CHAPTER 2

Using the Graphical User Interface

Cisco Prime Access Registrar (Prime Access Registrar) is a Remote Authentication Dial-In User Service (RADIUS) / Diameter server that enables multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

This chapter describes how to use the standalone graphical user interface (GUI) of Prime Access Registrar to:

- Configure Cisco Prime Access Registrar
- Manage Network Resources managed by Prime Access Registrar
- Administer Prime Access Registrar related activities

The following topics help you to work with and understand the Prime Access Registrar GUI:

- Launching the GUI
- Common Methodologies
- Dashboard
- Configuring Cisco Prime Access Registrar
- Network Resources
- Administration
- Read-Only GUI

Launching the GUI

Prime Access Registrar requires you to use Mozilla Firefox 88.0 or above, Google Chrome 90.0 or above and Microsoft Edge 90.0 or above. You start the GUI by pointing your browser to the Prime Access Registrar server and port 8080, as in the following:

http://*ar_server_name*:8080

Note It can be launched using IPv6 address also.

To start a secure socket layer (SSL) connection, use **https** to connect to the Prime Access Registrar server and port 8443, as in the following:

https://*ar_server_name*:8443

By default, both HTTP and HTTPS are enabled. The following sections describe how to disable HTTP and HTTPS:

- Disabling HTTP
- Disabling HTTPS

Note For proper function of Prime Access Registrar GUI, the DNS name resolution for the server's hostname should be defined precisely.

Disabling HTTP

To disable HTTP access, you must edit the **server.xml** file in the **/cisco-ar/apache-tomcat-9.0.44/conf** directory. You must have root privileges to edit this file.

Use a text editor such as **vi** to open the **server.xml** file, and comment out lines 96-99. Use the **<!--** character sequence to begin a comment. Use the **-->** character sequence to end a comment.

The following are lines 93-99 of the **server.xml** file:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
    <!-- CHANGE MADE: Note: to disable HTTP, comment out this Connector -->
<Connector port="8080" maxHttpHeaderSize="8192"
               maxThreads=”150 minSpare/Threads=”25” maxSpareThreads=”75”
               enableLookups="false" redirectPort="8443" acceptCount="100"
               connectionTimeout="20000" disableUploadTimeout="true" />
```

The following example shows these lines with beginning and ending comment sequences to disable HTTP:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
    <!-- CHANGE MADE: Note: to disable HTTP, comment out this Connector -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
               port="8080" minProcessors="5" maxProcessors="75"
               enableLookups="true" redirectPort="8443"
               acceptCount="10" debug="0" connectionTimeout="60000"/>
-->
```

After you modify the **server.xml** file, you must restart the Prime Access Registrar server for the changes to take effect. Use the following command line to restart the server:

/opt/CSCOar/bin/arserver restart

Disabling HTTPS

To disable HTTPS access, you must edit the **server.xml** file in the **/cisco-ar/apache-tomcat-9.0.44/conf** directory. You must have root privileges to edit this file.

Use a text editor such as **vi** to open the **server.xml** file, and comment out lines 116-121. Use the **<!--** character sequence to begin a comment. Use the **-->** character sequence to end a comment.

The following are lines 111-121 of the **server.xml** file:

```
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
    <!-- CHANGE MADE: enabled HTTPS.
```

```
        Note: to disable HTTPS, comment out this Connector -->
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads=”75”
               enableLookups="true" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="false"
               keystoreFile="/cisco-ar/certs/tomcat/server-cert.p12"
               keystorePass="cisco" keystoreType="PKCS12" sslProtocol="TLS" />
    </Connector>
```

The following example shows these lines with beginning and ending comment sequences to disable HTTPS.

```
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
    <!-- CHANGE MADE: enabled HTTPS.
        Note: to disable HTTPS, comment out this Connector -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
               port="8443" minProcessors="5" maxProcessors="75"
               enableLookups="true"
               acceptCount="10" debug="0" scheme="https" secure="true">
      <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
               keystoreFile="/cisco-ar/certs/tomcat/server-cert.p12"
               keystorePass="cisco" keystoreType="PKCS12"
               clientAuth="false" protocol="TLS"/>
    </Connector>
-->
```

After you modify the **server.xml** file, you must restart the Prime Access Registrar server for the changes to take effect. Use the following command line to restart the server:

```
/opt/CSCOar/bin/arserver  restart
```

Login Page

The login page has fields for a username and password. This page displays when you first attempt to log into the system, if a session times out, or after you log out of the system.

Logging In

Users who are configured as Administrators can log into the Prime Access Registrar server.

Note While logging in, do not enable the save password option in the browser.

Logging in

To log into the Prime Access Registrar GUI:

Step 1 Enter the relevant url in the browser. The Prime Access Registrar Login page is displayed.

Step 2 Enter the credentials in the provided fields.

Step 3 Click **Login**. The Prime Access Registrar main page is displayed.

Note After installation of Prime Access Registrar server, when you log into the application for the first time, the application redirects to the change password page.

Refreshing the pages using the GUI

To stop the server (when it is running), and then immediately start the server, click the **Reload** link.

Restarting the GUI

To restart the Prime Access Registrar server, click the **Restart** link.

Note If aregcmd interface is active, then it needs to be closed for restarting the Prime Access Registrar server.

Logging Out

To log out of the Prime Access Registrar GUI, click **Logout** in the upper right portion of the Prime Access Registrar GUI window.

Common Methodologies

This section explains the operations that are common across the GUI interface of Prime Access Registrar. The functions explained in this section are referred throughout to this help system.

This section describes the following:

- Filtering Records
- Deleting Records
- Setting Record Limits per Page
- Performing Common Navigations
- Relocating Records

Filtering Records

To filter a record:

Step 1 Navigate to the required page. For example, choose **Configuration** > **Profiles**. The Profile page is displayed.

Step 2 Enter the known details of the record in the **Filter** text box.

Step 3 Click **Go**. The matching records are displayed in the search criteria below.

Step 4 Click **Clear Filter** to clear the performed filter.

You can also perform the following:

- Deleting Records
- Editing Records
- Setting Record Limits per Page
- Performing Common Navigations
- Relocating Records

Editing Records

To edit the required records:

Step 1 Navigate to the required page.

Step 2 Search for a record using the filter option, if required.

Step 3 Choose the required record that you want to edit.

Step 4 Click **Edit**. The selected record details are displayed in the appropriate page.

Step 5 Make the necessary changes.

Step 6 Click **Submit** or **Update** to save the details. The page is displayed with the updated details and a message is prompted. Otherwise click **Cancel** to return to the page without saving the details.

You can also perform the following:

- Filtering Records
- Deleting Records
- Setting Record Limits per Page
- Performing Common Navigations
- Relocating Records

Deleting Records

To delete a record:

Step 1 Navigate to the required page. For example, choose **Configuration** > **Profiles**. The Profile page is displayed.

Step 2 Search for a record using the filter option, if required.

Step 3 Check the check box against the record that you want to delete.

Step 4 Click **Delete**. A message is displayed on successful deletion of the record.

You can also perform the following:

- Filtering Records
- Editing Records
- Setting Record Limits per Page
- Performing Common Navigations
- Relocating Records

Setting Record Limits per Page

To set the numbers of records to be displayed per page, select the record limit from the list available and click the **Go** button. The available denominations are **10**, **25**, **50**, **100**, and **All**.

You can also perform the following:

- Filtering Records
- Editing Records
- Deleting Records
- Performing Common Navigations
- Relocating Records

Performing Common Navigations

On existence of more records that cannot be accommodated in a page, the records are displayed in multiple pages. Table 2-1 describes the icons used for page navigation.

Table 2-1 Page Navigation Icons

Icons	Description
▶	To view the next page
◀	To return back to previous page
▶|	To view the last page
|◀	To return to the first page

You can also perform the following:

- Filtering Records
- Editing Records
- Deleting Records
- Setting Record Limits per Page
- Relocating Records

Relocating Records

Table 2-2 describes the icons used for relocating records.

Table 2-2 Icons for Relocating Records

Icons	Description
>	To move a record from the Available List to the Selected List
<	To move a record from the Selected List to the Available List
≫	To move all the records from the Available List to the Selected List
≪	To move all the records from the Selected List to the Available List
∧	To move the selected record one step above
∨	To move the selected record one step below
⤒	To move the selected record to the first position
⤓	To move the selected record to the last position

You can also perform the following:

- Filtering Records
- Editing Records
- Deleting Records
- Setting Record Limits per Page
- Performing Common Navigations

Dashboard

The dashboard of the Prime Access Registrar GUI shows you the overview on the status on the server and user session details. It consists of the three tabs: **Server Status**, **User Sessions**, and **System Information**.

The **Server Status** provides the following details:

- AAA Server status— includes the AAA Process, Process ID, and Status.
- Health status of the AAA Server— the status of the AAA Server with respect to the performance condition is displayed.

The **User Sessions** consists of two graphs.

- Number of Sessions versus Duration in Days
- Number of Sessions versus Duration in Weeks

The Number of Sessions vs Duration in Weeks report provides the session details with respect to the number of weeks for which it is queried. The Number of Sessions vs Duration in Days report provides the session details with respect to the number of days for which it is queried. The Time(mins) vs Username report provides the accumulated time with respect to the selected username. This report can also be viewed in the form of chart and grid. Click the relevant icons below the graph to view the details in the respective formats.

The **System Information** section consists of two graphs:

- Disk Availability for Prime Access Registrar Directory
- CPU Utilization

The Disk Availability for Prime Access Registrar Directory report provides the details of the available disk space and used disk space in the Prime Access Registrar directory. When you hover the mouse on the pie chart, the details of the disk space are displayed. The CPU Utilization report provides the utilization of the CPU for a specific time. The CPU usage is represented in kilobits per seconds.

Sessions

The Sessions feature of the dashboard helps you in viewing the records based on session id. Table 2-3 lists and describes the various session views in the page.

Table 2-3 Different Session Views

Fields	Description
Release	Click to release the selected session details.
Release All	Click to release all the records from the list.
Send CoA	Click to send the CoA packet to the client device.
SendPoD	Click to send the disconnect packet to the NAS to clear sessions and an Accounting-Stop notification to the client listed in the session record.
Query All Sessions	Click to query all the sessions in the server.

To view sessions details:

Step 1 Choose **Dashboard** > **Sessions**. The Sessions page appears.

Step 2 Choose the required session id to view **Release**, **Release All**, **Send CoA**, **Send PoD**, and **Query All Session** details. The session details are displayed as described in the above table.

Note You can locate the session id using the filter option. See Filtering Records for more details.

Configuring Cisco Prime Access Registrar

Prime Access Registrar's operation and configuration are based on a set of objects. On configuring the Prime Access Registrar major components, the server objects can be created. These objects include the following:

- RADIUS— the root of the configuration hierarchy
- Profiles—contains individual Profiles
- UserGroups—contains individual UserGroups
- UserList—contains individual UserLists which in turn contain users
- Users—contains individual authentication or authorization details of a user
- Scripts—contains individual Scripts
- Policies—contains a set of rules applied to an Access-Request
- GroupServers—contains Diameter remote server groups to enable group-based load balancing among Diameter peers
- Services—contains individual Services
- CommandSets—contains commands and the action to perform during Terminal Access Controller Access-Control System Plus (TACACS+) command authorization
- DeviceAccessRules—contains conditions or expressions and the applicable command sets for TACACS+ command authorization
- FastRules—provides a mechanism to easily choose the right authentication, authorization, accounting, and query service(s), drop, reject, or break flows, choose session manager or other rules required for processing a packet
- Replication—maintains identical configurations on multiple machines simultaneously
- RADIUSDictionary—passes information between a script and the RADIUS server, or between scripts running on a single packet
- VendorDictionary—allows to maintain the attributes of the vendor with respect to vendor id, vendor type and the attributes required to support the major NAS
- Vendor Attributes—communicates prepaid user balance information from the Prime Access Registrar server to the AAA client, and actual usage, either interim or total, between the NAS and the Prime Access Registrar server

- Vendors—contains individual Vendors
- Translations—adds new attributes to a packet or change an existing attribute from one value to another.
- TranslationGroups—add translation groups for different user groups
- SessionManagers—contains individual Session Managers
- ResourceManager—contains individual Resource Managers
- Remote Servers—contains individual Remote Servers
- Diameter—contains Session Management, Applications, Commands, Diameter Attributes
- Rules—allows to set rules for service selection

RADIUS

The **Radius** object is the root of the hierarchy. For each installation of the Cisco Prime Access Registrar server, there is one instance of the **Radius** object. You reach all other objects in the hierarchy from the **Radius**.

Table 2-4 lists and describes the fields in the Radius Properties page.

Note Fields which are represented with the term “required” in the windows of the Prime Access Registrar GUI, denote mandatory input.

Table 2-4 Radius Properties

Fields	Description
Name	Required; must be unique in the list of servers in the cluster.
Version	Required; the currently installed version of Prime Access Registrar.
Description	Optional; description of the server.
DefaultSessionManager	Cisco Prime Access Registrar uses this property if none of the incoming scripts sets the environment dictionary variable **Session-Manager**. This field is mandatory if you are upgrading to a later version of Prime Access Registrar.
IncomingScript	Optional; if there is a script, it is the first script Cisco Prime Access Registrar runs when it receives a request from any client and/or for any service.
OutgoingScript	Optional; if there is a script, it is the last script Cisco Prime Access Registrar runs before it sends a response to any client.
DefaultAuthenticationService	Optional; Cisco Prime Access Registrar uses this property when none of the incoming scripts sets the environment dictionary variable **Authentication-Service.**
DefaultAuthorizationService	Optional; Cisco Prime Access Registrar uses this property when none of the incoming scripts sets the environment dictionary variable **Authorization-Service.**

Table 2-4 Radius Properties (continued)

Fields	Description
DefaultAccountingService	Optional; Cisco Prime Access Registrar uses this property when none of the incoming scripts sets the environment dictionary variable **Accounting-Service.**
DefaultSessionService	Cisco Prime Access Registrar uses this property when none of the incoming scripts sets the environment dictionary variable **Session-Service**. This field is mandatory if you are upgrading to a later version of Prime Access Registrar.

Setting Up or Changing the Radius Properties

To set or change the Radius properties:

Step 1 Choose **Configuration** > **Radius**. The Radius Properties page appears.

Step 2 Specify the relevant details.

Step 3 Click **Save** to save the changes made to the Radius properties page.

On successful setting up of the RADIUS, a message is displayed.

Profiles

You use Profiles to group RADIUS attributes that belong together, such as attributes that are appropriate for a particular class of PPP or Telnet user. You can reference profiles by name from either the **UserGroup** or the **User** properties. Thus, if the specifications of a particular profile change, you can make the change in a single place and have it propagated throughout your user community.

Although you can use UserGroups or Profiles in a similar manner, choosing whether to use one rather than the other depends on your site. When you require some choice in determining how to authorize or authenticate a user session, then creating specific profiles, and creating a group that uses a script to choose among them is more flexible.

In such a situation, you might create a default group, and then write a script that selects the appropriate profile based on the specific request. The benefit to this technique is each user can have a single entry, and use the appropriate profile depending on the way they log in.

Table 2-5 lists and describes the fields in the Add Profiles page.

Table 2-5 Profile Properties

Fields	Description
Name	Required; must be unique in the Profiles list.
Description	Optional; description of the profile.
RADIUS	Optional; set Radius, if the attribute and value need to be defined for RADIUS.

Table 2-5 Profile Properties (continued)

Fields	Description
VENDOR	Optional; set Vendor, if the attribute and value need to be defined for Vendor.
DIAMETER	Optional; set Diameter, if the attribute and value need to be defined for Diameter.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
Value Attribute	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Radius and Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the Profiles page for the following:

- Filtering Records
- Adding Profile Details
- Editing Records
- Deleting Records

Adding Profile Details

To add new profile details:

Step 1 Choose **Configuration** > **Profiles**. The Profiles page is displayed.

Step 2 Click **Add**. The Add Profile page is displayed.

Step 3 Specify the required details.

Step 4 Click **Submit** to save the specified details in the Profiles page. Otherwise click **Cancel** to return to the Profiles page without saving the details. On successful creation of the profiles, the Profiles page is displayed else a respective error message is displayed.

UserGroups

The **UserGroups** objects allow you to maintain common authentication and authorization attributes in one location, and then have many users reference them. By having a central location for attributes, you can make modifications in one place instead of having to make individual changes throughout your user community.

For example, you can use several **UserGroups** to separate users by the services they use, such as a group specifying PPP and another for Telnet.

Table 2-6 lists and describes the fields in the Add User Groups page.

Table 2-6 UserGroups Properties

Fields	Description
General Properties tab	
UserGroup Name	Required; must be unique in the **UserGroup** list.
Description	Optional; description of the group.
BaseProfile	Optional; when you set this to the name of a profile, Cisco Prime Access Registrar adds the properties in the Profile to the response dictionary as part of the authorization.
AuthenticationScript	Optional; when you set this property to the name of a script, you can use the Script to perform additional authentication checks to determine whether to accept or reject the user.
AuthorizationScript	Optional; when you set this property to the name of a script, you can use the script to add, delete, or modify the attributes of the Response dictionary.
Attribute List tab	
RADIUS	Optional; set Radius, if the attribute and value need to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute and value need to be defined for Vendor.
DIAMETER	Optional; set Diameter, if the attribute and value need to be defined for Diameter.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
Attribute Value	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Name and Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
CheckItems List tab	
RADIUS	Optional; set Radius, if the attribute and value need to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute and value need to be defined for Vendor.
DIAMETER	Optional; set Diameter, if the attribute and value need to be defined for Diameter.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
Attribute Value	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Check Name and Check Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the User Groups page for the following:

- Filtering Records
- Adding UserGroup Details
- Editing Records
- Deleting Records

Adding UserGroup Details

To add new user groups details:

Step 1 Choose **Configuration** > **UserGroups**. The User Groups page is displayed.

Step 2 Click **Add** to add new user group details. The Add UserGroup page is displayed.

Step 3 Specify the required details.

Step 4 Click **Submit** to save the specified details in the User Groups page. Otherwise click **Cancel** to return to the User Groups page without saving the details.

On successful creation of the user groups, the User Groups page is displayed else a respective error message is displayed.

UserList

The UserLists object contains all of the individual UserLists, which in turn, contain the specific users stored within Prime Access Registrar. Prime Access Registrar references each specific UserList by name from a Service whose type is set to local. When Prime Access Registrar receives a request, it directs it to a Service. When the Service has its type property set to local, the Service looks up the user's entry in the specific UserList and authenticates and/or authorizes the user against that entry.

You can have more than one UserList in the UserLists object. Therefore, use the UserLists object to divide your user community by organization. For example, you might have separate UserLists objects for Company A and B, or you might have separate UserLists objects for different departments within a company.

Using separate UserLists objects allows you to have the same name in different lists. For example, if your company has three people named Bob and they work in different departments, you could create a UserList for each department, and each Bob could use his own name. Using UserLists lets you avoid the problem of Bob1, Bob2, and so on.

If you have more than one UserList, Prime Access Registrar can run a script in response to requests. The script chooses the Service, and the Service specifies the actual UserList which contains the user. The alternative is dynamic properties.

Note The attributes defined for a user list must match the protocol of the incoming packet. For example, if the incoming packet is a Diameter packet, the attributes defined must be specific to Diameter or common to both RADIUS and Diameter. Similarly, if the incoming packet is a RADIUS packet, the attributes defined must be specific to RADIUS or common to both RADIUS and Diameter. Otherwise, the incoming packet will not be processed.

Table 2-7 lists and describes the fields in the Add User List page.

Table 2-7 User List Properties

Fields	Description
UserList Name	Required; must be unique.
Description	Optional; description of the user list.

You can use the User List page for the following:

- Filtering Records
- Adding UserList Details
- Editing Records
- Deleting Records

Adding UserList Details

To add new user list details:

Step 1 Choose **Configuration** > **UserList**. The User List page is displayed.

Step 2 Click **Add** to add new user list details. The Add UserList page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the User List page. Otherwise click **Cancel** to return to the User List page without saving the details.

On successful creation of the user list, the User List page is displayed else a respective error message is displayed.

Note After adding a new user list, you can add users to the user list. See Adding User Details for more information.

Users

The user objects are created to hold the necessary details to authenticate or authorize a user. These users form the component of User Lists, where their details are stored within Prime Access Registrar. The users in local Userlist can have multiple profiles.

Note Usernames might not include the forward slash (/) character. If the Prime Access Registrar server receives an access request packet with a Username attribute containing a forward slash character and the Prime Access Registrar server uses an internal UserList to look up users, the server produces an error (AX_EINVAL) and might fail. If usernames require a forward slash, use a script to translate the slash to an acceptable, unused character.

Table 2-8 lists and describes the fields in the Add Users page.

Table 2-8 Users Properties

Fields	Description
General Properties tab	
Name	Required; must be unique.
Enabled	Required; must be checked to allow user access. If Enabled is not checked, user is denied access.
Allow Null Pwd	During authentication, if the Allow NULL Password environment variable is set to TRUE, user authentication is bypassed. By default, the Allow NULL Password environment variable is not set.
UserGroup	Use the drop-down list to select a UserGroup and use the properties specified in the UserGroup to authenticate and/or authorize the user. The default is none.
Password	Required; length must be between 0-253 characters.
Base Profile	Optional; use the drop-down list to select a Profile. If the service-type is not equal to Authenticate Only, Prime Access Registrar adds the properties in the Profile to the Response dictionary as part of the authorization. This field is optional for the CLI, but required for the GUI. Use the menu to select a profile other than the default None.
Confirm Password	Required; must match password.
User Defined	Optional; you can use this property to store notational information which you can then use to filter the UserList. This property also sets the environment variable for UserDefined.
Authentication Script	Optional; use the drop-down list to select the name of a script to perform additional authentication checks to determine whether to accept or reject the user. This field is optional for the CLI, but required for the GUI. Use the menu to select an Authentication Script other than the default None.
Authorization Script	Optional; use the drop-down list to select the name of a script to add, delete, or modify the attributes of the Response dictionary. This field is optional for the CLI, but required for the GUI. Use the menu to select an Authorization Script other than the default None.
Description	Optional; description of the user.
Attribute List tab	

Table 2-8 Users Properties (continued)

Fields	Description
RADIUS	Optional; set Radius, if the attribute and value need to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute and value need to be defined for Vendor.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
Attribute Value	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Name and Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
CheckItems List tab	
RADIUS	Optional; set Radius, if the attribute and value need to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute and value need to be defined for Vendor.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
Attribute Value	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Check Name and Check Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the Users page for the following:

- Filtering Records
- Adding User Details
- Editing Records
- Deleting Records

Adding User Details

To add new user details:

Step 1 Choose **Configuration** > **UserList**. The User List page is displayed.

Step 2 Click the user list name link. The Users page is displayed.

Step 3 Click **Add** to add new user details. The Add Users page is displayed.

Step 4 Specify the required details.

Step 5 Click **Submit** to save the specified details in the Users page. Otherwise click **Cancel** to return to the Users page without saving the details.

On successful creation of the user details, the Users page is displayed else a respective error message is displayed.

Scripts

The **Script** objects define the function Cisco Prime Access Registrar invokes whenever the **Script** is referenced by name from other objects in the configuration.

