CHAPTER 12

Deploying an SESM/SSG Solution

This section describes the attributes that control communication between components in an SESM deployment. In many cases, attributes with matching values must be set on both sides of the communication for the communication to be successful.

This section includes the following topics:

Communication Attributes for Interaction Between SESM and SSG

The section applies to all SESM deployments, regardless of the SESM mode.

Figure 12-1 shows the attributes whose values must match for successful communication between an SESM web application and SSG. Table 12-1 describes how to set these attributes on both sides of the communication.

Figure 12-1 Attributes for SESM to SSG Communication in All Modes

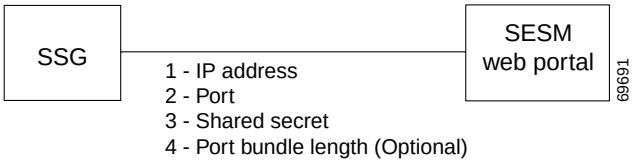


Table 12-1 Setting Attributes for SESM to SSG Communication in All Modes

Configuring Communication Between an SESM Web Application and SSG		
On the SSG side	Set these values using Cisco IOS commands on the SSG host. If the SSG is already configured, use **show run** to view the settings.	
	1.	IP Address—Use the following command to specify the network that the SESM web application is running on: `ssg default-network networkIPAddress mask`
	2.	Port—Use the following command to specify the port on the SSG host that handles RADIUS protocol communication between the SSG and the SESM web application: `ssg radius-helper auth-port port`
	3.	Shared Secret—Use the following command to specify the shared secret used in RADIUS protocol communication between the SSG and the SESM web application: `ssg radius-helper key secret`
	4.	(Optional) Host Key Port Bundle Length—When the host key feature is enabled on the SSG, the port bundle length defaults to 4 bits. You can use the following command to specify a different port bundle length: `ssg port-map length bits` **Note** Additional commands are required on SSG to enable and configure the host key feature. For more information, see the "Configuring the Host Key Port Bundle Feature on SSG" section on page F-2.
On the SESM web application side	**1.**	IP Address—Make sure to install SESM web applications and their containers (the J2EE web servers) on the SSG default network.
	Set the following values in the SSG MBean in the application MBean configuration file (nwsp.xml, for example):	
	2.	Port—Use the following attributes to set the RADIUS protocol ports for communication between the SSGs and SESM. These settings must match the settings on the SSG hosts. • PORT global attribute • PORT subnet attribute—Overrides the global setting if all of the SSGs are not configured the same.
	3.	Shared Secret—Use the following attributes to set the RADIUS protocol shared secrets for communication between the SSGs and SESM. These settings must match the settings on the SSG hosts. • SECRET global attribute • SECRET subnet attribute—Overrides the global setting if all of the SSGs are not set the same.
	4.	Host Key Port Bundle Length—Use the following attributes to set the port-bundle length to match the settings on the SSG hosts. • BUNDLE_LENGTH global attribute • BUNDLE_LENGTH subnet attribute—Overrides the global setting if all of the SSGs are not configured the same.

Attribute Definitions

The RADIUS protocol is the communication mechanism used between an SESM web application and SSG. The following attributes are required by the RADIUS protocol:

- IP address and port— In communications between SESM and SSG, SSG acts as the server and SESM is the client.In the RADIUS protocol, the client must know the IP address of the server and the port that the server listens on. SSG uses the concept of a RADUIS helper to define this port. The RADIUS helper port is a different attribute from the RADIUS port used for communication with a RADIUS server. However, the values of these two attributes might be the same. The value 1812 is common for both.
- Shared secrets—Shared secrets are the key for the MD5 encryption algorithm used by the RADIUS protocol. They are required in all RADIUS protocol communications. The shared secret value is known on each side of the communication but is never sent across the network.

The following attribute is used by the SSG port-bundle host key feature:

- Port-bundle length—This attribute controls how many ports are in each bundle in the SSG host key feature, and, indirectly, how many bundles are available within each host key source IP address as configured on the SSG. The length defines the number of bits required to represent the number of ports in each bundle. For example, a length of 4 (bits) means that the number of available ports in each bundle is 2^4, or 16 ports per bundle.

