
- Subscriber profiles must include subscriptions to the above services.
- For SPE mode, 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 SPE mode, 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 the SESM config directories contains many profile examples.

Configuring Unique Service Logon 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 logon page in NWSP.

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, follow these procedures:

Step 1 Open the captiveportal.xml file in a text editor. The location is:

```
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.

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

Note When the second argument is empty (or its system property default is empty), the value in the serviceRedirectDefaultURL attribute is used. By using a default page in serviceRedirectDefaultURL attribute, you do not have to enter the same URL for all the service redirections.

The default value provided by the installation program for the serviceRedirectDefaultURL attribute is the NWSP /serviceRedirect page.

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 minimal 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. (The automatic redirect feature can be turned off, in which case 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 attempts 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 has elapsed, 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 logon 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. The captive portal application 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 the Captive Portal application does not forward a duration attribute.

Configuring Redirection to a Predefined URL After Authentication

This section describes two 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.

Change the Captive Portal Application Configuration

You can change the value of MBean attributes used by the captive portal application to redirect all subscribers to the same predefined URL. Follow these steps:

Step 1 Prepare to modify the captiveportal MBean, either by using the CDAT Application Management tool or opening the captiveportal.xml file in an editor.

Step 2 Change the userRedirectURL attribute to:

<Set name="userRedirectURL">*urlNWSP*?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 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.

If you are editing the XML 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 the captiveportal application.

Adding a Home URL to the Subscriber Profile

You can add a home URL attribute to subscriber profiles, and code 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. Follow these steps:

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

- For RADIUS mode, 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 SPE mode, 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 portal application code.

The order of precedence for redirection is defined in the following JSP:

```
nwsp
    webapp
        decorators
           initUser.jsp
```

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.

Running the Sample Captive Portal Solution

This chapter describes how to start and stop the applications in the captive portal solution and how to optimize memory and performance. The topics are:

Script Names

This section lists 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 the chapter "Running SESM Web Portals" in the *Cisco Subscriber Edge Services Manager Web Portal Guide*.

The following table shows the script names for starting and stopping applications in the sample captive portal solution. 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 [-mode mode]`
		`jetty/bin/startMESSAGEPORTAL.sh [-mode mode]`
		`jetty/bin/startNWSP.sh [-mode mode]`

	Windows	`jetty\bin\startCAPTIVEPORTAL.cmd [mode]`
		`jetty\bin\startMESSAGEPORTAL.cmd [mode]`
		`jetty\bin\startNWSP.cmd [mode]`
		
		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`

Mode Argument in Startup Scripts

Note The mode for all of the applications in the captive portal solution (Captive Portal application, Message Portal application, and NWSP) must be the same.

SESM portal applications, including the applications in the captive portal solution, can run in the following modes:

- RADIUS
- SPE
- Demo

The mode is set as follows:

- The mode attribute in the SESM MBean—Initially set during installation, but you can change it
- The mode argument to the SESM portal startup scripts—Overrides the setting in the configuration file

If you installed the NWSP application separately from the captive portal solution, you might have choosen different installation modes during the installations. Either change the values in the configuration files to match, or override the values at run time.

MBeans in the Captive Portal Solution

This chapter describes the JMX MBean attributes in the captive portal solution. The SESM installation process uses default values and values you enter during installation to configure the sample captive portal solution. Read this chapter if you want to change or fine-tune configuration after installation.

The chapter contains the following topics:

Container MBeans and Configuration

All of the applications in the captive portal solution are SESM web portal applications. They run in a J2EE container. They are installed to run in a Jetty container. For information about configuring Jetty container MBeans and using containers other than Jetty, see the *Cisco Subscriber Edge Services Manager Web Portal Guide*.

MBeans in the Captive Portal Application

The captive portal application (the SESM application that listens for TCP redirections from SSG) uses the following MBeans:

Logger MBean

The Logger MBean configures the SESM logging and debugging tools:

- The logging tool logs application activity, such as messages received and processed.
- The debugging mechanism produces messages useful for debugging.

All SESM applications use the same logging and debugging mechanisms. However, each application uses its own version of the Logger MBean, so you can configure logging and debugging activity separately for each application.

For more information, see the "Logging and Debugging" chapter in the *Cisco Subscriber Edge Services Manager Application Management Guide*.

captiveportal MBean

Table 6-1 explains attributes in the captiveportal MBean.

Table 6-1 captiveportal MBean

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 6-1 captiveportal MBean (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 Web 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 6-1 captiveportal MBean (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 4-3 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 6-1 captiveportal MBean (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&key2=value2&..."`
	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 6-1 captiveportal MBean (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 redirect 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.

MBeans in the Message Portal Application

The Message Portal application uses the following MBeans:

- Logger MBean, page 6-6
- SESM MBean, page 6-7
- SESMDemoMode MBean, page 6-7
- DESSMode MBean, page 6-7
- messageportal MBean, page 6-7

Logger MBean

The Logger MBean configures the SESM logging and debugging tools:

- The logging tool logs application activity, such as messages received and processed.
- The debugging mechanism produces messages useful for debugging.

All SESM applications use the same logging and debugging mechanisms. However, each application uses its own version of the Logger MBean, so you can configure logging and debugging activity separately for each application.

For more information, see the "Logging and Debugging" section in the *Cisco Subscriber Edge Services Manager Application Management Guide*.

SESM MBean

The SESM MBean sets the mode for SESM applications. The *Cisco Subscriber Edge Services Manager Web Portal Guide* describes this MBean.

For the Message Portal application, the mode attribute must be one of the following:

- SPE, if the mode for the Captive Portal application is SPE.
- Demo, if the mode for the Captive Portal application is Demo.
- Demo or RADIUS, if the mode for the Captive Portal application is RADIUS. Use Demo mode and a flat file for subscriber profiles if you want the Message Portal application to obtain profiles in a non-SPE deployment. The Message Portal application, as installed, does not obtain subscriber profiles when running in RADIUS mode.

SESMDemoMode MBean

Portal applications running in Demo mode use the SESMDemoMode MBean. This MBean identifies the flat file that contains sample profiles for applications running in Demo mode. See the *Cisco Subscriber Edge Services Manager Web Portal Guide* for more information about this MBean.

If you run the message portal application in Demo mode, it obtains subscriber profiles from the file identified in this MBean. You can add interests (hobbies) to subscriber profiles in the demo data file using the $AA subattribute. See the *Cisco Subscriber Edge Services Manager Deployment Guide* for more information.

DESSMode MBean

Portal applications running in SPE mode use the DESSMode MBean. See the *Cisco Subscriber Edge Services Manager Web Portal Guide* for more information about this MBean.

messageportal MBean

Table 6-2 explains the configuration attributes in the messageportal MBean.

Table 6-2 messageportal MBean

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).

Table 6-2 messageportal MBean (continued)

Attribute Name	Explanation
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 4-3 for more information.
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.

Table 6-2 messageportal MBean (continued)

Attribute Name	Explanation

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`

Captive Portal Attributes in the NWSP WebAppMBean

The NWSP portal is the content application for unauthenticated user redirection and service redirections. The NWSP application contains the WebApp MBean. Table 6-3 explains configuration attributes in the WebAppMBean that are directly related to the captive portal solution.

The MBean configuration file for the NWSP portal is:

```
nwsp
    config
        nwsp.xml
```

Table 6-3 Captive Portal Attributes in the WebAppMBean

Attribute Name	Explanation
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.
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 SPE mode, the NWSP subscriptionManage page. • In RADIUS mode, the NWSP displays the page specified in the defaultURI attribute.
noSubscribePermission URI	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 RADIUS mode, or • The application is running in SPE mode, 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.

Configuring the SSG TCP Redirect Features

This chapter summarizes how to configure the Cisco IOS software TCP redirect features on the SSG platform. This chapter includes the following topics:

For complete information about the SSG TCP redirect features, see the SSG documentation.

Configuring SSG and Port-Bundle Host Key to Work with the Captive Portal Application

To allow the Captive Portal application to obtain the subscriber name from profiles, the following SSG configurations are required:

1. If the SESM single sign-on feature is turned on, the SSG profile cache feature must also be turned on:

   ```
   ssg profile-cache
   ```

2. If the SSG port-bundle host key feature is used, ensure that the destination range configured in the port-mapping command includes the port numbers you assigned during the captive portal configuration, in addition to the port number of the main SESM web application. (The suggested default values that the installation program uses for the Captive Portal configuration are 8090 to 8096.)

   Example port-bundle host key port mapping commands follow:

   ```
   ssg port-map enable
   ssg port-map destination range 8080 to 8100 ip 10.0.1.4
   ssg port-map source ip Loopback()
   ```

Using the ssgconfig.txt File

The SESM installation includes a sample configuration file containing Cisco IOS commands for the SSG TCP redirect features. The sample file is located in:

```
captiveportal
    config
        ssgconfig.txt
```

The examples in this chapter are copied from the ssgconfig.txt file. You can edit this file to supply valid IP addresses for your network, and then execute the file on your SSG platform to make the example captive portal solution work on your network.

Defining Captive Portal Groups and Port Lists

This section describes the SSG captive portal groups and port lists.

Captive Portal Groups

When SSG determines that a TCP packet must be redirected, it redirects the packet to a configured captive portal group. A captive portal group consists of one or more web servers running an application that can handle the redirected packet. If you deploy the SESM captive portal solution, the web servers in your captive portal groups are running the SESM Captive Portal application.

Grouping multiple instances of a captive portal application allows the SSG to apply sequential load balancing over the members of the group. The SSG monitors the web servers in the group and redirects packets only to those servers that respond.

You can configure as many captive portal groups as required. For example, you can specify different captive portal groups for each type of redirection, or different destination networks for different services in service redirects.

Use the following command to create a captive portal group and add web servers to the group.

ssg tcp-redirect server-group *group-name* **server** *ip-address port*

For the SESM example solution to work, you must assign the IP address and port of the SESM captive portal application to all of your server groups. Do this by using the following values in the above command:

- The IP address of the captive portal application.
- The port that you configured in the captiveportal.xml file for the specific type of redirection. The installation program initially sets these ports. Table 7-1 shows the port values that are configured at installation time if you accepted all of the default values during installation.

Table 7-1 Default Redirection Port Values Configured During Installation

Redirection Type	Default Port Value at Installation
Unauthenticated user redirections	8090
Initial logon redirections	8091
Advertising redirections	8092

Table 7-1 Default Redirection Port Values Configured During Installation

Redirection Type	Default Port Value at Installation
Unconnected service redirections:	--
default service redirection	8093
Service1	8094
Service2	8095
Service3	8096
https redirection	8099
Unauthenticated web proxy users	8101

Port Lists

A port list refers to the destination ports in the incoming TCP packets. For example, at most sites, ports 80 and 8080 would identify Internet packets, and port 70 would identify FTP packets. If you assign a port list to a captive portal group, you limit redirections to only the traffic arriving on the ports in the port list.

Note You can associate the same port-list to multiple captive portal groups.

Use the following command to create a port list.

