Configuring the Bundled SESM RADIUS Server

This appendix describes the configuration options for the bundled SESM RADIUS server. Topics are:

Bundled SESM RADIUS Server Installed Location

The bundled SESM RADIUS server is installed by default in both RADIUS and LDAP mode installations. None of the SESM installation parameters affects the default configuration of the bundled SESM RADIUS server.

The installed location of configuration files and startup scripts that support the bundled SESM RADIUS server is the tools directory under your SESM installation directory:

```
tools
    bin
        startAAA
    config
        aaa.xml
        erp.xml
        aaa.properties
```

The aaa.xml and erp.xml files are MBean configuration files for the bundled SESM RADIUS server. The aaa.properties file is a sample profile file.

Profile File Requirements

The bundled SESM RADIUS server requires a profile file in MERIT format.

The default configuration points to the aaa.properties file, a sample MERIT file installed with RDP. You can change this to point to a different file by changing the aaaFilename attribute in the AAA MBean. For example, you could point to the aaa.properties file in the NWSP directory.

The bundled SESM RADIUS server loads the contents of the profile file during startup. You must restart the RADIUS server if:

- You change the aaaFilename attribute to point to a different file.
- You make any changes to the profiles in the referenced file.

Defining New Attributes to the Bundled SESM RADIUS Server

All SESM applications, including the bundled SESM RADIUS server, internally predefine the standard RADIUS attributes and the Cisco vendor-specific attributes (VSAs) listed in Table C-2 and Table C-3 on page C-4.

To define additional attributes, such as Cisco VSAs not included in the above-referenced tables or other vendor VSAs:

- Define the new attribute in the RADIUSDictionary MBean. New attributes defined in this MBean can be used in your profiles.
- Define the new attribute in the profile itself, as described in "Dynamically Defining Attributes in Profiles for Testing and Development" section on page C-5.

Starting the Bundled SESM RADIUS Server

The bundled SESM RADIUS server is ready to run immediately after installation. To start it, execute the startup script with a port number, as follows:

- On Solaris and Linux:

  installDir/tools/bin/startAAA.sh *portNumber*

- On Windows:

  installDir\tools\bin\startAAA.cmd *portNumber*

Note You can edit the start script, inserting a default port number. In that case, you do not need to specify *portNumber* on the command line.

MBeans for the Bundled SESM RADIUS Server

The bundled SESM RADIUS server uses the following MBeans:

- Logger MBean, page D-3
- ManagementConsole MBean, page D-3
- RADIUSDictionary MBean, page D-3
- AAA MBean, page D-4

To change attributes in these MBeans, you can either:

- Edit the MBean configuration files:

```
tools
    config
       aaa.xml
```

```
erp.xml
```

- Make changes using the Agent View running on the server management port. The port numbers are:
  - server port—specified at run time on the command line or in the startup script
  - management port— server port + 100

Note The installation process does not add a link on the CDAT main window to this Agent View. You can add this link manually as described in "Adding a New Application to the CDAT Main Window" section on page 6-4. Before creating the link, edit the startAAA script, inserting a port number that you want to consistently use to start the bundled SESM RADIUS server. Then configure the link on the CDAT window to go to the configured RDP port + 100.

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs CDAT application activity. The debugging mechanism produces messages useful for debugging. This is the same logging and debugging mechanism used by the SESM portal applications. See the "Logger MBean" section on page 5-2, for more information.

ManagementConsole MBean

The ManagementConsole MBean configures the server management console port, including valid user names and passwords for accessing the console. See the "Configuring the ManagementConsole MBean" section on page 3-5 for more information.

RADIUSDictionary MBean

All SESM applications, including this RADIUS server, internally predefine the standard RADIUS attributes and the Cisco SSG vendor-specific attributes (VSAs). You can define additional attributes, such as additional Cisco VSAs or VSAs from other vendors, in the RADIUSDictionary MBean. When you define attributes in this MBean, you can use the defined attribute names in RADIUS profiles.

Note You can also define dynamic attributes directly in the profile, as described in the "Dynamically Defining Attributes in Profiles for Testing and Development" section on page C-5.

For a list of the standard RADIUS attributes that are predefined in SESM, see Table C-2 on page C-4. For a list of the Cisco SSG VSAs that are predefined in SESM, see Table C-3 on page C-4.

Table D-1 describes the attributes in the RADIUSDictionary MBean.

Table D-1 Bundled SESM RADIUS Server—RADIUSDictionary MBean

Attribute Name	Explanation
dynamicAttributes	An array of new attribute definitions. To define a new attribute, add a new item to this array. The format for an item is: *name*(*radiusAttributeId, vendorId, vendorSubattribute, datatype*) Where: • *name*—Is the new attribute name. • *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, or IPADDRESS. When *datatype* is BINARY, the value assigned to the attribute must be expressed as a hexadecimal string. For example: demoVSA(26, 1, 1, BINARY) Other valid syntax formats are represented below: *name*([[type=]26],[vendorId=]*vendorId*,[vendorType=]*vendorType*,[dataType=]*dataType*) For example: demoVSA(type=26, vendorId=1, vendorType=1,dataType=INTEGER)

AAA MBean

The AAA MBean configures the AAA listener, including its thread pool and socket (port).Table D-2 describes the configurable attributes in the AAA MBean.

Table D-2 Bundled SESM RADIUS Server—AAA MBean

Attribute Name	Explanation
handler	Defines the type of listener being configured. The value must be AAA to configure a bundled SESM RADIUS server.
dump	• true—Displays all RADIUS messages on the console (stderr) • false—Does not display messages Default: true
aaaFilename	Specifies the profile file name and path.You can change this reference to point to any file in the Merit file format. For example, you could use the NWSP aaa.properties file.
Note The following attributes are in the AAA MBean, RADIUSListener=AAA,component=Threadpool	
minThreads	Sets the minimum number of threads that this listener will maintain during periods of low load. This listener will always have system resources allocated for this number of threads. Default: 5

Table D-2 Bundled SESM RADIUS Server—AAA MBean (continued)

Attribute Name	Explanation
maxThreads	Sets the maximum number of threads that this listener can allocate resources for, even during peak loads. This listener can have up to this number of threads. Default: 255
Note The following attributes are in the AAA MBean, RADIUSListener=AAA,component=RADIUSServerSocket	
secret	The shared secret that must be used in RADIUS protocol messages sent to the bundled SESM RADIUS server. This attribute sets a global shared secret for all clients. To specify different shared secrets for each client, use the allowedClients attribute.
localPort	The port the RADIUS server listens on. It uses the same port for RADIUS Accounting-Requests and Access-Requests. The installed configuration file defines this attribute as a Java system property, which is assigned a value at run time: *application.portno*
allowedClients	Configures a list of clients from which the server can accept requests. Also configures shared secrets. Turn this feature on and off as follows: • Allow any client to access the RADIUS server—Comment out the allowedClients attribute in the XML file, or remove all clients from the allowedClients list. • Restrict client access—Uncomment the allowedClients attribute in the XML file. **Note** If you do not see the allowedClients attribute in the Agent View, check the configuration file (the XML file). The allowedClients attribute might be commented out. If so, remove the comment characters, save the XML file, and then restart the RADIUS server. You can add more clients by adding more elements to the allowedClients attribute. An element in allowedClients attribute has the following format: {hostName | IPAddress}[:localSecret] Where: *hostName* or *IPAddress* identify a client (an SSG, for example) that has access to the server. *localSecret* identifies the secret that this client uses for RADIUS communication.