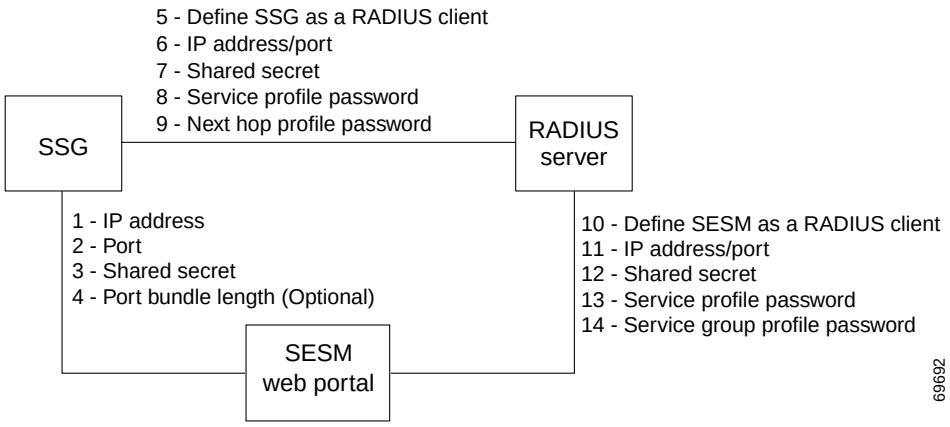
Note We strongly recommend using the same port bundle length on all SSGs in the same network. The default value of 4 is recommended, which results in 16 ports per bundle and 4032 bundles per host key source IP address.

Communication Attributes for RADIUS Mode

This section describes attributes in a RADIUS mode deployment whose values must match each other for successful communication to occur.

Figure 12-2 shows the attributes whose configured values must match. Table 12-2 describes how to set these attributes on each side of the communication.

Figure 12-2 Communication Attributes in a RADIUS Mode Deployment



\

Table 12-2 Setting Communication Attributes in a RADIUS Mode Deployment

Configuring Communication Between an SESM Application and SSG		
On the SESM and SSG Sides	**1 to 4**	See Table 12-1, "Setting Attributes for SESM to SSG Communication in All Modes"
Configuring Communication Between a RADIUS Server and SSG		
On the RADIUS Side	Set these values using the RADIUS product's native configuration procedures:	
	5.	Define SSG as a RADIUS Client—Define SSG as a NAS client.
	6.	IP address/port—The IP address is the address of the RADIUS server host machine. The port is the port the RADIUS server uses to listen for authentication and authorization requests. If you do not specifically set the authentication port, it usually defaults to port 1812.
	7.	Shared secret—The shared secret value is specified when you define the SSG as a NAS client.
	8.	Service password—The service password is included in the service profiles stored in the RADIUS database. Use the same password value in all service profiles.
	9.	(Optional) Next hop password—The password used in the next hop table profile stored in the RADIUS database. Next hop profiles are an optional feature in an SESM deployment. Use the same password value in all next hop profiles.
On the SSG Side	Set these values using Cisco IOS commands on the SSG host:	

	5.	Set up SSG as a RADIUS client—Use the following commands:
		`#aaa new-model`
		`#aaa authentication ppp default local group radius`
		`#aaa authorization network default local group radius`
		Note If the SSG is not supporting PPP connections, you do not need to use the **aaa authentication ppp** command.

	6.	IP address/port—Use the following command: `radius-server host` *`RadiusHostIpAddr`* `auth-port` *`port`*
	7.	Shared secret—Use the following command: `radius-server key` *`RadiusSharedSecret`*
	8.	Service Password—Use the following command: `ssg service-password` *`servicePassword`*
	9.	(Optional) Next Hop Password—Use the following command: `ssg next-hop download` *`nextHopTableName password`*

Table 12-2 Setting Communication Attributes in a RADIUS Mode Deployment (continued)