```
ssg tcp-redirect port-list
   port port
   port port
```

The examples in other sections of this chapter include commands that create port lists.

Configuring Unauthenticated User Redirection

Unauthenticated user redirection captures and redirects packets from subscribers who have not logged onto a SESM session (not authenticated).

When a subscriber successfully authenticates, SSG creates an edge session for that subscriber. When an edge session does not exist for the source address of a packet, SSG redirects the packet to the portal group associated with unauthenticated user redirection. The result is that subscribers cannot access any part of the network beyond the default network and configured open gardens without first authenticating.

If you do not configure a captive portal group to handle TCP packets from unauthenticated users, the following occurs:

- SSG discards packets from unauthenticated users, except those that are destined to the default network or open gardens.
- To obtain the SESM logon page, subscribers must enter the URL of the SESM web server.

If a TCP packet is destined to the SSG default network or an open garden network configured on the SSG, it is not a candidate for redirection.

Authentications for PPP Connections

Subscribers who are connecting to SSG over a PPP connection are already authenticated. The SSG accepts this authentication and creates the host object for the subscriber. If the subscriber logs out of SESM but does not log off of the PPP connection, the host object is marked inactive, and then unauthenticated redirection applies. When the PPP subscriber logs back into SESM (reauthenticates), the edge session is active again.

Cisco IOS Configuration Commands

Use the following command to specify which captive portal group will handle unauthenticated user redirections.

```
ssg tcp-redirect redirect unauthenticated-user to server-group
```

For example, the following commands from ssgconfig.txt configure unauthenticated user redirection:

```
ssg tcp-redirect
    server-group userRedirect server 10.0.1.4 8090
    redirect unauthenticated-user to userRedirect
```

The above example does the following:

- Creates a captive portal group named userRedirect.
- Assigns one web server, whose IP address is 10.0.1.4, to the group, with a listener on port 8090. (See Table 7-1 for details about the port number.)
- Associates the userRedirect group with unauthenticated user redirections.
- User redirection applies to all TCP packets whose source IP address does not have an edge session on the SSG. A port list cannot be assigned to this type of redirection.

Configuring Unauthorized Service Redirection

If a TCP packet is destined to the SSG default network or an open garden network configured on the SSG, it is not a candidate for service redirection. Also, if a packet is destined to a service to which the subscriber is already connected, the packet is not redirected.

Otherwise, service redirection redirects a TCP packet if all of the following conditions are true:

- The packet is destined for a service in a configured port-list. For example, you could configure a port-list that makes TCP packets destined for FTP (port 70) and HTTP (port 80) candidates for redirection.
- The packet is destined for a network in a configured network list. For example, you can limit access to specific networks for each service. The SSG rejects packets destined for other networks, unless you configure a default service redirection to redirect the packets destined for other networks.
- The subscriber is not authorized to use the service. Reasons for not being authorized are:
  - Not subscribed to the service
  - Not logged into the service
  - If the SSG prepaid feature is configured, insufficient quota in the account

Cisco IOS Configuration Commands

The following commands from the ssgconfig.txt file configure service redirections:

```
ssg tcp-redirect
 network-list serviceNetwork1
  network 1.1.1.0 255.255.255.0
 !
 network-list serviceNetwork2
  network 2.2.2.0 255.255.255.0
 !
 network-list serviceNetwork3
  network 3.3.3.0 255.255.255.0
 !
 port-list ports
  port 80
  port 8080
server-group serviceRedirect1
  server 10.0.1.4 8094
 !
 redirect port-list ports to serviceRedirect1
 redirect unauthorized-service destination network-list serviceNetwork1 to
serviceRedirect1
 !
 server-group serviceRedirect2
  server 10.0.1.4 8095
 !
 redirect port-list ports to serviceRedirect2
 redirect unauthorized-service destination network-list serviceNetwork2 to
serviceRedirect2
 !
 server-group serviceRedirect3
  server 10.0.1.4 8096
 !
 redirect port-list ports to serviceRedirect3
 redirect unauthorized-service destination network-list serviceNetwork3 to
serviceRedirect3

server-group defaultServiceRedirect
  server 10.0.1.4 8093
 !
 redirect port-list ports to defaultServiceRedirect
redirect unauthorized-service to defaultServiceRedirect
```

The above example does the following:

- Configures three specific service redirections and a default service redirection.
- Applies all of the service redirections to traffic coming into ports 80 and 8080.
- The web server in which the SESM Captive Portal application is running in this example is at IP address 10.0.1.4.
- Each type of service redirection uses a different port on the same web server. See Table 7-1 for more details about the port number.

Shared Address Spaces

It is possible for some services to share some of their address space. For example, consider an Internet service with allowable networks of 0.0.0.0 and a mask 0.0.0.0. (In effect, any address is permissible.) An IPTV service would have a much smaller network space—for example, 1.2.3.0 with a mask of 255.255.255.0). In this situation, having access to the Internet service should not automatically give access to the IPTV service.

You can configure the SSG to handle the situation described above by configuring a specific service redirection for the narrow address space. This takes precedence over the wider address space, thus ensuring that the specific service redirection occurs. You can also configure a wider address space and exclude specific networks in service profiles.

Specifying Service Redirection Networks in the Service Profile

In Cisco IOS Release 12.2.15BW and later, you can specify a service name as the redirected network for unconnected service redirections. SSG obtains the network information from the service profile.

The following commands redirect to a network specified in the service1 profile.

