SESM Features

This chapter describes the key features of the Cisco Subscriber Edge Services Manager (SESM). The topics in this chapter are:

- Service Selection and Connection Features with SSG, page 2-1
- Self-Care Features with SESM-SPE, page 2-5
- Captive Portal, Messaging, and Advertising Features, page 2-6
- Authentication Options, page 2-8
- Web Development Features, page 2-10
- SESM Location and Brand Awareness Features, page 2-11
- SESM Management Features, page 2-13
- Scaling, Redundancy, and Resiliency Features, page 2-15
- Accounting and Billing Interfaces, page 2-15
- Web Proxy Support, page 2-16
- Using the Web Services Gateway with Third-Party Portals, page 2-16

Service Selection and Connection Features with SSG

In solutions that use the Cisco Service Selection Gateway (SSG) to provide service connections, the SESM portal presents a service list from which the subscriber can select one or more services for connection. The connection features are implemented by SSG and controlled by attributes stored in the subscriber or service profiles. This section describes the following features:

- Service Selection from SESM Portals, page 2-2
- Service Authentication and Authorization, page 2-2
- Automatic Connections and Hidden Services, page 2-2
- Subscriber Sessions, page 2-3
- Service Status, page 2-3
- Mutually Exclusive Service Selection, page 2-4
- Service Selection by Bandwidth, page 2-4
- Supported Service Types, page 2-4

Service Selection from SESM Portals

In a service selection and connection solution, the SESM portal provides the web interface from which subscribers can:

- Authenticate—The SESM portal provides a logon window for subscribers.
- Select one or more services for connection—The SESM portal presents a list of subscribed services based on the subscriber profile. The subscriber connects to services by selecting them from the list. If appropriate, SESM can display a service logon page.
- Disconnect from services—Subscribers can disconnect from a single service, or by logging off of SESM, disconnect from all services.
- View session status information—Subscribers can see which services are active in their current session and view other session status information.

After a subscriber authenticates, the SESM portal displays subscribed services obtained from the subscriber profile. From the list of displayed services, the subscriber selects one or more services for connection. The portal can also display service groups, as defined in service group profiles. The web developer controls the format of the service list and how to portray service groups.

When SESM is deployed in SPE mode, self-care features can also be offered to subscribers. See the "Self-Care Features with SESM-SPE" section on page 2-5 for more information.

Service Authentication and Authorization

A preliminary level of service authorization is implied by the service selection list presented to a subscriber. The SESM portal presents for selection only those services to which a subscriber is subscribed, according to the subscriber profile. In SPE mode, when a subscriber self-subscribes to a new service, that service is added to the subscriber profile and immediate access to that service is possible.

The SESM web portal can present a service authentication page for services that require it. Service authentication can be based on user name and password. For proxy services, an option in the service profile specifies whether the CHAP or PAP protocol is used to authenticate for the service. For more information, see the chapter about RADIUS profiles in the *Cisco Subscriber Edge Services Manager Deployment Guide*.

Automatic Connections and Hidden Services

An automatically connected service is a service to which the subscriber gains access immediately after authenticating, without manually selecting the service from the SESM portal. Depending on configuration options, either SSG or SESM performs the connection immediately after the subscriber authenticates.

A hidden service is an automatically connected service that does not appear on the SESM service selection page.

A service is marked as an autoconnect service in the subscriber profile. By default, an autoconnect service is also a hidden service. Another entry in the subscriber profile can specify that the autoconnected service be included in the service selection list.

In SPE mode, the SESM portal can offer the subscriber the means to self-select or change the services that should be automatically connected and hidden.

Providers can use the automatic connection option as a way to provide always-on services or as a way to bypass the service selection feature. For example, a provider might choose to offer three always-on services to all subscribers, and mark those services as autoconnected in all subscriber profiles. If these are the only services offered by the provider, and the profiles indicate that they are hidden from the service selection list, the web portal could be customized to omit the service list.

Subscriber Sessions

When a subscriber successfully logs onto the SESM portal, the SSG creates an edge session for the subscriber on the SSG host platform. The session lasts until the subscriber logs off of SESM. The SSG keeps track of session status.

If the SSG port-bundle host key feature is not enabled, the SSG uses the subscriber IP address to identify a session.

