
# Configuring RADIUS for SESM Deployments

This appendix describes the configuration steps required to include a RADIUS server in a Cisco Subscriber Edge Services Manager (SESM) deployment. This appendix includes the following topics:



## Configuring SSG to Communicate with the RADIUS Server

You must configure SSG to communicate with the RADIUS server. To do so, use the **radius-server host** Cisco IOS command on the SSG host. Different ports are used for handling authentication and accounting packets. For example:

```
radius-server host 10.3.3.2 auth-port 1812 acct-port 1813 key cisco
```

To use different RADIUS servers for authentication and accounting, use two commands as follows:

```
radius-server host 10.3.3.2 auth-port 1812 acct-port 0 key cisco
radius-server host 10.3.3.3 auth-port 0 acct-port 1813 key cisco
```

## Configuring RADIUS Clients

The RADIUS protocol is based on a client server model. The RADIUS server is the server. Multiple dial-in Network Access Server (NAS) devices are the clients. Before communication can occur, each client must be configured on the server.

An SESM deployment requires that you configure the following NAS clients on the RADIUS server:

- The SSG host—This is the Cisco device on which SSG is running, such as the Cisco 7200, Cisco 7400, or a node route processor (NRP) on the Cisco 56. The RADIUS server must recognize each SSG host as a client.
- The SESM web portal—This is the NWSP application, or your customized SESM web application. SESM web portals query the RADIUS server directly for service information. The RADIUS server must recognize the SESM web portal as a client.

Table C-1 summarizes the information that might be required to define a NAS client on the RADIUS server. See your RADIUS server vendor documentation for more specific requirements, syntax, and procedures.

***Table C-1 NAS Client Configuration***

| Property | Description |
|---|---|
| Name or IP Address | Identifies the client. Use either IP address or host name. |
| Shared Secret | Must match a shared secret value configured on the client. If the shared secrets do not match, the RADIUS server issues an access-reject message.<br>A shared secret is a value that is configured on both the client and the server. It is never sent over the network. The shared secret is used for MD5 encryption of the profile password. |
| Type | For SSG—Cisco:NAS<br>For SESM—RAD_RFC+ACCT_RFC |

The following sample entries show a Merit RADIUS format defining SESM web portals and an SSG host as RADIUS clients. The examples use the value `cisco` as the shared secret on all of the clients.

```
#Entries for SESM-Server clients
10.3.3.2       cisco     type=RAD_RFC+ACCT_RFC
10.3.3.101     cisco     type=RAD_RFC+ACCT_RFC
10.3.3.102     cisco     type=RAD_RFC+ACCT_RFC

#Entries for SSG host
192.168.1.6     cisco     type=Cisco:NAS
```

# Defining Attributes

RADIUS servers use an attribute dictionary to define the attributes that can appear in profiles. An attribute dictionary contains:

- Standard RADIUS attributes as defined by RFC 2138.
- Vendor-specific attributes (VSAs) that extend the standard attributes. VSAs add new capabilities, supported by specific vendors, to the RADIUS server. The value of a VSA can be one or more subattributes whose meanings depend on the vendor's definition.

SESM applications, including RDP, CDAT, and the portal applications, internally predefine the standard RADIUS attributes and the Cisco SSG VSAs. You can use these predefined attributes in RADIUS and LDAP profiles whether or not they are defined in an attribute dictionary. See the "SESM Predefined Attributes" section on page C-3 for predefined attribute names.

# Defining New RADIUS Attributes for SESM Deployments

To define additional attributes to use in profiles, such as Cisco VSAs not predefined in the SESM code and non-Cisco VSAs, use the following methods:

- If SESM is running in RADIUS mode, define the attribute in the RADIUS server attribute dictionary. See your RADIUS server vendor's documentation for instructions and syntax. If you are using the bundled SESM RADIUS server, use the RADIUSDictionary MBean used by the bundled SESM RADIUS server. See the "RADIUSDictionary MBean" section on page D-3.
- If SESM is running in LDAP mode, you can define new RADIUS attributes in the RADIUSDictionary MBean used by the RDP application. See the "RADIUSDictionary MBean" section on page 7-4.

# SESM Predefined Attributes

Table C-2 lists the standard RADIUS attribute names that are predefined in SESM applications. Table C-3 shows the Cisco SSG VSAs that are predefined in SESM applications.

