



Deploying a Captive Portal Solution

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

- [Introduction, page 8-1](#)
- [SSG and SESM Release Requirements, page 8-2](#)
- [Solution Description, page 8-2](#)
- [Installing, Configuring, and Running the Sample Solution, page 8-8](#)
- [Configuration Details, page 8-13](#)
- [Configuring the SSG TCP Redirect Features, page 8-22](#)
- [Troubleshooting Captive Portal Configurations, page 8-26](#)

Introduction

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 an 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.
- Ensure that subscribers are only allowed to access the services that the service provider wants them to access.
- Ensure that subscribers are shown a specific message for a defined period while attempting to access services.
- Display advertising messages at specified intervals during an SESM session.
- Display advertising messages based on specific subscriber characteristics, such as hobbies.

All of the above mentioned uses of captive portal are demonstrated in the sample captive portal solution that comes with the SESM package. With some customized programming and development, the following additional types of activities could be achieved using an 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.

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 chapter assumes that you are using SESM applications.

Solution Description

The SESM installation package includes a sample captive portal solution using SESM portal applications. This section describes the components in the sample solution. Topics in this section are:

- [Solution Diagram, page 8-2](#)
- [SSG TCP Redirect Feature, page 8-3](#)
- [SESM Captive Portal Application, page 8-5](#)
- [Content Applications, page 8-6](#)
 - [NWSP Application, page 8-6](#)
 - [Message Portal Application, page 8-6](#)
- [Alternative Configuration Options for a Captive Portal Solution, page 8-7](#)

Solution Diagram

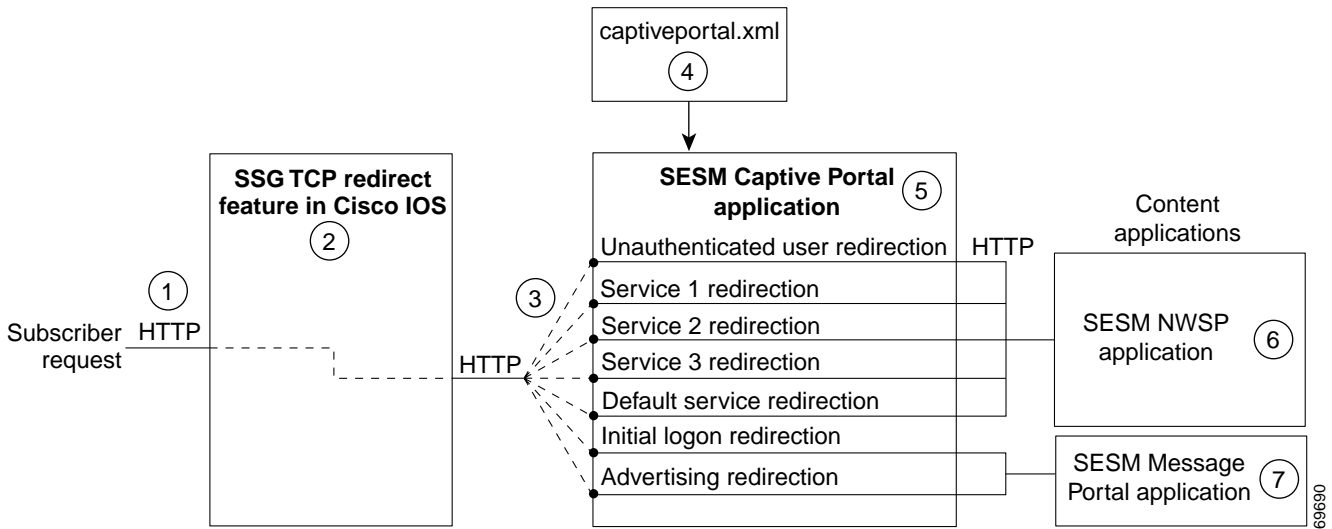
[Figure 8-1](#) illustrates how the components in the SESM captive portal solution work together to provide appropriate content to the subscriber.



Note

[Figure 8-1](#) 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 8-1 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. <ul style="list-style-type: none"> 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. |

SSG TCP Redirect Feature

The SSG TCP redirect feature intercepts TCP packets and reroutes them to a configured group of captive portal applications, usually SESM captive portal applications. The SSG modifies the IP address and the port in the TCP packet to cause the redirection. The reason for the redirection and the redirected destinations are configured on the SSG using Cisco IOS commands.