If the port-bundle host key feature is enabled, the SSG uses a unique key to identify each currently logged-on subscriber, regardless of the IP address being used. The port-bundle host key is an optional feature on SSG. When enabled, the feature allows SESM portals to support the following types of subscribers:

- Overlapping IP addresses in PPP and bridged environments—SESM can differentiate between various subscribers using the same IP address.
- Nonroutable subscriber IP addresses—SESM can support subscribers at sites using private IP addressing schemes, including subscribers of ISPs using private addressing schemes.

The SSG port-bundle host key feature also enhances configuration of large SESM deployments. When port-bundle host key is enabled, you do not need to map client subnets to SSGs.

Service Status

SESM portals can show service status in two ways.

- Status and connection metrics
- Service list images

Status and Connection Metrics

The SESM portal can display status and metrics about services that were connected during the current session. The web developer controls the types of status information and how it is presented. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information.

The sample status page in NWSP (see Figure 3-5) shows the following information about all connected services (including automatically connected services) during the current session:

- Currently connected services
- Services that were connected during the session but are currently not connected
- Connection length of time (for both current and previously connected services)
- Transmitted and received byte count on a per service basis

Service List Images

The SESM web developer kit provides a way to link images indicating status to the items in the service list. NWSP uses the following images next to the items in the service list (see Figure 3-4):

- Red X—Indicates an unconnected service
- Green arrow—Indicates a connected service

Mutually Exclusive Service Selection

Mutually exclusive service selection restricts a subscriber to accessing only one service at a time in a specified group of services. One use of this feature is described in the "Service Selection by Bandwidth" section on page 2-4.

A service group is a collection of services defined in a service group profile. A subscription to a service group implies subscription to all of the services in the group. It also implies the ability to select all of the services in the group. When a group is defined as mutually exclusive, SESM limits service selection to one service at a time within the group.

A configuration option controls the SESM action when a subscriber is already logged into one service and then selects another service in the group:

- SESM can automatically request SSG to disconnect the first service and connect the new service.
- SESM can prompt the subscriber to log off the first service. After the subscriber logs off, SESM requests the connection to the other service.

Note SESM waits for the first service to be disconnected before requesting connection to the new service. If the connection to the new service fails, the subscriber is not connected to either service.

A mutually exclusive service group is defined in a service group profile.

Service Selection by Bandwidth

SESM portals can support the SSG hierarchical policing feature in Cisco IOS Release 12.2(4)B by allowing subscribers to choose a different bandwidth from their regularly subscribed bandwidth for a particular service. For example, a subscriber might be subscribed to an Internet or video service with a 128-Kbps bandwidth, but have the option to select 512-Kbps or 1-Mbps service on demand.

To implement service selection by bandwidth, define the bandwidth options for each service as separate and mutually exclusive services within a service group. This restriction is important to prevent subscribers from simultaneously connecting to (and being billed for) the same service over two different bandwidths.

Supported Service Types

The service type is an attribute in a service profile. SESM can support a wide range of service types. In general, SESM supports the service types that are supported by the other elements in the network, such as the SSG.

Note Service type is known as service class in CDAT.

In Cisco IOS Release 12.2(4)B, the SSG supports the following types of service:

- Passthrough—The SSG can forward traffic through any interface using normal routing or a next-hop table. Passthrough service is ideal for standard Internet access.
- Proxy—When a subscriber selects a proxy service, the SESM portal prompts for the user name and password. After authentication, the service is accessible until the user logs out from the service, logs out from the SESM portal, or is timed out.
- Tunnel—When a subscriber selects a tunnel service, SESM displays a service authentication page to obtain service connection credentials from the subscriber.

Self-Care Features with SESM-SPE

Self-care features provide subscribers with write access to their account information, so that they can maintain the information themselves.

The SESM self-care features are implemented by the SPE component and are therefore available only when SESM is deployed in SPE mode.

This section describes the following SESM self-care features:

- Account Self-Management, page 2-5
- Account Self-Registration, page 2-5
- Service Self-Subscription, page 2-5
- Subaccount Creation and Management, page 2-6
- Personal Firewalls, page 2-6

Account Self-Management

Subscriber account self management allows subscribers to change their own account details, such as address information, phone numbers, passwords for account authentication, and credentials for proxy and tunnel service authentications. (Passwords are encrypted.) This subscriber updating capability relieves the service provider from customer care tasks.