*Table C-2 Standard RADIUS Attributes Predefined in SESM Applications*

| RADIUS Attribute Names[1] | | |
|---|---|---|
| USER_NAME | SESSION_TIMEOUT | ACCT_LINK_COUNT |
| USER_PASSWORD | IDLE_TIMEOUT | ACCT_INPUT_GIGAWORDS |
| CHAP_PASSWORD | TERMINATION_ACTION | ACCT_OUTPUT_GIGAWORDS |
| NAS_IP_ADDRESS | CALLED_STATION_ID | EVENT_TIMESTAMP |
| NAS_PORT | CALLING_STATION_ID | CHAP_CHALLENGE |
| SERVICE_TYPE | NAS_IDENTIFIER | NAS_PORT_TYPE |
| FRAMED_PROTOCOL | PROXY_STATE | PORT_LIMIT |
| FRAMED_IP_ADDRESS | LOGIN_LAT_SERVICE | LOGIN_LAT_PORT |
| FRAMED_IP_NETMASK | LOGIN_LAT_NODE | ARAP_PASSWORD |
| FRAMED_ROUTING | LOGIN_LAT_GROUP | ARAP_FEATURES |
| FILTER_ID | FRAMED_APPLETALK_LINK | ARAP_ZONE_ACCESS |
| FRAMED_MTU | FRAMED_APPLETALK_NETWORK | ARAP_SECURITY |
| FRAMED_COMPRESSION | FRAMED_APPLETALK_ZONE | ARAP_SECURITY_DATA |
| LOGIN_IP_HOST | ACCT_STATUS_TYPE | PASSWORD_RETRY |
| LOGIN_SERVICE | ACCT_DELAY_TIME | PROMPT |
| LOGIN_TCP_PORT | ACCT_INPUT_OCTETS | CONNECT_INFO |
| REPLY_MESSAGE | ACCT_OUTPUT_OCTETS | CONFIGURATION_TOKEN |
| CALLBACK_NUMBER | ACCT_SESSION_ID | EAP_MESSAGE |
| CALLBACK_ID | ACCT_AUTHENTIC | MESSAGE_AUTHENTICATOR |
| FRAMED_ROUTE | ACCT_SESSION_TIME | ARAP_CHALLENGE_RESPONSE |
| FRAMED_IPX_NETWORK | ACCT_INPUT_PACKET | ACCT_INTERIM_INTERVAL |
| STATE | ACCT_OUTPUT_PACKETS | NAS_PORT_ID |
| CLASS | ACCT_TERMINATE_CAUSE | FRAMED_POOL |
| VENDOR | ACCT_MULTI_SESSION_ID | |

1. A hyphen (-) can replace the underbar (_) in RADIUS attribute names. The attribute names are not case-sensitive.

*Table C-3 Cisco SSG VSAs Predefined in SESM Applications*

| RADIUS Attribute | Vendor ID | Subattribute | Name[1] | Type |
|---|---|---|---|---|
| 26 | 9 | 1 | Cisco-Av | String |
| 26 | 9 | 250 | Account-Info | String |
| 26 | 9 | 251 | Service-Info | String |
| 26 | 9 | 252 | Command-Code | BINARY |
| 26 | 9 | 253 | Control-Info | String |

1. The hyphen (-) and underbar (_) are interchangeable in RADIUS attribute names. The attribute names are not case-sensitive.

# Dynamically Defining Attributes in Profiles for Testing and Development

SESM allows you to dynamically define a new attribute when you first use it in a profile. This feature is intended only for testing, demonstration, and development purposes. Use the dynamic attribute feature only in the following circumstances:

- The SESM portal is running in Demo mode.
- The SESM portal is running in RADIUS mode, and the RADIUS server you are using is the bundled SESM RADIUS server.
- The SESM portal is running in LDAP mode in a testing or development environment.

Dynamic attributes are defined as new subattributes under the standard RADIUS vendor-specific attribute number 26.

Valid formats are:

[*attributeName*](*radiusAttributeId, vendorId, vendorSubattribute, datatype*)

**Note** If you omit *attributeName*, the parentheses surrounding the attribute definition are optional, but recommended.

Where:

- *attributeName*—Is the new attribute name.

  This field is optional. If it is used, subsequent profiles can use just the *attributeName*, without the attribute definition. However, you must be sure that the profile containing the attribute definition gets used before any other profiles that use only the *attributeName*.

**Note** To successfully use the attribute by name in a different profile, the user whose profile contains the attribute definition must logs onto the portal before any user whose profile contains only the new attribute name without the definition.

  If *attributeName* is not used, you use only the attribute definition in the profiles.

- *radiusAttributeId*—Use attribute value 26, the vendor-specific attribute.
- *vendorId*—A RADIUS vendor ID.
- *vendorSubattribute*— A unique number that distinguishes this attribute from other VSAs for the same vendor.
- *datatype*—One of the following values: BINARY, STRING, INTEGER, IPADDRESS. When datatype is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string.

An example follows:

demoVSA(26, 1, 1, BINARY)

Other valid syntax is:

*name*([[type=]26],[vendorId=]*vendorId*,[vendorType=]*vendorType*,[dataType=]*dataType*)

### Merit File Examples

In a Merit file, define a new attribute and assign a value in the following format:

[*attributeName*](*attributeDefinition*) = "*attributeValue*"

MY_ATTRIBUTE(type=26, vendorId=9, vendorType=555, dataType=INTEGER) = "34"

BINARY_ATTRIBUTE(type=26, vendorId=9, vendorType=556, dataType=BINARY) = "0x3F45"

(26,9557,IPADDRESS) = "34.43.54.240"

### CDAT Examples

In CDAT, define a new attribute and assign a value in the Local RADIUS attributes field as follows:

[*attributeName*](*attributeDefinition*):*attributeValue*

For example:

MY_ATTRIBUTE(type=26, vendorId=9, vendorType=555, dataType=INTEGER):34

BINARY_ATTRIBUTE(type=26, vendorId=9, vendorType=556, dataType=BINARY) :"0x3F45"

(26,9,557,IPADDRESS):34.43.54.240

# Configuring Service Profiles

Service profiles define the services that subscribers can select from an SESM web portal. You must configure a service profile for each service that will be accessible through the SESM web portal.