Table 8-1 describes the SSG TCP redirection types and how the SESM captive portal solution supports those redirection types.

Table 8-1 Supported Redirection Types

| Redirect Type | Role of SSG TCP Redirect Feature | Role of SESM Captive Portal Solution |
|---|---|---|
| Unauthenticated user redirection—Handles attempted access to services by subscribers who have not yet authenticated to SSG. | <p>Without TCP redirection, the SSG discards packets from unauthenticated users. That is, the subscriber needs to know the URL of a logon page, such as an SESM logon page, to authenticate with the SSG before accessing any services.</p> <p>With TCP redirection, these packets are allowed some controlled access to particular services within the SSG, such as access to a captive portal application.</p> | <p>Provides a logon page so the subscriber can authenticate.</p> <p>In a point-to-point protocol (PPP) client with single sign-on enabled, performs authentication transparently to the subscriber.</p> <p>After authentication, redirects the browser again to the subscriber's original request.</p> |
| Unconnected service redirection—Handles unauthorized attempts to access a service. | <p>Without TCP redirection, the SSG discards packets directed at services for which the subscriber is not authorized. With TCP redirections, these packets are allowed controlled access to particular services within the SSG, such as an SESM captive portal solution. There are two types of service redirection:</p> <ul style="list-style-type: none"> • Specific service redirection—Redirects access to specific networks. • Default service redirection—Redirects unauthorized access to networks not handled by the specific service redirections. | <p>For specific service redirections, presents a logon page specific to the service being requested.</p> <p>For default service redirections, displays a default service selection page. In an LDAP deployment, displays a self-subscription page if the subscriber is not already subscribed to the service.</p> |
| Initial logon redirection—Gives providers a way to deliver messages to subscribers when they first log in. | <p>Redirects all TCP packets destined to a configured list of ports when the host object is first created.</p> <p>Activates a timing mechanism for a specified duration, during which the subscriber is truly captivated and cannot redirect the browser. The configured Captive Portal application (as opposed to SSG) controls what occurs after the duration time elapses.</p> | <p>Provides message content.</p> <p>After the message duration time elapses, optionally redirects the browser to the original request with no further action required from the subscriber.</p> |
| Advertising redirection—Gives providers a way to deliver advertising or other messages at timed intervals during an active session. | <p>Redirects all TCP packets destined to a configured list of ports at specified intervals.</p> <p>Activates a session timing mechanism to keep track of the time since the last advertisement. When the configured interval elapses, SSG performs an advertising redirection the next time the subscriber initiates a TCP packet.</p> <p>Activates a message duration timing mechanism as described above for the initial logon redirection.</p> | <p>Provides advertising content.</p> <p>After the advertising duration time elapses, optionally redirects the browser to the previous URL with no further action required from the subscriber.</p> |
| 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

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.

The SESM Captive Portal application performs the following functions:

- Preserves information from the subscriber's original HTTP request.
- Issues an HTTP redirection that redirects the subscriber's browser to a content application that can handle the request appropriately and provide content to the subscriber. The HTTP redirect includes the preserved information from the original subscriber, in the form of parameters appended to the redirection URL.
- Determines which content application should handle the request based on configuration attributes that associate incoming port numbers to content application URLs. These URLs can point to different pages within the same application, or to different applications.

Table 8-2 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.

See Table 8-4 on page 8-15 for a description of the configuration attributes in the captiveportal.xml file.

Table 8-2 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. |
| 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. There are duration attributes on both the SSG side and the SESM side. See the "Message Duration Parameters" section on page 8-21 . |
| | 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 8-1 on page 8-4](#) for a description of the parameters that the Captive Portal application forwards to the NWSP application.

See [Table 8-6 on page 8-20](#) for a description of the configuration attributes in the `nwsp.xml` file related to captive portal.

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 8-1 on page 8-4](#) for a description of the parameters that the Captive Portal application forwards to the Message Portal application. See [Table 8-5 on page 8-17](#) for a description of the configuration attributes in the `messageportal.xml` file.

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 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 that redirection type on the SSG.