```
server-group serviceRedirect1
server 10.0.1.4 8094
!
redirect port-list ports to serviceRedirect1
redirect unauthorized-service service service1 to serviceRedirect1
```

Configuring Initial Logon Redirection

The initial logon redirection redirects all subscribers when they first authenticate, which is when SSG first creates the edge session.

Redirected Message Duration

The message duration is the length of time that the redirected page is displayed. Message duration is controlled by:

- A globally set parameter set by the Cisco IOS command described below.
- Subscriber-specific values set in the subscriber profiles. The profile value, if it exists, overrides the global value.

Note The SESM captive portal solution also uses duration parameters. See the "Summary of Message Duration Parameters" section on page 4-3 for more information.

Cisco IOS Configuration Commands for Initial Logon Redirection

Use the following command to specify which captive portal group will handle initial logon redirections and to set the duration of the display.

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

The following commands from ssgconfig.txt configure initial logon redirection:

```
ssg tcp-redirect
    port-list ports
        port 80
        port 8080
    server-group initialCaptivate
         server 10.0.1.4 8091
    redirect port-list ports to initialCaptivate
    redirect captivate initial default group initialCaptivate duration 10
```

The above example does the following:

- Creates a port list named ports and a captive portal group named initialCaptivate.
- Assigns one web server, whose IP address is 10.0.1.4, to the group, with a listener on port 8091. (See Table 7-1 for details about the port number.)
- Associates the initialCaptivate group with initial logon redirections.
- Sets the message captivation to last for 10 seconds. The subscriber profile can override the10-second duration value. See the "Summary of Message Duration Parameters" section on page 4-3.
- Specifies that redirections to the initialCaptivate group be applied to TCP packets arriving on the SSG at ports 80 or 8080.

Configuring Advertising Redirection

Advertising redirection redirects browsers to a configured page at timed intervals throughout the SESM session.

Message Duration and Frequency

The length of time that the message is displayed (the duration) and the frequency of the intervals are controlled by:

- Globally set parameters set by the Cisco IOS command described below.
- Subscriber-specific values set in the subscriber profiles. The profile value, if it exists, overrides the global value.

The frequency is approximate, because redirection can occur only when a TCP packet is initiated by the subscriber.

Note The Message Portal application also accepts a duration attribute. See the "Summary of Message Duration Parameters" section on page 4-3 for more information.

Cisco IOS Configuration Commands for Advertising Redirection

Use the following command to specify which captive portal group will handle advertising redirections, and to set the duration and frequency of the display. The valid range for duration and frequency is 1 to 65,536 seconds.

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

The following commands from ssgconfig.txt configure initial logon redirection:

```
ssg tcp-redirect
    port-list ports
        port 80
        port 8080
    server-group advertisingCaptivate
        server 10.0.1.4 8092
    redirect port-list ports to advertisingCaptivate
    redirect captivate advertising default group advertisingCaptivate duration 5
    frequency 60
```

The above example does the following:

- Creates a port list named ports and a captive portal group named advertisingCaptivate.
- Assigns one web server, whose IP address is 10.0.1.4, to the group, with a listener on port 8092.

  In the sample solution, this must be the IP address of the web server for the SESM captive portal application. The port must match the port you configured for advertising redirections in the captiveportal.xml file.
- Associates the advertisingCaptivate group with advertising redirections.
- Sets captivation to last for 5 seconds and to occur every 60 seconds. The subscriber profile can override the duration and frequency. See the "Summary of Message Duration Parameters" section on page 4-3.
- Specifies that redirections to the advertisingCaptivate group be applied to TCP packets arriving on the SSG at ports 80 or 8080.

Configuring Prepaid Redirection

Prepaid redirection is valid if the SSG Prepaid feature is implemented. The prepaid redirection specifies what happens when the prepaid quota is exhausted. This feature is available in Cisco IOS Release 12.2.8B and later.

Configure a default prepaid redirection group as follows:

```
ssg tcp-redirect
server-group PREPAID_REDIR_DEFAULT
server 10.0.1.4 8099
!
redirect prepaid-user to PREPAID_REDIR_SERVER
```

You can also configure a prepaid redirection group on a per service basis instead of a default as follows:

```
    ssg tcp-redirect
    server-group PREPAID_REDIR_SERVICE1
    server 10.0.1.4 8100
```

Configure the per-service redirection in a service profile using the Z subattribute code. For example:

```
    Z;PREPAID_REDIR_SERVICE1
```

Configuring https Redirection

The Captive Portal application includes an https redirect feature that allows SESM to capture users that make secure https requests from their browser. It is necessary to configure this feature after SESM installation using the procedures described in this section.

You use https redirection when a user makes a secure request from their browser. If they are either unauthenticated or they do not have a service connected, they will be TCP redirected by the SSG to the Captive Portal application. Captive Portal needs to receive this request on a particular port, which is specifically designed to handle it.

You can use this feature anywhere that the Captive Portal application is deployed. For example, in a PWLAN deployment, where unauthenticated users could be captured making any type of request.

You use https redirection because you want to provide a successful redirection to users that make secure requests while unauthenticated.

To configure the https redirect feature in Captive Portal involves the following stages:

- In the captive portal config file, captiveportal.xml, you configure the Captive Portal to redirect requests that it receives on its https listener to the appropriate location. See Configuring Captive Portal Using the captiveportal.xml File, page 7-9.
- You then need to configure a secure port-list on the SSG, create a new server-group that points to the https listener on Captive Portal and configure the redirection on the SSG. You do this by copying the relevant sections of the ssgconfig.txt file supplied with your SESM installation into the SSG running-config file. See Configuring the SSG running-config File, page 7-10.

Configuring Captive Portal Using the captiveportal.xml File

To configure the Captive Portal to redirect requests that it receives on its https listener to the appropriate location, proceed as follows:

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

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

Step 2 Within the captiveportal.xml file, locate the following section.

```
<Call name="defineGenericRedirect">
<Arg>8099</Arg>
<Arg>https://nwsp:8443</Arg>
<Arg>CPURL=capturedURL</Arg>
</Call>
```

Step 3 Within this section of the captiveportal.xml file replace the `<Arg>https://nwsp:8443</Arg>` line with the customer's server names, for example www.myself.com.

```
<Call name="defineGenericRedirect">
<Arg>8099</Arg>
<Arg>https://www.mysesm.com</Arg>
<Arg>CPURL=capturedURL</Arg>
</Call>
```

Step 4 Save the modified captiveportal.xml file.

Step 5 Edit the SSG running-config file using the procedures listed in Configuring the SSG running-config File, page 7-10.

Configuring the SSG running-config File

When you have configured the Captive Portal you then need to configure a secure port-list on the SSG, create a new server-group that points to the https listener on Captive Portal and configure the redirection on the SSG. You do this by copying the relevant sections of the ssgconfig.txt file supplied with your SESM installation into the SSG running-config file.

Step 1 Using a text editor, open the ssgconfig.txt file from the following location:

```
<SESM>/captiveportal/config/ssgconfig.txt
```

Step 2 Within the ssgconfig.txt file, copy the following sections of the ssgconfig.txt file into the *ssg tcp-redirect* section of yourSSG running-config file, using the correct IP address and ports where appropriate.

a. Create a new server-group that points to the https listener on Captive Portal using the following section of the ssgconfig.txt file.

```
server-group SECURE_SERVER
  server 192.168.130.10 8099
 !
```

b. Configure a secure port-list on the SSG using the following section of the ssgconfig.txt file.

```
port-list SECURE_PORTS
  port 443
  port 8443
 !
redirect port-list SECURE_PORTS to SECURE_SERVER
```

c. Configure the redirection on the SSG using the following sections of the ssgconfig.txt file.

```
network-list ALL
  network 0.0.0.0 0.0.0.0
 !

redirect unauthorized-service destination network-list ALL to SECURE_SERVER
 redirect unauthenticated-user to SECURE_SERVER
```

Step 3 Save the modified copy of your SSG running-config file.

Your Captive Portal can now handle https redirects.

Troubleshooting Captive Portal Configurations

This chapter describes some symptoms, possible causes, and corrective actions for captive portal installation and configuration problems. The chapter contains the following topics:

Troubleshooting Approach

The following approach is recommended to configure and troubleshoot a captive portal solution:

1. Start with the example configuration in the ssgconfig.txt file. Get this configuration working before proceeding.
2. After the example is working, you can begin to make changes in the configuration. Make changes in the following order:
   a. IP addresses
   b. Port numbers
   c. Server names

Some TCP Redirection Types Not Operational

If some TCP redirections do not seem to be occurring, check whether any of the following configuration problems exist:

Redirection Type Turned Off or Misconfigured in captiveportal.xml

Check the parameters in the captiveportal.xml file:

- Make sure that the redirection type is turned on (true). Check these attributes:
  - UserRedirectOn
  - InitialCaptivateOn
  - AdvertisingCaptivateOn
  - ServiceRedirectOn
- Make sure that URL attribute for the redirection type contains valid URL values.
- Make sure that the default value for the redirection type contains valid values.

Two Redirection Types Assigned to the Same Port in captiveportal.xml

If you use the same port number for more than one type of redirection in the captiveportal.xml file, only one of the redirections per port is operational. This might happen if, during captive portal installation, you change the default port numbers suggested by the installation program, and erroneously reuse the same port number.

The precedence order that determines which type of redirect is operational on a port is:

1. Unauthorized user redirections
2. Initial logon redirections
3. Advertising redirections
4. Service redirections

Redirection Type Not Configured on the SSG

Check the SSG configuration to make sure that:

- The redirection type is associated with a server group that uses the SESM Captive Portal application (and not the Message Portal application).
- The redirection type is associated with the same port that you specify in the captiveportal.xml file for that redirection type.

The following command associates a specific type of redirection to a server group:

```
ssg tcp-redirect redirect redirection-type to group-name
```

The following command assigns a specific application (using the application's IP address and port) to a server group:

```
ssg tcp-redirect server-group group-name server ip-address port
```

For the SESM example solution to work, you must assign the IP address and port of the SESM captive portal application to all of your server groups. Do this by using the following values in the above command:

- The IP address of the captive portal application.
- The port that you configured in the captiveportal.xml file for the specific type of redirection. The installation program initially sets these ports. Table 7-1 on page 7-2 shows the port values that are configured at installation time if you accepted all of the default values during installation.

Redirections Continuously Occur

If the browser is continuously redirected to the same page, investigate the following topics:

- Redirected Networks Do Not Match Service Routes, page 8-3
- Using HTTP1.1 with a Non-SESM Captive Portal Application, page 8-3

Redirected Networks Do Not Match Service Routes

The service route for a service, which is defined in the service profile, must exactly match the destination network that you configure in a service redirection for that service.

For example, suppose you want to establish service redirections for a service on network 10.1.1.1. If you define the incoming destination network that is eligible for redirections as follows:

```
ssg tcp-redirect
network-list serviceNetwork1
    network 10.1.1.0 255.255.255.0
```

You must then define the service route for the service using the same IP address and mask (10.1.1.0 and 255.255.255.0).

If you define the service route differently (for example, you use 10.1.1.1 and 255.255.255.255), then the service redirection occurs repeatedly. After the first and required service redirection, any subsequent requests are subject to the service redirection, even though the service is connected.

The symptom of this misconfiguration is the continuous redisplay of the redirect URL. For example, in the sample SESM solution, the NWSP service logon page appears each time you click the OK button, even though the service is already connected.

Using HTTP1.1 with a Non-SESM Captive Portal Application

If you deploy a web server other than the SESM Captive Portal application as the redirect server, and the web server uses HTTP1.1, make sure to use the protocol options that explicitly close the connection for each response from the web server.