Configuring Communication Between a RADIUS Server and an SESM Application		
On the RADIUS Side	Set these values using the RADIUS product's native configuration procedures:	
	10.	Define a RADIUS client—Define SESM as a NAS client.
	11.	IP address/port—You can set the port on the RADIUS server host machine that the RADIUS server uses to listen for authentication requests. The port is usually port 1812, which is the industry's default port for a RADIUS server.
	12.	Shared secret—You set the shared secret value when you define the SESM application as a NAS client. **Note** If you are configuring primary and secondary RADIUS servers, the shared secret value established for the SESM NAS client must be the same on both RADIUS servers.
	13.	Service password—The service password is included in the service profiles stored in the RADIUS database. Use the same password value in all service profiles.
	14.	Group password—The service group password is included in the service group profiles stored in the RADIUS database. Use the same password value in all service group profiles.
On the SESM web application side	Set the following value in the SESM MBean in the SESM web application configuration file (nwsp.xml, for example):	
	10.	Define a RADIUS client—The attribute name is mode. To deploy SESM in RADIUS mode, the value for mode must be RADIUS. **Note** You can override the value for mode on the command line when you start the SESM application. For more information, see the "Starting the SESM Portals" section on page 9-1.
	Set the following values in the AAA MBean in the SESM application configuration file (nwsp.xml, for example):	
	11.	IP Address/Port—The attribute names for identifying IP addresses and authentication ports on primary and secondary RADIUS servers are: • primaryIP • primaryPort • (Optional) secondaryIP • (Optional) secondaryPort
	12.	Shared Secret—The attribute name is secret. There is only one secret attribute because the the secret value must be the same on both the primary and secondary servers.
	13.	Service Password—The attribute name is servicePassword. Use this attribute to provide SESM with the generic password used in the service profiles.
	14.	Group Password—The attribute name is groupPassword. Use this attribute to provide SESM with the generic password used in the service group profiles.

Attribute Definitions

The RADIUS protocol is the communication mechanism used between all of the components in this deployment. The following attributes are required by the RADIUS protocol:

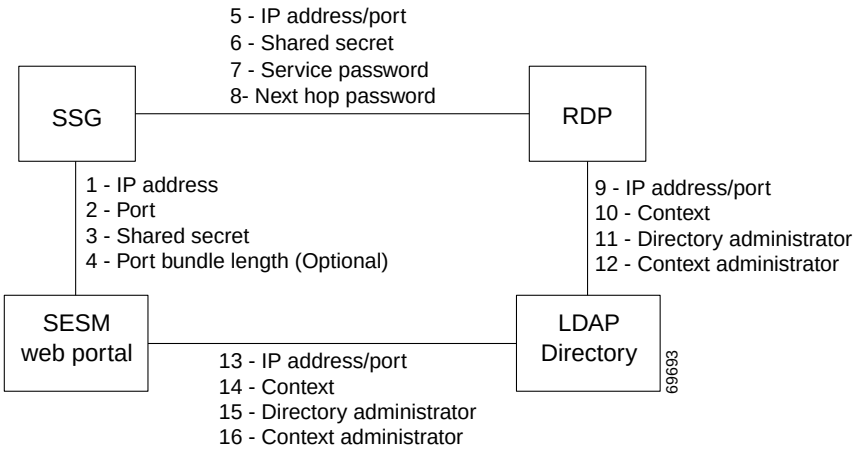
- RADIUS IP address and port—The RADIUS clients must know the IP address of the RADIUS server machine and the port that RADIUS uses for authentication and authorization requests. The port is set when the RADIUS server is configured. It is usually port 1812, which is the industry's default authentication and authorization port for a RADIUS server.
- Shared secrets—Shared secrets are the key for the MD5 encryption algorithm used by the RADIUS protocol. They are required in all communications between a RADIUS client and a RADIUS server. The shared secret value is known on each side of the communication but is never sent across the network.
- Profile passwords—In a RADIUS database, the service, service group, and next hop profiles include passwords. The RADIUS protocol requires that requests for these profiles include the profile password. In an SESM RADIUS mode deployment, all profiles of the same type must use the same password. For example, all service profiles use the same password; all service group profiles use the same password, and so forth. You provide these generic password values to the RADIUS clients (SSG or SESM) using configuration attributes.

Communication Attributes for LDAP Mode

This section describes attributes in a LDAP mode deployment whose values must match each other for successful communication to occur.

Figure 12-3 shows the attributes whose configured values must match on each side of the communication to successfully deploy SESM in LDAP mode. Table 12-3 describes how to set these attributes on each side of the communication.

Figure 12-3 Communication Attributes in an LDAP Mode Deployment



Note The service group password is not used in this deployment. Service group requests are obtained by the SESM web portal from the LDAP directory, and a password is not required.