Account Self-Registration

The SESM self-registration feature provides a way for subscribers to create their own new account, rather than depending on a service-provider administrator to create the initial record.

Service Self-Subscription

Self-subscription allows subscribers to sign up for new services and have immediate access to those services. This feature relieves the service provider from time-consuming service enrollment tasks. It also benefits the subscriber because there is no delay in receiving access to a new service. Subscribers can also unsubscribe from a service.

Subaccount Creation and Management

Subscriber subaccount creation and management allows a subscriber with a main account to create subaccounts, with different services and access information in each subaccount. For example, a family might have subaccounts for each family member, with a different set of authorized services within each subaccount. The main account can create and delete subaccounts and subscribe to services for the subaccounts, and control whether the subaccounts can subscribe to services themselves.

The service provider can impose limits on the number of subaccounts in a main account. This feature allows providers to sell accounts of differing sizes. It also prevents pranksters from creating an endless number of subaccounts.

Personal Firewalls

The SESM personal firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on a web portal page. The portal page presents a list of applications, configured by the deployer, that are available for firewall protection. Based on choices the subscriber makes on the portal page, SESM creates the access control list (ACL) commands that implement the traffic filters on the subscriber’s connection.

A parent account can have different filters than its subaccounts, and the parent account can restrict the subaccount from changing firewalls.

Captive Portal, Messaging, and Advertising Features

The SESM captive portal solution works with the TCP redirect features on the SSG to provide several types of subscriber captivation. With captivation, a subscriber’s original request is captured and the browser is appropriately redirected.

The SSG TCP redirect feature redirects incoming TCP packets to a specified SESM captive portal application. The SESM captive portal application issues an HTTP redirection to the subscriber’s browser, directing it to another application that returns content to the subscriber. These content applications can be SESM portals that:

- Present a session logon page to enforce authentication
- Redirect to services
- Display message pages at initial logon
- Display advertising pages at defined intervals

The following sections briefly describe these captivation types. For more information, see the *Cisco Subscriber Edge Services Manager Captive Portal Guide*.

Unauthenticated User Captivation

Unauthenticated subscribers are those who have submitted an HTTP request when there is no host object on the SSG. A host object exists only after successful authentication. Unauthenticated user captivation works as follows:

- The SSG TCP redirect feature redirects unauthenticated packets to the SESM captive portal solution.

- The SESM captive portal solution:
  - Redirects the browser to the login page of the SESM portal
  - Optionally preserves the originally requested URL and performs a second redirection after authentication to the original URL

Some benefits to implementing unauthenticated user captivation are:

- Subscribers do not need to know the URL to the SESM logon page because they are sent there automatically when they start a browser session.
- In a wireless LAN, the feature allows unauthenticated access to the default LAN network but then requires the subscriber to authenticate before accessing the Internet or other services.
- The SESM captive portal solution can redirect a subscriber to a home page URL or a predefined service address immediately after authentication.

Unconnected Service Redirection

Service redirection handles requests to service domains to which the subscriber is not yet connected. Rather than rejecting these requests, the SSG TCP redirect feature can redirect them to an SESM captive portal application, which can then handle the request in an appropriate way to gain connection or present an explanation to the subscriber.

Examples of how the SESM captive portal solution can support service captivations are:

- When a subscriber is not connected for a service, the captive portal solution can present a service logon page or perform the authentication on behalf of the subscriber.
- When the subscriber is not subscribed to a service, the captive portal solution can present a subscription page.
- When service connection is refused because of lack of funds in the subscriber account, the captive portal solution can present an explanation. See the "Prepaid Services" section on page 2-15 for more information.

Initial Logon Captivation

Initial logon captivation displays a message or greetings page to all subscribers immediately after authentication. This feature works as follows:

- The SSG TCP redirect feature redirects all authenticated subscribers to the captive portal application.
- The SESM captive portal solution can present any type of message for a specified length of time, after which the browser is redirected again to the originally requested service, to an SESM service selection page, or to an automatically connected service.

Initial logon captivation provides a way for providers to present important messages to their subscribers, including announcements of new services and procedures or identity and branding messages.