Table C-4 briefly describes the attributes in a RADIUS service profile. Use the following references for more information.

- If you are using the Cisco Access Registrar, see the "Configuring Cisco Access Registrar for SESM Deployments" section on page C-17 for service profile examples and syntax. Otherwise, see your RADIUS server vendor documentation for the syntax of a service profile
- For sample SESM service profiles, see the aaa.properties file located in the NWSP config directory (for example, nwsp/config/ aaa.properties). This file is installed whether or not you choose the demo option. It shows service and subscriber profiles in Merit RADIUS format.
- The SSG documentation describes service profile attributes and provides examples of their use. See the "Related Documentation" section on page xv for a link to online SSG documentation.

***Table C-4 Attributes in Service Profiles***

| Attribute | Description |
|---|---|
| Service profile name | An identifying name for a service profile. Each profile name must be unique.<br>Service profile names are used in the subscriber profiles to indicate that a subscriber is subscribed to the service. |
| Password | Must match the service password on the RADIUS server. SESM obtains the service password directly from the RADIUS server.<br>In SESM, configure this password in the servicePassword attribute in the AAA MBean. |
| Service-Type | Standard RADIUS attribute number 6. The value must be "outbound." |

*Table C-4 Attributes in Service Profiles (continued)*

| Attribute | Description |
|---|---|
| Session-Timeout | Standard RADIUS attribute number 27. Specifies the maximum length of time, in seconds, that this service (the service object on SSG) can remain active in a session at any one time. When the time expires, SSG deletes the service object, which disconnects the subscriber from the service. If the host key feature is enabled on the SSG, the SSG signals the state change to the SESM web portal.<br>**Note** The NWSP application does not relay this state change to the subscriber.<br>If Session-Timeout is not set, there is no limit on how long the subscriber can use the service.<br>In a dial-up networking or bridged (non-PPP) network environment, a subscriber can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, which can be a problem if the IP address is obtained by another user. You can use the Session-Timeout and the Idle-Timeout attributes to prevent this problem. |
| Idle-Timeout | Standard RADIUS attribute number 28. Specifies the maximum length of time, in seconds, that a service connection can remain idle before it is disconnected. See the explanation of the Session-Timeout attribute, above, for more information about setting this attribute. |
| Service-Info | A vendor-specific attribute (attribute number 26), vendor 9, subattribute 251. Valid values for Service-Info attributes are:<br>• **A***authenType*—Specifies whether SSG uses the CHAP or PAP protocol to authenticate users for proxy services.<br>• **I***description*—Service description. Optional. Describes the service.<br>• **T***type*—Type of service. Optional. Valid values for *type* are:<br>– P—Passthrough. This is the default.<br>– T—Tunnel<br>– X—Proxy. Indicates that the SSG performs proxy service.<br>• **M***mode*—Service mode. Optional. Valid values for *mode* are:<br>– S—Sequential mode. Prevents the subscriber from accessing any other services while connected to this service.<br>– C—Concurrent mode. This is the default. Allows the subscriber to simultaneously log onto this service while connected to other services.<br>• **R***ip_address;mask*—Service route (destination). Required. Specifies the network or the host where the service resides. Multiple instances of this attribute can exist within a single service profile, to specify multiple service destinations. An Internet service is typically specified as `"R0.0.0.0;0.0.0.0"`.<br>• **D***ip_address_1[;ip_address_2]*—DNS Server Address. Optional. Specifies the IP addresses for the primary and secondary DNS servers to use for the domains that are defined using the O option.<br>• **O***name1[name2]...[;nameX]*—Domain names. Optional.<br>• **S***RadiusServerAddress;authPort;acctPort;secret*—Remote server information. Required when type of service (T) is Proxy (X); not applicable for other service types. Specifies the remote RADIUS server that will perform authentication, authorization, and accounting for this service. |

*Table C-4 Attributes in Service Profiles (continued)*

| Attribute | Description |
|---|---|
| Service-Info (*continued*) | • **G***key*—Service next hop gateway. Specifies the next hop key for this service. Each SSG uses its own next hop gateway table that associates this key with a valid IP address. See the "Configuring Next Hop Gateway Profiles" section on page C-16 for information about creating a next hop gateway table.<br>• **U***url* or **H***url*—These attributes specify the URL that is displayed in the HTTP address field when the service opens. If the SESM web portal is designed to use HTML frames, then these options also specify whether the service is displayed in a new browser window or in a frame in the current (SESM) window, as follows:<br>– **U***url*—URL for a service displayed in its own browser window.<br>– **H***url*—URL for a service displayed in a frame in the SESM portal window.<br>**Note** In a frameless application, both U and H cause a new browser window to open for the service. The NWSP application is a frameless application.<br>• **B***size*—The PPP maximum transmission unit (MTU) for SSG as a LAC. By default, the PPP MTU size is1500 bytes.<br>• **X**—Indicates that the RADIUS authentication and accounting requests use the full user name (for example, user@service).<br>• **"QU**;*upstream-token-rate*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-token-rate*;*downstream-normal-burst*;[*downstream-excess-burst*]**"**—Indicates the hierarchical policing (quality of service) policies for this service.<br>• **V***string*—Service-defined cookie. Optional. Specifies any information that you wish to include in RADIUS authentication and accounting requests. SSG does not parse or interpret *string*. You must configure the proxy RADIUS server to interpret this attribute. SSG supports only one service-defined cookie per service profile. Use this attribute to add fields to accounting records. |