Eliminating J2EE Listeners

The web server container in which the captive portal application is running is configured with a separate listener for each TCP redirect port you configured. That is, there is a separate listener 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 would require 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, Configuring, and Running the Sample Solution

This section describes how to install and configure the sample solution in the quickest possible configuration. To alter the default configuration after installation, see the [“Configuration Details” section on page 8-13](#).

This section includes the following topics:

- [Installing and Configuring the Sample Solution, page 8-8](#)
- [Installation Results, page 8-9](#)
- [Additional Configuration Steps, page 8-9](#)
- [Starting the Sample Solution, page 8-11](#)
- [Demonstrating Captive Portal Features, page 8-12](#)

Installing and Configuring 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 captive portal installation starts in the [“Captive Portal Server Configuration” section on page 5-24](#).

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 8-9](#) 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
  docroot
  docs
messageportal
  config
    messageportal.xml
  docroot
  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 8-9](#)
- [Loading Sample Profiles for Captive Portal Demonstration, page 8-10](#)
- (Optional) [Configuring Unique Service Logon Pages for Service Redirections, page 8-10](#)

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 8-2](#). If not, upgrade the Cisco IOS release before proceeding.
- Step 2** Make sure that basic SSG functionality is enabled and configured, as described in [Appendix B, “Configuring the SSG.”](#)
- 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 program displays default inputs for captive portal group names and port numbers. The default inputs 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, changing 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 8-28.
- 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 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 7, “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).

Demonstrating Captive Portal Features

To demonstrate captive portal features:

Step 1 Make sure the SSG is configured as described in the [“Configuring the SSG to Match the Installed Captive Portal Solution” section on page 8-9](#).

Step 2 Start all of the applications in the captive portal solution by executing their startup scripts:

```
jetty
  bin
    startNWSP
    startCAPTIVEPORTAL
    startMESSAGEPORTAL
```

Step 3 Open a web browser from a network configured as an incoming network on the SSG. Attempt to go to a popular Internet page, 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 display.

Step 4 Sign on using a user ID and password from the subscriber profiles you loaded. After successful authentication, the following occurs:

1. The NWSP home page appears in the main window.
2. A pop-up window appears, intended for the www.yahoo.com URL.
3. Initial logon redirection causes the greetings page from the Message Portal application to display in the pop-up window.
4. After the length of time specified by the duration parameter, one of the following occurs:
 - If the `redirectOn` configuration parameter for Message Portal is set to true, the Message Portal application redirects the browser to the originally requested URL (www.yahoo.com). The service is subjected to service redirections (see the next item).
 - If the `redirectOn` configuration parameter for Message Portal is set to false, the greetings page continues to display until you enter another URL.
5. 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 it does not find the service, NWSP displays the home page.
 - Otherwise, NWSP attempts to start the service and brings the service pop-up window to the foreground.

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 pages, 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 redisplay.
-

Configuration Details

This section describes the configuration details for the SESM captive portal solution. Use this section if you want to change configuration after installation. This section includes the following topics:

- [Configuration File Summary, page 8-14](#)
- [captiveportal.xml Configuration File, page 8-15](#)
- [messageportal.xml Configuration File, page 8-17](#)
- [nwsp.xml Configuration File, page 8-20](#)
- [Message Duration Parameters, page 8-21](#)

Configuration File Summary

Table 8-3 lists all of the configuration files that affect the sample SESM captive portal solution.

Table 8-3 Configuration Files in the SESM Captive Portal Solution

| Component | File Path and Name | For More Information |
|--|--|--|
| J2EE configuration files | jetty config webdefault.xml | See the “ J2EE Configuration Files ” section on page 6-3 for a summary of these files. |
| | applicationName docroot WEB-INF web.xml | See the <i>Cisco Subscriber Edge Services Manager Web Developer Guide</i> for SESM-specific information in these files. |
| Jetty container MBean configuration file | jetty2 config captiveportal.jetty.xml nwsp.jetty.xml messageportal.jetty.xml | These files configure the jetty containers for each of the applications. For more information, see the following sections: <ul style="list-style-type: none"> • Configuring the J2EE Jetty Container, page 6-7 • Eliminating J2EE Listeners, page 8-7 |
| Application MBean configuration files | captiveportal config captiveportal.xml messageportal config messageportal.xml nwsp config nwsp.xml | The Captive Portal and Message Portal applications use an MBean to retrieve configuration attributes from an xml file in the same way that any SESM portal application retrieves configuration attributes. The following sections describe attributes related to captive portal configuration: <ul style="list-style-type: none"> • captiveportal.xml Configuration File, page 8-15 • messageportal.xml Configuration File, page 8-17 • nwsp.xml Configuration File, page 8-20 |

captiveportal.xml Configuration File

Table 8-4 explains the configurable attributes used by the Captive Portal application.