Advertisement Captivation

Advertisement captivation presents advertisements at specified intervals for specified durations. This feature works as follows:

- The SSG TCP redirect feature handles the interval timing mechanism. For each logged-on subscriber, when the specified interval elapses, SSG redirects the next TCP packet originating from the subscriber to the SESM captive portal application.
- The SESM captive portal solution presents the advertisement content.

Some possibilities for advertisement captivation using the SESM solution are:

- The captive portal solution can present service-specific advertisements by identifying the service name or service URL that is being requested, and presenting advertisements appropriate to users of the service.
- The SESM solution can display advertisements tailored to subscriber characteristics stored in the profile, such as hobbies, age, or gender.

Authentication Options

SESM passes authentication credentials to a cooperating network element in a RADIUS protocol format. Service providers can deploy SESM solutions using the following authentication options:

- 2-Key Authentication, page 2-8
- Authentication Using Multiple Keys, page 2-8
- Single Sign-on for PPP Clients, page 2-9
- Single Sign-on for non-PPP Clients, page 2-9
-

2-Key Authentication

The standard 2-key authentication method bases authentication decisions against the following attributes stored in the subscriber profile:

- User name
- Password

SESM includes these values in RADIUS requests as standard RADIUS protocol attributes. The sample SESM portal applications display a logon page that prompts for the two values listed above.

Authentication Using Multiple Keys

Some deployments might require more than the standard two keys for authentication. SESM supports any number of authentication keys. The keys can be any combination of any RADIUS attribute.

Some typical fields used for authentication are:

- Access point name (APN)—This is RADIUS attribute 30, CALLED_STATION_ID. This might be a GGSN.
- MSISDN—This is RADIUS attribute 31, CALLING_STATION_ID. This might be the subscriber's MSISDN or telephone number.
- Network access server (NAS) identifier—This is attribute 32, NAS_IDENTIFIER. In SESM deployments, the SSG is the NAS.

To implement multikey authentication:

- Use the SESM web developer kit to add the authentication fields to the portal logon page.

  The SESM web developer kit does not offer a way to collect an APN or NAS identifier. This function must be performed by the cooperating network element, such as the SSG.
- If SESM is deployed in RADIUS mode, logic to authenticate with multiple keys must exist in the RADIUS server you are using. Verify that this logic exists with your RADIUS server vendor.
- If SESM is deployed in SPE mode, you can configure the RDP Server to perform authentication using any number of standard RADIUS attributes.

  When provisioning subscriber profiles, administrators can enter the APN and NAS identifier attributes as group values. See the *Cisco Distributed Administration Tool Guide* for more information.

Single Sign-on for PPP Clients

The single sign-on feature removes the requirement for Point-to-Point Protocol (PPP) clients to enter authentication details twice. When single sign-on is enabled, the SESM portal does not ask a PPP subscriber to authenticate (log on). Instead, the SESM portal uses the PPP authenticated identity from a cooperating network element such as SSG.

Single Sign-on for non-PPP Clients

The single sign-on feature also is important for non-PPP subscribers. With single sign-on, if any subscriber authenticates using the SESM web portal, that subscriber does not need to sign on again for the duration of the session. The session exists as long as the cooperating network element has identifying information for it. For example, the SSG retains a host object until the subscriber ends the session by logging off.

This feature offers the following advantages to subscribers:

- Subscribers can stop the browser or navigate away from the SESM portal pages, and then return to the SESM pages later and not be required to reauthenticate.
- Subscribers do not need to reauthenticate when the SESM automatic memory manager clears sessions from the SESM portal host.

Message Authentication

Beginning with SESM Release 3.1(9), SESM applications include RADIUS message authentication features. Message authentication resolves the following vulnerabilities in SESM solutions:

- Integrity of packets sent between SESM solution components—Verify that the contents of packets are not altered during transmission.
- Authentication for accounting packets—Accounting packets do not include the User-Password attribute; therefore, the shared secret MD5 encryption check cannot be performed on those packets.

In SESM Web Portals and WSG

You can configure SESM web portal and WSG applications to send the RADIUS Message-Authenticator attribute (80) in access-requests to the Cisco edge device and validate received Message-Authenticator attributes.