There are four types of scripts:

- REX (RADIUS EXtension) scripts are written in C or C++, and thus are compiled functions that reside in shared libraries
- TCL scripts are written in TCL, and are interpreted functions defined in source files.
- Java scripts
- Internal scripts, which allow you to add, modify, or delete attributes in the request, response, and environment dictionaries for RADIUS, Diameter, and TACACS+. For more information about internal scripts, see the "Using Extension Points" chapter of the *Cisco Prime Access Registrar 9.2 Administrator Guide*.

When you use a Prime Access Registrar file service, Prime Access Registrar automatically closes any opened files. However, if you write scripts that manipulate files, you are responsible for closing them.

If you have more than one extension point script (defined under **/Radius/Scripts**) using the same Java class, only one instance of the class is created and used for all the extension point scripts.

For more information about scripts, see the "Using Extension Points" chapter of the *Cisco Prime Access Registrar 9.2 Administrator Guide*.

Table 2-9 lists and describes the fields in the Add Scripts page.

Table 2-9 Script Object Properties

Fields	Description
Script Name	Required; must be unique in the Scripts list.
Language	Required; specify either REX, TCL, Java, or Internal.
Description	Optional; description of the script.
File/Class Name	Required; specifies either a relative or absolute path. When you specify a relative path, the path must be relative to the **$INSTALL/scripts/radius/$Language** directory. When you specify an absolute path, the server must be able to reach it. For Java language scripts, the name of the class that implements the extension interface; the **.class** file should be placed in **/cisco-ar/scripts/radius/java**
Entry Point	Required; when not set, Prime Access Registrar uses the value specified in the **Name** property.
Init Entry Point	Optional; if set, it must be the name of the global symbol Prime Access Registrar should call when it initializes the shared library at system start up, and just before it unloads the shared library.

Table 2-9 Script Object Properties (continued)

Fields	Description
Init Entry Point Arg	Optional; when set, it provides the arguments to be passed to the **InitEntryPoint** in the environmental variable **Arguments**. **Note** The **InitEntryPoint** properties allow you to perform initialization before processing and then cleanup before stopping the server. For example, when Prime Access Registrar unloads the script (when it stops the RADIUS server) it calls the **InitEntryPoint** again to allow it to perform any clean-up operations as a result of its initialization. One use of the function might be to allow the script to close an open Accounting log file before stopping the RADIUS server.
The following fields appear if the language is set as **Internal**	
Protocol	Required; select RADIUS or Diameter to indicate the protocol for which the attributes are to be modified.
ActionStatements	Select one of following the options: • Simple Attribute Operation—allows you to add, modify, or delete an attribute value to the request, response, or environment dictionary • Copy an Attribute—allows you to copy an attribute value from one dictionary to another • Concatenate Operation—allows you to concatenate an attribute value from one dictionary to another • Replace Operation—allows you to replace an attribute value from one dictionary to another • Value Based Manipulations—allows you to manipulate attribute values in a dictionary based on a given text • Log or Trace Messages—allows you to create different levels of log or trace messages • I can do it myself—allows you to create your own script for the selected protocol
Left Side of Statement	
Operation	Choose the operation to perform as **Add**, **Modify**, or **Delete**.
Dictionary	Choose **Request**, **Response**, or **Environment** to specify the RADIUS dictionary to apply the action to.
Attr Type	Applicable for RADIUS protocol; select **RADIUS** or **VENDOR** to indicate the attribute type.
Group AVP	Applicable for Diameter protocol; select the group AVP and its level to apply the action to.
Attribute	Based on the attribute type/group AVP selected, choose the appropriate attribute to apply the action to.
Env Attribute	Enter the environment attribute to apply the action to. This field is available only if the Dictionary chosen is **Environment**.
Right Side of Statement	

Table 2-9 Script Object Properties (continued)

Fields	Description
Text	Enter the text that needs to be added, modified, or deleted to/from the given attribute in the selected dictionary. Only this field is available if the action statement is **Simple Attribute Operation** or **Replacement Operation**. This field is also available under the following circumstances: • If the action statement is **Copy an Attribute, Concatenate Operation,** or **Value Based Manipulations**, and if the type is chosen as **Custom Text**
Type	Select **Radius, Diameter,** or **Custom Text**.
Dictionary	If the type is set as Radius or Diameter, choose **Request**, **Response**, or **Environment** to specify the dictionary to apply the action to.
Attr Type	Applicable for RADIUS protocol; select **RADIUS** or **VENDOR** to indicate the attribute type.
Group AVP	Applicable for Diameter protocol; select the group AVP and its level to apply the action to.
Attribute	Based on the attribute type/group AVP selected, choose the appropriate attribute to apply the action to.
Env Attribute	Enter the environment attribute to apply the action to. This field is available only if the Dictionary chosen is **Environment**.
Concatenate / Replace Options	
This section is available if the Action Statements field is set to **Concatenate Operation** or **Replace Operation**.	
Type	Select **Radius**, **Diameter**, or **Custom Text**.
Text	Enter the text to concatenate to or replace the given attribute value in the selected dictionary. Only this field is available if the action statement is **Replace Operation**. This field is also available if the action statement is **Concatenate Operation** and if the type is chosen as **Custom Text**
Dictionary	If the type is Radius, choose **Request**, **Response**, or **Environment** to specify the RADIUS dictionary to apply the action to.
Attr Type	Applicable for RADIUS protocol; select **RADIUS** or **VENDOR** to indicate the attribute type.
Group AVP	Applicable for Diameter protocol; select the group AVP and its level to apply the action to.
Attribute	Based on the attribute type/group AVP selected, choose the appropriate attribute to apply the action to.
Env Attribute	Enter the environment attribute to apply the action to. This field is available only if the Dictionary chosen is **Environment.**
Text Manipulations	
This section is available if the Action Statements field is set to **Value Based Manipulations**.	

Table 2-9 Script Object Properties (continued)

Fields	Description
Operation	Select one of the following options: • Begins With—to manipulate the attribute value beginning with the given text • Contains—to manipulate the attribute value that contains the given text • Ends With—to manipulate the attribute value that ends with the given text • Strip Text—to strip the given text from the attribute value
Text	The text you need to manipulate the attribute value with.
This following fields are available if the Action Statements field is set to **Log or Trace Messages**.	
Log Type	Select one of the following options: • log—to add a log message • trace—to add a trace message
Level	Applicable only for logs; level of the log message to add.
Message	The log or trace message to add.
This following field is available if the Action Statements field is set to **I can do it myself**.	
Statement	Enter the action statement as a free text.

You can use the Scripts page for the following:

- Filtering Records
- Adding Script Details
- Editing Records
- Deleting Records

Adding Script Details

To add new script details:

Step 1 Choose **Configuration** > **Scripts**. The Scripts page is displayed.

Step 2 Click **Add** to add new scripts details. The Script Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Save** to save the specified details in the Scripts page. Otherwise click **Cancel** to return to the Scripts page without saving the details.

On successful creation of the scripts, the Scripts page is displayed else a respective error message is displayed.

Policies

A Policy is a set of rules applied to an Access-Request.

Table 2-10 lists and describes the fields in the Add Policies page.

Table 2-10 Policies Properties

Fields	Description
Name	Required; must be unique in the **Policies** list
Description	Optional; description of the Policy
Rules/Policies	Required; set the rules/polices to be grouped.
Operators	Required; set the operators to be grouped along with selected rules/policies. The selected rules and operators will be grouped and listed in the Grouping Box. To delete the available groups, select the relevant group from the Grouping list and click the **Delete** button below.
Grouping	Optional; grouping of rules.

You can use the Policies page for the following:

- Filtering Records
- Adding Policy Details
- Editing Records
- Deleting Records

Adding Policy Details

To add new policy details:

Step 1 Choose **Configuration** > **Policies**. The Policies page is displayed.

Step 2 Click **Add** to add new policy details. The Policy Details page is displayed.

Step 3 Specify the required details.

Step 4 Click **Submit** to save the specified details in the Policies page. Otherwise click **Cancel** to return to the Policies page without saving the details.

On successful creation of the policies, the Policies page is displayed else a respective error message is displayed.

GroupServers

Prime Access Registrar allows group-based load balancing among Diameter peers.

Group-Based Load Balancing

Using this option you can create two or more groups of Diameter remote servers. Each of these groups will have a unique set of remote servers, i.e. no two groups will share the same remote server.

The traffic between each of these groups is load-balanced in failover mode; while traffic between remote servers within the same group is load-balanced based on round-robin or failover mode depending on the Diameter group server properties. The priority of each of the groups is set with the help of metrics.

The workflow for group-based load balancing is as given below:

1. Traffic from Prime Access Registrar to a remote server, via Diameter proxy service, is directed through the first group, till Prime Access Registrar has active communication channel with at least one remote server belonging to the first group.
2. When Prime Access Registrar loses connectivity with all the remote servers in the first group, it directs the rest of the Diameter traffic towards remote servers belonging to the second group.

Table 2-11 Diameter GroupServer Properties

Fields	Description
General Properties tab	
Name	Required; name of the group server.
MultiplePeersPolicy	Required; Policy used by the Prime Access Registrar server to load balance the peers within the group. This could be one of the following: • FailOver—Traffic is directed towards first priority remote server within the group. When Prime Access Registrar loses connectivity with the first priority remote server, it directs the subsequent traffic towards the second priority remote server within the group. • RoundRobin—Traffic is distributed across all the active remote servers within the group.
GroupTimeOutPolicy	Required; action to perform when there is a timeout with the group server. This could be FailOver, DropPacket, or SendError.
DiameterRemoteServersList List of Diameter remote servers to add to the group.	
Name	Required; name of the peer.
Metric	Required; metric value for this peer entry. The higher the value the lower the preference. The highest value of preference is 0.
Weight	Required; default value is 0. Specifies the weight percentage for which the server group needs to load balance the peer. **Note** When you set the weight to a value other than 0, the weight should be in multiples of 10 and the sum of the weights configured in the peer list should be equal to 100.
IsActive	Optional; if this is checked, the new sessions will not go to the peer server. By default, this is unchecked.

You can use the GroupServers page for the following:

- Filtering Records
- Adding Group Server Details
- Editing Records

- Deleting Records

Adding Group Server Details

To add new group servers:

Step 1 Choose **Configuration** > **GroupServers**. The GroupServers page is displayed.

Step 2 Click **Add** to add new group server details. The Group Servers page is displayed.

Step 3 Specify the required details.

Step 4 Click **Save GroupServer** to save the specified details in the Group Servers page. Otherwise click **Cancel** to return to the GroupServers page without saving the details.

On successful creation of the group server, the GroupServers page is displayed else a respective error message is displayed.

Services

Cisco Prime Access Registrar supports authentication, authorization, and accounting (AAA) services. In addition to the variety of built-in AAA services (specified in the **Type** property),
Cisco Prime Access Registrar also enables you to add new AAA services through custom shared libraries.

This section lists the types of services available in Prime Access Registrar with their required and optional properties. The service you specify determines what additional information you must provide. The various types of services are:

- Simple Services
- ServiceWithRS
- PEAP Service
- EAP Service
- Diameter Service

Simple Services

Prime Access Registrar provides the following simple services:

- Rex
- File
- Trusted-ID
- Group
- Local
- Java
- WiMAX

- RADIUS-Query
- Dyn-Authz
- Diameter-RADIUS
- RADIUS-Diameter
- Diameter-Query
- 3GPPAuthorization
- 3GPP-Reverse-Authorization

Rex

Select rex service when a custom service needs to be created and a script for authentication, authorization, or accounting has to be used.

File

Select File type when local accounting is to be performed using a specific file. The files under the configuration will be saved in the configured name when the server is invoked even if the service is not being invoked by any request packets.

Prime Access Registrar flushes the accounting record to disk before it acknowledges the request packets. Based on the specified maximum file size and age, it closes the accounting file, moves it to a new name, and reopens the file as a new file. The file names are based on its creation and modification dates.

Trusted-ID

Select the trusted-id service type to authorize and authenticate a user based on a Trusted ID. Using SSG's Transparent Auto-Login (TAL) feature, a TAL access-request packet contains a Trusted ID, such as a MAC address, that identifies the user without the user's real username and password. If Prime Access Registrar knows the user associated with the Trusted ID, it uses the Trusted ID to authenticate and authorize the user. For more information, see the “Using Trusted ID Authorization with SESM” chapter of the *Cisco Prime Access Registrar 9.2 Administrator Guide*.

Group

A group service contains a list of references to other services and specifies whether the responses from each of the services should be handled as a logical AND or OR function, which is specified in the Result-Rule attribute of Group Services. The default value is AND.

When the Result-Rule attribute is set to AND or OR, each referenced service is accessed sequentially, and the Group Service waits for a response from the first referenced service before moving on to the next service (if necessary).

The ResultRule settings parallel-and and parallel-or are similar to the AND and OR settings except that they ask each referenced service to process the request simultaneously instead of asking each referenced server sequentially, thereby saving processing time.

Local

Select local services when authentication and authorization needs to be performed by Prime Access Registrar server using a specific UserList.

Java

Select Java service type when a custom service needs to be created and to use an extension point script to provide the service's functionality and handle both RADIUS and TACACS requests for authentication, authorization, or accounting.

WiMAX

Prime Access Registrar uses the Extensible Authentication Protocol (EAP) to enable the WiMAX feature. It captures the IP attributes and Mobility Keys that are generated during network access authentication.

RADIUS-Query

Select this service type to query cached data through RADIUS Packets. It contains the list of session managers to be queried from and a list of (cached) attributes to be returned in the Access-Accept packet in response to a RADIUS Query request. It is initiated through an extension point script or through the Rule and Policy Engine by setting it to a new environment variable named Query-Service.

Dyn-Authz

Select this service type to process dynamic authorization requests. This involves Change of Authorization (COA) and Packet of Disconnect (POD) features. For more information about these features, see Chapter 9, "Using Cisco Prime Access Registrar Server Features."

Diameter-RADIUS

Select this service for Diameter to RADIUS translation to translate incoming Diameter request to a RADIUS equivalent and then the RADIUS response to Diameter equivalent. Prime Access Registrar provides scripting points, which operate on the original packet and on the newly translated packet based on request and response mapping. For more information, see *Chapter 4, "Diameter."*

RADIUS-Diameter

Select this service for RADIUS to Diameter translation to translate incoming RADIUS request to a Diameter equivalent and then the Diameter response to RADIUS equivalent. Prime Access Registrar provides scripting points, which operate on the original packet and on the newly translated packet based on request and response mapping. For more information, see *Chapter 4, "Diameter."*

Diameter-Query

Select this service type to query cached data through Diameter Packets. It contains the list of session managers to be queried from and a list of (cached) attributes to be returned in the Access-Accept packet in response to a Diameter Query request. It is initiated through an extension point script or through the Rule and Policy Engine by setting it to a new environment variable named Query-Service.

3GPPAuthorization

Select this service to enable 3GPP authorization of subscribers. For more information about 3GPP authorization, see the "Wireless Support" chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*.

3GPP-Reverse-Authorization

Select this service to enable 3GPP reverse authorization of subscribers. For more information about 3GPP reverse authorization, see the "Wireless Support" chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*.

Table 2-12 lists and describes the fields in the Services Details page. The fields listed below are the entire list of all the available types. The fields are displayed based on the type selected.

Table 2-12 Simple Service Properties

Fields	Description
Service Name	Required; must be unique in the Services list.
Incoming Script	Optional; name of script to run when the service starts.
Type	Required; must set it to a valid Prime Access Registrar service.
Outgoing Script	Name of script to run when the service ends.
Description	Optional; description of the service.
Outage Script	Optional; if you set this property to the name of a script, Cisco Prime Access Registrar runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
Outage Policy	Required; the default is **DropPacket**. This property defines how Cisco Prime Access Registrar handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
The following properties appear for the job type **rex**.	
Filename	Required; must be either a relative or an absolute path to the shared library containing the Service. When the pathname is relative, it must be relative to **$INSTALL/Scripts/Radius/rex**.
EntryPoint	Required; must be set to the function's global symbol.
InitEntryPoint	Required; must be the name of the global symbol Cisco Prime Access Registrar should call when it initializes the shared library and just before it unloads the shared library. A rex service must have an InitEntryPoint even if the service only returns REX_OK.
InitEntryPointArgs	Optional; when set, it provides the arguments to be passed to the **InitEntryPoint** in the environmental variable **Arguments**.
The following properties appear for the job type **file**.	
FilenamePrefix	Required; a string that specifies where Cisco Prime Access Registrar writes the account records. It must be either a relative or absolute path. When you specify a relative path, it must be relative to the **$INSTALL/logs** directory. When you specify an absolute path, the server must be able to reach it. The default is **Accounting**.

Table 2-12 Simple Service Properties (continued)

Fields	Description
MaxFileAge	Optional; stored as a string, but is composed of two parts, a number and a units indicator (<*n*> <*units*>) in which the unit is one of: H, Hour, Hours, D, Day, Days, W, Week, Weeks. The default is one day.
RolloverSchedule	Indicates the exact time including the day of the month or day of the week, hour and minute to roll over the accounting log file.
MaxFileSize	Optional; stored as a string, but is composed of two parts, a number and a units indicator (<n> <units>) in which the unit is one of: K, kilobyte, or kilobytes, M, megabyte, or megabytes, or G, gigabyte, or gigabytes. The default is ten megabytes.
UseLocalTimeZone	When set to TRUE, indicates the accounting records' TimeStamp is in local time. When set to FALSE, the default, accounting records' TimeStamp is in GMT.
FileType	Choose **log** or **csv** to indicate the file type to export the accounting records to. If you choose **log**, the Prime Access Registrar server writes accounting messages to the **accounting.log** file in the **/opt/CSCOar/logs** directory. If you choose **csv**, the Prime Access Registrar server writes accounting messages to the **accounting.csv** file in the **/opt/CSCOar/logs** directory.
EnableRollOverIntelligence	Check the box to enable rollover intelligence for the accounting records based on the accounting service properties. For more information, see Rolling Encryption Support for Pseudonym Generation in EAP-SIM, EAP-AKA, and EAP-AKA' Services, page 5-50.
AttributesToBeLogged	The selected list of attributes that must be logged. If the list is empty, the accounting file service logs all the attributes of the packet.
Delimiter	The delimiter to use in the accounting file. This field is available if you set the FileType as **csv**. Delimiters could be ';', ',', and ':' and default value is ','.
The following properties appear for the job type **trusted-id**.	
UserService	Required; name of service that can be used to authenticate.
SessionManager	Required; select the required session manager from the available list.
The following properties appear for the job type **group**.	
Result Rule	When set to AND (the default), the response from the GroupService is positive if each of the services referenced return a positive result. The response is negative if any of the services reference return a negative result. When set to OR, the response from the GroupService is positive if any of the services referenced return a positive result. The response is negative if all the referenced services return a negative result. The settings parallel-AND or parallel-OR are similar to AND and OR settings, except that each referenced service processes requests simultaneously instead of asking each reference service sequentially to save processing time.

Table 2-12 Simple Service Properties (continued)

Fields	Description
GroupServices	Optional; use the GroupServices subdirectory to specify the subservices in an indexed list to provide specific ordering control of which services to apply first. Each subservice listed must be defined in the Services section of the RADIUS configuration and cannot be a of type *g*roup, eap-leap, or eap-md5. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
The following properties appear for the job type **local**.	
UserList	Required; this object contains all of the individual UserLists, which in turn, contain the specific users stored within Prime Access Registrar. Cisco Prime Access Registrar references each specific UserList by **name** from a Service whose type is set to **local**. When Cisco Prime Access Registrar receives a request, it directs it to a Service. When the Service has its type property set to **local**, the Service looks up the user's entry in the specific UserList and authenticates and/or authorizes the user against that entry.
Enable Device Access	Check the box to enable TACACS+ command authorization. **Note** Device Access Rules are applicable for TACACS+ command authorization. For more information, see TACACS+ Support for AAA, page 9-66.
Device Access Rule	Select a device access rule and click **Add**. The selected access rule is displayed in the Device Access Rules list box.
Default Device Access Action	Select the default action to perform on the commands for all the access rules in the authorization service. Options are **PermitAll** and **DenyAll**.
The following properties appear for the job type **java**.	
Class name	Optional; set to the name of a class that implements the Extension interface.
InitializeArg	Optional; set to a string to be passed to the Initialize method if the class implements the optional ExtensionWithInitialization interface.
The following properties appear for the job type **wimax**.	
HARKKey	Required; used as the base key to generate random HARKKey for all the HAs that are configured in Prime Access Registrar. By default, the value is `cisco112`.You can change this value.
WimaxAuthenticationService	Required; a valid EAP service which can be used for WiMAX authentication. By default, this value is none.
HARKLifeTime	Required; used as time (in minutes) to regenerate the HARKKeys based on its lifetime.
WimaxSessionManager	Required; set a valid session manager which has HA and HA Cache as resource managers. By default, this value is none.
WimaxQueryService	Required; set a valid RADIUS query service which is configured with WiMAX session manager. By default, this value is none.
WimaxPrepaidService	Optional; set a valid prepaid service to carry out the prepaid functionality of WiMAX. Otherwise this value is set to none.

Table 2-12 Simple Service Properties (continued)

Fields	Description
AllowAAAToIncludeKeys	Optional; If this is set, the HAAA will include the hHA-RK-Key, hHA-RK-SPI and hHA-RK-Lifetime in the Access-Accept. Otherwise, those attributes will not be in the Access-Accept. By default this value is True.
RequiredMSK	Optional; If this is set, the MSK will be provided by the AAA server as a result of successful EAP-Authentication. By default, this value is False.
The following properties appear for the job type **radius-query**.	
Attribute List tab	
Attribute type	Select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list. Select the attributes from the available list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
Session Manager tab	
Session Manager	Select the required session manager from the available list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
The following property appears for the job type **dyn-auth**.	
Session Cache Query Service	Select the session cache query service to use for dynamic authorization.
The following properties appear for the job type **diameter-radius** or **radius-diameter**.	
ProxyServiceName	Select the Diameter proxy service name.
DiameterApplicationID	Select the Diameter service application ID. This field appears only for radius-diameter service type.
EnableRequestCommandMappings	Check this box to enable command mapping.
SendRAR-ASRToClient	Check the box if the COA/POD packets received by Prime Access Registrar are to be translated and sent as Re-Auth-Request (RAR) / Abort Session Request (ASR) to a Diameter client. This field appears only for radius-diameter service type.
ClientHostName	Hostname of the Diameter client to which the translated RAR/ASR must be sent. If the session manager is configured, the client host name can be acquired from it using the Session-Manager AVP. This field appears only for radius-diameter service type.
UseFor3GPPReverseAuthorizationService	Check the box to enable 3GPP authorization service in the translation framework. This field appears only for radius-diameter service type.
PreRequestTranslationScript	Select the scripting point to be called on the original request packet.
PostRequestTranslation Script	Select the scripting point to be called on the translated request packet.
PreResponseTranslation Script	Select the scripting point to be called on the response packet.