*Table C-4 Attributes in Service Profiles (continued)*

| Attribute | Description |
|---|---|
| Cisco-AVpair | A vendor-specific attribute (attribute number 26), vendor 9, subattribute 1. Valid values for the Cisco-AVpair attribute in a service profile are:<br>• **"ip:inacl**[*#number*]={*standardACL* \| *extendedACL*}**"**—Upstream access control list (ACL). Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to upstream traffic coming from the subscriber.<br>• **"ip:outacl**[*#number*]={*standardACL* \| *extendedACL*}**"**—Downstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to downstream traffic going to the subscriber.<br>– *number*—Identifies the access list. If a profile includes multiple inacl or outacl attributes, the attributes are downloaded and executed according to the order implied by *number*.<br>– *standardACL*—A Cisco IOS standard ACL.<br>– *extendedACL*—A Cisco IOS extended ACL.<br>**Note** A profile can include multiple instances of inacl attributes and multiple instances of outacl attributes. Use one attribute for each ACL statement. Multiple attributes can be used for the same ACL.<br>• **"vpdn:ip-addresses=***address1*[<*delimiter*>*address2*][<*delimiter*>*address3*]...**"**—Virtual private dial-up network (VPDN) IP address. Specifies the IP addresses of the home gateways (LNSs) to receive the L2TP connections.<br>– *address*—IP address of the home gateway.<br>– <*delimiter*>—A comma (,) or a space ( ) indicates that the SSG selects load sharing among IP addresses. A slash (/) indicates that the SSG considers IP addresses on the left side of the slash a higher priority than those on the right side of the slash.<br>• **"vpdn:tunnel-id=***name***"**—VPDN tunnel ID. Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.<br>• **"vpdn:tunnel-password=***secret***"**—L2TP tunnel password. Specifies the secret (password) used for L2TP tunnel authentication.<br>• **"vpdn:l2tp-hello-interval=***interval***"**—L2TP hello interval. Specifies the number of seconds for the hello keepalive interval. |

# Example Service Profiles

The service configuration examples in this section use a Merit RADIUS format.

### Example Service Profile for Passthrough Service

```
internet Password = "servicecisco", Service-Type = Outbound
    Service-Info = "IInternet",
    Service-Info = "R153.153.153.0;255.255.255.0",
    Service-Info = "MC",
    Service-Info = "TP"
```

### Example Service Profile for Proxy Service

```
corporate Password = "servicecisco", Service-Type = Outbound
    Service-Info = "ICorporate Intranet (proxy)",
```

```
    Service-Info = "R154.154.154.0;255.255.255.0",
    Service-Info = "S10.3.3.101;1812;1813;cisco",
    Service-Info = "MC",
    Service-Info = "TX"
```

### Example Service Profile Using Timeout Values

```
iptv Password = "servicecisco", Service-Type = Outbound
    Service-Info = "IIP/TV",
    Service-Info = "R160.160.160.0;255.255.255.0",
    Service-Info = "MC",
    Service-Info = "TP"
    Idle-Timeout = 60,
    Session-Timeout = 60
```

# Configuring Service Group Profiles

Service group profiles contain a list of services. Table C-5 briefly describes the attributes in a RADIUS service group profile.

***Table C-5 Attributes in Service Group Profiles***

| Attribute | Description |
|---|---|
| Password | The password required to obtain the profile. |
| Service-Type | Standard RADIUS attribute number 6. The level of service. Must be outbound. |
| Account-Info | A vendor-specific attribute (attribute number 26), vendor 9, subattribute 250. Valid values for Account-Info attributes are:<br>• **"I***description***"**—Describes the service group. If this field is omitted, the service group profile name is used.<br>• **"G***Name***"**—Service group name.<br>• **"N***name***"**—Lists the services that belong to the group.<br>• **"TE"**—Indicates that this is a mutually exclusive service group. |

# Example Service Group Profiles

The service group configuration examples in this section use a Merit RADIUS format.

### Example Service Group Profile

```
SvcGroup1 Password = "servicecisco", Service-Type = Outbound
    Account-Info = "Nvidconf",
    Account-Info = "Ndistlearn",
    Account-Info = "Ncorporate",
    Account-Info = "Nbanking"
```

### Example Service Group Profile for a Mutex Group

```
MutexGrp1 Password = "groupcisco", Service-Type = Outbound
    Account-Info = "IBandwidth-QoS",
    Account-Info = "Nbw-gold",
    Account-Info = "Nbw-silver",
    Account-Info = "Nbw-bronze",
    Account-Info = "TE"
```

# Configuring Subscriber Profiles

Subscriber profiles define SESM logon names and passwords, access control lists associated with each logon, and subscribed services for each logon.

In an SESM RADIUS mode deployment, you must define a subscriber profile for each subscriber that will sign onto an SESM portal from a web browser.

