Deploying a Captive Portal Solution

This chapter describes how to configure the SESM sample captive portal solution. The chapter contains the following topics:

SSG and SESM Release Requirements

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

Captivation Type	Required Cisco IOS Release Level (SSG)	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.

Solution Description

This section describes the SESM captive portal solution. It contains the following topics:

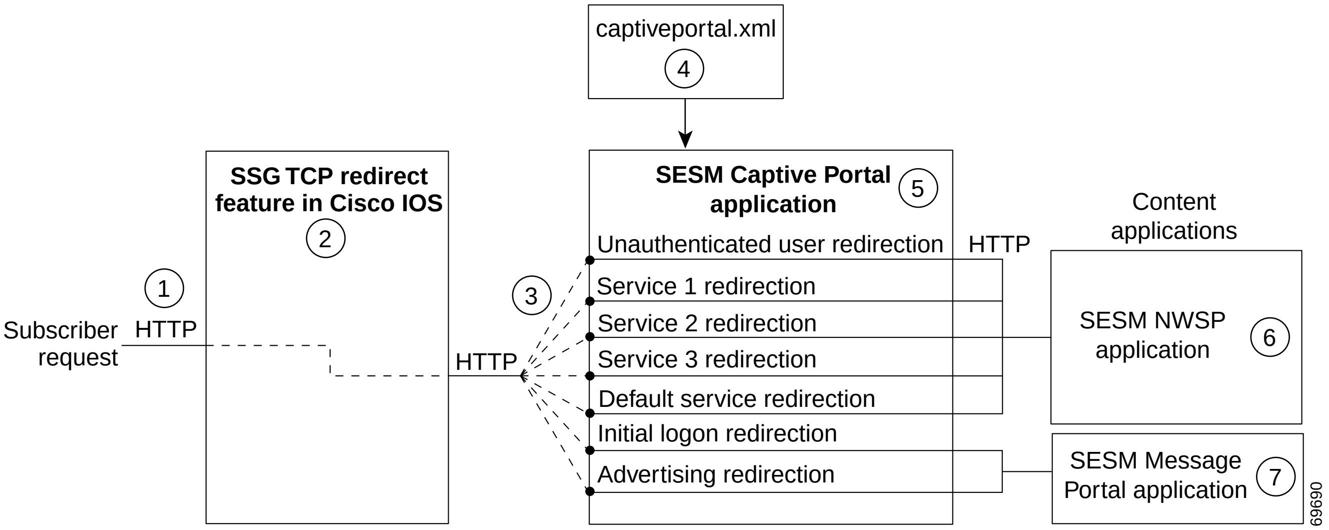
- Solution Diagram, page 11-2
- SESM Captive Portal Application, page 11-3
- Content Applications, page 11-4
- Alternative Configuration Options for a Captive Portal Solution, page 11-5

Solution Diagram

Figure 11-1 illustrates how the components in the SESM captive portal solution work together to provide appropriate content to the subscriber.

Note Figure 11-1 shows the sample solution configured using all of the default values provided by the SESM installation program. There are many possible variations to this default deployment.

Figure 11-1 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 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. • The IP address must identify a web server running an SESM Captive Portal application. All types of redirection can use the same web server (the same IP address). • Each type of redirection must use a different port value. The port number identifies the type of redirection to the SESM Captive Portal application.

4	The captiveportal.xml file associates an incoming port number to a content application URL. The SESM Captive Portal application uses the services of a JMX server to obtain the attribute values from the XML file.
5	The SESM Captive Portal application acts as a gateway to the content applications. It issues an HTTP redirect that redirects the subscriber's browser to an appropriate content application. 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 NWSP portal is the content application that services unauthenticated user redirection and service redirections.
7	The Message Portal is the content application that services initial logon and advertising redirections.

SESM Captive Portal Application

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 preserve and pass along information from the original subscriber request to the content applications.

Table 11-1 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 11-1 Parameters Appended to URLs in HTTP Redirections

Type of SSG TCP Redirection	Parameter Name in SESM Captive Portal HTTP Redirect	Explanation and Usage by the Content Applications
Unauthenticated user redirection	CPURL	The URL in the subscriber's original request. The NWSP application uses this value to redirect the browser to this original request after successful authentication.
Service redirection	service	The service name that was requested in the original request.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 "Message Duration Parameters—Summary" section on page 11-17.
	CPSUBSCRIBER	The subscriber name as obtained from the subscriber profile.

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

The NWSP application is the content application for unauthenticated user redirections and unauthorized service redirections.

