CHAPTER 8

Configuring Security Policy Engine for SESM

This chapter describes how to configure the Security Policy Engine (SPE) component to work with SESM applications. The chapter includes the following topics:

SPE Attributes

SPE uses the following MBeans:

- Directory MBean, page 8-2
- Connection MBeans, page 8-3—Two connection MBeans might be configured:
  - Connection MBean, instance=Primary
  - Connection MBean, instance=Secondary

The SPE MBeans are used by any application that incorporates the SPE, which could include SESM portals deployed in LDAP mode, RDP, and CDAT. If these applications are installed:

- In the same directory—They share the same SPE component and use the same MBeans with the same attribute values.
- On different hosts or in different directories—Each separate directory has an SPE component, and the SPE MBeans can contain different attribute values in each location.

To change attributes in the SPE MBeans, you can either:

- Edit the SPE MBean configuration file:

```
dess-auth
    config
       config.xml
```

- Make changes using the Agent View for an application that incorporates the SPE APIs.

Note The SPE component does not have its own management console. Rather, the SPE MBeans are included in the application's MBean list, on the application's management console.

Directory MBean

The Directory MBean configures logging and caching attributes for executing classes in the Dess and Auth APIs. Table 8-1 describes the attributes in the Directory MBean.

Table 8-1 Attributes in the Directory MBean

Attribute Name	Explanation
connectionNameRoot	Root name of the individual connection Mbeans. This MBean searches for other mbeans that begin with this name and assumes that those MBeans are connections to the directory.
factory	Do not change the installed value.
context	Default LDAP context. This is the organization and organizational unit that was created to hold the SESM data.
DESSPrincipal	Name used to connect to the SESM organization and organization unit. This user must have permission to create objects in the SESM context.
alwaysGetAllAttributes	If set to true, all the attributes of an LDAP entry are returned for each query.
traceFileName	Name of the directory log file.
traceLevel	Should be one of: NONE, ERROR, BRIEF, VERBOSE, or DEBUG.
printTraceToConsole	If set to true, the application sends trace messages to the console and writes them into the log file.
stackTrace	If set to true, the application prints a stack trace with each trace message.
cacheMaxObjects	Specifies the maximum number of software objects to hold in the cache. Objects represent subscribers, services, privileges, roles, and so on. When the cache contains cacheMaxObjects, old objects are deleted from cache, regardless of available cache space. Set this value high to allow the available cache space to be the determining factor for cache management. Installed default: 50000
cacheMinFreeMem	Specifies the percentage of Java virtual memory that must remain available (that is, not used by the cache) after the application is loaded into memory. You can calculate the specific amount of memory available for the cache as follows: *cacheSize* = (*JavaVM* – *applCodeSize*) * (100% – *cacheMinFreeMem*) Where: *JavaVM* is the maximum virtual memory size specified at application startup time with the jvm argument. The installed startup scripts use the following values: • The startNWSP script uses 64 MB • The runrdp script uses 20 MB *applCodeSize* is the application size. The NWSP is approximately 18 MB. *cacheMinFreeMem* is the percentage of JVM that must remain available after the application is loaded into memory. For example, the *cacheSize* for NWSP is 90% of 14 MB, or 12.6 MB: *cacheSize* = (32 MB – 18 MB) * (100% – 10%) Default: 10

Table 8-1 Attributes in the Directory MBean (continued)

Attribute Name	Explanation
cacheSessionTimeout	Specifies the timeout of inactive client sessions in seconds. Default: 600
cacheExpireInterval	Specifies the interval in seconds after which the cache attempts to expire objects. **Note** Do not set this attribute to 0. A value of 0 causes *every* request to go to the directory, bypassing caching and any memory storage from a recent request for the same object. A value of 0 degrades performance substantially. Default: 600
cacheObjectTimeout	Specifies the number of seconds before objects time out. Default: 600

Connection MBeans

The Connection MBeans configure location and security attributes required to connect to an LDAP directory. If you configure and deploy two LDAP directories for failover protection, make sure to configure two instances of the connection MBean, using the appropriate connection information for the primary and secondary directories. The connection MBean names are:

- Connection, instance=Primary
- Connection, instance=Secondary

Table 8-2 describes the attributes in the Connection MBeans.