Table 2-12 Simple Service Properties (continued)

Fields	Description
PostResponseTranslationScript	Select the scripting point to be called on the translated response packet.
CommandMappings	This tab allows you to map commands.
ResultCodeMappings	This tab allows you to map result codes.
RequestAVPMappings	This tab allows you to map request AVPs.
RequestAVPsToBeAdded	This tab allows you to map request AVPs to be added.
RequestEnvironmentMappings	This tab allows you to map request environment variables.
ResponseAVPMappings	This tab allows you to map response AVPs.
ResponseAVPsToBeAdded	This tab allows you to map response AVPs to be added.
ResponseEnvironmentMappings	This tab allows you to map response environment variables.
The following properties appear for the job type **diameter-query**.	
UpdateSessionLastAccessTime	Check the box to update the timestamp when the Diameter session was last accessed or called.
Attribute List tab	
Attribute type	Select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list. Select the attributes from the available list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
Session Manager tab	
Session Manager	Select the required session manager from the available list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
The following property appears for the job type **3gpp-authorization**.	
Protocol	Required; select RADIUS or Diameter to indicate the protocol to use for 3GPP authorization.
FetchLocationInformation	Check the box to fetch location related information of the RADIUS/Diameter client for the 3GPP authorization service. Prime Access Registrar allows or blocks access of a subscriber to voice over Wi-Fi (VoWiFi) based on the location information. For more details on voice over Wi-Fi (VoWiFi) location-based authentication, see the "Wireless Support" chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*
TranslationService	Required if the protocol selected is RADIUS; translation service to use during 3GPP authorization.
DiameterProxyService	Required if the protocol selected in Diameter; diameter proxy service to use during 3GPP authorization.
The following properties appear for the job type **3gpp-reverse-authorization**.	
TranslationService	Required; the translation service to use for 3GPP reverse authorization.

You can use the Simple Services List page for the following:

- Filtering Records
- Adding Simple Service Details
- Editing Records
- Deleting Records

Adding Simple Service Details

To add new simple service details:

Step 1 Choose **Configuration > Services > Simple**. The Services List(REX, FILE, LOCAL, GROUP, JAVA...) page is displayed.

Step 2 Click **Add** to add new simple service details. The Services Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the Services List(REX, FILE, LOCAL, GROUP, JAVA...) page. Otherwise click **Cancel** to return to the Services List(REX, FILE, LOCAL, GROUP, JAVA...) page without saving the details.

On successful creation of the simple service properties, the Services List(REX, FILE, LOCAL, GROUP, JAVA...) page is displayed else a respective error message is displayed.

ServiceWithRS

The RemoteServers directory lists one or more remote servers to process access requests. The servers must also be listed in order under /Radius/RemoteServers. The order of the RemoteServers list determines the sequence for directing access requests when MultipleServersPolicy is set to RoundRobin mode. The first server in the list receives all access requests when MultipleServersPolicy is set to Failover mode.

The RemoteServers object can be used to specify the properties of the remote servers to which Services proxy requests. RemoteServers are referenced by name from the RemoteServers list in either the RADIUS, LDAP or TACACS-UDP Services.

Table 2-13 lists and describes the fields in the Services Details page.

Table 2-13 Remote Server Service Properties

Fields	Description
Service Name	Required; name of the remote server service
Incoming Script	Optional; name of script to run when the service starts
Type	Required; Remote service Type must be set to one of the following: **ldap**, **ldap-accounting**, **odbc-accounting**, **odbc**, **oci-accounting**, **oci, prepaid**, **radius**, **radius-session**, **m3ua**, **extended-eap**, or **rest**.
Outgoing Script	Optional; name of script to run when the service ends.

Table 2-13 Remote Server Service Properties (continued)

Fields	Description
Outage Script	Optional; if you set this property to the name of a script, Prime Access Registrar runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
Outage Policy	The default is **DropPacket**. This property defines how Prime Access Registrar handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
Description (optional)	Optional; description of the remote server service
MultipleServersPolicy	Required; must be set to either **Failover** or **RoundRobin**. When you set it to **Failover**, Prime Access Registrar directs requests to the first server in the list until it determines the server is offline. At which time, Prime Access Registrar redirects all requests to the next server in the list until it finds a server that is online. When you set it to **RoundRobin**, Prime Access Registrar directs each request to the next server in the RemoteServers list to share the resource load across all of the servers listed in the RemoteServers list.
NASIDList	Mandatory for extended-EAP service. Select a valid user list as configured under RADIUS > UserLists. Extended-EAP is used as an authorization service to retrieve authorization information from the remote web server using the REST interface. To configure a REST remote server for extended-EAP service, see REST, page 2-148
RemoteServers	Select the required remote server from the available list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
AuthorizationInfoLookUp	Applicable only for the m3ua service type. Choose one of the following from the drop-down list: • MSISDN-IMSI—To fetch MSISDN in the request and send IMSI in the response to the HLR. • IMSI-MSISDN—To fetch IMSI in the request and send MSISDN in the response to the HLR. • MAP-RESTORE—To fetch the profile information of a subscriber from the HLR. For more information on configuring the M3UA service with Map Restore Data authorization, see Configuring M3UA Service with Map Restore Data Authorization, page 14-15.
MapVersion	Applicable only for the m3ua service type; select the map version that HLR supports.
Device Access Rules This section is applicable for TACACS+ command authorization and is available only for service types local-user, oci, odbc, and ldap. For more information on TACACS+ command authorization, see TACACS+ Support for AAA, page 9-66.	
Enable Device Access	Check the box to enable TACACS+ command authorization.

Table 2-13 Remote Server Service Properties (continued)

Fields	Description
Device Access Rule	Select a device access rule and click **Add**. The selected access rule is displayed in the Device Access Rules list box.
Default Device Access Action	Select the default action to perform on the commands for all the access rules in the authorization service. Options are **PermitAll** and **DenyAll**.
Restore Data Mappings Section	
IMSI	IMSI received in the response from HLR.
Naea-Preferred CI	North American Equal Access preferred Carrier ID List. A list of the preferred carrier identity codes that are subscribed to.
Roaming Restricted In Sgsn Due To Unsupported Feature	Indicates that a subscriber is not allowed to roam in the current Service GPRS Support Node (SGSN) or Cisco Mobility Management Entity (MME) area.
Network Access Mode	The Network Access Mode (NAM) defines if the subscriber is registered to get access to the CS (non-GPRS/EPS network), to the PS (GPRS/EPS) network, or to both networks. NAM describes the first level of the subscriber data pseudo-tree below the IMSIroot. It is permanent subscriber data stored in the HSS / HLR and the SGSN with the Gs interface option, and the MME with the SGs interface option.
LMU Indicator	Indicates the presence of an LMU.
IST Alert Timer	Indicates the IST alert timer value that must be used in the Mobile Switching Center (MSC) to inform the HLR about the call activities that the subscriber performs.
Super Charger Supported In HLR	Indicates whether super charger concept is supported in HLR.
CS Allocation Retention Priority	Allocation-retention priority for Circuit Switched (CS). This parameter specifies relative importance to compare with other bearers about allocation and retention of bearer.
ChargingCharacteristics	Subscribed charging characteristics.
Access Restriction Data	Allowed Recipient Access Table (RAT) according to subscription data.
UE Reachability Request Indicator	Indicates that the Home Subscriber Server (HSS) is awaiting a notification of user equipment (UE) reachability.
Category	Calling party category
LSA Information	These parameters refer to one or more localized service areas (LSAs) a subscriber may be a member of, together with the priority, the preferential access indicator, the active mode support indicator and active mode indication of each localized service area. The access right outside these localized service areas is also indicated.
Subscriber Data	
MSISDN	MSISDN value in the subscriber data.

Table 2-13 Remote Server Service Properties (continued)

Fields	**Description**
Subscriber Status	Barring status of the subscriber, which could be Service Granted or Operator Determined Barring.
Roaming Restriction Due To Unsupported Feature	Indicates that the subscriber is not allowed to roam in the current MSC area.
Bearer Service List	List of extensible bearer services subscribed. Configure the index value to fetch only the required bearer services.
TeleService List	List of extensible teleservices subscribed. Configure the index value to fetch only the required teleservices.
Provisioned SS	List of supplementary services provisioned. Configure the index value to fetch only the required supplementary services.
ODB-Data	Operator Determined Barring (ODB) general data and ODB Home Public Land Mobile Network (HPLMN) specific data.
Regional Subscription Data	List of regional subscription areas (zones) in which the subscriber is allowed to roam. Configure the index value to fetch only the required zones.
VBS Subscription Data	List of Voice Broadcast Services (VBS) subscribed. Configure the index value to fetch only the required VBS.
VGCS Subscription Data	List of Voice Group Call Services (VGCS) subscribed. Configure the index value to fetch only the required VGCS.
LCS Information Live Communication Server (LCS) related information for the subscriber.	
GMLC-List	List of Gateway Mobile Location Centers (GMLCs) that are permitted to issue a call/session unrelated or call/session related MT-LR request. Configure the index value to fetch only the required GMLCs.
LCS-Privacy Exception List	Classes of LCS client that are allowed to locate any target Mobile Station (MS). Configure the index value to fetch only the required classes.
MOLR-List	Code and status of Mobile Originating Location Request (MO-LR) subscribed. Configure the index value to fetch only the required requests.
MC-SS-Info Parameters identifying Multicall (MC) supplementary services (SS) that are subscribed.	
MC-SS-Code	Code of the MC SS.
MC-SS-Status	Status of the MC SS.
NbrSB	Maximum number of parallel bearers that may be used as defined by the user's subscription.
NbrUser	Maximum number of parallel bearers that may be used as defined by the user at registration of the MC SS.

Table 2-13 Remote Server Service Properties (continued)

Fields	Description
SGSN-CAMEL-Subscription Info Parameters identifying the subscribers as having Customized Application for Mobile Enhanced Logic (CAMEL) services that are invoked in the SGSN.	
GPRS-CSI	Identifies the subscriber as having GPRS originating SMS CAMEL services.
MO-SMS-CSI	Identifies the subscriber as having mobile originating SMS CAMEL services.
MT-SMS-CSI	Identifies the subscriber as having mobile terminating SMS CAMEL services.
ProfileMappings	
Attribute	Select an RADIUS attribute to map the fetched profile data.
Value:Profile	Enter a value for the attribute.
ProfileList	Select one of the profile lists and click **Add**. The entered profile details are displayed in the list box in the ProfileMappings section. You can delete a profile attribute from the list as required.

You can use the ServiceWithRS List page for the following:

- Filtering Records
- Adding Remote Server Service Details
- Editing Records
- Deleting Records

Adding Remote Server Service Details

To add new remote server service details:

Step 1 Choose **Configuration > Services > ServiceWithRS**. The Services List (..with Remote Servers) page is displayed.

Step 2 Click **Add** to add new remote server service details. The Services Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the Services List (..with Remote Servers) page. Otherwise, click **Cancel** to return to the Services List (..with Remote Servers) List page without saving the details.

On successful creation of the properties, the Services List (..with Remote Servers) page is displayed else a respective error message is displayed.

PEAP Service

Protected EAP (PEAP) is an authentication method designed to mitigate several weaknesses of EAP. PEAP leverages Industry standard authentication of the server using certificates TLS (RFC 2246) and creation of a secure session that can then be used to authenticate the client.

The PEAP protocol consists of two phases, an authentication handshake phase and a tunnel phase where another complete EAP authentication exchange takes place protected by the session keys negotiated by phase one. Prime Access Registrar supports the tunneling of other EAP methods within the PEAP phase two exchange.

Prime Access Registrar supports the two major existing variants of PEAP:

- PEAP Version 0 (Microsoft PEAP)
- PEAP Version 1 (Cisco Prime PEAP)

PEAP Version 0

PEAP Version 0 also called as Microsoft PEAP is described in IETF drafts (draft-kamath-pppext-peapv0-00.txt and draft-josefsson-pppext-eap-tls-eap-02.txt). This version of PEAP uses either EAP-MSChapV2 or EAP-SIM as an authentication method. The testing method used for this version of PEAP is radclient.

PEAP Version 1

PEAP Version 1 also called as Cisco Prime PEAP is described by IETF draft (draft-zhou-pppext-peapv1-00.txt). This version can use either EAP-GTC or EAP-SIM as an authentication method. The testing method used for this version of PEAP is radclient.

Table 2-14 lists and describes the fields in the PEAP Services Details page. The fields listed below are the entire list of all the available types. The fields are displayed based on the type selected.

Table 2-14 PEAP Service Properties

Fields	Description
Service Name	Required; service name
Incoming Script	Optional; script Prime Access Registrar server runs when it receives a request from a client.
Type	Required; must set it to a valid Prime Access Registrar service.
Outgoing Script	Optional; script Prime Access Registrar server runs before it sends a response to a client.
Maximum Message Size	Indicates the maximum length in bytes that a PEAP or EAP-TLS message can have before it is fragmented.
Server Certificate File	Required; the full pathname of the file containing the server's certificate or certificate chain used during the TLS exchange. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The two valid encoding prefixes are PEM and DER. If an encoding prefix is not present, the file is assumed to be in PEM format. The following example assumes that the subdirectory **pki** under **/cisco-ar** contains the server's certificate file. The file **server-cert.pem** is assumed to be in PEM format; note that the file extension ***.pem*** is not significant. **set ServerCertificateFile PEM:/cisco-ar/pki/server-cert.pem**
Private Key Password	Required; the password used to protect the server's private key.
Server RSA Key File	Required; the full pathname of the file containing the server's RSA private key.

Table 2-14 PEAP Service Properties (continued)

Fields	Description

CRL Distribution URL	Optional; The URL that Prime Access Registrar should use to retrieve the CRL.You can specify a URL that uses HTTP or LDAP.
	The following is an example for an HTTP URL:
	`<http://crl.verisign.com/pca1.1.1.crl>.`
	The following is an example for an LDAP URL:
	`ldap://209.165.200.225:388/CN=development-CA,CN=acs-westcoast2,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cisco,DC=com`

CA Certificate File	Optional; the full pathname of the file containing trusted CA certificates used for client verification. The file can contain more than one certificate, but all certificates must be in PEM format. DER encoding is not allowed.
Certificate Verification Mode	Optional; specifies the type of verification used for client certificates. Must be set to one of RequireCertificate, None, or Optional. • RequireCertificate causes the server to request a client certificate and authentication fails if the client refuses to provide one. • None will not request a client certificate. Optional causes the server to request a client certificate but the client is allowed to refuse to provide one.
CA Certificate Path	Optional; the name of a directory containing trusted CA certificates (in PEM format) used for client verification. This parameter is optional, and if it is used there are some special preparations required for the directory it references. Each certificate file in this directory must contain exactly one certificate in PEM format. The server looks up the certificate files using the MD5 hash value of the certificate's subject name as a key. The directory must therefore also contain a set of symbolic links each of which points to an actual certificate file. The name of each symbolic link is the hash of the subject name of the certificate. For example, if a certificate file name **ca-cert.pem** is located in the CACertificatePath directory, and the MD5 hash of the subject name contained in **ca-cert.path.pem** is 1b96dd93, then a symbolic link named 1b96dd93 must point to the **ca-cert.pem** file. If there are subject name collisions such as multiple certificates with the same subject name, each link name must be indexed with a numeric extension as in 1b96dd93.0 and 1b96dd93.1.
Verification Depth	Optional; specifies the maximum length of the certificate chain used for client verification.
Enable Session Cache	Optional; specifies whether TLS session caching (fast reconnect) is enabled or not. Set to True to enable session caching; otherwise set to False.
Tunnel Service	Required; must be the name of an existing EAP-MSCHAPv2 or EAP-SIM service.
Authentication Timeout	Required; specifies time (in seconds) to wait before an authentication request times out; defaults to 120.
Description (optional)	Optional; description of the PEAP service.

Table 2-14 PEAP Service Properties (continued)

Fields	Description
Session Timeout	Optional; if TLS session caching (fast reconnect) is enabled, SessionTimeout specifies the maximum lifetime of a TLS session. Expired sessions are removed from the cache and will require a subsequent full authentication. SessionTimeout is specified as a string consisting of pairs of numbers and units, where units might be one of the following: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, Weeks, as in the following: **Set SessionTimeout "1 Hour 45 Minutes"**
Use ECC Certificates	Check this box, to use the ECC, RSA, or combination of both the certificates for certificate based verification. When this field is disabled, only RSA is used for certificate based verification. The default location to fetch the certificate file is **/cisco-ar/pki**.
Enable Auto Chaining	When set to TRUE, Prime Access Registrar sends its server certificate chain (Server-Cert -> IntermediateCA -> RootCA) while presenting the server certificate to the client for server side authentication. When set to FALSE, Prime Access Registrar sends only the server certificate (Server-Cert) to the client.
Enable WPS	Optional; When set to TRUE, enables Windows Provisioning Service (WPS) and provides two other properties, MasterURL and WPSGuestUserProfile. The default value is FALSE.
Master URL	Optional; when using WPS, specifies the URL of the provisioning server which is modified with the appropriate fragment and sent to the client.
WPS Guest User Profile	Optional; when using WPS, specifies a profile to be used as a guest user profile; must be a valid profile under **/Radius/Profiles.** This profile is used for guests and users whose account has expired. This profile normally contains attributes denoting the VLAN-id of the guest network (which has the provisioning server alone) and might contain IP-Filters that would restrict the access of the guest (to only the provisioning server).

You can use the PEAP Services List page for the following:

- Filtering Records
- Adding PEAP Service Details
- Editing Records
- Deleting Records

Adding PEAP Service Details

To add new PEAP service details:

Step 1 Choose **Configuration > Services > PEAP**. The PEAP Services List page is displayed.

Step 2 Click **Add** to add new PEAP service details. The PEAP Services Details page is displayed.

Step 3 Specify the relevant PEAP service details.

Step 4 Click **Submit** to save the specified details in the PEAP Services List page. Otherwise click **Cancel** to return to the PEAP Services List page without saving the details.

On successful creation of the PEAP service properties, the PEAP Services List page is displayed else a respective error message is displayed.

EAP Service

Prime Access Registrar supports the Extensible Authentication Protocol (EAP) to provide a common protocol for differing authentication mechanisms. It provides dynamic selection of the authentication mechanism at the time of authentication based on information transmitted in the Access-Request.

Prime Access Registrar supports the following EAP authentication methods:

- EAP-AKA
- EAP-AKA-Prime
- EAP-GTC
- EAP-LEAP
- EAP-MD5
- EAP-Negotiate
- EAP-MSChapV2
- EAP-SIM
- EAP-Transport Level Security (TLS)
- EAP-TTLS

EAP-AKA

Authentication and Key Agreement (AKA) is an EAP mechanism for authentication and session key distribution. It is used in the 3rd generation mobile networks Universal Mobile Telecommunications System (UMTS) and CDMA2000. AKA is based on symmetric keys, and typically runs in a UMTS Subscriber Identity Module (USIM), or a (Removable) User Identity Module ((R) UIM), similar to a smart card. EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) includes optional identity privacy support, optional result indications, and an optional fast reauthentication procedure. The EAP-AKA authentication service is extended to generate a Diameter message Multimedia-Authentication-Request (MAR), with the subscriber identity (IMSI), to the Home Subscriber Server (HSS) when it requires the authentication vectors. The HSS sends a Diameter Mutlimedia-Authentication-Answer (MAA) back containing the number of quintuplets.

EAP-AKA-Prime

EAP-AKA-Prime (EAP-AKA') is an EAP authentication method, with a small revision to the existing EAP-AKA method. EAP- AKA' has a new key derivation function, which binds the keys derived within the method to the name of the access network. This limits the effects of compromised access network nodes and keys. EAP-AKA’ supports SHA-256 instead of SHA-1.

EAP-GTC

This method defined in RFC 2284, is used for transmitting a username and password to an authentication server.

Note It should not be used except as an authentication method for PEAP Version 1 because the password is not protected.

EAP-LEAP

The new AAA Cisco-proprietary protocol called Light Extensible Authentication Protocol (LEAP) supported by Prime Access Registrar, is a proprietary Cisco authentication protocol designed for use in IEEE 802.11 wireless local area network (WLAN) environments. Important features of LEAP include:

- Mutual authentication between the network infrastructure and the user
- Secure derivation of random, user-specific cryptographic session keys
- Compatibility with existing and widespread network authentication mechanisms (e.g., RADIUS)

Note Prime Access Registrar supports a subset of EAP to support LEAP. This is not a general implementation of EAP for Prime Access Registrar.

The Cisco-Wireless or LEAP is an EAP authentication mechanism where the user password is hashed based on an MD4 algorithm.

EAP-MD5

This is another EAP authentication exchange. In EAP-MD5 there is a CHAP-like exchange and the password is hashed by a challenge from both client and server to verify the password. On successful verification, the connection proceeds, although the connection is periodically rechallenged (per RFC 1994).

EAP-Negotiate

This is a special service used to select at runtime the EAP service to be used to authenticate the client. It is configured with a list of candidate EAP services that represent the allowable authentication methods in preference order.

EAP-Negotiate is useful when the client population has deployed a mix of different EAP methods that must be simultaneously supported by Prime Access Registrar. EAP-Negotiate solves the problem of distinguishing client requirement by using the method negotiation feature of the EAP protocol.

EAP-MSChapV2

EAP-MSChapv2 encapsulates the MSChapV2 protocol (specified by RFC 2759) and can be used either as an independent authentication mechanism or as an inner method for PEAP Version 0 (recommended). This is based on draft-kamath-pppext-eap-mschapv2-00.txt, an informational IETF draft document.

EAP-SIM

An access point uses the Prime Access Registrar RADIUS server to perform EAP-SIM authentication of mobile clients. Prime Access Registrar must obtain authentication information from the HLR. Prime Access Registrar contacts the MAP gateway that performs the MAP protocol over SS7 to the HLR, or alternately it can contact the HLR (through STP in some cases) using the SIGTRAN-M3UA interface. The EAP-SIM authentication service is extended to generate a Diameter message Multimedia-Authentication-Request (MAR), with the subscriber identity(IMSI), to the HSS when it requires the authentication vectors. The HSS sends a Diameter Mutlimedia-Authentication-Answer (MAA) back containing the number of triplets.

EAP-Transport Level Security (TLS)

This is an authentication method (described in RFC 2716) which leverages TLS, described in RFC 2246, to achieve certificate-based authentication of the server and the client (optionally). It provides many of the same benefits as PEAP but differs in the lack of support for legacy authentication methods.

EAP-TTLS

The Extensible Authentication Protocol Tunneled TLS (EAP-TTLS) is an EAP protocol that extends EAP-TLS. EAP- TTLS extends the authentication negotiation EAP-TLS by using the secure connection established by the TLS handshake to exchange additional information between client and server. It leverages TLS (RFC 2246) to achieve certificate-based authentication of the server (and optionally the client) and creation of a secure session that can then be used to authenticate the client using a legacy mechanism.

EAP-TTLS is a two-phase protocol. Phase 1 conducts a complete TLS session and derives the session keys used in Phase 2 to securely tunnel attributes between the server and the client. The attributes tunneled during Phase 2 can be used to perform additional authentication(s) via a number of different mechanisms.

The authentication mechanisms used during Phase 2 include PAP, CHAP, MS-CHAP, MS-CHAPv2, and EAP. If the mechanism is EAP, then several different EAP methods are possible.

Table 2-15 lists and describes the fields in the EAP Services Details page. The fields listed below are the entire list of all the available types. The fields are displayed based on the type selected.

Table 2-15 EAP Service Properties

Fields	Description
Service Name	Required; service name
Incoming Script	Optional script Prime Access Registrar server runs when it receives a request from a client.
Type	Required; must set it to a valid Prime Access Registrar service
Outgoing Script	Optional script Prime Access Registrar server runs before it sends a response to a client
Description (optional)	Optional; description of the PEAP service.
Authentication Timeout	Mandatory; specifies time (in seconds) to wait before an authentication request times out; defaults to 120.
UserService	Required; name of service that can be used to authenticate using cleartext passwords.
ServiceList	List of preconfigured EAP authentication services. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
Maximum Message Size	Required; indicates the maximum length in bytes that a PEAP message can have before it is fragmented.
Server Certificate File	Required; the full pathname of the file containing the server's certificate or certificate chain used during the TLS exchange. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The two valid encoding prefixes are PEM and DER. If an encoding prefix is not present, the file is assumed to be in PEM format.
Private Key Password	Required; the password used to protect the server's private key.