To configure the Message-Authenticator feature in the SESM web portal and WSG applications, set the following attribute in the SSG MBean used by the application to true.

```
<Set name="generateMessageAuthenticators" type="boolean">false</Set>
```

In RDP

If the Message-Authenticator attribute is included in messages to RDP, the RDP validates it and responds with a Message-Authenticator attribute. If the RDP is configured to proxy authentication requests, RDP regenerates, if necessary, the Message-Authenticator attribute before proxying or responding.

These validations occur automatically in RDP without any specific configuration.

In SSG

Currently, SSG does not validate Message-Authenticator attributes and does not include the attribute in responses to SESM requests. A future release of SSG will include this capability.

Web Development Features

The SESM web development kit includes technologies and development features for customizing SESM web portals. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for detailed descriptions of the following and additional web development features:

- Localization and Internationalization, page 2-10
- Java Server Pages, page 2-10
- SESM User Shape Mechanism, page 2-11
- Library Resources, page 2-11

Localization and Internationalization

SESM portals, RDP, and CDAT can support Unicode Transformation Format Version 8 (UTF-8) character representations. UTF-8 supports the traditional 1-byte character sets and double-byte character sets.

Web developers can use the following techniques to localize and internationalize SESM web portals:

- SESM web portals can use conventional Java techniques for internationalization and localization.
- SESM includes additional development components that improve upon the standard Java locale-related classes and help reduce the complexity of localizing SESM web applications. Some localization subjects addressed by the SESM components are: time zone, language, and preferred formats for currency, numbers, dates, and times.
- Resource bundles contain locale-specific data that varies depending on the user's language and region, such as translatable text for status and error messages and for labels on GUI elements. The developer can add additional resource bundles to a web application to accommodate new locales.

Java Server Pages

Java Server Pages (JSPs) provide a standard way to integrate Java code with HTML, XML, and WML. The SESM portal and captive portal applications use JSPs to present interactive, dynamically updated, personalized, and branded web pages to subscribers.

The JSPs contain the elements that the developer modifies for the specific requirements of the provider. No servlet programming is required.

SESM User Shape Mechanism

The SESM user shape mechanism is a method for combining any number of subscriber attributes to determine which resources to use in the JSP returned to a subscriber. This mechanism eases the task of adding more attributes to the decision.

The SESM portal detects information about a subscriber from the initial HTTP request. For example:

- The subscriber's preferred language setting in the browser sets the locale.
- The access device, browser type, and the IP address are available from the initial request.

The portal developer can use one or all of these attributes in the user shape to determine the look and feel of the JSP returned to the subscriber’s browser. For example:

- If the subscriber's browser language is French and the receiving device is a desktop PC, the response can be rendered in French using HTML.
- If another subscriber's browser language is Spanish and the receiving device is a WAP cell phone, the response can be rendered in Spanish using Wireless Markup Language (WML).

Library Resources

The SESM development components include Dreamweaver templates. These templates are useful for customizing or maintaining a web application's JSP pages when many pages have the same layout. By modifying a template and then updating the JSP pages that use the template, you can change the look and feel of an entire set of pages quickly.

SESM Location and Brand Awareness Features

The SESM portal can derive the location or service brand of a subscriber and present branded retail pages or different elements within a page based on those attributes.

Some examples of how you might use location information in customized SESM portals are:

- Location-based branding—Brand the portal pages and offer free or different services accordingly.
- Personalized portals—Taylor the subscriber experience based on location characteristics.
- Access policies—Allow free services to a certain segment of subscribers based on connection characteristics, such as VPI ranges or subinterface ranges. For example, location awareness could permit certain subscribers from a certain location to gain access to the Internet service without authentication.
- Redirections—Redirect all browsers with particular location characteristics to a specified portal page.

The SESM location awareness feature relies on the physical location characteristics of an edge session. SESM obtains this location information from the SSG as part of the session’s initial connection request. The specific attributes used to determine the location, and hence the location branding, are configurable.

SESM currently has three ways to configure location and brand awareness:

- Location or Brand Awareness Based on Complete ID Attributes, page 2-12

- Location or Brand Awareness Based on IP Addresses, page 2-12
- Brand Awareness Based on Subscriber Groups, page 2-12

Location or Brand Awareness Based on Complete ID Attributes

Note This is the recommended method for defining location awareness.