Table 8-2 Attributes in the Connection MBeans

Attribute Name	Explanation
poolSize	Number of active connections allowed to the LDAP server.
URL	URL of the LDAP server.
principal	Name used when connecting to the LDAP server.
credentials	Credentials (such as password) used for connecting to the LDAP server.

Extending the Directory Schema and Loading Initial RBAC Objects

An SESM deployment running in LDAP mode requires the following update activities on the LDAP directory:

- Extend the directory schema. These extensions include the dess and auth classes and attributes that will hold the SESM data. For more information about the extensions, see the *Cisco Distributed Administration Tool Guide*.
- Install initial RBAC objects. Some initial top-level rules and roles must be created in the directory before an administrator can log into CDAT and create additional objects.

The SPE installation process optionally performs these two update activities. If you did not choose these options during the installation, you must do them before running CDAT or an SESM application running in LDAP mode.

Note If the SESM components are distributed among different servers, which means that SPE might be installed in more than one location, you only need to perform these update activities one time against the LDAP directory.

To perform these updates after the initial SPE installation, use either of the following procedures:

- Use the SESM installation process to perform the updates by running a custom installation of the SPE component.
- Perform the updates manually using native administration tools and commands.

Using an SESM Custom Installation to Update the Schema and Load RBAC Objects

To use the SESM custom installation process to extend the directory schema and load initial RBAC objects, follow these procedures:

Step 1 Make sure the LDAP directory server is running.

Step 2 Make sure you know the following user IDs and passwords:

- A user ID and password that allows you to update the directory schema
- A user ID and password that allows you to update the container (organization and organizational unit) that you created for SESM data.

Step 3 Execute the SESM installation program on a server that has network access to the LDAP directory.

Step 4 When the installation program prompts for setup type, choose **Custom**.

Step 5 When the installation program prompts for the components to install, choose **SPE**.

Step 6 When the installation program prompts for directory connection information, provide correct information to access the directory. This includes the names of the organization and organizational unit you created to hold the SESM data.

Step 7 When the installation program displays the options, click the **Update schema** and **Install RBAC** check boxes.

Using LDIF Commands to Update the Directory Schema

To use LDIF commands to manually update the directory, follow these procedures:

Step 1 Make sure the LDAP directory server is running.

Step 2 Make sure you have a user ID and password for the directory that allows you to update the schema.

Step 3 Obtain the required updates from the following location under your installation directory. Choose NDS or Netscape, depending on the LDAP directory you are using:

```
dess-auth
    schema
        NDS
        Netscape
```

Apply the contents of all of the ldf files found under the NDS or Netscape directories:

```
authattr.ldf
authclas.ldf
dessattr.ldf
dessclas.ldf
Policy15.ldf
```

Step 4 Use the **ldapmodify** command to apply all of the preceding files to your directory.

On successful completion, you have applied all of the required updates.

Loading Sample Data

Before any administrator can log into CDAT to create objects, some initial RBAC rules and roles must be loaded into the directory. Load these top level objects by loading the sample RBAC data files that are installed with SPE. You can also use your own data generating tool.

The sample data is located in the following directory:

```
dess-auth
    schema
```

Note The sample data uses common name (cn) as a component of distinguished name (dn). If your LDAP directory uses unique identifier (uid) rather than common name to allow access to the directory, you must edit the sample data files before loading them, replacing all occurrences of cn with uid.

See the *Cisco Distributed Administration Tool Guide* for information about the initial RBAC objects and logging into CDAT. See the *Release Notes for Cisco Subscriber Edge Services Manager Release 3.1(5)* for instructions about loading sample data.