



SESM Solutions for Captive Portals

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

- [Captive Portal Solution Description, page 4-1](#)
- [Captive Portal Solution Diagram, page 4-2](#)
- [Captive Portal Solution Components, page 4-3](#)
- [Captive Portal Configuration Requirements, page 4-6](#)
- [Captive Portal Demo, page 4-6](#)

Captive Portal Solution Description

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

- Direct subscribers to the SESM web portal application even if they do not know the URL to the web server.
- Force subscribers to authenticate before accessing the network or specific services.
- 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 the 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 the SESM captive portal solution:

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

Captive Portal Solution Diagram

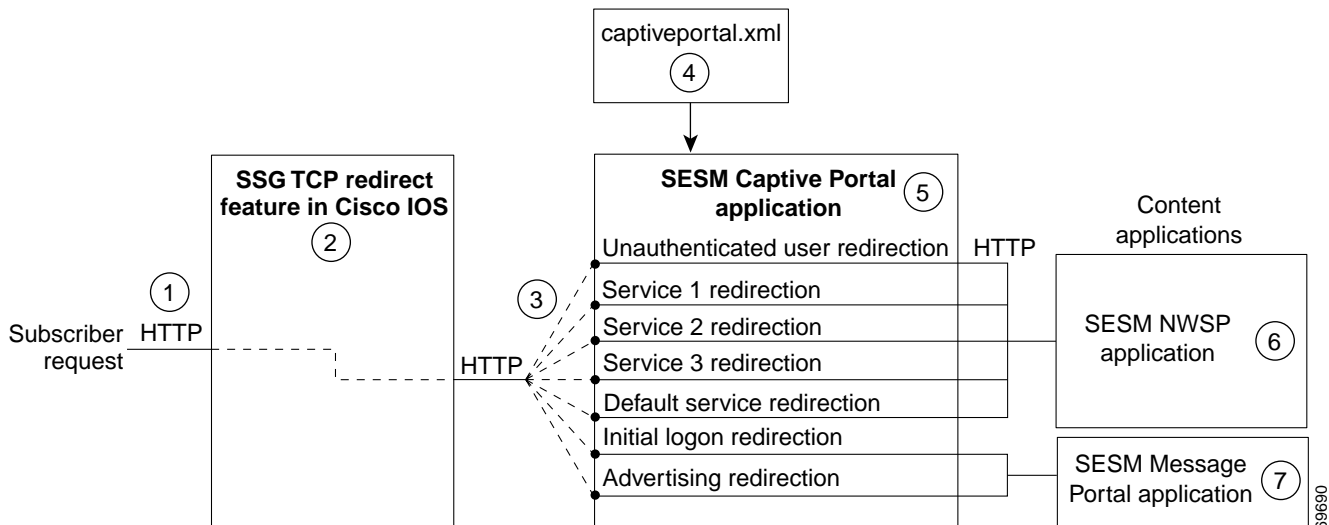
Figure 4-1 illustrates how the components in the SESM captive portal solution work together to provide appropriate content to the subscriber.



Note

Figure 4-1 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 4-1 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 the 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.

Captive Portal Solution Components

This section describes the components of the sample captive portal solution installed with SESM:

- [SSG TCP Redirect Feature, page 4-3](#)
- [SESM Captive Portal Application, page 4-4](#)
- [Content Applications, page 4-4](#)
 - [NWSP Application, page 4-5](#)
 - [Message Portal Application, page 4-5](#)

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 4-1](#) describes the SSG TCP redirection types and how the SESM captive portal solution supports those redirection types.

Table 4-1 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 the 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 the 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>

Table 4-1 Supported Redirection Types (continued)

Redirect Type	Role of SSG TCP Redirect Feature	Role of SESM Captive Portal Solution
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 the 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 the 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.

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.

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.

Captive Portal Configuration Requirements

Table 4-2 summarizes the steps required to deploy the sample captive portal solution.

Table 4-2 Configuration Requirements for SESM Captive Portal Solutions

Deployment Step	References
<ol style="list-style-type: none"> 1. Install the sample captive portal solution from the SESM installation package. You must choose Custom Install to install the captive portal solution. Captive portal is not included in a typical installation. Accept all of the default values presented during SESM captive portal installation. 	<p><i>Cisco Subscriber Edge Services Manager Installation and Configuration Guide</i>, Chapter 11, “Deploying a Captive Portal Solution”</p> <p>The online link is: http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_315/instconf/11cp.htm#xtocid0</p>
<ol style="list-style-type: none"> 2. Use the ssgconfig.txt file to configure the SSG TCP redirect features. The configuration values in ssgconfig.txt match the default values used in the SESM installation program. 	
<ol style="list-style-type: none"> 3. Create sample profiles suitable for a captive portal demonstration. 	

Captive Portal Demo

The following procedure assumes that you have a fully configured SESM deployment in RADIUS or LDAP mode. To demonstrate captive portal features:

-
- Step 1** Start all of the applications in the captive portal solution by executing their startup scripts.
- ```
jetty
 bin
 startNWSP
 startCAPTIVEPORTAL
 startMESSAGEPORTAL
```
- Step 2** Open a web browser from a network configured as an incoming network on the SSG. Enter a URL, such as www.yahoo.com, or allow the browser to attempt to display a home page setting.  
Unauthenticated user redirection causes the NWSP logon page to appear.
- Step 3** Sign on using a user ID and password from the subscriber profiles you created specifically for this demonstration. After successful authentication, the following occurs:
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 appear in the pop-up window.

4. After the length of time specified by the duration parameter, the next action depends on how the redirectOn configuration parameter for Message Portal is set:
  - True—The Message Portal application redirects the browser to the originally requested URL (www.yahoo.com). The service is subjected to service redirections.
  - False—The greetings page continues to display until you enter another URL. Enter the URL after the duration time expires.
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 NWSP does not find the service, the home page appears.
  - Otherwise, NWSP attempts to start the service. It brings the service pop-up window to the foreground.

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

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

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

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

---