```
//Close connection for HTTP 1.1 - this is essential
        response.setHeader("Connection","close");
```

HTTP1.1 persists connections. The persistent connection causes the SSG to continue redirecting for subsequent requests because it is still handling the same connection. The SSG continues redirecting even after the mapping times out on the SSG. This behavior is particularly noticeable for initial captivation, where one would expect the redirection to occur only one time.

User Name Not Passed in Unauthenticated User Redirections

If the captive portal application is not passing the subscriber name (CPSUBSCRIBER) in the HTTP redirection for unauthenticated user redirections:

- Ensure that the SSG is configured as described in the "Defining Captive Portal Groups and Port Lists" section on page 7-2.
- Check the following two attributes in captiveportal.xml. If they are empty, the captive portal application does not attempt to retrieve or pass the subscriber name.

- messageRedirectSubscriberParam
- serviceRedirectSubscriberParam

Note When these two attributes are empty, the user name feature is turned off. This might be desirable, for example, for performance reasons.

Captive Portal Demo

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

Assumptions

The procedures in this appendix make the following assumptions:

- You have a fully configured SESM deployment in RADIUS or LDAP mode, including verified communication with an SSG.
- You installed the SESM captive portal solution using the default configuration values presented by the installation program.
- You completed the configuration of the captive portal solution, described in Chapter 4, "Configuring the Captive Portal Solution."

Demo Procedures

To demonstrate captive portal features, follow these steps:

Step 1 Start all of the applications in the captive portal solution by executing their startup 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 attempt to display a home page setting.