Table 2-15 EAP Service Properties (continued)

Fields	Description
Server Key File	Required; the full pathname of the file containing the server's RSA private key. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The two valid encoding prefixes are "PEM" and "DER". If an encoding prefix is not present, the file is assumed to be in PEM format. The following example assumes that the subdirectory **pki** under **/cisco-ar** contains the server's certificate file. The file **server-key.pem** is assumed to be in PEM format. The file extension ***.pem*** is not significant. **set ServerRSAKeyFile PEM:/cisco-ar/pki/server-key.pem**
CRL Distribution URL	Optional; enter the URL that Prime Access Registrar should use to retrieve the CRL.You can specify a URL that uses HTTP or LDAP. The following is an example for an HTTP URL: `<http://crl.verisign.com/pca1.1.1.crl>.` The following is an example for an LDAP URL: `ldap://209.165.200.225:388/CN=development-CA,CN=acs-west coast2,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cisco,DC=com`
CA Certificate File	Optional; the full pathname of the file containing trusted CA certificates used for client verification. The file can contain more than one certificate, but all certificates must be in PEM format. DER encoding is not allowed.
Certificate Verification Mode	The value is set to optional by default. If set to RequireCertificate, the client certificate will always be verified. If set to optional, client certificate verification happens optionally.
CA Certificate Path	The name of a directory containing trusted CA certificates (in PEM format) used for client verification. This parameter is optional and if it is used there are some special preparations required for the directory it references. Each certificate file in this directory must contain exactly one certificate in PEM format. The server looks up the certificate files using the MD5 hash value of the certificate's subject name as a key. The directory must therefore also contain a set of symbolic links each of which points to an actual certificate file. The name of each symbolic link is the hash of the subject name of the certificate. For example, if a certificate file named **ca-cert.pem** is located in the CACertificatePath directory, and the MD5 hash of the subject name contained in **ca-cert.path.pem** is 1b96dd93, then a symbolic link named 1b96dd93 must point to **ca-cert.pem**. If there are subject name collisions such as multiple certificates with the same subject name, each link name must be indexed with a numeric extension as in 1b96dd93.0 and 1b96dd93.1.
Verification Depth	Optional; specifies the maximum length of the certificate chain used for client verification.

Table 2-15 EAP Service Properties (continued)

Fields	Description
Enable Session Cache	Optional; specifies whether TLS session caching (fast reconnect) is enabled or not. Set to True to enable session caching; otherwise set to False.
Session Timeout	Required; if TLS session caching (fast reconnect) is enabled, SessionTimeout specifies the maximum lifetime of a TLS session. Expired sessions are removed from the cache and will require a subsequent full authentication. SessionTimeout is specified as a string consisting of pairs of numbers and units, where units might be one of the following: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, Weeks, as in the following: **Set SessionTimeout "1 Hour 45 Minutes"**
UseECCCertificate	Determines the applicability of the authentication mechanism in SmartGrid Solutions. When you check this check box, it can use the ECC, RSA, or combination of both certificate for certificate based verification. When you uncheck this check box, it can only use the RSA certificate for certificate based verification. The default location to fetch the certificate file is **/cisco-ar/pki**.
EnableAutoChaining	When set to TRUE, Prime Access Registrar sends its server certificate chain (Server-Cert -> IntermediateCA -> RootCA) while presenting the server certificate to the client for server side authentication. When set to FALSE, Prime Access Registrar sends only the server certificate (Server-Cert) to the client.
Authentication Service	Specifies the name of the EAP-GTC service used for authentication. The named service must have the UseLabels parameter set to True.
User Prompt	Optional string the client might display to the user; default is Enter password:" Use the **set** command to change the prompt, as in the following: **set UserPrompt "Admin Password:"**
UseLabels	Required; must be set to FALSE for PEAP authentication. Set to FALSE by default.
SystemID	Optional; string that identifies the sender of the MSChapV2 challenge message.
IsWindows7Client	Optional; must be set to TRUE for EAP-MSChapV2 authentication. Set to FALSE by default.
Authority Identifier	Required; a string that uniquely identifies the credential (PAC) issuer. The client uses this value to select the correct PAC to use with a particular server from the set of PACs it might have stored locally.
Authority Information	Required; a string that provides a descriptive text for this credential issuer. The value can be displayed to the client for identification purposes and might contain the enterprise or server names.

Table 2-15 EAP Service Properties (continued)

Fields	Description
Credential Life Time	Optional; specifies the maximum lifetime of a Protected Access Credential (PAC). Clients that successfully authenticate with an expired PAC will be reprovisioned with a new PAC. CredentialLifetime is specified as a string consisting of pairs of numbers and units, where units might be one of the following: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, Weeks. Credentials that never expire should be specified as Forever.
Provision Service	Required; specifies the name of the EAP-MSChapV2 service used for provisioning.
Provision Mode	Required; specifies the TLS mode used for provisioning. Clients only support the default Anonymous mode.
Always Authenticate	Optional; indicates whether provisioning should always automatically rollover into authentication without relying on a separate session. Most environments, particularly wireless, will perform better when this parameter is set to True, the default value.
SubscriberDBLookup	Specifies the type of communication with the HLR/HSS server. Based on the type selected, the communication happens with the HLR/HSS server using the diameter Wx interface, MAP protocol, or SIGTRAN-M3UA protocol. This field is displayed when you select the eap-sim option in the Type field.
Subscriber_DBLookup	Specifies the type of communication with the HLR/HSS server. Based on the type selected, the communication happens with the HLR/HSS server using the diameter Wx interface, SIGTRAN protocol, or SIGTRAN-M3UA protocol. This field is displayed when you select the eap-sim, eap-aka, or eap-aka' option in the Type field.
DestinationRealm	Required. Destination realm to send Diameter packets to the remote server. The role of the remote server should be Relay.
PreRequestTranslationScript	Optional. Prime Access Registrar server runs before sending the request to the Diameter remote server. The script can modify the RADIUS packet dictionaries.
PostRequestTranslationScript	Optional. Prime Access Registrar server runs before sending the request to the Diameter remote server. The script can modify the Diameter packet dictionaries.
PreResponseTranslationScript	Optional. Prime Access Registrar server runs after receiving the response from the Diameter remote server. The script can modify the Diameter packet dictionaries.
PostResponseTranslationScript	Optional. Prime Access Registrar server runs after receiving the response from the Diameter remote server. The script can modify the RADIUS packet dictionaries.
FetchAuthorizationInfo	When you check this check box, it fetches MSISDN from HLR.

Table 2-15 EAP Service Properties (continued)

Fields	Description
General tab The details in the tab are displayed based on the eap-sim, eap-aka, or eap-aka-prime option you select in the Type field.	
MultipleServersPolicy	Required. Must be set to either Failover or RoundRobin. When set to Failover, Prime Access Registrar directs requests to the first server in the list until it determines the server is offline. At that time, Prime Access Registrar redirects all requests to the next server in the list until it finds a server that is online. When set to RoundRobin, Prime Access Registrar directs each request to the next server in the RemoteServers list to share the resource load across all of the servers listed in the RemoteServers list.
NumberOfTriplets	Required; number of triplets (1, 2, or 3) to use for authentication; default is 2.
PseudonymSecret	Required; the secret string that is used as the basis for protecting identities when identity privacy is enabled. This should be at least 16 characters long and have a value that is impossible for an outsider to guess. The default value is secret. This field is not available if EnableRollingPseudonymSecret field is checked. **Note** It is very important to change PseudonymSecret from its default value to a more secure value when identity privacy is enabled for the first time.
PseudonymRenewtime	Required; specifies the maximum age a pseudonym can have before it is renewed. When the server receives a valid pseudonym that is older than this, it generates a new pseudonym for that subscriber. The value is specified as a string consisting of pairs of numbers and units, where the units might be of the following: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, Weeks. The default value is “24 Hours”. Examples are: “8 Hours”, “10 Hours 30 Minutes”, “5 D 6 H 10 M”
PseudonymLifetime	Required; specifies the maximum age a pseudonym can have before it is rejected by the server, forcing the subscriber to authenticate using it’s permanent identity. The value is specified as a string consisting of pairs of numbers and units, where the units might be one of the following: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, Weeks. It can also be Forever, in which case, pseudonyms do not have a maximum age. The default value is “Forever”. Examples are: “Forever”, “3 Days 12 Hours 15 Minutes”, “52 Weeks”

Table 2-15 EAP Service Properties (continued)

Fields	Description
NotificationService	(Optional); Notification service is an authorization service and is used to send a notification code to the client in case of an authorization failure. For more information about the Notification-Code variable, see the "Environment Dictionary" chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*. This can be any of the services configured under /radius/services/ except eap services, accounting services, radius-session, radius-query, and diameter.
ReauthenticationTimeout	Required; specifies the time in seconds that reauthentication identities are cached by the server. Subscribers that attempt to reauthenticate using identities that are older than this value will be forced to use full authentication instead. The default value is 3600 (one hour).
EnableReauthentication	Optional; when True, the fast reauthentication option is enabled. The default value is False.
UseOutagePolicyforReauth	Default value is FALSE. When set to TRUE, Prime Access Registrar drops or rejects reauthentication requests as per outage policy when the remote server is down. This can be processed only when there is at least one failed full authentication before proceeding with reauthentication.
OutagePolicy	Required for EAP-SIM, EAP-AKA, and EAP-AKA' services; the default is DropPacket. This property defines how Prime Access Registrar handles requests if all servers listed in the RemoteServers tab are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
UseProtectedResults	Optional; enables or disables the use of protected results messages. Results messages indicate the state of the authentication but are cryptographically protected.
ReauthenticationRealm	Optional; realm to use for reauthentication.
MaximumReauthentications	Required; specifies the maximum number of times a reauthentication identity might be reused before it must be renewed. The default value is 16.
TripletCacheTimeout	Required for eap-sim service; time in seconds an entry remains in the triplet cache. A zero (0) indicates that triplets are not cached. The maximum is 28 days; the default is 0 (no caching).
QuintetCacheTimeout	Required for eap-aka or eap-aka' service; time in seconds an entry remains in the quintet cache. A zero (0) indicates that quintets are not cached. The maximum is 28 days; the default is 0 (no caching).
QuintetGenerationScript	Available for eap-aka or eap-aka' service; script required for quintet generation.
Authentication Timeout	Required; time in seconds to wait for authentication to complete. The default is 2 minutes; range is 10 seconds to 10 minutes.
UseSimDemoTriplets	Optional; set to TRUE to enable the use of demo triplets. This must be disabled for release builds.

Table 2-15 EAP Service Properties (continued)

Fields	Description
AlwaysRequestIdentity	Optional; when True, enables the server to obtain the subscriber's identity via EAP/SIM messages instead of relying on the EAP messages alone. This might be useful in cases where intermediate software layers can modify the identity field of the EAP-Response/Identity message. The default value is False.
EnableIdentityPrivacy	Optional; when True, the identity privacy feature is enabled. The default value is False.
Generate3GPPCompliantPseudonym	Optional; the value is set to False by default. If set to TRUE then Prime Access Registrar generates a 12 octet 3GPP compliant pseudonym identity. The Pseudonym username identities are used to protect the privacy of subscriber identities.
SendReAuthIDInAccept	Optional; the value is set to False by default. When set to True, Prime Access Registrar sends SN-Fast-ReAuth-UserName (Starent VSA) in access-accept message.
Outage Script	Optional; if you set this property to the name of a script, Prime Access Registrar runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
NetworkName	Required for eap-aka-prime service type. Name of the access network for which the authentication is performed. This attribute is captured to ensure that the peer and the server know the name of the access network for performing the EAP authentication.
MapVersion	Required for SIGTRAN-M3UA remote server; select the map version HLR supports.
DiameterInterface	Select SWx or Wx to indicate the Diameter protocol to use for the service.
ProxyService	Select the diameter proxy service to use.
EnableRollingPseudonymSecret	Check this box to activate rolling encryption process that involves generating rolling pseudonym secrets for the service. This option is available only when EnableIdentityPrivacy check box is checked. For more information about rolling encryption support, see Rolling Encryption Support for Pseudonym Generation in EAP-SIM, EAP-AKA, and EAP-AKA' Services, page 5-50.
EnableEncryptedIMSI	Check this box to look out for encrypted IMSI in the incoming EAP response. For more information, see Support for Decrypting Encrypted-IMSI for EAP-SIM, EAP-AKA, and EAP-AKA' Services, page 5-53. The following three fields are available when you check this option.
EncryptedIMSIDelimiter	Delimiter value to identify whether the incoming EAP response is encrypted or not. Default value is '\0' (NULL), which indicates the incoming message contains encrypted IMSI.

Table 2-15 EAP Service Properties (continued)

Fields	Description
EncryptedIMSIKeyIdDelimiter	Delimiter value to indicate the key identifier from the incoming EAP response. Default value is ‘,’ (comma). The data that exists between the IMSI delimiter (‘\0’) and Key ID delimiter (‘,’) in the incoming EAP response, is the encrypted IMSI. The data that follows this Key ID delimiter (‘,’) helps the server to locate the private key that can be used to decrypt the incoming encrypted IMSI.
DefaultPrivateKey	Default private key to use for decryption if no private key is configured under **Advanced** > **EncryptedIMSI-PrivateKeys**. For more information, see Encrypted IMSI Private Keys
EnableStateStickiness	This field appears for **eap-sim**, **eap-aka**, and **eap-aka-prime** services. Check this box to configure a state attribute value. If this box is unchecked, the Diameter remote server name will be carried as the state attribute value by default.
StateValue	This field appears if **EnableStateStickiness** is checked. Enter a state attribute value.
MEIdentityLookup	Check this box to enable Equipment Identity Registrar (EIR) check for the service. This is used for checking the mobile equipment’s identity status. For more details, see the “Mobile Equipment Identity Check Support in Cisco Prime Access Registrar” section in the “Wireless Support” chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*.
The following fields appear if MEIdentityLookup option is enabled.	
IMEIUnavailable	Select one of the following options: • **Continue**—Prime Access Registrar will continue the authentication/authorization even if the IMEI information is not received from the client. • **Terminate**—Prime Access Registrar will terminate the authentication/authorization if the IMEI information is not received from the client.
GreyListPolicy	Select one of the following options: • **Accept**—Prime Access Registrar will continue the authentication/authorization even if the equipment status is grey-listed from EIR check. • **Reject**—Prime Access Registrar will reject the authentication/authorization if the equipment status is grey-listed from EIR check.
EIRProxyService	Separate proxy service for EIR that should be mapped with EIR remote servers.

Table 2-15 EAP Service Properties (continued)

Fields	Description
EmergencyServiceMEIdentityLookup	Check this box to perform MEIdentityLookup during emergency services based on the **EmergencyServicesPolicy** set up under Radius/Advanced/Diameter/General.
MEIdentityLookupFailurePolicy	Select one of the following options: • **Continue**—Prime Access Registrar will continue the authentication for emergency ME Identity Lookup EIR failure cases. • **Terminate**—Prime Access Registrar will terminate the authentication for emergency ME Identity Lookup EIR failure cases. This option is available only if **EmergencyServiceMEIdentityLookup** is checked.
Remote Servers tab	
Attribute	Optional; list of remote RADIUS servers which are map gateways. The remote server type must be set to map-gateway. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.

You can use the EAP Services List page for the following:

- Filtering Records
- Adding EAP Service Details
- Editing Records
- Deleting Records

Adding EAP Service Details

To add new EAP service details:

Step 1 Choose **Configuration > Services > EAP**. The EAP Services List page is displayed.

Step 2 Click **Add** to add new EAP service details. The EAP Services Details page is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Submit** to save the specified details in the EAP Services List page. Otherwise click **Cancel** to return to the EAP Services List page without saving the details.

On successful creation of the EAP Service properties, the EAP Services List page is displayed else a respective error message is displayed.

Diameter Service

Proxy agents assist in routing Diameter messages using the Diameter routing table. Diameter proxy service works in tandem with the rule policy engine to perform the routing for multiple realms or applications. The following are the multiple peer policies supported by the proxy service:

- RoundRobin
- FailOver
- GroupFailOver
- IMSI Range Based.

Table 2-16 lists and describes the fields in the Diameter-Services page. The fields listed below are the entire list of all the available roles. The fields are displayed based on the role selected.

Table 2-16 Diameter Service Properties

Fields	Description
Name	Required; name of the Diameter server.
Description	Optional; description of the Diameter server.
Realm	Required; realm of the route. Must be unique for a route table.
Role	Required; specifies the role that the Diameter entity will play in resolving messages matching the realm. The role can be any one of the following: Relay - Application acting as a Relay Agent. Redirect - Application acting as a Redirect Agent. Proxy - Application acting as a Proxy Agent. When the role is set to Proxy, the IncomingScript and OutgoingScript points are enabled. Local - Application processes the requests locally. When the role is set to Local, the AuthenticationService and AccountingService are enabled. By default, the Proxy option is selected. However, you can select another option from the drop-down list.
Incoming Script	Optional; enabled when role is set to Proxy or Local. When set, must be the name of a known incoming script. Prime Access Registrar runs the IncomingScript before proxying the Diameter packet to the remote Diameter server.
Outgoing Script	Optional; enabled when role is set to Proxy or Local. When set, must be the name of a known outgoing script. Prime Access Registrar runs the OutgoingScript after it receives the response from the remote Diameter server.
Authentication Service	Required; used when service is configured to process the Diameter requests locally. Set to valid service of type (local/ldap/odbc) to authenticate the user. This field is displayed when you select the role type as ‘Local’ in the Role field.

Role	Required; specifies the role that the Diameter entity will play in resolving messages matching the realm. The role can be any one of the following: Relay - Application acting as a Relay Agent. Redirect - Application acting as a Redirect Agent. Proxy - Application acting as a Proxy Agent. When the role is set to Proxy, the IncomingScript and OutgoingScript points are enabled. Local - Application processes the requests locally. When the role is set to Local, the AuthenticationService and AccountingService are enabled. By default, the Proxy option is selected. However, you can select another option from the drop-down list.
Incoming Script	Optional; enabled when role is set to Proxy or Local. When set, must be the name of a known incoming script. Prime Access Registrar runs the IncomingScript before proxying the Diameter packet to the remote Diameter server.
Outgoing Script	Optional; enabled when role is set to Proxy or Local. When set, must be the name of a known outgoing script. Prime Access Registrar runs the OutgoingScript after it receives the response from the remote Diameter server.
Authentication Service	Required; used when service is configured to process the Diameter requests locally. Set to valid service of type (local/ldap/odbc) to authenticate the user. This field is displayed when you select the role type as ‘Local’ in the Role field.

Table 2-16 Diameter Service Properties (continued)

Fields	Description
VendorSpecific	Required; the default is FALSE. If set to FALSE, the application is ordinary application and user is prompted to enter the ApplicationID. If set to TRUE, the application is a VendorSpecific Application. User is prompted to enter VendorSpecificApplicationID and VendorID.
VendorID	Required; specifies the VendorID for the application. Example: DIAMETER 3GPP Cx APPLICATION VendorSpecificApplicationID 16777216 VendorID 10415
VendorSpecificApplicationID	Required; specifies the integer value for the vendor specific application.
ApplicationID	Required; application used in the route. The application Id should be available in /Advanced/Diameter/Applications.
Applications This is displayed when you select the 'Proxy' option in the Role field.	
Name	Required; name of the application.
Description	The description of the application.
ApplicationID	Required; specifies the unique integer value for the application. It represents the application id of the Application used for load balancing the Diameter messages.
EnableSticky	Required; default is FALSE. If set to True, the sticky entries for load balancing is enabled and the user is prompted to enter the values for StickySessionKey, StickyCreationCmdList, and StickyDeletionCmdList.
MultiplePeersPolicy	Required; Policy used by the Prime Access Registrar server to load balance the peers. Must be set to one of the following: • RoundRobin—You can list the Diameter remote servers in the tab below. • FailOver—You can list the Diameter remote servers in the tab below. • GroupFailover—You can create individual groups of Diameter remote servers and list them in the tab below. This option allows you to perform group-based load balancing. For more information, see Group-Based Load Balancing, page 2-23. • IMSIRangeBased—You can add the list of IMSI ranges in the tab below.
PeerTimeoutPolicy/GroupTimeoutPolicy	Required; action to perform when there is a timeout with the Diameter peer or group server.

Table 2-16 Diameter Service Properties (continued)

Fields	Description
StickySessionKey	Required; used as the sticky key for mapping the sticky sessions. Set the value to a valid attribute-value pair (AVP) in order to use the sticky key for maintaining Diameter sessions. This ensures that Prime Access Registrar maps the request to the same server for all the subsequent messages using the sticky key. For example, set StickyAVP “Session-Id”. When the Prime Access Registrar server receives the CCR-I request, Prime Access Registrar extracts the Session-Id from the request packet, maps the Session to the peer configured in the list, and forwards the request to the chosen peer. Prime Access Registrar chooses the same peer for all the subsequent messages(CCR-Update/CCR-Terminate) with same Session-Id.

StickyCreationCmdList	Required; specifies the command list to create the sticky entries. Specify the list of ‘||’ separated command code, AVP name, and its value to create the sticky sessions.
	The following is the StickyCreationCmdList format:
	`<commandcode1>::<AVPName1=Value1> ||`
	`<commandcode2<::<AVPName2=Value2>||<commandcode3>`
	For example, if the sticky session entries need to created based on command code ‘265’or based on command code ‘271’ with Accounting-Record-Type value as 2, use the format below:
	`Set StickyCreationCmdList “265||271::`
	`Accounting-Record-Type=2”`

StickyDeletionCmdList	Required; specifies the command list to delete the sticky entries.Specify the list of ‘||’ separated command code, AVP name, and its value to delete the sticky sessions.
	The following is the StickyDeletionCmdList format:
	`<commandcode1>::<AVPName1=Value1> ||`
	`<commandcode2<::<AVPName2=Value2>||<commandcode3>`
	For example, if the sticky session entries need to deleted based on command code ‘271’ with Accounting-Record-Type value as 4, use the format below:
	`Set StickyDeletionCmdList “271::`
	`Accounting-Record-Type=4”`

PEER Definitions Proxy	
Name	Required; name of the peer.
Host Name	Required; hostname or IP address of the peer. The HostName must exist in the client list for the route to be active.
Metric	Required; metric value for this peer entry. The higher the value the lower the preference. The highest value of preference is 0.

Table 2-16 Diameter Service Properties (continued)

Fields	Description
Weight	Required; default value is 0. Specifies the weight percentage for which the service needs to load balance the peer. **Note** When you set the weight to a value other than 0, the weight should be in multiples of 10 and the sum of the weights configured in the peer list should be equal to 100.
IMSIRanges	Required; used for load balancing. The value is set to comma separated values of IMSI Ranges. For example, set IMSIRanges “112156000000001-112156001000000,112156010000001-112156011000000” **Note** Prime Access Registrar uses the AVP configured in StickyAVP property to check whether the IMSI is in valid range.
IsActive	Optional; if this is set to true, the new sessions will not go to the peer server. By default, this is set as false.