Table 12-3 Setting Communication Attributes in an LDAP Mode Deployment

Configuring Communication Between an SESM Web Application and SSG		
On the SESM and SSG Sides	**1 to 4**	See Table 12-1, "Setting Attributes for SESM to SSG Communication in All Modes"
Configuring Communication Between RDP and SSG		
On the RDP side	Set the following values in the RDP MBean on the RDP host machine.	
	5.	IP address/port—The attribute names are: • localIPAddress—The IP Address or host name of the RDP host machine. (You cannot enter the value localhost or 127.0.0.1.) • localPort—The port on which RDP will listen for RADIUS authentication and authorization requests. The value is usually 1812, which is the industry's default authentication and authorization port.
	6.	Shared secret—The attribute name is secret. This is the RADIUS protocol shared secret value used for communication between SSG and RDP.
	7.	Service password—The attribute name is servicePassword. Replace `servicecisco` with the service password set on the SSG side.
	8.	(Optional) Next hop password—The attribute name is nextHopPassword. Replace `nexthopcisco` with the next hop password set on the SSG side. Next hop profiles are an optional feature in an SESM deployment.
On the SSG side	Set the following values using Cisco IOS commands on the SSG:	
	5.	IP address/port—Use the following command: `radius-server host` *`RDPhostIpAddr`* `auth-port` *`port`*
	6.	Shared secret—Use the following command: `radius-server key` *`RDPSharedSecret`*
	7.	Service password—Use the following command to set the key that SSG uses in service requests: `ssg service-password` *`servicePassword`*
	8.	(Optional) Next hop password—Use the following command to set the key that SSG uses in next hop table requests: `ssg next-hop download` *`nextHopTableName password`*

Table 12-3 Setting Communication Attributes in an LDAP Mode Deployment (continued)

Configuring Communication Between RDP and an LDAP Directory		
SPE configuration on the RDP side	Set these values in the dess-auth configuration file on the RDP host machine (dess-auth/config/config.xml, for example).	
	9.	IP Address/Port—The attribute name is URL. Provide the complete URL of the directory server, including the ldap protocol label and a port number. An example entry is: `ldap://127.0.0.1:389/` You provide the initial value for this attribute during installation. The installation program prompts you for a directory address and directory port, and then it combines your responses, prefaces it with the ldap protocol label, and inserts the resulting string in the URL field in the config.xml file.
	10.	Context—The attribute name is context. Provide the organizational unit and organization in the LDAP directory that holds the SESM data. An example entry is: `ou=sesm,o=cisco` You provide the initial value for this attribute during installation. The installation program prompts you for the directory container.

	11.	Directory administrator—The attribute names are:
		• principal—This must be an administrator ID that exists in the LDAP directory with permissions to extend the LDAP directory schema. An example entry is:
		`cn=admin,ou=sesm,o=cisco`
		or
		`uid=Directory Manager, ou=sesm, o=cisco`
		• credentials—Provide the password that goes with the principal.
		You provide the initial values for these attributes during installation. The installation program prompts you for directory server admin information.

	12.	Context administrator—The attribute name is DESSPrincipal. This is an administrator ID with permissions to access and create objects in the organization and organizational unit identified by the context attribute described above. An example entry is: `cn=user,ou=sesm,o=cisco` You provide the initial values for this attribute during installation. The installation program prompts you for directory container admin information.
On the LDAP Directory Side	**9 to 12**	Use native administration tools for the LDAP directory product to configure the directory for SESM deployment. See the Appendix B, "Configuring an LDAP Directory for SESM Deployments," for guidelines and requirements.

Table 12-3 Setting Communication Attributes in an LDAP Mode Deployment (continued)

Configuring Communication Between an SESM Application and an LDAP Directory		
SPE configuration on the SESM application side	**13 to 16**	If the RDP and SESM applications are installed on the same machine, the same config.xml file applies to both applications. In that case, the values you configured for fields 9 to 12 above are also used for communication between the SESM application and the directory. If the RDP and SESM web applications are installed on different machines, you must maintain two versions of the dess-auth configuration file. In that case, follow the instructions in fields 9 to 12 above to configure the config.xml file on the SESM web application's host machine.
On the LDAP directory side	**13 to 16**	You only need to configure the LDAP directory one time.