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

- Subscriber IP address range
- Virtual path identifier (VPI) range
- Subinterface, such as an Ethernet interface

More attributes might be added in future releases.

Note To use location awareness based on complete ID attributes, your SSG platforms must be running Cisco IOS Release 12.3(1)T or the X train for Release 12.2(8)B.

The Location MBean used by the web portal defines location names and the attributes that are associated with each location. See the *Cisco Subscriber Edge Services Manager Web Portal Guide* for more information.

Location or Brand Awareness Based on IP Addresses

You can configure brand or location awareness based on the following IP addresses or subnets:

- If the port-bundle host key feature is used—SSG IP address subnetwork ranges
- If the port-bundle host key feature is not used—Subscriber IP address subnetwork ranges

With this method, you configure the SSG MBean used by the web portal to assign a location or brand to the IP address associated with a request.

See the *Cisco Subscriber Edge Services Manager Web Portal Guide* for more information about how to configure branding based on IP addresses.

Brand Awareness Based on Subscriber Groups

Another way to implement brand awareness is based on subscriber groups. The group is an attribute of a subscriber profile, and a group represents a brand. The SESM portal detects the branding for a subscriber based on the group in which that subscriber is assigned and returns pages appropriate to the brand of that group.

Note Subscriber groups are known as user groups in CDAT and the RADIUS profiles.

SESM portals can implement differences among branded groups in many ways, including:

- Each brand could have different subscriber privileges.
- Each brand could have different subscribed and available services.
- Each brand could have a different look and feel to the browser pages, such as different colors or different menu options.

The sample data installed with SESM defines three subscriber groups for branding purposes: bronze, silver, and gold groups. The sample data also defines one user for each of these groups: bronzeuser, silveruser, and golduser. To illustrate branding possibilities, PDA uses a different look and feel and different colors for each brand. NWSP uses different menu options.

SESM Management Features

SESM includes two web-based management tools for service provider administrators:

- Application Manager—A management tool for remotely accessing and changing configuration attributes for all SESM applications.
- CDAT—A management tool for the SPE extensions in an LDAP directory.

Note The Advanced windows in the new Application Manager replace the JMX Agent View provided as a management tool in previous releases. The AgentView is also included in SESM Release 3.1(9). However, the preferred remote management tool for SESM is the new Application Manager.

Application Manager

The Application Manager is a web application that remotely manages SESM applications. It can manage multiple instances of SESM web portal and captive portal applications, RDP, CDAT, WSG, and other Application Manager instances. These applications can be installed on the same or different systems from the Application Manager, and a firewall may exist between them.

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

Two types of management windows are available:

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

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

- View monitoring (read-only) attribute values

VRemote Monitoring of SESM Applications

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

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

LDAP Directory Information Management

For SPE mode deployments, CDAT provides the management interface for maintaining SESM information in the LDAP directory. From CDAT, administrators can maintain:

- Subscriber profiles
- Service profiles
- CDAT administrators
- Access policies for subscribers and CDAT administrators

See the *Cisco Distributed Administration Tool Guide* for more information about these management features.

For RADIUS mode deployments, use administrative tools provided by the vendor of the RADIUS server you are using to maintain subscriber and service profiles.

User Groups and Role Based Access Control

Role based access control (RBAC) is an access model that defines access privileges for roles, rather than for individuals, and then assigns individuals to a role. The Cisco implementation extends the model, allowing administrators to manage groups of subscribers, rather than individuals. Using this group-based RBAC model, administrators define roles, which have specific privileges, and groups, which have assigned roles. Individual subscribers are then assigned to a group and inherit the roles of that group.

The RBAC model applies to data stored in an LDAP directory using the SPE extensions that are delivered as part of the SESM SPE mode installation. Administrators use the Cisco Distributed Administration Tool (CDAT) to enter and manage the RBAC data in the directory.

Support for Generic RADIUS Attributes

Administrators can enter any generic RADIUS attribute in a subscriber profile by using the LOCAL RADIUS attribute field in the CDAT interface.