You can use the Diameter Services List page for the following:

- Filtering Records
- Adding Diameter Service Details
- Editing Records
- Deleting Records

Adding Diameter Service Details

To add a new Diameter Service details:

Step 1 Choose **Configuration > Services > Diameter**. The Diameter Services page is displayed.

Step 2 Click **Add** to add new Diameter service details. The DIAMETER Services Details page is displayed.

Step 3 Specify the required details in the **PEER Statements**, **Applications**, and **PEER Definitions Proxy** specific sections.

Step 4 Click **Save DIAMETER Service** to save the specified details in the Diameter Services page. Otherwise click **Cancel** to return to the Diameter Services page without saving the details.

On successful creation of the Diameter Service properties, the Diameter Services page is displayed else a respective error message is displayed.

Note You may need to enter **PEER Statements, Applications,** and **PEER Definitions Proxy** details based on the **Role** that you select in the DIAMETER-Services page.

Adding the PEER Statements Details

To add new PEER Statement details:

Step 1 Click **Add** to add new PEER Statements details section. The fields specific to PEER Statements are displayed.

Step 2 Specify the required details.

Step 3 Click **Save** to save the specified details in the PEER Statements section. Otherwise click **Cancel** to return to the PEER Statements section without saving the details.

On successful creation of the Diameter Service properties, the Diameter Services page is displayed else a respective error message is displayed.

Adding the Applications Details

To add new Application details:

Step 1 Click **Add** to add new Applications details in the Application List section. The fields specific to Applications are displayed.

Step 2 Specify the required details.

Step 3 Click **Save Appln** to save the specified details in the Application List section. Otherwise click **Cancel Appln** to return to the Application List section without saving the details.

Adding the PEER Definitions Proxy Details

To add PEER Definitions Proxy details:

Step 1 Click **Add** to add new Proxy PEER Statements in the PEER Definitions Proxy section. The fields specific to Proxy PEER Statements are displayed.

Step 2 Specify the required details.

Step 3 Click **Save** to save the specified details in the Proxy PEER Statements section. Otherwise click **Cancel** to return to the Proxy PEER Statements section without saving the details.

CommandSets

A command set consists of commands and the action to perform during TACACS+ command authorization.

Adding a Command Set

To add a new command set:

Step 1 Choose **Configuration > Command Sets**. Prime Access Registrar lists all the command sets available in the system. You can edit or delete an existing command set.

Step 2 Click **Add** to add a new command set.

Step 3 Enter a name and description for the command set.

Step 4 Provide the Command Set parameters. Table 2-17 lists the parameters in the Add Command section.

Table 2-17 Command Set Parameters

Field	Field Description
Action	Select **Permit** or **Deny** to indicate the action to be performed on the command during TACACS+ command authorization.
Command	The command to add in the set. Example: `show`
Arguments	The arguments for the command. Example: `~/serial*/` **Note** Prime Access Registrar supports POSIX Extended Regular Expression (ERE) for command arguments.

Step 5 Click **Add** to add the new command to the set. The command details are displayed in the **Commands** section. You can edit or delete a command from the list as required.

Step 6 Click **Submit** to save the command set details.

You can use the Command Sets page to perform the following as well:

- Filtering Records
- Editing Records
- Deleting Records

DeviceAccessRules

A device access rule consists of conditions or expressions and the applicable command sets for TACACS+ command authorization.

Adding a Device Access Rule

To add a new device access rule:

Step 1 Choose **Configuration > Device Access Rules**. Prime Access Registrar lists all the device access rules available in the system. You can edit or delete an existing device access rule.

Step 2 Click **Add** to add a new device access rule.

Step 3 Enter a name and description for the device access rule.

Step 4 Choose the default device access action to perform on all commands in the device access rule. Options are **Permit All** or **Deny All**.

Step 5 In the Conditions field, include the expressions with **AND** or **OR** conditional operator.

Step 6 Select a command set from the drop-down list box and click **Add**. The selected command set is displayed in the Command Set Names list box available. Click **Delete** to remove any command set from the list.

Step 7 Provide the expression details for the device access rule. Table 2-18 lists the parameters for adding expressions.

Table 2-18 Expression Parameters

Field	Field Description
Name	Name of the expression to include in the device access rule.
Description	Description of the expression.
Attribute	Parameter to apply the condition on.
Value	Value of the parameter. **Note** Prime Access Registrar supports POSIX Extended Regular Expression (ERE) for condition expression value property.

Step 8 Click **Add** to add the expression to the list-box available in the Condition Expressions section. You can edit or delete the expression from the list as required.

Step 9 Click **Submit** to save the device access rule details.

FastRules

FastRules provides a mechanism to easily choose the right authentication, authorization, accounting, and query service(s), drop, reject, or break flows, run a script, choose a session manager and/or a chain of fast rules required for processing a packet.

FastRules has the following capabilities:

- Provides maximum flexibility and ease in matching information in the incoming packets for choosing the appropriate service to apply
- Provides an option to match values in AVPs based on value ranges, exact match, and simple string comparisons using regex
- Provides easy and efficient alternative to rule/policy engine and scripting points for most common use cases—reduces the use of external scripts to choose an appropriate service

For more information about FastRules and the workflow, see Chapter 11, "Using FastRules to Process Packet Flow."

Adding a Fast Rule

To add a new fast rule:

Step 1 Choose **Configuration > FastRules**. Prime Access Registrar lists fast rules available for RADIUS, Diameter, and TACACS in the respective tabs. You can edit or delete an existing fast rule.

Step 2 Click **Add** to add a new fast rule. Table 2-19 provides the list of parameters in the FastRules Details page.

Table 2-19 FastRules Details

Field	Field Description
Name	Required; name of the fast rule.
Description	Optional; description of the fast rule.
Protocol	Required; select the type of packet that the fast rule is applicable for from one of the following options: • Radius • Diameter • Tacacs
Condition	Condition based on which the fast rule will be run on the incoming packet. If the condition is success, enter the action to be performed in the Success field. If the condition is failure, enter the action to be performed in the Failure field.
Attributes	
Name	Name of the attribute to include in the condition.
Description	Description of the attribute.
Dictionary	Select type of the dictionary variable as **Environment**, **Request**, or **Response** to map the attribute to.

Step 3 Add Success and Failure attribute values to the Success Mapping and Failure Mapping fields in the respective sections.

Step 4 Click **Save** to save the fast rules details.

Replication

The replication feature of Prime Access Registrar allows you to maintain identical configurations on multiple machines simultaneously. It eliminates the need to have administrators with multiple Prime Access Registrar installations, make the same configuration changes at each of their installations. Instead, only the master's configuration must be changed and the slave is automatically configured eliminating the need to make repetitive, error-prone configuration changes for each individual installation. In addition to enhancing server configuration management, using replication eliminates the need for a hot-standby machine.

Employing Prime Access Registrar's replication feature, both servers can perform RADIUS request processing simultaneously, eliminating wasted resources. It focuses on configuration maintenance only, not session information or installation-specific information.

Table 2-20 lists and describes the fields in the Replication Details page.

Table 2-20 Replication Properties

Fields	Description
General Properties tab	
Replication Type	Indicates the type of replication
Transaction Sync Interval (in ms)	Duration between periodic transmission of the TransactionSync message expressed in milliseconds. The default is 60000 or 1 minute.
Transaction Archive Limit	The default setting is 100. The value set for RepTransactionArchiveLimit should be the same on the master and the slave.
Replication Secret	The value of this setting must be identical on both the master and the slave.
Is Master	On the master, set RepIsMaster to TRUE. On the slave, set it to FALSE.
Master IP Address	Specifies the IP Address of the master.
Master Port	Specifies the port to be used to send replication messages to the master.
Replication IP Address	The value is set to the IP Address of the machine containing the Prime Access Registrar installation.
Replication Port	Defaults to port1645.
Replication Members tab	
Name	Name of the slave. The name must be unique.
IP Address	Indicates the IP Address of the slave.
Port	Port upon which the master will send replication messages to the slave.

You can use the Replication Details page for the following:

- Filtering Records
- Adding Replication Details
- Adding the Replication Member Details
- Editing Records
- Deleting Records

Adding Replication Details

To add new replication details:

Step 1 Choose **Configuration > Replication**. The Replication Details page is displayed.

Step 2 Specify the replication details.

Step 3 Enter the Replication Member Details, if needed.

Step 4 Click **Save** to save the new replication details. Otherwise click **Reset** to restore the default values.

On successful creation of the replication details, a success message is displayed else a respective error message is displayed.

Adding the Replication Member Details

To add new replication member details:

Step 1 Click the **Replication Members** tab. The List of Replication Members section is displayed.

Step 2 Enter the required details.

Step 3 Click **Submit** to save the new replication member details.

RADIUSDictionary

The RADIUS dictionary passes information between a script and the RADIUS server, or between scripts running on a single packet.

Table 2-21 lists and describes the fields in the Add Radius Attributes page. The fields listed below are the entire list of all the available types. The fields are displayed based on the type selected.

Table 2-21 RADIUS Dictionary Properties

Fields	Description
Name	Required; must be unique in the RADIUS dictionary list
Description	Optional; description of the attribute
Attribute	Required; must be a number between 1-255. It must be unique within the Attribute dictionary list.
Type	Required; type governs how the value is interpreted and printed.
Minimum	Set to zero
Maximum	Set to 253
Enum Number	Enums allow you to specify the mapping between the value and the strings. After you have established this mapping, Prime Access Registrar then replaces the number with the appropriate string. The min/max properties represent the lowest to highest values of the enumeration.
Enum Equivalent	The value can range from 1 through 255. Click the **Add** button to save the details and list it in the Enums list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
Tag	The tag number value can range from 0 through 31. The default value is zero.

You can use the Radius Attributes page for the following:

- Filtering Records
- Adding RADIUS Dictionary Details
- Editing Records
- Deleting Records

Adding RADIUS Dictionary Details

To add new RADIUS dictionary details:

Step 1 Choose **Configuration > Radius Dictionary**. The Radius Attributes page is displayed.

Step 2 Click **Add** to add new RADIUS dictionary details. The Add RADIUS Dictionary page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the Radius Attributes page. Otherwise click **Cancel** to return to the Radius Attributes page without saving the details.

On successful creation of the Radius Attributes, the Radius Attributes page is displayed else a respective error message is displayed.

VendorDictionary

The vendor dictionary allows the user to maintain the attributes of the vendor with respect to vendor id, vendor type and the attributes required to support the major NAS.

Table 2-22 lists and describes the fields in the Add Vendor Dictionary page. The fields listed below are the entire list of all the available types. The fields are displayed based on the type selected.

Table 2-22 Vendor Dictionary Properties

Fields	Description
Name	Required; must be unique in the Vendor dictionary list
Description	Optional; description of the attribute
Vendor ID	Required; must be a valid number and unique within the entire attribute dictionary
Type	Required; type governs how the value is interpreted and printed.
Minimum	Optional; set to zero
Maximum	Optional; set to 253
Enum Number	Optional; enums allow you to specify the mapping between the value and the strings. After you have established this mapping, Prime Access Registrar then replaces the number with the appropriate string. The min/max properties represent the lowest to highest values of the enumeration.

Table 2-22 Vendor Dictionary Properties (continued)

Fields	Description
Enum Equivalent	Optional; the value can range from 1 through 255. Click the **Add** button to save the details and list it in the Enums list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
Tag	Optional; the tag number value can range from 0 through 31. The default value is zero.
Vendor Size	Optional; set the vendor size to 8, 16, or 32 bit
HasSubAttributeLengthField	Optional; indicates that the value field of the attribute has the length field for the sub attribute.

You can use the Vendor Dictionary page for the following:

- Filtering Records
- Adding Vendor Dictionary Details
- Editing Records
- Deleting Records

Adding Vendor Dictionary Details

To add new vendor dictionary details:

Step 1 Choose **Configuration > Vendor Dictionary**. The Vendor Attributes page is displayed.

Step 2 Click **Add** to add new Vendor dictionary details. The Add Vendor Dictionary page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the Vendor Attributes page. Otherwise click **Cancel** to return to the Vendor Attributes page without saving the details.

On successful creation of the vendor dictionary details, the Vendor Attributes page is displayed else a respective error message is displayed.

Note After adding new vendor dictionary details, you can add vendor attributes details. Or you can also add vendor attributes details by clicking the link in the vendor dictionary list, see Adding Vendor Attributes for details.

Vendor Attributes

Vendor-specific attributes are included in specific RADIUS packets to communicate prepaid user balance information from the Prime Access Registrar server to the AAA client, and actual usage, either interim or total, between the NAS and the Prime Access Registrar server.

Table 2-23 lists and describes the fields in the Add Vendor Attributes page.

Table 2-23 Vendor Attribute Properties

Fields	Description
Name	Required; must be unique in the Vendor attribute list
Description	Optional; description of the attribute
Attribute	Required; must be a valid number and unique within the entire attribute dictionary
Type	Required; type governs how the value is interpreted and printed.
Minimum	Optional; set to zero
Maximum	Optional; set to 253
Enum Number	Optional; enums allow you to specify the mapping between the value and the strings. After you have established this mapping, Prime Access Registrar then replaces the number with the appropriate string. The min/max properties represent the lowest to highest values of the enumeration.
Enum Equivalent	Optional; the value can range from 1 through 255. Click the **Add** button to save the details and list it in the Enums list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
Tag	Optional; the tag number value can range from 0 through 31. The default value is zero.

You can use the Vendor Attributes page for the following:

- Filtering Records
- Adding Vendor Attributes
- Editing Records
- Deleting Records

Adding Vendor Attributes

To add new Vendor attributes:

Step 1 Choose **Configuration** > **Vendor Dictionary**. The Vendor Attributes page is displayed.

Step 2 Click the Vendor name link. The Vendor Attributes page is displayed.

Step 3 Click **Add** to add new Vendor attributes. The Add Vendor Attributes page is displayed.

Step 4 Enter the required details.

Step 5 Click **Submit** to save the specified details in the Vendor Attributes page. Otherwise click **Cancel** to return to the Vendor Attributes page without saving the details.

On successful creation of the vendor attributes, the Vendor Attributes page is displayed else a respective error message is displayed.

Vendors

The **Vendor** object provides a central location for specifying all of the request and response processing a particular NAS or Proxy vendor requires. Depending on the vendor, it might be necessary to map attributes in the request from one set to another, or to filter out certain attributes before sending the response to the client. For more information about standard RADIUS attributes, see the "RADIUS Attributes" chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*.

Note When you have also set **/Radius/IncomingScript**, Cisco Prime Access Registrar runs that script before the vendor's script. Conversely, when you have set a **/Radius/Outgoing** script, Cisco Prime Access Registrar runs the vendor's script before that script.

Table 2-24 lists and describes the fields in the Add Vendor page.

Table 2-24 Vendor Properties

Fields	Description
Name	Required; must be unique in the Vendors list.
IncomingScript	Optional; when you specify an IncomingScript, Cisco Prime Access Registrar runs the script on all requests from clients that specify that vendor.
Description	Optional; description of the vendor.
OutgoingScript	Optional; when you specify an OutgoingScript, Cisco Prime Access Registrar runs the script on all responses to the Client.

You can use the Vendors page for the following:

- Filtering Records
- Adding Vendor Details
- Editing Records
- Deleting Records

Adding Vendor Details

To add new Vendor details:

Step 1 Choose **Configuration > Vendors**. The Vendors page is displayed.

Step 2 Click **Add** to add new Vendor details. The Add Vendor page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the Vendors page. Otherwise click **Cancel** to return to the Vendors page without saving the details.

On successful creation of the vendor details, the Vendors page is displayed else a respective error message is displayed.

Translations

Translations add new attributes to a packet or change an existing attribute from one value to another. The **Translations** subdirectory lists all definitions of **Translations** the RADIUS server can apply to certain packets.

Under the **/Radius/Translations** directory, any translation to insert, substitute, or translate attributes can be added. The following is a sample configuration under the **/Radius/Translations** directory:

```
cd /Radius/Translations
Add T1
cd T1
Set DeleAttrs Session-Timeout,Called-Station-Id
cd Attributes
Set Calling-Station-Id 18009998888
```

DeleAttrs is the set of attributes to be deleted from the packet. Each attribute is comma separated and no spaces are allowed between attributes. All attribute value pairs under the attributes subdirectory are the attributes and values that are going to be added or translated to the packet.

Under the **/Radius/Translations/T1/Attributes** directory, inserted or translated attribute value pairs can be set. These attribute value pairs are either added to the packet or replaced with the new value.

If a translation applies to an Access-Request packet, by referencing the definition of that translation, the Prime Access Registrar server modifies the Request dictionary and inserts, filters, and substitutes the attributes accordingly. You can set many translations for one packet and the Prime Access Registrar server applies these translations sequentially.

Note Later translations can overwrite previous translations.

Table 2-25 lists and describes the fields in the Add Translations page.

Table 2-25 Translations Properties

Fields	Description
General Properties tab	
Name	Required; must be unique in the Translations list.
Description	Optional; description of the Translation

Table 2-25 Translations Properties (continued)

Fields	Description
Attribute Type	Optional; select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list. Select the attributes from the available list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.
Attributes tab	
Attribute Type	Optional; select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
Attribute Value	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Radius and Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the Translations page for the following:

- Filtering Records
- Adding Translation Details
- Editing Records
- Deleting Records

Adding Translation Details

To add new translation details:

Step 1 Choose **Configuration > Translations**. The Translations page is displayed.

Step 2 Click **Add** to add new translations details. The Add Translations page is displayed.

Step 3 Enter the required details.

Step 4 Click **Add Translation** to save the specified details in the Translations page. Otherwise click **Cancel** to return to the Translations page without saving the details.

On successful creation of the translation details, the Translations page is displayed else a respective error message is displayed.

TranslationGroups

You can add translation groups for different user groups under **TranslationGroups**. All Translations under the Translations subdirectory are applied to those packets that fall into the groups. The groups are integrated with the Prime Access Registrar Rule engine.

The Prime Access Registrar Administrator can use any RADIUS attribute to determine the **Translation Group**. The incoming and outgoing translation group can be different translation groups. For example, you can set one translation group for incoming translations and one for outgoing translations.

Under the **/Radius/TranslationGroups** directory, translations can be grouped and applied to certain sets of packets, which are referred to in a rule. The following is a sample configuration under the **/Radius/TranslationGroups** directory:

```
cd /Radius/TranslationGroups
Add CiscoIncoming
cd CiscoIncoming
cd Translations
Set 1 T1
```

The translation group is referenced through the Prime Access Registrar Policy Engine in the **/Radius/Rules/**<*RuleName*>**/Attributes** directory. **Incoming-Translation-Groups** are set to a translation group (for example `CiscoIncoming`) and **Outgoing-Translation-Groups** to another translation group (for example `CiscoOutgoing`).

Table 2-26 lists and describes the fields in the Add Translation Groups page.

Table 2-26 TranslationGroups Properties

Fields	Description
Name	Required; must be unique in the Translations list.
Description	Optional; description of the Translation Group.
Translations	Optional; lists of translation. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.

You can use the Translation Groups page for the following:

- Filtering Records
- Adding Translation Group Details
- Editing Records
- Deleting Records

Adding Translation Group Details

To add new translation group details:

Step 1 Choose **Configuration > TranslationGroups**. The Translation Groups page is displayed.

Step 2 Click **Add** to add new translation group details. The Add TranslationGroup page is displayed.

Step 3 Enter the required details.

Step 4 Click **Add TranslationGroup** to save the specified details in the Translation Groups page. Otherwise click **Cancel** to return to the Translation Groups page without saving the details.

On successful creation of the translation group details, the Translation Groups page is displayed else a respective error message is displayed.

Diameter

Diameter is a computer networking protocol for Authentication, Authorization and Accounting (AAA). It is a successor to RADIUS or an enhanced version of the RADIUS protocol. It includes numerous enhancements in all aspects, such as error handling and message delivery reliability. It extracts the essence of the AAA protocol from RADIUS and defines a set of messages that are general enough to be the core of the Diameter Base protocol. The various applications that require AAA functions can define their own extensions on top of the Diameter base protocol, and can benefit from the general capabilities provided by the Diameter base protocol.

The following sections can be used to configure Diameter transport management properties, session management properties, add new application, commands associated with it and application specific AVPs:

- General
- Session Management
- Applications
- Commands
- DiameterAttributes

General

This section explains how to set Diameter general configuration such as product name, version, and transport management properties.

Setting General Diameter Parameters

Table 2-27 lists and describes the fields in the General Diameter Properties page.

Table 2-27 General Diameter Properties

Fields	Description
General section	
Product	Optional; name of the product.
AuthApplicationIdList	Specifies the list of AuthApplications that the Prime Access Registrar server registers to Diameter Base stack during start up. It is a combination of Auth ApplicationId's separated by a colon.
Version	Optional; version number.

Table 2-27 General Diameter Properties (continued)

Fields	Description
AcctApplicationIdList	Specifies the list of AcctApplications that the Prime Access Registrar server registers to Diameter Base stack during start up. It is a combination of Acct ApplicationId's separated by a colon.
EmergencyServicesPolicy	Emergency Services support is applicable for packets containing Emergency-Services AVP in the incoming Diameter-EAP-request. Choose one of the following: • All—For all users. Prime Access Registrar skips authorization and authentication and generates EAP-Master-Session-Key using IMEI from user in Terminal-Information AVP. • UnauthenticatedIMSI—When authentication is failed, EAP-Notification is skipped. It returns unknown user error and the next request comes with IMEI from the user. • AuthenticatedIMSI—When authorization is failed, it returns Diameter-Success with the emergency information acquired from HSS. • Authenticated-AuthorizedIMSI—When both are successful, only APN-Configuration is removed and emergency information from HSS is sent.
Transport Management section	
Identity	Required; identity of the system on which Diameter application is running. Must be set to a valid resolvable string.
BindingAddress	Local IPv4/IPv6 address the server will use for outbound connections. This should be used if the host has a virtual IP address or when the host has multiple addresses to assure the correct address is used for these connections. If the configured address is not available at the time when an outbound connection is initiated, the connection fails and the server retries to connect periodically. Ensure that the correct address is configured. **Note** You can only configure this to be an IPv4 or IPv6 address, not both.
Realm	Required; must be set to a valid Realm in the domain.
EnableIPV6	Required; if set to TRUE it enables IPV6 for the Diameter application.
ValidateIncomingMessages	Check the box to validate incoming messages.
ValidateOutgoingMessages	Check the box to validate outgoing messages.

Table 2-27 General Diameter Properties (continued)

Fields	Description
MaximumNumberofDiameterPackets	Required; the maximum number of Diameter packets that can be processed. Following features are supported for Diameter transactions based on the input queue value set in this field: • Queue-based Throttling; see Queue-Based Throttling Support, page 4-32 for more details. • Preallocation of Memory; see Support for Preallocation of Memory, page 4-32 for more details.
DiameterPacketSize	Required; the Diameter packet size that can be processed. An incoming Diameter packet with a packet size more than the value set in this field will be dropped.