- For unauthenticated user redirections—NWSP presents the SESM login page so the subscriber can authenticate.
- For unauthorized access to specific 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 LDAP 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 (unauthorized 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 11-1 on page 11-3 for a description of the parameters that the Captive Portal application forwards to the NWSP application.

Message Portal Application

The SESM Message Portal application provides the message pages for initial and advertisement captivation. It provides the following content pages:

- Greetings page for initial captivation
- Advertising page for advertising captivation
- In LDAP mode, the Message Portal application displays an advertisement 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 11-1 for a description of the parameters that the Captive Portal application forwards to the Message Portal application.

Alternative Configuration 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 Some 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 Some 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 Different 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 Different Captive Portal Application

The SSG TCP redirect feature can accept any type of web application in the SSG captive portal groups. There is no requirement to use the SESM Captive Portal application. In addition, there is no requirement to use the 2-tiered approach used by the SESM solution. However, using the 2-tiered approach with 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.
- It simplifies configuration when you want to add or change content applications to your solution. In those cases, 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 host device.

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 and Running the Sample Solution

This section describes how to install and configure the sample captive portal solution in the quickest possible configuration. To alter the default configuration after installation, see the "MBeans in the Captive Portal Solution" section on page 11-9.

This section includes the following topics:

- Installing the Sample Solution, page 11-6
- Installation Results, page 11-6
- Additional Configuration Steps, page 11-7
- Starting the Sample Captive Portal Solution, page 11-9

Installing the Sample Solution

Install the sample captive portal solution from the SESM installation package. Detailed installation procedures for captive portal are included with the installation procedures for other SESM components. .

The following information concerning captive portal installation is important:

- You must choose **Custom Install** to install the captive portal solution. Captive portal is not included in a typical installation.
- Many of the captive portal installation parameters must match TCP redirect configuration values on the SSG. 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 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 11-7 for instructions on using ssgconfig.txt.

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
```

Additional Configuration Steps

This section describes configuration that you must perform before you can see the captive portal solution in operation. These tasks are in addition to the configuration performed by the installation program.

- Configuring the SSG to Match the Installed Captive Portal Solution, page 11-7
- Loading Sample Profiles for Captive Portal Demonstration, page 11-8
- (Optional) Configuring Unique Service Logon Pages for Service Redirections, page 11-8

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 device is running the appropriate Cisco IOS release, as described in the "SSG and SESM Release Requirements" section on page 11-1. 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 on page F-1.

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 commands required to configure the four types of TCP redirection that the sample captive portal solution can demonstrate. The commands in this file will configure SSG to match the default values presented during the captive portal installation. The file includes placeholder 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 database or LDAP directory. To fully demonstrate all of the features of the solution, the profiles should include:

- Service profiles should 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 Must Match Service Routes" section on page 11-24.
- Subscriber profiles must include subscriptions to the above services.
- For LDAP mode, subscriber profiles should include hobbies. Hobbies are required to illustrate the Message Portal's capability to display messages tailored to the first hobby listed in the subscriber profile.

In LDAP mode, create some basic subscriber profiles using CDAT. You can then use the NWSP account management feature to modify interests (hobbies) or add subscriptions.

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.

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.

Starting the Sample Captive Portal Solution

The following table shows the startup script names for the applications in the sample captive portal solution.

Platform	Startup Scripts

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

Windows NT	`jetty\bin\startCAPTIVEPORTAL.cmd`
	`jetty\bin\startMESSAGEPORTAL.cmd`
	`jetty\bin\startNWSP.cmd`

For information about the contents of these startup scripts, see Chapter 9, “Running SESM Components.” The optional mode argument described in that chapter can be used with these startup scripts. However, the run mode for the Captive Portal and Message Portal applications must agree with the run mode of the main portal application (NWSP).

MBeans in the Captive Portal Solution

This section describes the MBeans in the captive portal solution. The topics are:

- MBeans in the Captive Portal Application, page 11-10
- Message Portal Application MBeans, page 11-13
- Captive Portal Attributes in the NWSP WebAppMBean, page 11-16

MBeans in the Captive Portal Application

The captive portal application uses the following MBeans:

- Logger MBean, page 11-10
- ManagementConsole MBean, page 11-10
- captiveportal MBean, page 11-11

To change attributes in these MBeans, you can use either of the following methods:

- Edit the captive portal MBean configuration file:

```
captiveportal
    config
       captiveportal.xml
```

- Make changes using the Agent View running on the Captive Portal management port. The installation process uses the following default port numbers for captive portal:
  - Captive portal port—8090
  - Captive portal management port—8190

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs captive portal application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the "Logger MBean" section on page 5-2 for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the management console port for CDAT, including valid user names and passwords for accessing the console. See the "Configuring the ManagementConsole MBean" section on page 3-5 for more information.

captiveportal MBean

Table 11-2 explains attributes in the captiveportal MBean.

Table 11-2 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 that 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 and/or addresses. The application uses this attribute to detect loops. If the request host and this host value match, as well as the request port and the listener port, the captive portal application redirects the browser to the URL in errorURL.
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.	
userRedirectURL initialCaptivateURL advertisingCaptivateURL	The URL that you want the subscriber's browser to be redirected to after each type of redirection. Each URL is constructed as: http://*host*:*portURI* where: • *host* is the IP address or host name of the web server for the content application that will handle the redirection type. The host is defined as one of the following java system properties: – serviceportal.host (usually the NWSP IP address) – messageportal.host (usually the Message Portal IP address) • *port* is the port that the web server is listening on. The port is defined as one of the following java system properties: – serviceportal.port – messageportal.port • *URI* is the absolute path for the page within the content application that you want the subscriber's browser to be redirected to. The default values used during installation are: – For user redirections: /home, which is the NWSP logon page. – For initial logon redirections: /initial, which is the Message Portal greetings page. – For advertising redirections: /advertising, which is the Message Portal advertising page. The default values for the system properties and the URIs were set during installation in the URL Out fields.

Table 11-2 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 • initialCaptivate.port • advertisingCaptivate.port 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 "Message Duration Parameters—Summary" section on page 11-17 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. If you change a port value, also change the SSG configuration to send the service redirection to the same port value. **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 11-2 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.

Message Portal Application MBeans

The Message Portal application uses the following MBeans:

- Logger MBean, page 11-14
- ManagementConsole MBean, page 11-14
- SESMMBean, page 11-14
- SESMDemoMode MBean, page 11-14
- DESSMode MBean, page 11-14
- messageportal MBean, page 11-15

To change attributes in these MBeans, you can use either of the following methods:

- Edit the Message Portal MBean configuration file:

```
messageportal
    config
       messageportal.xml
```

- Make changes using the Agent View running on the messageportal management port. The installation process uses the following default port numbers for message portal:
  - Message portal port—8085
  - Message portal management port—8185

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs Message Portal application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the "Logger MBean" section on page 5-2, for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the management console port for the Message Portal application, including valid user names and passwords for accessing the console. See the "Configuring the ManagementConsole MBean" section on page 3-5 for more information.

SESMMBean

The SESMMBean is required in all SESM portal applications. It sets the SESM mode for the application. The "SESM MBean" section on page 5-4 describes this MBean.

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

- LDAP, if the mode for the Captive Portal application is LDAP.
- Demo, if the mode for the Captive Portal application is RADIUS. (The Message Portal application does not obtain any subscriber profile information from a RADIUS database; therefore RADIUS mode is not implemented in this sample application. Demo mode provides all of the required SESM functionality.)

SESMDemoMode MBean

The SESMDemoMode MBean is required in all SESM portal applications that are running in Demo mode. See the "SESMDemoMode MBean" section on page 5-6 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, as described in Table C-6 on page C-11, "Attributes in Subscriber Profiles".

DESSMode MBean

The DESSMode MBean is required in all SESM portal applications that are running in LDAP mode. See the "DESSMode MBean" section on page 5-6 for more information about this MBean.

messageportal MBean

Table 11-3 explains the configuration attributes in the messageportal MBean.

Table 11-3 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).
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 the redirection to the subscriber's originally requested URL. **Note** The SSG TCP redirect commands also accept a duration attribute. See the "Message Duration Parameters—Summary" section on page 11-17 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 11-3 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 LDAP 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 11-4 explains configuration attributes in the WebAppMBean that are directly related to the captive portal solution.

Table 11-4 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.

Table 11-4 Captive Portal Attributes in the WebAppMBean (continued)

Attribute Name	Explanation
defaultURI	For service redirections, tells NWSP which page to redirect to if: • The service specified in the HTTP request from the Captive Portal application is not available. • The service exists, the subscriber is not subscribed to it, and the subscriber does not have permission to visit the subscription page. • Any other unexpected conditions The default value that exists after installation is the NWSP home page.
serviceSubscriptionURI	For service redirections, tells NWSP which page to redirect to if the subscriber is not subscribed to the service that is specified in the HTTP request from the Captive Portal application. The default value that exists after installation is: • In LDAP 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 LDAP 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.

Message Duration Parameters—Summary

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 longer 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 SSG TCP redirect commands.
- 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.

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 the SSG TCP Redirect Features

This section summarizes how to configure the TCP redirect features on the SSG host device. For additional information, see the SSG documentation listed in the "Related Documentation" section on page xv.

This section includes the following topics:

- Configuring SSG and Port-Bundle Host Key to Work with the Captive Portal Application, page 11-19
- Defining Captive Portal Groups and Port Lists, page 11-19
- Configuring Unauthenticated User Redirection, page 11-20
- Configuring Unauthorized Service Redirection, page 11-20
- Configuring Initial Logon Redirection, page 11-22
- Configuring Advertising Redirection, page 11-22

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 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()
   ```