Scaling, Redundancy, and Resiliency Features

The SESM portal offers the following scaling, redundancy, and resiliency features:

- You can deploy multiple instances of the same SESM web portal and balance the load as you would with any web server application. The Cisco Content Services Switch 11000 is recommended for load balancing.
- Beginning with SESM Release 3.1(9), you can configure the SESM web portals to include the RADIUS Framed-IP-Address attribute in Access-Requests to the SSG. This attribute allows the load balancer, which is placed between the web portal and the SSG, to route all requests from the same session to the same SSG. The load balancer must be configured to examine the Framed-IP-Address attribute and route packets based on its value.
- The SSG port-bundle host key feature simplifies large deployments by eliminating manual mapping of subscriber subnets to SSGs.
- SESM applications are highly resilient because they are completely stateless regarding subscriber sessions. SESM applications obtain session status information from the SSG. Therefore, the SESM applications can be started and stopped without affecting a subscriber.

Accounting and Billing Interfaces

The accounting and billing solutions that work with an SSG/SESM deployment are based on actual services used and the duration of use. These interfaces are implemented and configured on the SSG.

RADIUS Accounting

SSG can be configured to send accounting requests to a RADIUS server. The RADIUS server generates the accounting records.

Prepaid Services

The SSG Prepaid feature in Cisco IOS Release 12.2(4)B and later supports an interface to a third-party billing server. The third-party server performs billing and accounting functions, which can include prepaid services features. See *SSG Features in Release 12.2(4)B* for more information about the SSG Prepaid feature.

Enhancing Prepaid Services Using SESM Captive Portal

The SESM captive portal features can be used in conjunction with the SSG Prepaid feature to enhance the subscriber’s experience in a prepaid business model. When a service connection is refused or a current session is disconnected because of lack of funds, the SESM captive portal solution can display a message page to the subscriber explaining the reasons for the service refusal.

In a prepaid services business model, service connection is denied (unauthorized) if there are no funds in the subscriber’s account. The SSG Prepaid feature allows SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and the length of the connection. The SSG Prepaid feature also supports reauthorizations after connection is granted. If funds are depleted for the account, SSG logs the subscriber off the service.

Web Proxy Support

The SESM Release 3.1(9) Captive Portal application includes features that handle subscribers with a web-proxy configured in their browsers.

PAC File Emulation

Subscribers might have a Proxy Automatic Configuration (PAC) script configured in their browsers. When this is the case, the browser, at startup, requests the PAC file in an attempt to obtain the settings defined in the file and apply them prior to issuing any requests for a page.

For an unauthenticated subscriber in a SESM deployment, the request for the PAC file reaches the SESM Captive Portal application. In Release 3.1(9), the Captive Portal application can recognize the PAC file request and respond with its own example PAC file as a substitute. The browser session uses the settings in the Captive Portal PAC file rather than those in the original PAC file.

Web Proxy Notification Page

Subscribers might have a web proxy configured with an IP address (or DNS name) and a port. When this is the case, the browser, at startup, submits a request to the web proxy for a specific page.

For an unauthenticated subscriber in a SESM deployment, the request reaches the SESM Captive Portal application. In Release 3.1(9), the Captive Portal application can recognize the difference between a proxy request and a non-proxy or regular HTTP request. You can configure the SESM Captive Portal application to react to proxy requests by redirecting the browser to a customized message page. This page could, for example, inform the subscriber that a web-proxy is configured in the browser and how to disable it.

Web-Proxy Support

You can configure the Captive Portal application to handle a proxy request directly. In this case, when the Captive Portal application recognizes that an unauthenticated subscriber has a web proxy configured, it captures the browser and proxies a login page to the browser. After authenticating and connecting to services on the SSG, the subscriber might (depending on the specific service connections made) have access to the configured web proxy and request connection to it.

Using the Web Services Gateway with Third-Party Portals

The SESM Web Services Gateway (WSG) application provides a Simple Objects Access Protocol (SOAP)-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. Any client application can interface with SSG through the WSG using SOAP over HTTP communication.

The SESM WSG installation includes a web application configured to run in a Jetty container and a command-line client script for demonstration purposes. The WSG web application runs in RADIUS and SPE modes. It does not work in Demo mode.

In this first release, the WSG client interface enables access to the SSG for the following activities:

- Authenticating, starting, and ending sessions on the SSG

  - Obtaining session status
  - Connecting and disconnecting services

Note This first release of WSG offers a preview of future development efforts. We invite interested parties to contact us through a Cisco account representative to discuss potential uses for WSG and participate in feature planning efforts for future releases.