Table 2-27 General Diameter Properties (continued)

Fields	Description
SystemStatsLogFrequencyInSecs	When this is set to a non-zero value, Prime Access Registrar allows you to log the following statistics for the configured duration: • CPU Utilization • Memory Utilization • NFSIOstats • Peak Worker Thread Queue / sec (for reporting of All Workers Temporarily Busy warning) **Global Statistics:** • TimedOut MAR/SAR/UDR • Throttled Packets Count • PacketsInUse Count • DEA EAP Multi-Round Auth Success Responses • DER Challenge Requests Count • DuplicateSessionID Packets Count • TimerQueue Entries Count **Per Connection Statistics:** • TimedOut MAR/SAR/UDR • Throttled Packets Count • Dropped DuplicateSessionID Packets Count • Dropped Outgoing Responses for STA/AAA/DEA • Dropped Incoming Responses for MAA/SAA/UDA/CEA/DWA • Incoming Requests per Second • Outgoing Requests per Second, • Retransmitted Requests per Second • Incoming Responses per Second • Outgoing Responses per Second By default this value is set to zero. The system statistics are saved in the system_stats_log file.

Table 2-27 General Diameter Properties (continued)

Fields	Description
ThrottlingMonitorFrequencyInSecs	Prime Access Registrar monitors whether traffic is throttled every second over the configured interval. If throttling occurs for at least half of the configured seconds, a throttling trap is sent from Prime Access Registrar. E.g. if the configured value is 60 seconds, and throttling occurs for at least 30 seconds during the configured period of 60 seconds, then throttling trap is sent from Prime Access Registrar. When no throttling occurs during the entire interval, a throttling reset trap is sent. By default, this value is set to zero (0), which indicates that throttling trap functionality is disabled and throttling traps should not flow even if throttling conditions are met. The minimum non-zero value that can be configured is 20. For details about the relevant traps, refer to SNMP Traps, page 15-3.
EnablePreeemptiveRecovery	If checked (TRUE), this indicates that preemptive recovery feature is enabled for Prime Access Registrar. By default, this is disabled. Preemptive recovery enables the automatic recovery of Prime Access Registrar when it enters into a presumed un-recoverable state. When this is enabled and the presumed unrecoverable state is detected, Prime Access Registrar sends a **PreemptiveRecoveryTrap** and restarts the RADIUS process. For details about the trap, refer to SNMP Traps, page 15-3.
MinDEA1Threshold	Indicates the minimum number of DEA EAP-AKA Multi-Round Auth (DEA1) responses sent over the past 120 seconds, that will kick off the preemptive recovery condition check. This is available only if **EnablePreeemptiveRecovery** is TRUE. Default value is 5000.
WatchdogTimeout	Required; specifies the time interval between watch dog messages.
ReserveDiameterPacketPool	Percentage of the Diameter packet pool to reserve for the Diameter remote server responses.
TCPListenPort	Required; port number on which the Prime Access Registrar server listens for TCP peer connections.
SCTPListenPort	Required; port number on which the Prime Access Registrar server listens for SCTP peer connections.
ReconnectInterval	Required; specifies the time interval between which Prime Access Registrar server attempts to connect to a disconnected peer. If set to 0, then no attempt will be made to connect to a disconnected peer.

Table 2-27 General Diameter Properties (continued)

Fields	Description
MaxReconnections	Required; specifies the number of times Prime Access Registrar server tries to make a reconnection attempt. If set to 0, then no attempt will be made to reconnect.
RequestRetransmissionInterval	Required; the time for which retransmission of pending requests will be done. If set to 0, then no attempt will be made to retransmit.
MaxRequestRetransmissionCount	Required, maximum number of times Prime Access Registrar server tries to retransmit a pending request. If set to 0, then no attempt will be made to retransmit.
Receive BufferSize	Required; initial size of buffer that is preallocated for message reception.
SCTPOptions Section	
MaxInitRetry	Maximum number of retries for INIT message to open a connection. Valid range is 0 - 255. Set to 0 to retry indefinitely.
MaxInboundStream	Maximum number of incoming streams per connection. Valid range is 1 - 65545.
MaxOutboundstream	Maximum number of outgoing streams per connection. Valid range is 1 - 65545.
HeartbeatInterval	Default heartbeat interval for a connection.
EnableHeartbeat	Indicates whether to enable or disable heartbeat to monitor the connections and allow earlier detection of loss connections.
AdvertisedHostName	Optional, specifies the local hostname address that will be advertised by the Prime Access Registrar server to other peers during CER/CEA exchange. For example: AdvertisedHostNames = toby-ar1.cisco.com

Setting Up the General Diameter Parameters

To set up the general Diameter parameters:

Step 1 Choose **Configuration** > **Diameter > General**. The General Diameter page is displayed.

Step 2 Specify the required details.

Step 3 Click **Set** to save the specified details.

On successful creation of the general Diameter parameters, a success message is displayed else a respective error message is displayed.

Session Management

Diameter Base protocol stack provides the functionality of Session Management. Base Stack maintains sessions separately for authentication and accounting messages. Session-Id AVP is used to identify the user session.

Table 2-28 lists and describes the fields in the Session Management page.

Table 2-28 Session Management Properties

Fields	Description
Session Management section	
MaxNumberOfSessions	Required; specifies the maximum number of concurrent Diameter sessions the Prime Access Registrar server will maintain. These sessions include both Auth and Acct sessions.
AuthSessions section	
EnableStatefulSessions	If set to TRUE, the server will enforce stateful sessions and the client will hint for stateful sessions. Default Value is TRUE. Set the property to FALSE to disable stateful sessions.
AuthSessionTimeout	Required; specifies the timeout in seconds before a session requires reauthentication.
LifeTimeTimeout	Required; specifies the timeout in seconds before a session is terminated regardless of whether the session has been re-authenticated.
GracePeriodTimeout	Required; specifies the grace period after the life timeout and before the full termination of the session.
AbortRetryTimeout	Required; specifies the timeout between the subsequent Abort Session Request (ASR) messages if the initial attempt fails.
AcctSessions section	
AcctSessionTimeout	Required; specifies the timeout in seconds before a session requires reauthentication.
InterimInterval	Required; specifies the interim interval dictated to the client if the entity is a server or hint to the server if the entity is a client.
RealTime	Required; RealTime value dictated to the client.

Setting Session Management Properties

To set up the session management properties:

Step 1 Choose **Configuration > Diameter>SessionManagement**. The Session Management page is displayed.

Step 2 Enter the required details and click **Set**.

On successful creation of the parameters, a success message is displayed else a respective error message is displayed.

Applications

A Diameter application is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 6733). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs.

When you click the Add button in the Applications page, the Application Details page is displayed. Table 2-29 lists and describes the fields in the Application Details page.

Table 2-29 Diameter Application Properties

Fields	Description
Name	Required; name of the application.
Description	Optional; description of the application.
VendorSpecific	Required; the default is FALSE. If set to FALSE, the application is ordinary application and user is prompted to enter the ApplicationID. If set to TRUE, the application is a VendorSpecific Application. User is prompted to enter VendorSpecificApplicationID and VendorID.
AuthApplication	Required; if set to TRUE the application represents AuthApplication else it represents Accounting Application.
ApplicationURI	Optional; specifies the URI of the Application. Eg: "ftp://ftp.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-12.txt"
ApplicationID	Required; specifies the unique integer value for the application. The following are examples of Diameter application: NASREQ 1 Mobile-IP 2 Diameter Base Accounting 3 **Note** ApplicationURI property must be set to 0 for Base Protocol.
VendorSpecificApplicationID	Required; specifies the integer value for the vendor specific application.

Table 2-29 Diameter Application Properties (continued)

Fields	Description
VendorID	Required; specifies the VendorID for the application. Example: DIAMETER 3GPP Cx APPLICATION VendorSpecificApplicationID 16777216 VendorID 10415
Commands	Required; an indexed list from 1 to <n>. Each entry in the list is the name of the command. It specifies the list of commands associated with the application. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.

You can use the Applications page for the following:

- Filtering Records
- Adding Diameter Application Details
- Commands
- Editing Records
- Deleting Records

Adding Diameter Application Details

To add new Diameter application details:

Step 1 Choose **Configuration** > **Diameter > Applications**. The Applications page is displayed.

Step 2 Click **Add**. The Application Details page is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Add Application** to save the specified details in the Application Details page. Otherwise click **Cancel** to return to the Applications page without saving the details.

On successful creation of the Applications details, a success message is displayed else a respective error message is displayed.

Commands

Each command in Diameter is associated with a command code. The command can be a request command or an answer command which is identified by the 'R' bit in the Command Flags field of the Diameter header.

When you click the Add button in the commands page, the Command Details page is displayed. Table 2-30 lists and describes the fields in the Command Details page.

Table 2-30 Diameter Commands Properties

Fields	Description
Name	Required; name of the command.
Description	Optional; description of the command.
Command Code	Required; specifies the integer code of the command.
EnableProxyBit	Required; default is TRUE. When enabled it represents the message is proxiable.
RequestFixed tab	Defines the fixed position of AVP in a request message.
RequestRequired tab	The AVP must be present and can appear anywhere in the request message.
RequestOptional tab	The AVP name in optional cannot evaluate to any avp name which is included in a fixed or required directory. The avp can appear anywhere in the request message.
AnswerFixed tab	Defines the fixed position of AVP in the answer message.
AnswerRequired tab	The AVP must present and can appear anywhere in the answer message.
AnswerOptional tab	The AVP name in optional cannot evaluate to any avp name which is included in a fixed or required directory. The avp can appear anywhere in the answer message.

You can click the Add button in the Command Details page to add the AVP details. Table 2-31 lists and describes the fields displayed on clicking the **Add** button.

Table 2-31 Request/Answer Msg AVP Properties

Fields	Description
Name	Required; name of the AVP.
Description	Optional; description of the AVP.
Min	Specifies the minimum number of times AVP element may be present in a request. The default value is 0.
Max	Specifies the maximum number of times the element may present in a request. A value of zero implies AVP is not present in the request.

Adding Diameter Commands

To add the Diameter commands:

Step 1 Choose **Configuration** > **Diameter > Commands**. The Commands page is displayed.

Step 2 Click **Add**. The Add Commands page is displayed.

Step 3 Enter the relevant details.

Step 4 Click the required tab and click **Add** to enter the AVP details.

Step 5 Click **Save** to save the AVP details or click **Cancel** to exit the page without saving the details.

Step 6 Click **Add Command** to save the specified details in the Add Commands page. Otherwise click **Cancel** to return to the Commands page without saving the details.

The Commands page is displayed with the newly added details or a respective error message is displayed.

DiameterAttributes

You can define the attributes to use in the Diameter EAP application.

Table 2-32 lists and describes the fields in the DiameterAttributes page.

Table 2-32 Diameter Attributes Properties

Fields	Description
Name	Required; name of the attribute.
Description	Optional; description of the attribute.
Attribute	Required; attribute value.
VendorID	Required; Vendor ID of the Diameter application.
Mandatory	Indicates whether the attribute is mandatory or not. Options are May, Must, and MustNot.
May-Encrypt	Choose **Yes** or **No** to indicate whether the attribute value can be encrypted or not.
Protected	Indicates whether the attribute value is protected or not. Options are May, Must, and MustNot.
Type	Choose the type of the attribute.
Minimum	Minimum value for the attribute.
Maximum	Maximum value for the attribute.

Adding Diameter Attributes

To add the Diameter attributes:

Step 1 Choose **Configuration** > **Diameter > DiameterAttributes**. The DiameterAttributes page is displayed.

Step 2 Click **Add**.

Step 3 Provide the relevant details as explained in Table 2-32.

Step 4 Click **Add DiameterAttributes** to save the specified details. Otherwise click **Cancel** to return to the previous page without saving the details.

The DiameterAttributes page is displayed with the newly added details or a respective error message is displayed.

Advanced

Advanced objects allow configuring system-level properties and the Attribute dictionary. Under normal system operation, the system-level properties should not be changed.

The following list helps you in defining the system-level properties and attribute dictionary:

- Default
- BackingStore/ServerParam
- RemoteSessionServer
- SNMP and Server Monitor
- DDNS
- Encrypted IMSI Private Keys
- ODBC DataSources
- Log
- Ports
- Interfaces
- Attribute Groups
- DOIC Priorities
- Health Monitor

Default

This feature of GUI allows you in configuring the default values for other functionalists of GUI. The configurations set in this feature reflects on all the other features.

Table 2-33 lists and describes the fields in the Default Advanced Details page.

Table 2-33 Default Configuration Details

Fields	Description
Default section	
AAAFileServiceSyncInterval	Required; specified in milliseconds, the default is 75. This property governs how often the file AAA service processes accounting requests and writes the accounting records to the file. You can lower the number to reduce the delay in acknowledging the **Account-Request** at the expense of more frequent flushing of the accounting file to disk. You can raise the number to reduce the cost of flushing to disk, at the expense of increasing the delays in acknowledging the **Accounting-Request**s. The default value was determined to provide a reasonable compromise between the two alternatives.
RemoteRadiusServerInterface	When set, specifies the local interface to bind to when creating the RemoteRadiusServer socket. If not set, the Prime Access Registrar binds to IPADDR_ANY.

Table 2-33 Default Configuration Details (continued)

Fields	Description
MaximumNumberOfXML-Packets	Required when using identity caching. Indicates the maximum number of XML packets to be sent or received. The minimum value is 1 and the maximum is a 32-bit unsigned integer. The default is 1024.
MaximumODBCResultSize	Required; specifies maximum size in bytes for an ODBC mapping. This parameter affects both ODBC result sizes and the trace log buffer for tracing script calls that access any of the dictionaries. (Default value is 256.)
XMLUDPPacketSize	Required when using identity caching. Indicates the maximum size of XML packets to be sent or received. The minimum value is 1 and the maximum is a 32-bit unsigned integer. The default is 4096.
InitialBackgroundTimerSleepTime	Required; the default is 5. This property specifies the amount of time the time queue should initially sleep before beginning processing. This property is only used for initial synchronization and should not be changed.
RemoteLDAPServerThread-TimerInterval	Required; specified in milliseconds, the default is 10. This property governs how often the ldap RemoteServer thread checks to see if any results have arrived from the remote LDAP server. You can modify it to improve the throughput of the server when it proxies requests to a remote LDAP server.
AdvancedDuplicateDetectionMemoryInterval	Required when the Advanced Duplicate Detection feature is enabled. This property specifies how long (in milliseconds) Cisco Prime Access Registrar should remember a request. You must specify a number greater than zero. The default is 10,000.
RollingEncryptionKey-ChangePeriod	Used in conjunction with the session-cache ResourceManager, this property specifies the length of time a given EncryptionKey will be used before a new one is created. When the session-cache Resource-Manager caches User-Password attributes, Prime Access Registrar encrypts the User-Password so it is not stored in memory or persisted on disk in clear text. Prime Access Registrar uses up to 255 encryption keys, using a new one after each RollingEncryptionKeyChange-Period expires. If RollingEncryptionKeyChangePeriod is set to *2 days*, Prime Access Registrar will create and begin using a new EncryptionKey every two days. The oldest key will be retired, and Prime Access Registrar will re-encrypt any User-Passwords that used the old key with the new key. This way, if the RollingEncryptionKey-ChangePeriod is set to *1 day*, no key will be older than 255 days.
DefaultReturnedSubnetSizeIfNoMatch	Optional; used with the ODAP feature and reflects the returned size of the subnet if no matched subnet is found. There are three options to select if an exactly matched subnet does not exist: Bigger, Smaller, and Exact. The default is Bigger.
ODBCEnvironmentMultiValueDelimiter	Optional; allows you to specify a character that separates multivalued attributes in the marker list when using ODBC accounting

Table 2-33 Default Configuration Details (continued)

Fields	Description
RemoteSigtranServerThread-TimerInterval	Required; specified in milliseconds, the default is 10. This property governs how often the sigtran RemoteServer thread checks to see if any results have arrived from the remote HLR/AuC server. You can modify it to improve the throughput of the server when it proxies requests to a remote sigtran server.
AdditionalNativeOracleErrors	Optional; 5 digit Oracle native error in order to disconnect the ODBC/OCI remote servers.
EnableLengthFlag	Check this box to enable the length flag.
FlushDiskInBackground	Check this box to allow Prime Access Registrar to flush the accounting record to disk before it acknowledges the request packets.
InitialSessionBufferSize	Indicates the estimated session capacity, which the particular Prime Access Registrar instance can hold. This indicates the average or estimated value and not the maximum capacity. Setting this to a larger value impacts the startup performance. With this enhancement, Prime Access Registrar session containers are initialized to hold the number of sessions based on the configured parameter value. Setting this value to zero, will disable preallocation and enable on-demand growth of the container.
EnableDuplicateSessionId-Detection	Prime Access Registrar can detect duplicate authentication requests based on UE session ID. If any diameter request packet has a Session ID same as that of a packet that is already being processed, the new request is silently dropped/ignored from processing. By default, this parameter is enabled. This enhancement is primarily provided so that the server does not respond with a 3004 (Diameter Too Busy) status for a request that is already in progress; instead drop the duplicate request packet silently.
SendOpCodeInISDResponse	Check this box to send operator code in the ISD response.
EnableRoutingContextInM3UA	Check this box to enable routing context in M3UA.
DefaultRadiusSharedSecret	Enter the default shared secret for RADIUS server.
ReserveRADIUSPacketPool	Percentage of the RADIUS packet pool to reserve for the RADIUS remote server responses.
TLSv1Enabled	Applicable only for Diameter; Set to TRUE to use TLS version 1.0 and above for Diameter connection. Set to FALSE to use TLS version greater than 1.0 for Diameter connection.

Table 2-33 Default Configuration Details (continued)

Fields	Description
EnableLocationCapability	Check the box to enable location-based attributes within RADIUS and Diameter that can be used to convey location-related information for authentication and accounting exchanges. If this option is enabled, Prime Access Registrar retrieves the location information from the client and processes the incoming packet for AA services. For more information on location information delivery flows, refer to RFC 5580. For information on location-based attributes in Prime Access Registrar, see the “Environment Dictionary” chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide*.
DisplayUserForFailedLogin	Prime Access Registrar provides an option to capture the username as part of the aregcmd_log during login failures. If this option is enabled, during login failures, username is captured along with the failure reason as part of the aregcmd_log.
DiameterSessionRestorationPurgeTime	The time at which Prime Access Registrar must run the Diameter session restoration process. Format is HH:MM:SS (24 hrs format) and default value is 02:00:00. Recommended time is when the incoming traffic is minimal. **Note** This time should always be two hours behind the Diameter stale session purge time.
DiameterStaleSessionPurgeTime	The time at which Prime Access Registrar must check for Diameter stale sessions. Format is HH:MM:SS (24 hrs format) and default value is 00:00:00. Recommended time is when the incoming traffic is minimal.
SocketWaitTime	Fixed wait time for receiving socket data.
ServerStatusSharedSecret	The shared secret for the RADIUS remote server status.
UserLogDelimiter	Delimiter value to be used for the user/subscriber log data.
DiameterStaleConnectionDeletionTimeout	The timeout value in milliseconds, after which Prime Access Registrar deletes the Diameter stale peer connections. Default value is 300000.
EnableDNAAA	Check this box to enable 5G DNAAA RADIUS and Diameter protocol compliance. Uncheck for backward compatibility to disable this feature.
DiameterStaleSessionPurgeFrequency	The interval at which Prime Access Registrar must check for Diameter stale sessions.

Table 2-33 Default Configuration Details (continued)

Fields	Description
LDAPMultiValDelimiter	Delimiter to use for LDAP multi-value attributes. LDAP attributes mapping support has been enhanced to accommodate multiple values to get mapped with the information fetched from LDAP. The LDAP query returns multi-value attributes in LDAP Authentication services. These will get mapped to corresponding attributes based on the LDAPToEnvironmentMappings. E.g. the parameter Data under LDAPToEnvironmentMappings is mapped to two values NAS-Identifier and Reply-Message using a supported delimiter configured in this field. The default delimiter is comma (,).
LDAPTLSVersion	Supported TLS versions for the LDAP server, which could be TLSv1.1, TLSv1.2, or TLSv1.3. Default is TLSv1.2. Any changes to this parameter requires at least a reload of Prime Access Registrar.

Table 2-33 Default Configuration Details (continued)

Fields	Description
AR Flags section	
HideSharedSecretAndPrivateKeys	Optional; the default value is TRUE. The HideSharedSecretAndPrivateKeys property hides: • The secret that is shared between a RADIUS Client and a RADIUS Server or between two RADIUS servers in a RADIUS proxy scenario. • The PrivateKeyPassword under the certificate-based EAP services. When this property is set to TRUE, the following properties are displayed as <encrypted>: • PrivateKeyPasswords in: – peap-v0 service – peap-v1 service – eap-tls service – eap-ttls service • SharedSecret in: – RemoteServers of type RADIUS – RemoteServers of type map-gateway – Clients object – Resource Manager of type usr-vpn under Gateway subobject • PseudonymSecret in eap-sim service • DynamicAuthSecret under DynamicAuthorizationServer subject in Clients object • RepSecret under Replication • Secret in /radius/advanced/DDNS/TSIGKeys When the value for this property is set to FALSE, all the above properties are displayed in clear text.
ListenForDynamicAuthorizationRequests	Must be set to TRUE when using the Change of Authorization (CoA) feature or Packet of Disconnect (POD) feature. Default is FALSE.
RequireNASsBehindProxyBeInClientList	Optional; the default is FALSE. If you accept the default, Cisco Prime Access Registrar only uses the source IP address to identify the immediate client that sent the request. Leaving it FALSE is useful when this RADIUS Server should only know about the proxy server and should treat requests as if they came from the proxy server. This might be the case with some environments that buy bulk dial service from a third party and thus do not need to, or are unable to, list all of the NASs behind the third party's proxy server. When you set it to TRUE, you must list all of the NASs behind the Proxy in the Clients list.

Table 2-33 Default Configuration Details (continued)

Fields	Description
UseAdvancedDuplicateDetection	Required; the default is FALSE. Set this property to TRUE when you want Cisco Prime Access Registrar to use a more robust duplicate request filtering algorithm.
DetectOutOfOrderAccountingPackets	Optional; used to detect accounting packets that arrive out of sequential order. The default is FALSE. This property is useful when using accounting and session management in a RADIUS proxy service. When the DetectOutOfOrderAccountingPacket property is enabled (set to TRUE), a new *Class* attribute is included in all outgoing Accept packets. The value for this Class attribute will contain the session magic number. The client will echo this value in the accounting packets, and this will be used for comparison. The session magic number is a unique number created for all sessions when the session is created or reused and the DetectOutOfOrderAccountingPacket property is set to TRUE. The DetectOutOfOrderAccountingPacket property is used to detect out-of-order Accounting-Stop packets in roaming scenarios by comparing the session magic number value in the session with the session magic number value contained in the Accounting packet. The value of 0xffffffff is considered by the Prime Access Registrar server to be a wild card magic number. If any accounting stop packets contain the value of 0xffffffff, it will pass the session magic validation even if the session's magic number is something else. The format of the class attribute is as follows: <4-byte Magic Prefix><4-byte server IP address><4-byte Magic value>
Java and EAP Parameters section	
ClasspathForJavaExtensions	A string which is the classpath to be used to locate Java classes and jar files containing the classes required for loading the Java extensions, either Java extension points or services. **Note** The classpath will always contain the directory **$INSTALLDIR/scripts/radius/java** and all of the jar files in that directory.
JavaVMOptions	A string that can contain options to be passed to the JRE upon startup. JavaVMOptions should be used only when requested by Cisco TAC.
EapBadMessagePolicy	Set to one of two values: SilentDiscard (the default) or RejectFailure. When set to SilentDiscard, the Prime Access Registrar server silently discards and ignores bad EAP messages unless the protocol specification explicitly requires a failure message. When set to RejectFailure, the Prime Access Registrar server sends RADIUS Access-Rejects messages with embedded EAP-Failure in response to bad EAP messages as described in Internet RFC 3579.