Table C-6 briefly describes the attributes in a RADIUS subscriber profile. Use the following references for more information:

- If you are using the Cisco Access Registrar, see the "Configuring Cisco Access Registrar for SESM Deployments" section on page C-17 for subscriber profile examples and syntax. Otherwise, see your RADIUS server vendor documentation for the syntax of a subscriber profile
- For sample SESM subscriber profiles, see the aaa.properties file located in the NWSP config directory (for example, nwsp/config/ aaa.properties). This file is installed whether or not you choose the demo option. It shows service and subscriber profiles in Merit RADIUS format.
- The SSG documentation describes subscriber profile attributes and provides examples of their use. See the "Related Documentation" section on page xv for a link to online SSG documentation.

***Table C-6 Attributes in Subscriber Profiles***

| Attribute | Description |
|---|---|
| User-Name | Standard RADIUS attribute number 1. The subscriber name used for authentication. |
| User-Password | Standard RADIUS attribute number 2. The subscriber password used for authentication. |
| Called-Station_Id | Standard RADIUS attribute number 30. The access point name (APN), which can optionally be used for authentication. |
| Calling-Station_Id | Standard RADIUS attribute number 31. The MSISDN, which can optionally be used for authentication. |
| NAS-Identifier | Standard RADIUS attribute number 32. The NAS identifier, which can optionally be used for authentication. |
| Session-Timeout | Standard RADIUS attribute number 27. Specifies the maximum length of time, in seconds, that this subscriber session (the edge session on SSG) can remain active at any one time. When the time expires, SSG ends the session. If the host key feature is enabled on the SSG, the SSG signals the state change to the SESM web portal.<br>**Note** The NWSP application does not relay this state change to the subscriber.<br>If Session-Timeout is not set, there is no limit on how long the session lasts.<br>In a dial-up networking or bridged (non-PPP) network environment, a subscriber can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, which can be a problem if the IP address is obtained by another user. You can use the Session-Timeout and the Idle-Timeout attributes to prevent this problem. |
| Idle-Timeout | Standard RADIUS attribute number 28. Specifies the maximum length of time, in seconds, that a subscriber session can remain idle before it is disconnected. See the explanation of the Session-Timeout attribute, above, for more information about setting this attribute. |

*Table C-6 Attributes in Subscriber Profiles (continued)*

| Attribute | Description |
|---|---|
| Account-Info | **Note** In SSG Release 12.2.4(B) or later, if a point-to-point protocol (PPP) subscriber profile does not include any VSAs, the SSG does not create a host object for the subscriber and therefore, the SSG does not apply any control over the subscriber's access. The fact that the PPP link is established and the SSG is not applying any control means that the subscriber has unrestricted access to any downstream connections defined in the subscriber's profile or by the Cisco IOS configuration on the SSG host device. If it is important to avoid this situation, make sure that all PPP clients are subscribed to at least one service or define any other Cisco SSG VSA in the profile, such as a **U***url* or **H***url* attribute.<br><br>A vendor-specific attribute (attribute number 26), vendor 9, subattribute 250. Valid values for Account-Info attributes are:<br>• **"N***serviceName***"**—Service name. Subscribes the subscriber to the specified service and includes the service in the service list obtained by the SESM web portal. The *serviceProfileName* must be defined in a service profile. There can be multiple instances of this attribute within a subscriber profile.<br>• **"G***serviceGroupProfileName***"**—Service group. Creates a folder for the service group on the subscriber's SESM web portal. The *serviceGroupProfileName* must be defined in a service group profile. There can be multiple instances of this attribute within a subscriber profile.<br>• **"A***autoConnectServiceName***"**—Automatic connection. Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon.<br>**Note** The service list displayed by SESM does not include A entries. It only shows N entries. To display an auto connect service on the SESM service list, include both an A and an N entry for the service in the profile. See the "Example Subscriber Profile for Auto Services" section on page C-15 for an example.<br>• **"U***url* or **H***url***"**—These attributes specify the URL for the user's preferred Internet home page. If the SESM web portal is designed to use HTML frames, then these options also specify whether the home page is displayed in a new browser window or in a frame in the current (SESM) window, as follows:<br>– **U***url*—URL for the home page displayed in its own browser window.<br>– **H***url*—URL for the home page displayed in a frame in the SESM browser window.<br>**Note** In a frameless application, both U and H cause a new browser window to open for the home page. The NWSP application is a frameless application.<br>• **"RI***group*;*duration*[;*service*]**"**—Overrides the TCP redirect configuration on the SSG for initial logon redirections. The *group* is the captive portal group to use for initial logon redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The *duration* is the duration of the captivation (in seconds). If you specify the optional *service* field, initial logon redirection occurs only when the subscriber requests connection to the named service.<br>• **"RA***group*;*duration*;*frequency*[;*service*]**"**—Overrides the TCP redirect configuration on the SSG for advertisement redirections. The *group* is the captive portal group to use for advertisement redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The *duration* is the duration of the captivation (in seconds). The frequency is the approximate interval between redirections (in seconds). If you specify the optional *service* field, redirection occurs only when the subscriber requests connection to the named service. |