Attribute Definitions

RDP and SESM web applications use the LDAP protocol to communicate with the LDAP directory. Some of the LDAP attributes required for communication are:

- IP address/port—These attributes identify the location of the LDAP directory.
- Context—This attribute identifies the container within the LDAP directory that was created specifically for the SESM data.
- Directory administrator—This is a top-level administrator who has permissions to create new contexts within the directory and extend the contexts with application-specific definitions.
- Context administrator—This is an administrator of the context that was created for the SESM data. This administrator must have permissions to add objects into the SESM-specific context.

RDP and SESM web applications use the RADIUS protocol to communicate with SSG. Some of the attributes are:

- IP address/port—RDP is a proxy RADIUS server. You configure SSG to communicate with RDP using the same commands that you use to configure SSG to RADIUS server communication.
- Shared secrets—Shared secrets are the key for the MD5 encryption algorithm used by the RADIUS protocol. They are required in all communications between a RADIUS client and a RADIUS server. The shared secret value is known on each side of the communication but is never sent across the network.
- Service and next hop passwords—The service and next hop requests that SSG sends to RDP include a key word, or password. RDP uses this key word to identify the type of request it has just received and to determine how to process the request. You must configure matching password values on both SSG and RDP for this mechanism to work.

Communication Attributes for LDAP Mode with RDP in Proxy Mode

This section describes the attributes that must be configured to use a proxy RADIUS server in an LDAP mode configuration.

Figure 12-4 shows the attributes whose configured values must match on each side of the communication between RDP in proxy mode and the RADUIS Server. Table 12-4 describes how to set these attributes on each side of the communication.

All other communication in this deployment are the same as described in the previous section.

Figure 12-4 Communication Attributes in an LDAP Mode Deployment with RDP in Proxy Mode

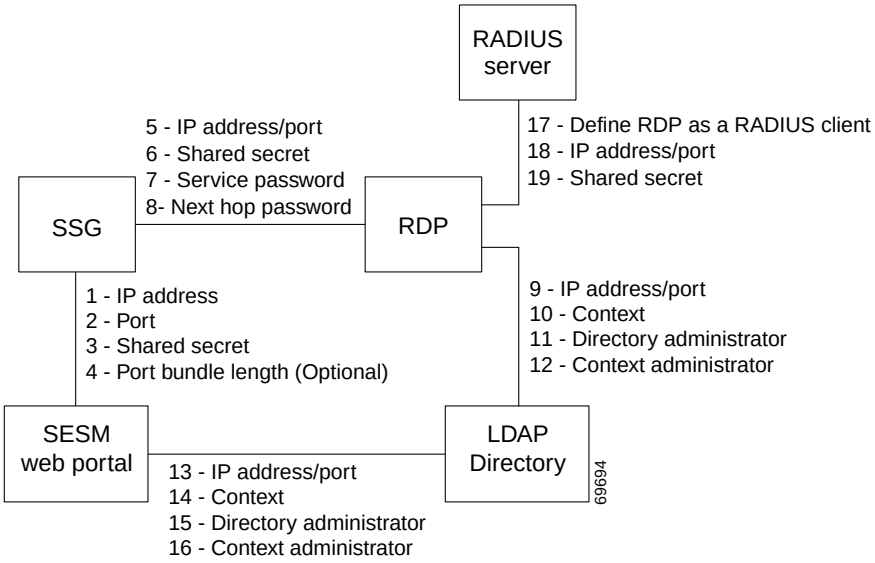


Table 12-4 Setting Communication Attributes in an LDAP Mode Deployment with RDP Proxy

Configuring Communication Between Components in LDAP Mode		
See Table 12-3.	**1 to 16**	See Table 12-3, "Setting Communication Attributes in an LDAP Mode Deployment"
Configuring Communication Between RDP and a RADIUS Server		
On the RADIUS side	Set these values using the RADIUS product's native configuration procedures:	
	17.	Set up a RADIUS Client—Define RDP as a NAS client.
	18.	IP Address/Port—You can set the port on the RADIUS server host machine that the RADIUS server uses to listen for authentication requests. The port is usually port 1812, which is the industry's default authentication and authorization port for a RADIUS server.
	19.	Shared secret—You set the shared secret value when you define the RDP application as a NAS client. **Note** If you are configuring primary and secondary RADIUS servers, the shared secret value must be the same on both RADIUS servers.