Table 2-33 Default Configuration Details (continued)

Fields	Description
CertificateDBPath	Required if you are using an LDAP RemoteServer and you want Prime Access Registrar to use SSL when communicating with that LDAP RemoteServer. This property specifies the path to the directory containing the client certificates to be used when establishing an SSL connection to an LDAP RemoteServer. This directory must contain the **cert7.db** and **cert5.db** certificates and the **key3.db** and **key.db** files database used by Netscape Navigator 3.x (and above) or the **ServerCert.db** certificate database used by Netscape 2.x servers. Any changes to this parameter requires a restart of Prime Access Registrar.
UISessionTimeoutInMins	Required; maximum value is 30 minutes. When set to a non-zero value, an administrator will be able to hold only one active session. This includes GUI, CLI, and REST API sessions. GUI or CLI session will be logged out automatically, if left inactive for the configured timeout value. After three consecutive failed login attempts, administrator will be blocked for the configured time i.e. the administrator will be able to login only after the time (in mins) mentioned in this field.

Setting Default Configuration

To set up the default configuration details:

Step 1 Choose **Configuration** > **Advanced > Default**. The Default Advanced Details page is displayed.

Step 2 Enter the relevant details.

Step 3 Click **Set** to save the specified details in the Default Advanced Details page. Otherwise, click **Reset** to restore the default values. On successful creation of the default configurations, a success message is displayed else a respective error message is displayed.

BackingStore/ServerParam

The Backing Store is a Parsing Tool which helps you in analyzing the session backing store files. It retrieves the information on RADIUS sessions, clears phantom sessions details manually and processes the binary log files information to user-readable format.

The Server parameters are set to configure objects to remote server using the relevant aregcmd commands.

Table 2-34 lists and describes the fields in the Backing/ServerParam Advanced Details page.

Table 2-34 BackingStore/ServerParameter Properties

Fields	Description
Backing Store section	
SessionBackingStoreSyncInterval	Sessions will be written to the backing store at this interval
PacketBackingStoreSyncInterval	The minimum value is 1 and the maximum is a 32-bit unsigned integer. The default is 75.
SessionBackingStorePruneInterval	Required; specifies the sleep time interval of the session backing store pruning thread. The recommended and default value is 6 hours, but you can modify this based on the traffic patterns you experience. With SessionBackingStorePruneInterval set to 6 hours, pruning will occur 6 hours after you restart or reload the Prime Access Registrar server and recur every 6 hours. You can set a very low value for this property to make pruning continuous, but there might not be enough data accumulated for the pruning to occur and pruning might be less effective compared to the default setting.
PacketBackingStorePruneInterval	Required; specifies the sleep time interval of the packet backing store pruning thread. The recommended value is 6 hours, but you can modify this based on the traffic patterns you experience. When PacketBackingStorePruneInterval is set to 6 hours, pruning will occur 6 hours after you restart or reload the Prime Access Registrar server and recur every 6 hours. You can set a very low value for this property to make pruning continuous, but there might not be enough data accumulated for the pruning to occur and pruning might be less effective compared to the default setting.
BackingStoreDiscThreshold	Required; the default is 10 gigabytes. The value of BackingStoreDisc- Threshold is made up of a number of units which can be K, kilobyte, or kilobytes, M, megabyte, or megabytes, or G, gigabyte, or gigabytes. BackingStoreDiscThreshold is used with session management and ODBC accounting and ensures that any data log files generated will not cross the BackingStoreDiscThreshold.

Table 2-34 BackingStore/ServerParameter Properties (continued)

Fields	Description
SessionPurgeInterval	Optional; the SessionPurgeInterval property determines the time interval at which to check for timed-out sessions. If no value is set, the session timeout feature is disabled. The checks are performed in the background when system resources are available, so checks might not always occur at the exact time set. The minimum recommended value for SessionPurgeInterval is 60 minutes. The SessionPurgeInterval value is comprised of a number and a units indicator, as in n units, where a unit is one of minutes, hours, days, or weeks.
StaleSessionTimeout	Required; the default value is “1 hour.” Specifies the time interval to maintain a session when a client does not respond to Accounting-Stop notification. When the Prime Access Registrar server does not receive an Accounting-Response from a client after sending an Accounting-Stop packet, Prime Access Registrar maintains the session for the time interval configured in this property before releasing the session. This property is stored as a string composed of two parts: a number and a unit indicator (<n> <units>) similar to the MaxFileAge property where the unit is one of: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, or Weeks.
NumberOfRadiusIdentifiersPerSocket	This represents the number of RADIUS Identifiers that Prime Access Registrar can use per source port, while proxying requests to remote servers. To use a different source port for every request that is proxied, you need to set the value of this property to one.
EnableStickySessionCount	Required; either True or False and the default value is True. When set to True, Prime Access Registrar displays the peer specific stats showing the number of sticky sessions associated with a peer for Diameter proxy service in name_radius_log file.
StickySessionCountInterval	Required; specified in milliseconds and the default is 60000. When the EnableStickySessionCount is set to True, this field specifies how often the Diameter proxy service will display the number of sticky sessions associated with a peer.
StickySessionSyncInterval	Required; specified in milliseconds and the default value is 500. Specifies how often the Diameter proxy service will write the sticky sessions to a file located in /cisco-ar/temp/__sticky_sessions_store location.

Table 2-34 BackingStore/ServerParameter Properties (continued)

Fields	Description
Server Parameters section	
MaximumNumberOfRadiusPackets	Required; the default is 8192. This is a critical property you should set high enough to allow for the maximum number of simultaneous requests. When more requests come in than there are packets allocated, Cisco Prime Access Registrar will drop those additional requests.
NumberOfRemoteUDPServerSocket	Required; the default value for this property is 4. The NumberOfRemoteUDPServerSockets property allows you to configure the number of source ports used while proxying requests to a remote RADIUS server. If the NumberOfRemoteUDPServerSockets property is set to a value *n*, all remote servers share and use *n* sockets. The NumberOfRemoteUDPServerSockets value comprises a number, as in *n*, where *n* should be less than or equal to the current process file descriptor limit divided by 4. **Note** By default, the RADIUS process supports up to 1024 file descriptors. To increase the file descriptors, stop the arserver; in the arserver script, specify the required value to "NUMBER_OF_FILE_DESCRIPTORS" and restart the server. The value for "NUMBER_OF_FILE_DESCRIPTORS" should be in the range between 1024 to 65535.
MemoryLimitForRadiusProcess	This property is used to avoid crashing of the RADIUS process. The default value is 3500 Megabytes. This property is under **/radius/advanced**. When the RADIUS process uses memory more than the configured limit, further sessions are not created and Prime Access Registrar rejects further incoming requests.
MemorySizeCheckInterval	This property is used to avoid crashing of the RADIUS process. This is used in conjunction with **MemoryLimitForRadiusProcess**. The default value is 5 minutes. **MemorySizeCheckInterval** is a hidden parameter in mcd database. To modify the default value, you need to export the mcd database. Typically, a separate thread is created to monitor the RADIUS process memory usage for every 5 minutes.
UDPPacketSize	Required; the default is 4096. RFC 2138 specifies the maximum packet length can be 4096 bytes. Do not change this value.

Table 2-34 BackingStore/ServerParameter Properties (continued)

Fields	Description
PerPacketHeapSize	Required; the default is 6500. This property sets the size of the initial heap for each packet. The heap is the dynamic memory a request can use during its lifetime. By preallocating the heap size at the beginning of request processing, we can minimize the cost of memory allocations. If PerPacketHeapSize is too low, Prime Access Registrar will ask the system for memory more often. If PerPacketHeapSize is too high, Prime Access Registrar will allocate too much memory for the request causing the system to use more memory than required.
MinimumSocketBufferSize	Required; the default is 65536 (64 K). This property governs how deep the system's buffer size is for queueing UDP datagrams until Cisco Prime Access Registrar can read and process them. The default is probably sufficient for most sites. You can, however, raise or lower it as necessary.
MaximumOutstandingRequests	Optional; the default value for this property is 0. The MaximumOutstandingRequests property is used to limit the incoming traffic in terms of "requests processed". Serves as a hard limit. The MaximumOutstandingRequests property comprises a number *n*, where *n* can be any nonzero value.
MaximumIncomingRequests	Optional; the default value for this property is 0.
ARIsCaseInsensitive	When set to FALSE, requires that you provide exact pathnames with regard to upper and lower case for all objects, subobjects, and properties. The default setting, TRUE, allows you to enter paths such as **/rad/serv** instead of **/Rad/Serv**. **Note** Prime Access Registrar always authenticates the RADIUS attribute User-Name with regard to upper and lower case, regardless of the setting of this flag.
EnableDiameter	Optional; Either TRUE or FALSE; default is TRUE. Set to True when you want to use the Diameter protocol in Prime Access Registrar.
KeyStores This section is available for each of the following EAP services: • EAP-SIM • EAP-SIM-3GPP • EAP-AKA • EAP-AKA-3GPP • EAP-AKA-PRIME • EAP-AKA-PRIME-3GPP	

Table 2-34 BackingStore/ServerParameter Properties (continued)

Fields	Description
NumberOfKeys	Maximum number of keys stored for generating pseudonym secrets. Value can be from 1 till 1024.
RolloverPeriod	Duration between key updates. Default is 1 week. In case of rolling encryption, this denotes the duration for which a key is active, after which the key is expired and the next key is considered as an active key for pseudonym generation. For more information on rolling encryption, see Rolling Encryption Support for Pseudonym Generation in EAP-SIM, EAP-AKA, and EAP-AKA' Services, page 5-50.

Setting Server Parameters

To set up new server parameters:

Step 1 Choose **Configuration** > **Advanced > Backing/ServerParam**. The Backing/ServerParam Advanced Details page is displayed.

Step 2 Specify the relevant details.

Step 3 Click **Set** to save the specified details in the Backing/ServerParamAdvanced Details page.

On successful creation of the server parameters, a success message is displayed else a respective error message is displayed.

RemoteSessionServer

Prime Access Registrar sessions can also be stored on a remote database. This improves the overall scalability of the number of sessions that Prime Access Registrar can simultaneously handle.

The remote session manager internally uses the following two ODBC remote servers:

- Internal-ODBC-Read-Server
- Internal-ODBC-Write-Server

Configurations pertaining to these internal remote servers can be done under the RemoteSessionServer section.

Note Ensure that the length of fields such as Username, Session/Resource Manager name Session-Key, Query-Key and so on are limited to the value specified in the schema, while it is configured. Although the field length of entire session record is 3KB it is limited to 2KB. This is practically sufficient to hold all the session parameters as well as the cached attributes (if any). For more information about the schema, see Remote Session Management, page 9-57.

Note Remote session manager will work only with Oracle database.

Table 2-35 lists and describes the fields in the RemoteSessionServer Advanced Details page.

Table 2-35 RemoteSessionServer Properties

Fields	Description
RemoteSessionServer section	
ReactivateTimerInterval	Mandatory time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms.
Timeout	Mandatory time interval (in seconds) to wait for SQL operation to complete; defaults to 15 seconds
DataSourceConnections	Mandatory number of connections to be established; defaults to 8
ODBCDataSource	Name of the ODBCDataSource to use and must refer to one entry in the list of ODBC datasources configured under **/Radius/Advanced/ODBCDataSources**. Mandatory; no default.
KeepAliveTimerInterval	Mandatory time interval (in milliseconds) to send a keepalive to keep the idle connection active; defaults to zero (0) meaning the option is disabled
MaximumBufferFileSize	Mandatory if BufferAccountingPackets is set to TRUE, determines the maximum buffer file size, defaults to 10 Megabyte)
CacheLimit	Default is 250000; This represents the overall limit on cache of all 'remote' session managers. This value is interpreted as the maximum number of packets that can be present in cache. When the number of sessions hits this limit, sessions will be 'cached out'. This cache out operation will continue, until the cache is at least 20% free.
BufferAccountingPackets	Mandatory, TRUE or FALSE, determines whether to buffer the accounting packets to local file, defaults to TRUE which means that packet buffering is enabled. **Note** When set to TRUE, a constant flow of incoming accounting packets can fill the buffer backing store files in **/cisco-ar/data/odbc** beyond the size configured in MaximumBufferFileSize. Configure BackingStoreDiscThreshold in **/Radius/Advanced** when using ODBC accounting.
UseCacheIndex	Mandatory; If set to 1, it enables a fast cache based lookup index for the items in the database. This optimizes the number of queries to the database hence will improve performance, but limits the number of sessions that can be scaled. If set to 0, it disables fast cache based lookup index.
OCITimeOutCount	Required; continuous timeout count to disconnect the selected connection. Default value is 10.

Table 2-35 RemoteSessionServer Properties (continued)

Fields	Description
OCIConnectionReactivation-Interval	Required; time interval for attempting to reconnect the disconnected OCI remote server session. Default value is 3000 ms.
OCIActiveConnection-ThresholdCount	Required; threshold count of disconnections after which Prime Access Registrar will mark the remote server as down and try to reactivate it. Default value is 4.

Setting RemoteSessionServer Details

To set a new RemoteSessionServer details:

Step 1 Choose **Configuration** > **Advanced > RemoteSessionServer**. The RemoteSessionServer Advanced Details page appears.

Step 2 Specify the relevant details.

Step 3 Click **Set** to save the specified details in the RemoteSessionServer Advanced Details page.

On successful creation of the RemoteSessionServer details, a success message is displayed else a respective error message is displayed.

SNMP and Server Monitor

Prime Access Registrar provides SNMP MIB for users of network management systems. The supported MIBs enable the network management station to collect state and statistic information from a Prime Access Registrar server. It enables a standard SNMP management station to check the current state of the server as well as the statistics on each client or each proxy remote server. These messages contain information indicating that either the server was brought up or down or that the proxy remote server is down or has come back online.

Table 2-36 lists and describes the fields in the Advanced Details page.

Table 2-36 SNMP Properties

Fields	Description
SNMP Info section	
InputQueueHighThreshold	Percentage that indicates the upper limit of the packet input queue usage. Default is 90. Prime Access Registrar supports traps to indicate input queue usage. When the input buffer exceeds the given high threshold value, Prime Access Registrar generates a carInputQueueFull trap.

Table 2-36 SNMP Properties (continued)

Fields	Description
InputQueueLowThreshold	Percentage that indicates the lower limit of the packet input queue usage. Default is 60. After reaching the high threshold, if the buffer usage drops below a low threshold value, Prime Access Registrar generates a carInputQueueNotVeryFull trap.
DiaInputQueueHighThreshold	Percentage that indicates the maximum number of incoming Diameter packets. Default is 90. When the input buffer exceeds the given high threshold value, Prime Access Registrar generates a carDiaInputQueueFull trap.
DiaInputQueueLowThreshold	Percentage that indicates the minimum number of incoming Diameter packets. Default is 60. After reaching the high threshold, if the buffer usage drops below a low threshold value, Prime Access Registrar generates a carDiaInputQueueNotFull trap.
Enabled	Check the box to enable SNMP settings.
TracingEnabled	Check the box to enable all possible tracing in SNMP agent. Tracing is used for debugging purposes.
MasterAgentEnabled	To use SNMP, enable the master agent. Prime Access Registrar responds to SNMP queries through the SNMP master agent.
EnableDiaPacketSizeTrap	Check the box to receive carDiaPacketSizeErr trap.
RFC Compliance Info section	
AllowRejectAttrs	When AllowRejectAttrs is set to FALSE, Reply-Message attributes will not be passed in an Access Reject packet. When AllowRejectAttrs is set to TRUE, attributes will be allowed to pass in an Access Reject packet.
AllowEAPRejectAttrs	When AllowEAPRejectAttrs is set to FALSE, Reply-Message attributes will not be passed in an Access Reject packet if the packet contains EAP-Message attribute. When AllowEAPRejectAttrs is set to TRUE, attributes will be allowed to pass in an Access Reject packet even if the packet contains EAP-Message attribute.
Reply Messages section	
Default	Optional; when you set this property, Cisco Prime Access Registrar sends this value when the property corresponding to the reject reason is not set.
UnknownUser	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever Cisco Prime Access Registrar cannot find the user specified by **User-Name**.
UserNotEnabled	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever the user account is disabled.

Table 2-36 SNMP Properties (continued)

Fields	Description
UserPasswordInvalid	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever the password in the Access-Request packet did not match the password in the database.
UnableToAcquireResource	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever one of the Resource Managers was unable to allocate the resource for this request.
ServiceUnavailable	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever a service the request needs (such as a RemoteServer) is unavailable.
InternalError	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever an internal error caused the request to be rejected.
MalformedRequest	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever a required attribute (such as **User-Name**) is missing from the request.
ConfigurationError	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever the request is rejected due to a configuration error. For example, if a script sets an environment variable to the name of an object such as **Authentication-Service**, and that object does not exist in the configuration, the reason reported is ConfigurationError.
IncomingScriptFailed	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever one of the **IncomingScripts** fails to execute.
OutgoingScriptFailed	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever one of the **OutgoingScripts** fails to execute.
IncomingScriptRejectedRequest	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever one of the **IncomingScripts** rejects the Access-Request.
TerminationAction	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever Cisco Prime Access Registrar processes the Access-Request as a Termination-Action and is being rejected as a safety precaution.
OutgoingScriptRejectedRequest	Optional; when you set this property, Cisco Prime Access Registrar sends back this value in the **Reply-Message** attribute whenever one of the **OutgoingScripts** rejects the Access-Request.
Server Monitor section The following parameters enable monitoring the performance of Prime Access Registrar server.	

Table 2-36 SNMP Properties (continued)

Fields	Description
TPSHighThreshold	Absolute integer value that indicates the maximum transactions per second (TPS) value for the server. Helps monitoring the TPS capacity of the server. Default is 0. When the transactions exceed the given high threshold value, Prime Access Registrar generates a carTPSCapacityFull trap.
TPSLowThreshold	Absolute integer value that indicates the minimum TPS value for the server. Helps monitoring the TPS capacity of the server. Default is 0. After reaching the high threshold, if the TPS value drops below a low threshold value, Prime Access Registrar generates a carTPSCapacityNotFull trap.
SigtranTPSHighThreshold	Absolute integer value that indicates the maximum TPS value for SIGTRAN server. Helps to monitor the TPS capacity of the SIGTRAN server. Default is 0. When the transactions exceed the given high threshold value, Prime Access Registrar generates a carSigtranTPSCapacityFull trap.
SigtranTPSLowThreshold	Absolute integer value that indicates the minimum TPS value for the SIGTRAN server. Helps to monitor the TPS capacity of the SIGTRAN server. Default is 0. After reaching the high threshold, if the TPS value drops below a low threshold value, Prime Access Registrar generates a carSigtranTPSCapacityNotFull trap.
SMHighThreshold	Absolute integer value that indicates the maximum number of sessions that can be handled by the server. Default is 0. When the number of sessions exceeds the given high threshold value, Prime Access Registrar generates a carSessionCapacityFull trap.
SMLowThreshold	Absolute integer value that indicates the minimum number of sessions that can be handled by the server. Default is 0. After reaching the high threshold, if the number of sessions drops below a low threshold value, Prime Access Registrar generates a carSessionCapacityNotFull trap.
SigtranSMHighThreshold	Absolute integer value that indicates the maximum number of sessions that can be handled by the SIGTRAN server. Default is 0. When the number of sessions exceeds the given high threshold value, Prime Access Registrar generates a carSigtranSessionCapacityFull trap.
SigtranSMLowThreshold	Absolute integer value that indicates the minimum number of sessions that can be handled by the SIGTRAN server. Default is 0. After reaching the high threshold, if the number of sessions drops below a low threshold value, Prime Access Registrar generates a carSigtranSessionCapacityNotFull trap.
ServerMonitorLogFreqInsecs	Frequency (in seconds) of monitoring the TPS and sessions.

Setting SNMP Details

To set up new SNMP details:

Step 1 Choose **Configuration** > **Advanced > SNMP**. The SNMP Advanced Details page is displayed.

Step 2 Specify the relevant details.

Step 3 Click **Set** to save the specified details in the SNMP Advanced Details page.

On successful creation of the SNMP details, a success message is displayed else a respective error message is displayed.

DDNS

Prime Access Registrar supports Dynamic DNS Remote server. It is a method, protocol, or network that notifies the server to change the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

You can click the Add button in the DDNS Details page to enter the TSIGKeys details in the TSIGKeys Details section.

Table 2-37 lists and describes the fields in the TSIGKeys Details section.

Table 2-37 TSIGKeys Properties

Fields	Description
Name	Name of the TSIG Key.
Secret	Set to the same base64-encoded string as defined in the DNS server.
Description	Description of the TSIG Key

You can use the DDNS Details page for the following:

- Filtering Records
- Setting DDNS Details
- Adding the TSIGKeys for DDNS
- Editing Records
- Deleting Records

Setting DDNS Details

To set up new DDNS details:

Step 1 Choose **Configuration > Advanced > DDNS**. The DDNS Details page is displayed.

Step 2 Check the **SynthesizeReverseZone** check box, and click **Set DDNS**.

Adding the TSIGKeys for DDNS

To add TSIGKeys details for DDNS:

Step 1 Choose **Configuration > Advanced > DDNS**. The DDNS Details page is displayed.

Step 2 Click **Add**. The TSIGKeys details section is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Add** to save the specified details in the TSIGKeys Details section.

On successful creation of the TSIGKeys details, a success page is displayed else a respective error message is displayed.

Encrypted IMSI Private Keys

Prime Access Registrar allows you to set up private keys that can help in decrypting an encrypted IMSI from an incoming message for EAP-SIM, EAP-AKA, and EAP-AKA' services.

Table 2-38 lists and describes the fields in the **EncryptedIMSI-PrivateKeys Details** page.

Table 2-38 Encrypted IMSI-Private Key Details

Fields	Description
AllowedKeyIdentifiers	Allowed key identifier value. This is the key identifier that appears in the incoming EAP response. Click **SetAllowedKeyIdentifiers** to set the entered value as the default key identifier.
Name	Name of the private key to map to the key identifier, that can be used to decrypt the incoming encrypted IMSI.
Identifier	The key identifier value.
PrivateKey	The private key value.

Note You need to save and reload for the changes to take effect.

You can use the EncryptedIMSI-PrivateKeys Details page for the following:

- Filtering Records
- Adding Encrypted IMSI Private Keys
- Editing Records
- Deleting Records

Adding Encrypted IMSI Private Keys

To add private keys for encrypted IMSI:

Step 1 Choose **Configuration > Advanced > EncryptedIMSIPrivateKeys**. The **EncryptedIMSI-PrivateKeys** page is displayed.

Step 2 Click **Add** to add new private keys.

Step 3 Enter the relevant details.

Step 4 Click **Add** to save the specified details.

The **EncryptedIMSI-PrivateKeys** page is displayed with the newly added keys and a success message is displayed else a respective error message is displayed.

Note You need to save and reload for the changes to take effect.

ODBC DataSources

Prime Access Registrar uses ODBC as the datasource name to be used by the remote server. Multiple remote servers can use the same ODBCDataSource. Under the ODBCDataSource object definition, a list defines **ODBC.ini** filename/value pairs for a connection. The list includes a Type field and a Driver field, different for each Driver and Data Source, to indicate its Driver and Data Source. Prime Access Registrar supports only the Easysoft Open Source Oracle Driver.