*Table C-6 Attributes in Subscriber Profiles (continued)*

| Attribute | Description |
|---|---|
| Account-Info *(continued)* | • **"RS"**—The subscriber has SMTP forwarding capability.<br>• **"QU**;*upstream-token-rate*;*upstream-normal-burst*;[*upstream-excess-burst*];**D**;*downstream-token-rate*;*downstream-normal-burst*;[*downstream-excess-burst*]"—Indicates hierarchical policing (quality of service) policies for this subscriber.<br>**Note** The **$** in a subattribute code indicates that the subattribute is used only by SESM, and not by SSG or other Cisco network devices.<br>**Note** Deployers might see **$** subcodes in access accept messages from SSG that are not documented below. SSG uses **$** subcodes to identify information about the subscriber that it passes along for SESM use, such as MAC address, VPI/VCI, MSISDN number, and other connection information. Those codes are not documented in this guide because they are not used in subscriber profiles.<br>• **"$PE***permission***"—**Meaningful in Demo mode only, to demonstrate the LDAP mode self-management, self-subscription, and sub-account creation features. Use this attribute to assign specific permissions to the subscriber for use in a demo. The *permission* is one of the following:<br>– Service Selection—The permission to perform service selection and disconnect from services is implied and does not have to be explicitly coded in the profile.<br>– Self Manage—Use this string to demonstrate the LDAP mode feature that allows a subscriber to update their own account attributes, such as name, address, e-mail, and hobbies.<br>– Subaccount Manage—Use this string to demonstrate the LDAP mode feature that allows a subscriber to create, delete, and manage subaccounts. The Demo mode does not create an actual subaccount; the supporting subaccount profile must be defined in the aaa.properties file. Define the subaccount profile and use the $**FA** attribute.<br>– Service Subscription—Use this string to demonstrate the LDAP mode feature that allows a subscriber to subscribe and unsubscribe to services and service groups. If you use this string, you must also add a **$SA** or **$GA** attribute.<br>• **"$SA***service***"**—Meaningful in Demo mode only, to demonstrate the LDAP mode self-subscription feature. Use this attribute to list services to which the subscriber can self-subscribe. The *service* must be defined in a service profile.<br>• **"$GA***serviceGroupName***"**—Meaningful in Demo mode only to demonstrate the LDAP mode self-subscription feature. Use this attribute to list service groups to which the subscriber can self-subscribe. The *serviceGroupName* must be defined in a service group profile.<br>• **"$UG***userGroupName***"**—Meaningful in Demo mode only to demonstrate the LDAP mode user group features, including user group branding. This subcode adds the user to a user group. The *userGroupName* can be any value. (User groups are an LDAP mode concept. RADIUS profiles do not provide a way to define valid user group names.)<br>The PDA application running in Demo mode demonstrates brand awareness by displaying different branded pages based on the user group values of bronze, silver, and gold. See the aaa.properties file. |

*Table C-6 Attributes in Subscriber Profiles (continued)*

| Attribute | Description |
|---|---|
| Account-Info *(continued)* | • **"$AA***accountAttributeName;type;attributeValue***"**—Meaningful in Demo mode only to demonstrate the LDAP mode account self-care features. Use this attribute to specify the initial values that will appear in the fields on the My Account page in the NWSP application running in Demo mode. Use a separate attribute line for each field.<br><br>The *accountAttributeName* is a name for a field on the My Account page in the NWSP application. These are X.500 fields. See the *Cisco Distributed Administrator Tool Guide* for a list of the X.500 names. You can add more fields to the demo if you alter the NWSP application to display more fields, as described in the *Cisco Subscriber Edge Services Manager Web Developer Guide*.<br><br>The *type* indicates a type for *attributeValue* and is one of the following:<br>– S—*attributeValue* is a simple string.<br>– V—*attributeValue* is an array of strings.<br><br>The *attributeValue* indicates the value to be displayed in the field in NWSP. If type is V, surround *attributeValue* with braces ({}) and delimit each element in the array with a semicolon.<br><br>For example:<br>`"$AAgivenName;S;James"`<br>`"$AAhobbies;V;{sports;news;travel}"`<br><br>• **"$FA***parent***"**—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. This subcode identifies this subscriber as a subaccount. The *parent* is the user name of the parent account and must be defined in a subscriber profile.<br><br>The NWSP application running in Demo mode demonstrates subaccounts. In the aaa.properties file, subgolduser is defined as a subaccount to golduser.<br><br>• **"$SB***serviceBlocked***"**—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. In a subaccount profile, this subcode identifies a service that is blocked (not available) to the subaccount. The parent account can unblock a service and make it available for subscription. The *service Blocked* must be defined in a service profile.<br><br>• **"$GB***serviceGroupBlocked***"**—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. In a subaccount profile, this subcode identifies a service group that is blocked (not available) to the subaccount. The parent account can unblock a service group and make it available for subscription. The *serviceGroupBlocked* must be defined in a service group profile.<br><br>• **"$SL***subaccountLimit***"**—Meaningful in Demo mode only to demonstrate the LDAP mode subaccount features. In a parent account profile, this subcode defines the number of subaccounts that the parent can create. If this subcode is not included in the profile, no limit is enforced. The *subaccountLimit* is an integer value from 0 to any limit imposed by the deployer.<br><br>• **"$SO***singleSignOn***"**—Meaningful in Demo mode only. Allows you to disable single sign-on for individual users when the SESM global sign-on is in effect. If this attribute is not defined, the default value 1 is used. Values are<br>– 0—Single sign-on is not permitted for this subscriber.<br>– 1 (the default)—Single sign-on is permitted for this subscriber. |

