CHAPTER 7

Configuring the RADIUS Data Proxy

The RADIUS Data Proxy (RDP) translates RADIUS protocol messages into LDAP protocol messages with SPE DESS extensions. RDP is available for installation when you install SESM in LDAP mode. This section describes how to configure the RDP application. Topics are:

Configuring Listeners and Handlers

RDP receives RADIUS protocol messages on one listener. The listener is configured in the RDP MBean.

RDP processes the messages using multiple handlers. Each handler performs some processing and calls the next handler. The chain of handlers that processes a message is configured in the RDP MBean and is determined by:

- The basic configuration options that you specify during installation.
- The type of message; for example, requests for authorization or authentication use different handlers than requests to obtain profile information.

The RDP application is easily extensible because the chain of handlers is configurable in the MBeans. New handlers can be plugged in to handle new or customized configuration requirements.

Note To maintain the correct processing sequence for the installed RDP application, do not change the name and nexthandler attributes in the RDP MBeans.

See the "Summary of RDP Protocol Handlers" section on page 7-8 for a summary of the chain of RDP handlers that processes RADUIS protocol messages in the installed RDP application.

Changing Installed Configuration Options

RDP configuration options are chosen and configured during RDP installation. This section describes how to change those configuration options. The topics are:

Changing the RADIUS Data Proxy Mode

The RDP can run in the following modes:

- Default (non-proxy) mode—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the SPE API to send authorization requests to the LDAP directory.
- Proxy mode—In this mode, RDP forwards authentication requests to a configured RADIUS server. RDP uses the SPE API to send authorization requests to the directory.

  If you use Proxy mode, see the"Configuring Profiles for Proxy Mode" section on page 7-3 for important information about configuring subscriber profiles.

To change the RDP mode, we recommend that you reinstall the RDP component.

Note The alternative is to manually edit the configuration files, commenting out the inappropriate handlers, removing the comments surrounding other handlers, and configuring those handlers.

RDP can also run in LOCAL mode, during which it obtains profiles from a Merit flat file. This mode is useful for testing environments. To switch to LOCAL mode, use the LOCAL attribute in the RDP MBean.

Adding Service Information to Replies

To change this option, we recommend that you reinstall the RDP component.

Note The alternative is to manually edit the configuration files, commenting out the inappropriate handlers, removing the comments surrounding other handlers, and configuring those handlers.

Choose this option if you want the SSG to perform automatic connections to services when a subscriber's profile includes the autoconnect attribute. When you choose this option, RDP includes the subscriber's service list and related information in replies to SSG. The service information consumes memory on the SSG device.

Do not choose this option if memory is a consideration on the SSG device. Instead, you can configure the SESM application to initiate automatic connections with the autoConnect attribute in the SESM MBean. See the "SESM MBean" section on page 5-4 for more information.

Using a Restricted Client List

This option is easily changed after installation. For instructions, see the addClientList attribute in the "RDP MBean" section on page 7-5.

Configuring Profiles for Proxy Mode

In Proxy mode, the RDP forwards authentication requests to a configured RADIUS server. The basic meaning of authentication is validating the user. However, the RDP authentication handler also adds attributes from the subscriber profile to the access-accept message, as described in the "Summary of RDP Protocol Handlers" section on page 7-8.

In the case of Proxy mode, if you want to add additional authentication attributes for a subscriber, you must add them in the profiles used by the proxied RADIUS server. If you add the attributes to the profiles on the LDAP directory, they are ignored.

Note In releases earlier than SESM Release 3.1(5), these additional authentication attributes are processed from the profiles on the LDAP directory.

RADIUS Data Proxy MBeans

RDP uses the following MBeans:

- Logger MBean, page 7-4
- ManagementConsole MBean, page 7-4
- RADIUSDictionary MBean, page 7-4
- RDP MBean, page 7-5

To change attributes in these MBeans, you can either:

- Edit the RDP MBean configuration files:

```
rdp
    config
       rdp.xml
tools
    config
       erp.xml
```

- Make changes using the Agent View running on the RDP management port.

Default port numbers used by the installation process are:

- RDP port—1812
- RDP management port—1912

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool logs RDP 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 RDP 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 the RDP, 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 third-party VSAs, in the RADIUSDictionary MBean. When you define attributes in this MBean, you can use the defined attribute names in the profiles on the LDAP directory.

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 7-1 describes the attributes in the RADIUSDictionary MBean.

Table 7-1 RDP—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, 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 formats are represented below: *name*([[type=]26],[vendorId=]*vendorId*,[vendorType=]*vendorType*,[dataType=]*dataType*) For example: demoVSA(type=26, vendorId=1, vendorType=1,dataType=INTEGER)

RDP MBean

The RDP MBean configures the RDP listener, including its thread pool and sockets (ports), and all of the handlers. Table 7-2 describes the configurable attributes in the RDP MBean.

Note Unless you are customizing the RDP application, the attributes in Table 7-2 are the only ones you should change. All other attributes affect the processing sequence of the RDP protocol handler. See the "Changing Installed Configuration Options" section on page 7-2 for more information.