Defining Captive Portal Groups and Port Lists

SSG sends a redirected TCP packet to a 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
```

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 the following sections illustrate how to create port lists and captive portal groups.

Configuring Unauthenticated User Redirection

When a subscriber is authenticated, SSG creates a host object for that subscriber. The absence of a host object relating to the source address of the packet indicates the need to redirect the packet to the portal group that is associated with unauthenticated user redirection. The result is that subscribers cannot access any part of the network beyond the SSG without first authenticating.

If you do not configure a captive portal group to handle TCP packets from unauthenticated users, SSG discards packets from unauthenticated users. To obtain the SESM logon page, subscribers must enter the URL of the SESM web server.

PPP Connections—A Special Case

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 host object 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 group-name
```

The following commands from ssgconfig.txt create a captive portal group named userRedirect. The group consists of one web server whose IP address is 10.0.1.4, with a listener on port 8090. (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 unauthenticated user redirections in the captiveportal.xml file.) The userRedirect group is associated with unauthenticated user redirections. A port list cannot be assigned to this type of redirection—user redirection applies to all TCP packets that are not authenticated.

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

Configuring Unauthorized Service Redirection

If a TCP packet is destined to the SSG default network or Open Gardens, it is not a candidate for service redirection. Also, if it is destined to a service to which the subscriber is already connected, the packet is not examined for redirection.

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, not enough funds in the account

Cisco IOS Configuration Commands

The following IOS commands from ssgconfig.txt configure three specific service redirections and a default service redirection. All of the service redirections are applied only to traffic coming into ports 80 and 8080. Each type of service redirection uses a different port on the same web server (the web server at IP address 10.0.1.4, which is the web server in which the SESM Captive Portal application is running).

```
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
```

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.

Configuring Initial Logon Redirection

The initial logon redirection redirects all subscribers when they first log on, which is when SSG first creates the host object for the session. (is that true?). The length of time that the message is displayed 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 "Message Duration Parameters—Summary" section on page 11-17 for more information.

Cisco IOS Configuration Commands

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 create a port list named ports and a captive portal group named initialCaptivate. The group consists of one web server whose IP address is 10.0.1.4, with a listener on port 8091. (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 initial logon redirections in the captiveportal.xml file.) The initialCaptivate group is associated with initial logon redirections. The message captivation lasts for 10 seconds, unless the subscriber profile overrides that value. Redirections to this group are applied to TCP packets arriving on the SSG at ports 80 or 8080, as specified in the port list.

```
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
```

Configuring Advertising Redirection

The advertising redirection redirects subscribers at timed intervals throughout the current session. 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 "Message Duration Parameters—Summary" section on page 11-17 for more information.

Cisco IOS Configuration Commands

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 create a port list named ports and a captive portal group named advertisingCaptivate. The group consists of one web server whose IP address is 10.0.1.4, 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.) The advertisingCaptivate group is associated with advertising redirections. The captivation lasts for 5 seconds and occurs every 60 seconds, unless the subscriber profile overrides those values. Redirections to this group are applied to TCP packets arriving on the SSG at ports 80 or 8080, as specified in the port list.

```
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
```

Troubleshooting Captive Portal Configurations

This section describes some potential problems with captive portal installation and configuration:

- Some TCP Redirection Types Not Operational, page 11-23
- Redirections Continuously Occur, page 11-24
- User Name Not Passed in Unauthenticated User Redirections, page 11-25

Some TCP Redirection Types Not Operational

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

- Redirection Type Turned Off in captiveportal.xml, page 11-24
- Two Redirection Types Assigned to the Same Port in captiveportal.xml, page 11-24
- Redirection Type Not Configured on the SSG, page 11-24

Redirection Type Turned Off in captiveportal.xml

Check the following parameters in the captiveportal.xml file to make sure that the redirection type is turned on in the captive portal application:

- userRedirectOn
- initialCaptivateOn
- advertisingCaptivateOn
- serviceRedirectOn

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 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.

Redirections Continuously Occur

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

- Redirected Networks Must Match Service Routes, page 11-24
- Using HTTP1.1 with a Non-SESM Captive Portal Application, page 11-25

Redirected Networks Must 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
```

then you must 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.

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 11-19.
- 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.