*Table C-6 Attributes in Subscriber Profiles (continued)*

| Attribute | Description |
|---|---|
| Cisco-AVpair | A vendor-specific attribute (attribute number 26), vendor 9, subattribute 1. Valid values for the Cisco-AVpair attribute in a subscriber profile are:<br>• **"ip:inacl**[*#number*]={*standardACL* \| *extendedACL*}**"**—Upstream access control list (ACL). Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to upstream traffic coming from the subscriber.<br>• **"ip:outacl**[*#number*]={*standardACL* \| *extendedACL*}**"**—Downstream ACL. Specifies either a Cisco IOS standard ACL or an extended ACL to be applied to downstream traffic going to the subscriber.<br>– *number*—Identifies the access list. If a profile includes multiple inacl or outacl attributes, the attributes are downloaded and executed according to the order implied by *number*.<br>– *standardACL*—A Cisco IOS standard ACL.<br>– *extendedACL*—A Cisco IOS extended ACL.<br>**Note** A profile can include multiple instances of inacl attributes and multiple instances of outacl attributes. Use one attribute for each ACL statement. Multiple attributes can be used for the same ACL. |

# Example Subscriber Profiles

The subscriber profile examples in this section are in a Merit RADIUS format.

### Example Subscriber Profile for Auto Services

```
user1 Password = "cisco"
    Service-Type = Framed-User,
    Account-Info = "Ainternet",      (hidden on the subscriber's web page)
    Account-Info = "Ninternet"       (makes it visible)
```

**Note** The first Account-Info line specifies automatic connection to the service. If you do not include the second line, the auto connection service does not appear on the SESM web portal. To display the service on the SESM web portal, you must include both entries as shown in the example.

### Example Subscriber Profile for Demo Mode

```
golduser Password = "cisco"
    Service-Type = Framed-User,
    Account-Info = "$UGgold",
    Account-Info = "Ainternet_gold",
    Account-Info = "Ninternet_gold",
    Account-Info = "Ncorporate",
    Account-Info = "Ngames",
    Account-Info = "Ndiscount_shopping",
    Account-Info = "Hhttp://www.spiderbait.com",
    Account-Info = "$PESelf Manage",
    Account-Info = "$PESubaccount Manage",
    Account-Info = "$PEService Subscription",
    Account-Info = "$SAbanking",
    Account-Info = "$GAnewsgroup",
    Account-Info = "$AAinitials;V;{A}",
    Account-Info = "$AAgender;S;female",
    Account-Info = "$AAsurname;S;Goodbody",
```

```
    Account-Info = "$AAtitle;S;Miss",
    Account-Info = "$AAgivenName;S;Felicity",
    Account-Info = "$AAhobbies;V;{science;news;travel}"
```

See the aaa.properties file in the nwps/config directory for more examples.

# Configuring Next Hop Gateway Profiles

Next Hop Gateway profiles associate next hop gateway keys with IP addresses. Because multiple SSGs might access services from different networks, service profiles can specify next hop keys. (See the service-info G attribute in Table C-4 on page C-6.) If this is the case, you must configure a next hop gateway pseudo-service profile to resolve the keys to valid IP addresses.

An example next hop gateway pseudo-service profile follows:

```
ssg-next-hop Password = "xssg-key"
    Control-Info = "Gl2tp-net7;192.168.1.101",
    Control-Info = "Gl2tp-net40;192.168.1.102",
    Control-Info = "Gweb-key;192.168.1.101",
    Control-Info = "Gproxy-radius-key;192.168.1.101",
    Control-Info = "Gxint-24;192.168.1.101"
```

# Configuring the RADIUS Accounting Feature

If you configure a RADIUS accounting port, SSG generates accounting records and forwards them to the RADIUS server. To configure a RADIUS server for accounting only, you must perform the following configuration steps.

- Configure the NAS clients as described in the "Configuring RADIUS Clients" section on page C-1.
- Add the Cisco VSAs to the RADIUS server attribute dictionary, as described in the "Defining Attributes" section on page C-2.
- Configure an accounting port, as described in the "Configuring SSG to Communicate with the RADIUS Server" section on page C-1.

**Note** You do not need to provide service and subscriber profiles if you are using the RADIUS server solely for accounting purposes.

The subscriber actions that cause SSG to generate a RADIUS accounting record are:

- Subscriber logs in
- Subscriber logs off
- Subscriber accesses a service
- Subscriber terminates a service

Use the following references for more information:

- SSG documentation—Describes the attributes contained in the accounting records
- RADIUS server vendor documentation—Describes RADIUS accounting capabilities

# Configuring Cisco Access Registrar for SESM Deployments

This section describes how to configure the Cisco Access Registrar (Cisco AR) for an SESM deployment. The section includes profile examples in Cisco AR format.