Table 8-4 Attributes in the Captive Portal MBean Configuration File

| Object Name | Attribute Name | Explanation |
|--|---|--|
| Logger | | See the Logger object in Table 6-4 on page 6-16. |
| ManagementConsole | | See the ManagementConsole object in Table 6-4 on page 6-16. |
| captiveportal | userRedirectOn initialCaptiveOn advertisingCaptiveOn serviceRedirectOn | <p>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:</p> <ul style="list-style-type: none"> • 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. |
| The following attributes have 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. | | |
| captiveportal | userRedirectURL initialCaptiveURL advertisingCaptiveURL | <p>The URL that you want the subscriber's browser to be redirected to after each type of redirection. Each URL is constructed as:</p> <p><code>http://host:portURI</code></p> <p>where:</p> <ul style="list-style-type: none"> • <i>host</i> 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: <ul style="list-style-type: none"> – serviceportal.host (usually the NWSP IP address) – messageportal.host (usually the Message Portal IP address) • <i>port</i> is the port that the web server is listening on. The port is defined as one of the following java system properties: <ul style="list-style-type: none"> – serviceportal.port – messageportal.port • <i>URI</i> 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: <ul style="list-style-type: none"> – For user redirections: /home, which is the NWSP logon page. |
| | | |

Table 8-4 Attributes in the Captive Portal MBean Configuration File (continued)

| Object Name | Attribute Name | Explanation |
|------------------------------|--|--|
| captiveportal (continued) | | <ul style="list-style-type: none"> – For initial logon redirections: /initial, which is the Message Portal greetings page. – For advertising redirections: /advertising, which is the Message Portal advertising page. <p>The default values for the system properties and the URIs were set during installation in the “URL Out” fields.</p> |
| | userRedirectPort initialCaptivePort advertisingCaptivePort | <p>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:</p> <ul style="list-style-type: none"> • userRedirect.port • initialCaptive.port • advertisingCaptive.port <p>The default values for the system properties are the values you provided during installation in the “Port In” fields.</p> <p>If you change a port value, you must also change the SSG configuration to send redirections to the same port.</p> |
| | initialCaptiveDuration advertisingCaptiveDuration | <p>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.</p> <p>Note The SSG TCP redirect commands also accept a duration attribute. See the “Message Duration Parameters” section on page 8-21 for more information.</p> |
| | serviceRedirectDefaultURL | <p>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.</p> |
| | defineServiceRedirect | <p>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.</p> <ol style="list-style-type: none"> 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. <p>If you change a port value, also change the SSG configuration to send the service redirection to the same port value.</p> <ol style="list-style-type: none"> 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. <p>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.</p> |

Table 8-4 Attributes in the Captive Portal MBean Configuration File (continued)

| Object Name | Attribute Name | Explanation |
|------------------------------|--|---|
| captiveportal (continued) | | 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. |
| | 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: <ul style="list-style-type: none"> • userRedirectURLParam • serviceRedirectURLParam • serviceRedirectServiceParam • serviceRedirectSubscriberParam • messageRedirectURLParam • messageRedirectSubscriberParam • messageRedirectDurationParam | <p>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.</p> <p>These parameter names are visible to the subscriber in the browser's URL field. They appear in the query string appended to the URL.</p> |

messageportal.xml Configuration File

Table 8-5 explains the configuration attributes used by the Message Portal application.