Unauthenticated user redirection causes the NWSP logon 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 pop-up window appears, intended for the originally requested URL (www.yahoo.com).

c. Initial logon redirection causes the greetings page from the Message Portal application 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—The Message Portal application redirects the browser to the originally requested URL (www.yahoo.com). The service is subjected to service redirections. See Appendix B, "Message Redirection" for the message redirection sequence diagram.
- False—The greetings page continues to display 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 logon 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 attempts to start the service. It brings the service pop-up window to the foreground.

See Appendix B, "Prepaid Session Redirection" for the prepaid session redirection sequence diagram.

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, from the NWSP service selection list, select a service with an IP address outside the destination networks of all the specific service redirections. It does not matter if the subscriber is subscribed to the service or not.

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 could 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:

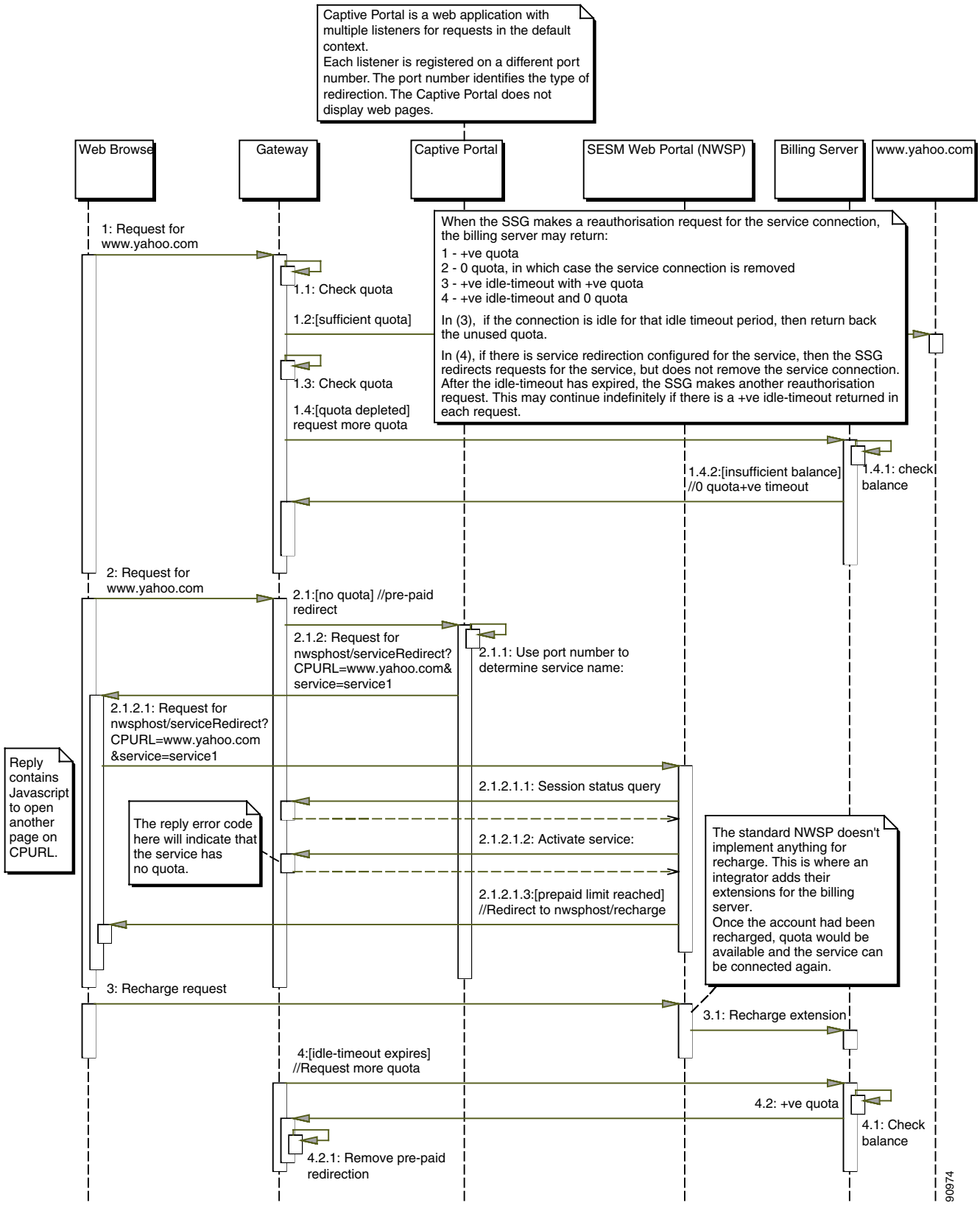
1. Wait until the configured TCP advertising interval time has elapsed. (The default time interval used during installation is 60 seconds.)
2. Perform some action on the SESM web page, such as selecting another service or requesting the status page. The SSG intercepts the request with an advertising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

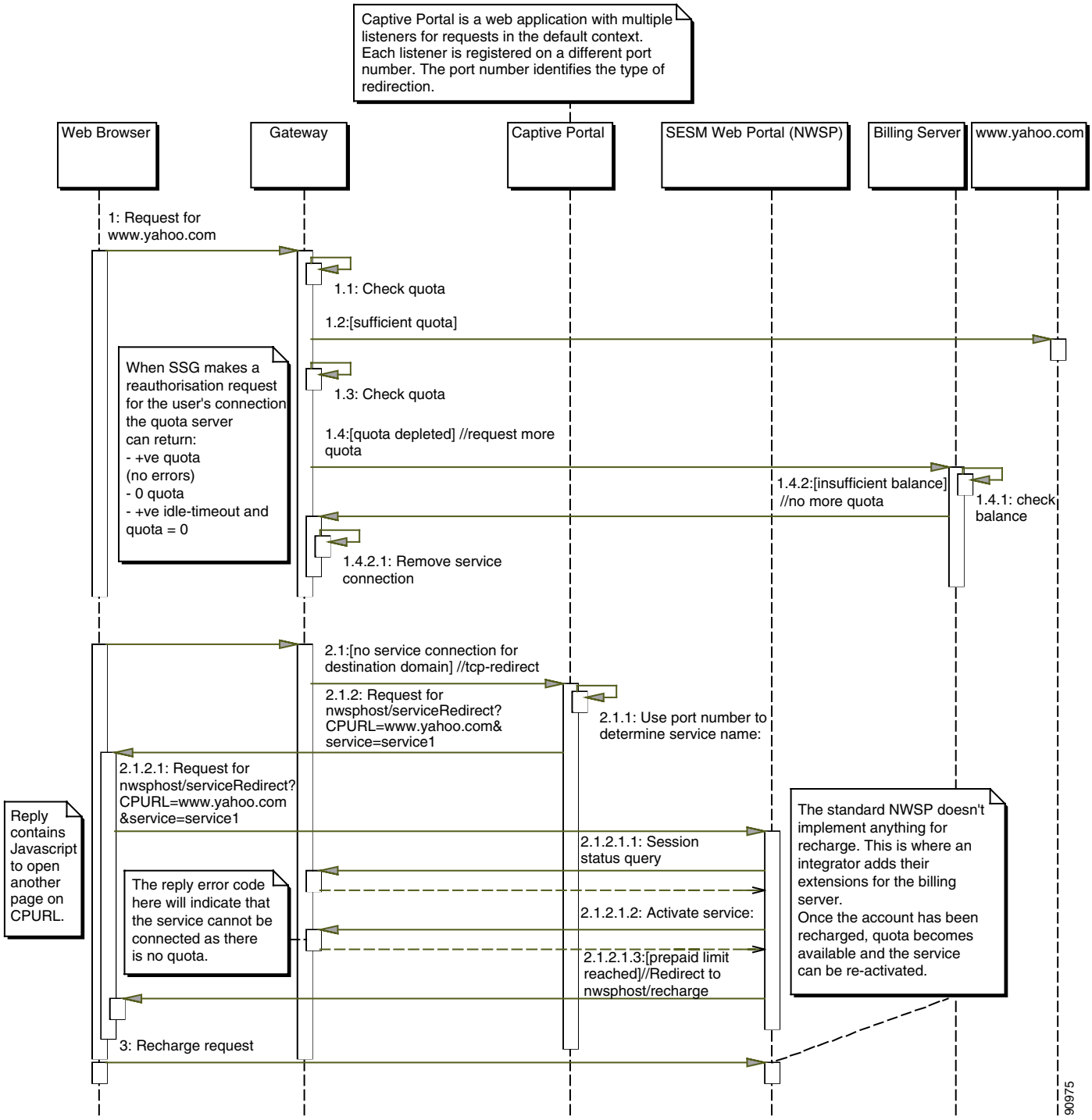
Captive Portal Sequence Diagrams

This appendix contains sequence diagrams for the following scenarios:

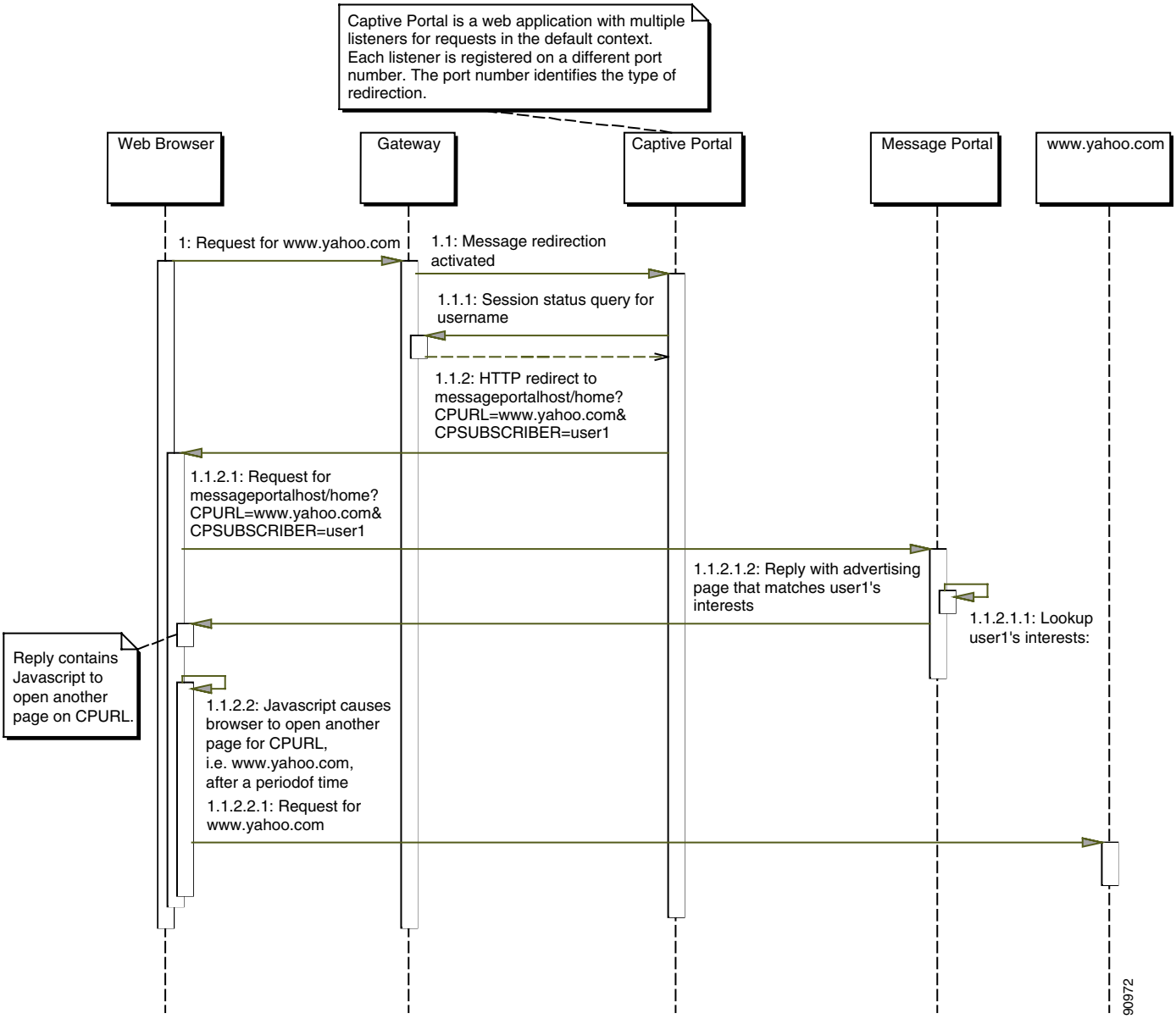
Prepaid Session Redirection



Prepaid Service Redirection



Message Redirection



A

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

W

Z