## Configuring the RADIUS Ports

By default, Cisco Access Registrar listens on ports 1645 and 1646 for any type of RADIUS request. You can configure Cisco Access Registrar to listen on ports 1812 and 1813 instead by entering the following commands:

```
add /Radius/Advanced/Ports/1812
add /Radius/Advanced/Ports/1813
```

These commands cause Cisco Access Registrar to listen on the explicitly defined ports, 1812 and 1813, for all types of RADIUS requests. It no longer listens on the default ports.

## Cisco SSG VSAs in Cisco Access Registrar Dictionary

Cisco Access Registrar is installed with the following Cisco VSAs already defined in its attribute dictionary:

- Cisco-AVPair
- Cisco-SSG-Account-Info
- Cisco-SSG-Service-Info
- Cisco-SSG-Command-Code
- Cisco-SSG-Control-Info

## Configuring NAS Clients in Cisco Access Registrar

Use the following commands to configure the NAS clients required by an SESM deployment:

```
add /Radius/Clients/SESM1 "" 10.3.3.2 cisco
add /Radius/Clients/SESM2 "" 10.3.3.101 cisco
add /Radius/Clients/SESM1 "" 10.3.3.102 cisco
```

## Configuring Attribute Profiles in Cisco Access Registrar

This section shows commands for creating sample profiles in Cisco Access Registrar format.

#### Internet Service Profile

```
add /Radius/Profiles/internet-profile
set /Radius/Profiles/internet-profile/Attributes/Cisco-SSG-Service-Info IInternet
    R153.153.153.0;255.255.255.0 MC TP
```

#### Corporate Service Profile

```
add /Radius/Profiles/corporate-profile
set /Radius/Profiles/corporate-profile/Attributes/Cisco-SSG-Service-Info "ICorporate
    Intranet(proxy)" R154.154.154.0;255.255.255.0 S10.3.3.101;1812;1813;cisco MC TX
```

#### IPTV Profile

```
add /Radius/Profiles/iptv-profile
set /Radius/Profiles/iptv-profile/Attributes/Cisco-SSG-Service-Info IIP/TV
    R160.160.160.0;255.255.255.0 MC TP
set /Radius/Profiles/iptv-profile/Attributes/Idle-Timeout 60
set /Radius/Profiles/iptv-profile/Attributes/Session-Timeout 60
```

#### Standard Subscriber Profile

```
add /Radius/Profiles/std-user-profile
set /Radius/Profiles/std-user-profile/Attributes/Service-Type Framed
set /Radius/Profiles/std-user-profile/Attributes/Cisco-SSG-Account-Info Ainternet
    Ninternet
```

#### Pseudo-service Profile

```
add /Radius/Profiles/pseudo-service-profile
set /Radius/Profiles/pseudo-service-profile/Attributes/Cisco-SSG-Control-Info
    Gl2tp-net7;192.168.1.101 Gl2tp-net40;192.168.1.102 Gweb-key;192.168.1.101
    Gproxy-radius-key;192.168.1.101 Gxint-24;192.168.1.101
```

## Configuring Cisco Access Registrar Userlists and Authentication and Authorization Services

This section describes how to configure userlists and authentication and authorization services on Cisco Access Registrar.

#### Configuring Userlist for SESM Services

The following commands configure userlists containing SESM services and corresponding attribute profiles.

```
add /Radius/Userlists/SESMservices
add /Radius/Userlists/SESMservices/internet "" servicecisco TRUE "" internet-profile
add /Radius/Userlists/SESMservices/corporate "" servicecisco TRUE "" corporate-profile
add /Radius/Userlists/SESMservices/iptv "" servicecisco TRUE "" iptv-profile
```

#### Configuring Userlist for SESM Users

The following commands configure userlists containing SESM users and corresponding attribute profiles.

```
add /Radius/Userlists/SESMusers
add /Radius/Userlists/SESMusers/user1 "" cisco TRUE "" std-user-profile
add /Radius/Userlists/SESMusers/ssg-next-hop "" xssg-key TRUE "" pseudo-service-profile
```

#### Configuring AA Services

The following commands configure Cisco Access Register AA services. The first command configures services for the SESM services userlist. The second command configures services for SESM users userlist.

```
add /Radius/Services/Outbound "" local "" "" RejectAll "" SESMservices
add /Radius/Services/SESMdefault "" local "" "" RejectAll "" SESMusers
```

### Checking the Service-Type Attribute

The following commands configure Cisco Access Registrar to check the Service-Type attribute in the request. If Service-Type is set to Outbound, then the Outbound AA service is used; otherwise, the SESM default AA service is used.

```
set /Radius/DefaultAuthenticationService ${q|Service-Type}{SESMdefault}
set /Radius/DefaultAuthorizationService ${q|Service-Type}{SESMdefault}
```

## Configuring Accounting on Cisco Access Registrar

To configure accounting services, use the following commands:

```
add /Radius/Services/SESMaccounting "" file
set /Radius/DefaultAccountingService SESMaccounting
```

## Saving the Configuration and Reloading the Server

To save the configuration and reload the Cisco Access Registrar server, use the following commands:

```
save
reload
```

# Example RADIUS Profiles

The SESM product includes sample RADIUS profiles in MERIT flat file formats. The SESM sample portal applications running in Demo mode use the profiles in these MERIT files. The installation includes a separate MERIT file for each of the sample portal applications. The files are located in the config directory under each portal application directory. For example:

```
nwsp
    config
         aaa.properties
```