Table 7-2 RDP—RDP MBean

Attribute Name	Explanation
handler	Defines the type of listener being configured. The value must be RDP to configure an RDP protocol handler.
dump	• true—Displays all RADIUS messages on the console (stderr) • false—Does not display messages Default: true

Table 7-2 RDP—RDP MBean (continued)

Attribute Name	Explanation

servicePassword
groupPassword
nextHopPassword
	RDP requires passwords to obtain service, group, and next hop profiles. The SSG sets the password in the request. Therefore, the values you configure here must match the values configured on the SSG, or, in the case of the groupPassword, in SESM configuration. If the configured password does not match the password in a profile, RDP returns an access-reject message.
	• servicePassword—Requests containing this password value are requests for a single service profile. RDP uses the SPE API to obtain a list of authorized services for a subscriber. This servicePassword must match the password configured on the SSG with the following command:
	`ssg service-password servicePassword`
	• groupPassword—Requests containing this password value are requests for a service group profile. RDP forwards requests to a RADIUS server to obtain a list of authorized services for the group of which the subscriber is a member. Group requests are relevant only when RDP is configured in proxy mode. The groupPassword value must match the password configured on the SESM portal in the serviceGroupPassword attribute in the AAA MBean.
	• nextHopPassword—Requests containing this password value are requests for a next hop table profile. RDP passes authentication requests to the AAAMBean when the RDP is configured in proxy mode, or through SPE to the directory when the RDP is not in proxy mode. On the SSG side, set this password using the following command:
	`ssg next-hop download nextHopTableName password`

Note The following attributes are in RDP MBean, RADIUSListener=RDP,component=Threadpool	
minThreads	Sets the minimum number of threads that this listener maintains during periods of low load. This listener always has system resources allocated for this number of threads. Default: 5
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 RDP MBean, RADIUSListener=RDP,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*

Table 7-2 RDP—RDP MBean (continued)

Attribute Name	Explanation
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 RDP—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 RDP. RDP clients are SSGs. 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 RDP. *localSecret* identifies the secret that this client uses for RADIUS communication If the client is an SSG, this value must match the shared secret configured on the SSG device: `radius-server key SharedSecret`
Note The following attributes are in RDP MBean, PROXY=ProxyHandler,component=RADIUSClientSocket. This component is used only when RDP is configured in Proxy mode.	
throttle	The maximum number of simultaneous requests that RDP can send to a RADIUS server. This is a RADIUS protocol attribute. The RADIUS protocol queues additional requests and issues them as the server returns responses or timeout messages for previous requests. Default: 256
timeOut	The number of seconds that RDP waits before timing out RADIUS packets that it sends to the AAA server. Default: 4000
maxRetries	The number of times RDP resends packets to the AAA server if no response is received. Default: 3
primaryIP	The IP address or the host name of the primary AAA server.
primaryPort	The port number that the primary RADIUS server listens on. Default: 1812
secret	The shared secret used between the RADIUS server and RDP. The shared secret must be the same for the primary and secondary servers. It must match the secret specified when you configured RDP as a NAS client on the RADIUS server. Default: `cisco`.

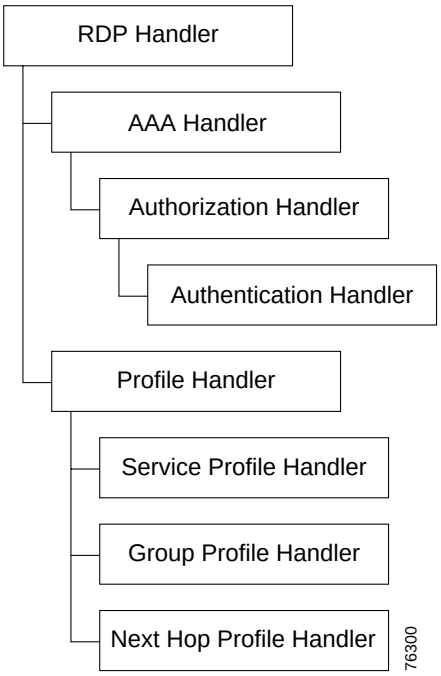
Table 7-2 RDP—RDP MBean (continued)

Attribute Name	Explanation
secondaryIP	The IP address or host name of the secondary AAA server. If you are not using a secondary RADIUS server, reenter the primary server.
secondaryPort	The port number that the secondary RADIUS server listens on. If you are not using a secondary server, reenter the primary server. Default: 1812

Summary of RDP Protocol Handlers

Figure 7-1 shows the processing sequence that RDP uses for handling packets.

Figure 7-1 RDP Handlers



Each protocol handler has a special purpose:

- RDP handler—Determines whether the request requires the AAA handler or Profile handler.
- AAA Handler—Coordinates handling of AVPairs, authorization, and authentication.
- Authorization Handler—Adds a service list to the ACCESS-ACCEPT response.
- Authentication Handler—Authenticates the request and adds other attributes to the response, including:
  - Adds extra AV pairs to the response. This includes firewall settings and any other AV pairs set in CDAT.
  - Generates IP pool names from primary services and adds the pool name.
  - Adds the home URL.

  - Adds TCP redirect attributes.
  - Adds idle timeout and session timeout attributes.

Note When RDP is running in Proxy mode, RDP performs all of the above authentication work using information in the profile obtained from a RADIUS server. If you are using Proxy mode, be sure to add these attributes to the subscriber profiles on the RADIUS server, as opposed to the ones on the LDAP server.

- Profile Handler—Handles profile requests and passes them on to the appropriate specific profile handler.
- Service Profile Handler—Handles a service profile request.
- Group Profile Handler—Handles a service group profile request.
- Next Hop Profile Handler—Handles a next hop table profile request.