Table 8-5 Attributes in the Message Portal MBean Configuration File

| Object Name | Attribute Name | Explanation |
|-------------------|----------------|---|
| Logger | | See the Logger object in Table 6-4 on page 6-16 . |
| ManagementConsole | | See the ManagementConsole object in Table 6-4 on page 6-16 . |
| SESMBean | | <p>See the description for SESM, page 6-19.</p> <p>The mode attribute for the Message Portal application must be one of the following:</p> <ul style="list-style-type: none"> • 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.) |

Table 8-5 Attributes in the Message Portal MBean Configuration File (continued)

| Object Name | Attribute Name | Explanation |
|---------------|-----------------|--|
| SESMDemoMode | | See the description for SESMDemoMode , page 6-21. If you run Message Portal in Demo mode, it obtains subscriber profiles from the file identified in this MBean. You can add interests (hobbies) to the demo data file as described in Table 4-4 on page 4-9 , “ Special Attributes for Demonstrating LDAP Features in Demo Mode ” earlier in this guide. |
| DESSMode | | See the description for DESSMode , page 6-21. |
| messageportal | defaultPage | For advertisement redirections, specifies the default page to redirect to if: <ul style="list-style-type: none"> • 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 ” section on page 8-21 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: <ul style="list-style-type: none"> • 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. |

Table 8-5 Attributes in the Message Portal MBean Configuration File (continued)

| Object Name | Attribute Name | Explanation |
|------------------------------|----------------|---|
| messageportal (continued) | redirectOn | <p>For initial logon and advertisement redirections, indicates action to take after the captivation duration elapses:</p> <ul style="list-style-type: none"> • True—Issue another redirection to the original page requested before the logon or advertisement redirection occurred. This is the URL specified in CPURL parameter in the query string of the HTTP request from the Captive Portal application. • False—Do not issue another redirection. The message or advertisement page remains displayed until the subscriber enters another URL. |
| | interests | <p>Specifies the interest values that can appear in a subscriber profile. Separate each interest value with a comma. For example:</p> <pre>cinema, science, internet, news, sports, travel, finance, community</pre> <p>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.</p> |
| | interestPages | <p>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.</p> <p>To use the default page for an interest, use any single character in the interestPages list.</p> <p>In the following example, subscribers whose profile contains science as the first interest see the default page as an advertisement.</p> <pre>cinema.jsp, ., internet.jsp, news.jsp, sports.jsp, travel.jsp, finance.jsp, community.jsp</pre> |

nwsp.xml Configuration File

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

Table 8-6 explains configuration attributes in nwsp.xml that are directly related to the captive portal solution.

Table 8-6 Captive Portal Attributes in nwsp.xml

| Object Name | Attribute Name | Explanation |
|-------------|------------------------|--|
| WebAppMBean | 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • In LDAP mode, the NWSP subscriptionManage page. • In RADIUS mode, the NWSP displays the page specified in the defaultURI attribute. |
| | 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

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 will be too soon and will not happen.

Durations on the SSG Side

On the SSG side, the message duration controls how long 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:

- initialCaptiveDuration
 - advertisingCaptiveDuration
- 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 8-22](#)
- [Defining Captive Portal Groups and Port Lists, page 8-22](#)
- [Configuring Unauthenticated User Redirection, page 8-23](#)
- [Configuring Unauthorized Service Redirection, page 8-24](#)
- [Configuring Initial Logon Redirection, page 8-25](#)
- [Configuring Advertising Redirection, page 8-26](#)

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

Overview

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. 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”](#) section on page 8-21 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 the value. Redirections to this group are applied to TCP packets arriving on SSG 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”](#) section on page 8-21 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 captive 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 advertisingCaptive. 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 advertisingCaptive group is associated with advertising redirections. The captivation lasts for 5seconds 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 advertisingCaptive
    server 10.0.1.4 8092
  redirect port-list ports to advertisingCaptive
  redirect captive advertising default group advertisingCaptive 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 8-27
- [Redirections Continuously Occur](#), page 8-27
- [User Name Not Passed in Unauthenticated User Redirections](#), page 8-28

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 8-27](#)
- [Two Redirection Types Assigned to the Same Port in captiveportal.xml, page 8-27](#)
- [Redirection Type Not Configured on the SSG, page 8-27](#)

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
- initialCaptiveOn
- advertisingCaptiveOn
- 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 8-28](#)
- [Using HTTP1.1 with a Non-SESM Captive Portal Application, page 8-28](#)

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 will occur 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 8-22](#).
- 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.