Table 2-39 lists and describes the fields in the Add ODBC DataSources page.

Table 2-39 ODBCDataSource Properties

Fields	Description
Name	Name of the ODBCDataSource
Description	Optional; Description of the ODBC Data Source
Type	Required; type of the ODBC data source, which could be myodbc or oracle_oci.
Driver	Required; **liboarodbc.so** (default value) **Note** This attribute is supported only for OBDC.
UserID	Required; database username (no default value)
Password	Optional; user password; shown encrypted
DataBase	Required; Oracle Client configuration database name (no default value)
Server	Set the name of the server
Port	Set the port details.
SSLSecureTransport	Check this box to configure the MySQL server to connect over SSL.
TLSVersion	Supported TLS version for the ODBC data source, which could be Default, TLSv1.1, TLSv1.2, or TLSv1.3. Default value is TLSv1.2.
SSLCA	Path to a local file that contains a list of trusted Certificate Authorities.

Table 2-39 ODBCDataSource Properties (continued)

Fields	Description
SSLCERT	Path to a local file that contains a list of trusted SSL client certificates.
SSLKEY	Path to a local file that contains a list of trusted SSL client keys.

You can use the ODBC DataSources page for the following:

- Filtering Records
- Adding ODBC Data Source
- Log
- Editing Records
- Deleting Records

Adding ODBC Data Source

To add new ODBC data source details:

Step 1 Choose **Configuration > Advanced > ODBC DataSources**. The ODBC DataSources page is displayed.

Step 2 Click **Add** to add new ODBC data source details. The ODBC DataSources Details page is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Submit** to save the specified details. Otherwise click **Cancel** to return to the ODBC DataSources page without saving the details.

The ODBC DataSources page is displayed with the newly added details and a success message is displayed else a respective error message is displayed.

Log

The log files defined in Prime Access Registrar assist you in identifying the issues related to it. Prime Access Registrar holds sets of log files to store information relevant to server agent processes, monitoring arserver utility, execution of aregcme commands, mcd internal database details, RADIUS server processes and debug details of RADIUS request process.

Table 2-40 lists and describes the fields in the Log Files page.

Table 2-40 Log Details

Fields	Description
GUI Log Settings section	
LOG LEVEL	Select either Debug level or Error.
MaxFileSize	Set the maximum size of the log file.
Advance Details section	

Table 2-40 Log Details (continued)

Fields	Description
LogFileSize	Required; the default is 1 megabyte. This property specifies the maximum size of the RADIUS server log file. The value for the **LogFileSize** field is a string composed of two parts; a number, and a units indicator (<n> <units>) in which the unit is one of: K, kilobyte, kilobytes, M, megabyte, megabytes, G, gigabyte, or gigabytes. The **LogFileSize** property does not apply to the **config_mcd_1_log** or **agent_server_1_log** files. **Note** This does not apply to the trace log.
LogFileCount	Required; the default is 2. This property specifies the number of log files to be kept on the system. A new log file is created when the log file size reaches **LogFileCount**. The **LogFileCount** property does not apply to the **config_mcd_1_log** or **agent_server_1_log** files.
TraceFileSize	Required; the default is 1 GB. This property specifies the size of the trace files to be kept on the system. A new trace file is created when the trace file size reaches **TraceFileSize**. The value for the **TraceFileSize** field is a string composed of two parts; a number, and a units indicator (<n> <units>) in which the unit is one of: K, kilobyte, kilobytes, M, megabyte, megabytes, G, gigabyte, or gigabytes.
TraceFileCount	Required; this value can be set from 1–100, and the default is 2. This property specifies the number of trace files to maintain. A value of 1 indicates that no file rolling occurs.
LogServerActivity	Required; the default is FALSE, which means Cisco Prime Access Registrar logs all responses except Access-Accepts and Access-Challenges. Accepting the default reduces the load on the server by reducing that amount of information it must log. Note, the client is probably sending accounting requests to an accounting server, so the Access-Accept requests are being indirectly logged. When you set it to TRUE, Cisco Prime Access Registrar logs all responses to the server log file.
TraceLevel	Set the trace level.
LogTPSActivity	When set to TRUE, this property enables to log the TPS usage in a CSV file.The TPS is logged in the following format: *<mm-dd-yyyy>, <hh:mm:ss>, <tps-value>* For example, 04-01-2013, 12:00:01, 102 The default is False.
TPSLogFileCount	Required only if you check the LogTPSActivity check box; the number of TPS Sampling log files to maintain in the repository. The default value is 2.

Table 2-40 Log Details (continued)

Fields	Description
TPSLogFileNamePrefix	Required only if you check the LogTPSActivity check box; this represents the prefix of the CSV file which will be available in the logs directory of Prime Access Registrar. The following represents the CSV filename format: *<user-prefix>-<mm-dd-yyyy>*.csv tps-04-01-2013.csv
TPSSamplingPeriodInSecs	Required only if you check the LogTPSActivity check box; this represents the TPS sampling period in seconds. The minimum sampling period is set to 5. The default is 30.
EnableSIGTRANStackLogs	When set to TRUE, this property enables to log the SIGTRAN stack logs in stack.log file.
SIGTRANStackLogFileSize	Required if you check the EnableSIGTRANStackLogs check box. This property specifies the maximum size (in megabyte) of the SIGTRAN stack log file.
SIGTRANLogFileCount	Required if you check the EnableSIGTRANStackLogs check box. This value can be set from 1–100, and the default is 10. This property specifies the number of SIGTRAN log files to maintain in the repository.
LogSessionActivity	When set to TRUE, this property enables Prime Access Registrar to log the session count in the server.
SessionLogFileCount	Required only if you check the LogSessionActivity check box; the number of session log files to maintain in the repository. The default value is 2.
SessionLogFileNamePrefix	Required only if you check the LogSessionActivity check box; this represents the prefix of the session log file which will be available in the logs directory of Prime Access Registrar.
SessionSamplingPeriodIn-Secs	Required only if you check the LogSessionActivity check box; this represents the session sampling period in seconds. The minimum sampling period is set to 5. The default is 30.

You can use the Log Files page for the following:

- Filtering Records
- Viewing Log Details
- Downloading Log Details
- Setting Log Details

Viewing Log Details

To view the log files:

Step 1 Choose **Configuration > Advanced > Log**. The Log Files page is displayed.

Step 2 Choose the appropriate radio button and click **View** to view the file.

Downloading Log Details

To download the log files:

Step 1 Choose **Configuration > Advanced > Log**. The Log Files page is displayed.

Step 2 Choose the appropriate radio button and click **Download** to download the file.

Setting Log Details

To set the log details:

Step 1 Choose **Configuration > Advanced > Log**. The Log Files page is displayed.

Step 2 Enter the relevant details and click **Set** to save the specified details.

Ports

The Ports list specifies which ports to listen to for requests. When you specify a port, Prime Access Registrar makes no distinction between the port used to receive Access-Requests and the port used to receive Accounting-Requests. Either request can come in on either port.

Most NASs send Access-Requests to port 1812 and Accounting-Requests to 1813, however, Prime Access Registrar does not check.

When you do not specify any ports, Prime Access Registrar reads the /etc/services file for the ports to use for access and accounting requests. If none are defined, Prime Access Registrar uses the standard ports (1812 and 1813).

Table 2-41 lists and describes the fields in the Ports page.

Table 2-41 Port Properties

Fields	Description
Port	Required; allows you to use ports other than the default, 1812 and 1813. You can use this option to configure Prime Access Registrar to use other ports,. If you add additional ports, however, Prime Access Registrar will use the added ports and no longer use the default ports 1812 and 1813. These default ports can still be used by adding them to the list of ports to use.
Type	Set the port type.
Description	Optional; description of the port.

You can use the Ports page for the following:

- Filtering Records

- Adding Port Details
- Interfaces
- Editing Records
- Deleting Records

Adding Port Details

To add new port details:

Step 1 Choose **Configuration > Advanced > Port**. The Ports page is displayed.

Step 2 Enter the relevant details and click **Add**. The new port details will be listed in the Ports page.

Interfaces

The Interfaces list specifies the interfaces on which the RADIUS server receives and sends requests. You specify an interface by its IP address.

- When you set an IP address, Prime Access Registrar uses that interface to send and receive Access-Requests.
- When no interfaces are listed, the server performs an interface discover and uses all interfaces of the server, physical and logical (virtual).

Note The IP address format is enhanced to support both IPv4 and IPv6.

You can use the interfaces page for the following:

- Filtering Records
- Adding IP Addressing Interface
- Deleting Records

Adding IP Addressing Interface

To add a new IP address interface to define an interface:

Step 1 Choose **Configuration > Advanced > Interfaces**. The Interfaces page is displayed.

Step 2 Enter the **IP Address** and click **Add**.

The Interfaces page is displayed with the newly added details and a success message is displayed else a respective error message is displayed.

Attribute Groups

The Attributes can be grouped using Prime Access Registrar Profile object. The attributes for a particular user group can be grouped under a profile and the attributes contained in the profiles will be returned in their access-accepts.

Table 2-42 lists and describes the fields in the Attribute Groups Details page.

Table 2-42 AttributeGroups Properties

Fields	Description
Name	Name of the attribute group.
Description	Optional; description of the attribute group.
Attribute type	Select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list.
Attribute Name	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected. Click the **Add** button to save the details and list it in Attribute list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the Attribute Groups page for the following:

- Filtering Records
- Adding Attribute Group Details
- Rules
- Editing Records
- Deleting Records

Adding Attribute Group Details

To add new attribute groups details:

Step 1 Choose **Configuration > Advanced > Attributes Groups**. The Attribute Groups page is displayed.

Step 2 Click **Add** to add new attribute group details. The Attribute Group Details page is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Submit** to save the specified details in the Attribute Groups Details page. Otherwise click **Cancel** to return to the Attribute Groups page without saving the details.

The Attribute Groups page is displayed with the newly added details or a respective error message is displayed.

DOIC Priorities

Diameter Overload Indication Conveyance (DOIC) is an IETF standard for supporting dynamic overload controls between Diameter servers and Diameter clients. This allows Diameter servers to send overload reports to Diameter clients requesting reduction in traffic (throttling) for any duration of time.

This feature allows you to configure message priorities from P0 to P4 based on which the incoming request messages will be forwarded, diverted, or dropped to control the overload between the peers when under active overload conditions.

Table 2-42 lists and describes the fields in the **Priority Details** page.

Table 2-43 DOIC Priority Details

Fields	Description
Name	Name of the DOIC priority message.
Description	Optional; description of the DOIC priority message.
ApplicationID	Application ID of the DOIC priority.
CommandCodeList	Multiple command codes supported by the given application ID, separated by a comma (,). Example: 303,258,305

You can use the Attribute Groups page for the following:

- Filtering Records
- Adding Attribute Group Details
- Rules
- Editing Records
- Deleting Records

Adding DOIC Priority Details

To add new attribute groups details:

Step 1 Choose **Configuration > Advanced > DOICPriorities > Priority0 - Priority4**. The Priorities page is displayed.

Step 2 Click **Add** to add new priority details. The Priority Details page is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Submit** to save the specified details in the Priority Details page. Otherwise click **Cancel** to return to the Priorities page without saving the details.

The Priorities page is displayed with the newly added details or a respective error message is displayed.

Health Monitor

When the Prime Access Registrar Health System rule is evaluated, system health parameters are examined as a result of values exceeding the rule for a specified time interval. Prime Access Registrar supports regular health monitoring for RADIUS server. Using the enhanced health monitoring feature, you can monitor specific health parameters such as percentage of CPU utilization, percentage of memory consumption, packet buffer, peer connectivity, and so on for RADIUS and Diameter. If these parameters hit the threshold value, an alarm is triggered, and the corresponding health status is captured as part of the statistics.

Table 2-44 lists and describes the fields in the **Health Monitoring** page.

Table 2-44 Health Monitoring Details

Fields	Description
EnableHealthMonitoring	Check this box to enable health monitoring for RADIUS/Diameter in Prime Access Registrar.
CPUUtilizationWarningThreshold	Warning threshold for CPU utilization. If the CPU utilization reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
CPUUtilizationErrorThreshold	Error threshold for CPU utilization. If the CPU utilization reaches a steady state of the error threshold, an error trap is initiated.
MemoryWarningThreshold	Warning threshold for memory utilization. If the memory utilization reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
MemoryErrorThreshold	Error threshold for memory utilization. If the memory utilization reaches a steady state of the error threshold value, an error trap is initiated.
PacketsInUseWarningThreshold	Warning threshold for packet buffer. If the packet buffer reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketsInUseErrorThreshold	Error threshold for packet buffer. If the packet buffer reaches a steady state of the error threshold value, an error trap is initiated.
WorkerThreadsWarningThreshold	Warning threshold for worker threads. If the worker thread count reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
WorkerThreadsErrorThreshold	Error threshold for worker threads. If the worker thread count reaches a steady state of the error threshold value, an error trap is initiated.
PacketRejectsWarningThreshold	Warning threshold for packet rejects. If the packet reject count reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketRejectsErrorThreshold	Error threshold for packet rejects. If the packet reject count reaches a steady state of the error threshold value, an error trap is initiated.
PacketTimedOutsWarningThreshold	Warning threshold for packet timeouts. If the packet timeout count reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketTimedOutsErrorThreshold	Error threshold for packet timeouts. If the packet timeout count reaches a steady state of the error threshold value, an error trap is initiated.
PacketDropsWarningThreshold	Warning threshold for packet drops. If the packet dropout count reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketDropsErrorThreshold	Error threshold for packet drops. If the packet dropout count reaches a steady state of the error threshold value, an error trap is initiated.
PeerConnectivityWarningThreshold	Warning threshold for peer connectivity. If the peer connectivity count reaches a steady state of the warning threshold, the corresponding health is decremented and a warning trap is initiated.

Table 2-44 Health Monitoring Details

Fields	Description
PeerConnectivityError-Threshold	Error threshold for peer connectivity. If the peer connectivity count reaches a steady state of the error threshold value, an error trap is initiated.
HealthMonitorFreqInsecs	The frequency, in seconds, to monitor the health parameters.

Note All the above parameters are represented in percentage values from 0 - 100. You can choose to set up a value more than zero only for those parameters for which you wish to enable monitoring. For CPU Utilization parameter, the warning and error threshold values are configured in percentile based on the server needs.

Note When the overall health of Prime Access Registrar reaches 1 and there is no recovery even after 24 hours, an SNMP trap for recovery action is triggered. If the health is getting recovered above the steady state of the warning threshold, an SNMP reset trap is initiated. For more details about the traps, see Supported Traps, page 15-4 section of Chapter 15, "Using SNMP."

You can use the Attribute Groups page for the following:

- Filtering Records
- Adding Attribute Group Details
- Rules
- Editing Records
- Deleting Records

Rules

A Rule is a function that selects services based on all input information used by the function.

Table 2-45 lists and describes the fields in the Add Rules List page.

Table 2-45 Rule Properties

Fields	Description
General Properties tab	
Name	Required; must be unique in the Rule list.
Description	Optional; description of the rule.
Type	Required; specifies the type of the rule which can be Radius or Diameter.
Script Name	Name of the script.
Attribute Details tab These fields are displayed based on the type of the rule selected in the Type field.	

Table 2-45 Rule Properties (continued)

Fields	Description
RADIUS	Optional; set Radius, if the attribute and value need to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute and value need to be defined for Vendor.
AttributeName	Optional; based on the Attribute Type selected, the attribute name is automated. Set the relevant name for the attribute type selected.
AttributeValue	Optional; set the value for the selected attribute. Click the **Add** button to save the details and list it in Name and Value list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the Rules List page for the following:

- Filtering Records
- Setting Rules
- SessionManagers
- Editing Records
- Deleting Records

Setting Rules

To set new rules:

Step 1 Choose **Configuration > Rules**. The List of Rules page is displayed.

Step 2 Click **Add**. The Rules Details page is displayed.

Step 3 Enter the relevant details.

Step 4 Click **Submit** to save the specified details in the Rules Details page. Otherwise click **Cancel** to return to the List of Rules page without saving the details.

The List of Rules page is displayed with the newly added details or a respective error message is displayed.

SessionManagers

You can use Session Managers to track user sessions. The Session Managers monitor the flow of requests from each NAS and detect the session state. When requests come through to the Session Manager, it creates sessions, allocates resources from appropriate Resource Managers, and frees and deletes sessions when users log out.

The Session Manager enables you to allocate dynamic resources to users for the lifetime of their session. You can define one or more Session Managers and have each one manage the sessions for a particular group or company.

Note Session record size is limited by the operating system (OS) paging size (4 KB in Linux). If a request triggers creation of a session that exceeds the OS paging size, the request will be dropped and the session will not be created.

Note In this release of Prime Access Registrar, the memory capacity is enhanced to store more than 4 million active session's by storing the active session records in database server instead of storing it in the main memory. The capacity is dependent on the number of attributes that are being captured for each session.

Note If the disk partition where Prime Access Registrar stores session backing store data (usually the disk partition where Prime Access Registrar is installed, such as **/opt/CSCOar**) is full, the subsequent packets that try to create sessions will be dropped and no sessions will be created due to lack of disk space.

Session Managers use Resource Managers, which in turn, manage a pool of resources of a particular type.

Table 2-46 lists and describes the fields in the Session Manager Details page.

Table 2-46 Session Manager Properties

Fields	Description
Name	Required; must be unique in the Session Managers list.
Description	Optional description of the Session Manager.
Type	Required; set to local or remote. Local is the traditional session manager that maintains sessions in memory and has good performance. The remote session manager operates on a remote ODBC database, and its performance is highly dependent on the performance of the ODBC database.
EnableDiameter	Optional; check the box if you want to use the session manager for Diameter services.

Table 2-46 Session Manager Properties (continued)

Fields	Description

SessionKey	SessionKey property is used to set the sessionkey value for the Session Manager.
	The SessionManager checks whether the environmental variable **Session-Key** is set or not. If the environmental variable is set, the server uses it as the sessionkey. If environmental variable **Session-Key** is not set then SessionManager gets the value configured in the SessionKey property under SessionManager.
	SessionKey can be a combination of attributes separated by a colon. The values for those attributes are obtained from the RequestDictionary. If any one of the attribute that is configured for the sessionkey is not present in the RequestDictionary, Prime Access Registrar will drop the request.
	However, if **Session-Key** is not set, SessionManager uses NAS-Identifier and NAS-Port to create the sessionkey. An example configuration,
	`--> set SessionKey "User-Name:NAS-Port"`
	The following shows the sample configuration of sessionkey for Session Manager:
	`[ //localhost/Radius/SessionManagers/session-mgr-1 ]`
	`Name = session-mgr-1`
	`Description =`
	`Type = local`
	`EnableDiameter = FALSE`
	`IncomingScript =`
	`OutgoingScript =`
	`AllowAccountingStartToCreateSession = TRUE`
	`SessionTimeOut =`
	`PhantomSessionTimeOut =`
	`SessionKey =`
	`ResourceManagers/`

AllowAccountingStartTo-CreateSession	Set to TRUE by default; start the session when the Prime Access Registrar server receives an Access Accept or an Accounting-Start. When set to FALSE, start the session when the Prime Access Registrar server receives an Access Accept.
IncomingScript	Optional; name of script to run when the service starts. This script is run as soon as the session is acquired in Prime Access Registrar.
OutgoingScript	Optional; script to be run just before the session is written to backing store.

Table 2-46 Session Manager Properties (continued)

Fields	Description
SessionTimeOut	The SessionTimeOut property is optional; no value for this property means the session timeout feature is disabled. Used in conjunction with **/Radius/Advanced/SessionPurgeInterval** for the session timeout feature. Enables the session timeout feature for a Session Manager. If the SessionTimeOut property is set to a value under a session manager, all sessions that belong to that session manager will be checked for timeouts at each SessionPurgeInterval. If any sessions have timed out, they will be released, and all resources associated with those sessions are also released. The SessionTimeOut property determines the timeout for a session. If the time difference between the current time and the last update time is greater than this property's value, the session is considered to be stale. The last update time of the session is the time at which the session was created or updated. The SessionTimeOut value is comprised of a number and a units indicator, as in *n units*, where a unit is one of minutes, hours, days, or weeks. The default unit is 'days'.
PhantomSessionTimeOut	Optional; no value for this property means the phantom session timeout feature is disabled. The PhantomSessionTimeOut property is used in conjunction with **/Radius/Advanced/SessionPurgeInterval** to enable the phantom session timeout feature for Session Manager. If the PhantomSessionTimeOut property is set to a value under a session manager, all sessions that belong to that session manager will be checked for receipt of an Accounting-Start packet. Sessions that do not receive an Accounting-Start packet from creation until its timeout will be released. The PhantomSessionTimeOut value comprises a number and a units indicator, as in *n* units, where a unit is one of minutes, hours, days, or weeks. The default unit is 'days'
SessionCreationCmdList	Available only if you check the EnableDiameter check box; session created for the configured application, command code, and AVP.
SessionDeletionCmdList	Available only if you check the EnableDiameter check box; session deleted for the configured application, command code, and AVP.

Table 2-46 Session Manager Properties (continued)

Fields	Description
SessionRestorationTimeout	Determines the restoration timeout for a session. No value indicates that the session restoration feature is disabled for this session manager. Used in conjunction with **/Radius/Advanced/DiameterSessionRestorationPurgeTime**. This value comprises a number and a units indicator, as in 'n' units, where a unit could be minutes, hours, days, or weeks. The default unit is 'days'. The minimum recommended value is **24hr** or **1Day**. If this value is set for a session manager, all sessions that belong to that session manager will be checked for timeouts at DiameterSessionRestorationPurgeTime. If any session is timed out, a Re-Authorization-Request will be triggered for the timed-out session. And, if Re-Authorization-Answer comes with the Result-Code Diameter-Unknown-Session-Id, then the particular session will be released and all resources associated with the session will also be released. If the time difference between the current time and the last update time for the session is greater than this value, the session is considered to be stale and must be restored. **Note** Session restoration works only if the session manager is Diameter enabled and it has a 3GPP resource manager.
Resource Managers List	Ordered list of Resource Managers. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details.

You can use the Session Managers page for the following:

- Filtering Records
- Adding Session Manager Details
- Editing Records
- Deleting Records

Adding Session Manager Details

To add new session manager details:

Step 1 Choose **Configuration > Session Managers**. The Session Managers page is displayed.

Step 2 Click **Add**. The Session Manager Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Add** to save the specified details in the Session Manager Details page. Otherwise click **Cancel** to return to the Session Managers page without saving the details.

The Session Managers page is displayed with the newly added details or a respective error message is displayed.

ResourceManager

Resource Managers allow you to allocate dynamic resources to user sessions. The following lists the different types of Resource Managers.

- **IP-Dynamic**—manages a pool of IP addresses that allows you to dynamically allocate IP addresses from a pool of addresses
- **IP-Per-NAS-Port**—allows you to associate ports to specific IP addresses, and thus ensure each NAS port always gets the same IP address
- **IPX-Dynamic**—manages a pool of IPX network addresses
- **Subnet-Dynamic**—manages a pool of subnet addresses
- **Group-Session-Limit**—manages concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions after the configured limit has been reached
- **User-Session-Limit**—manages per-user concurrent sessions; that is, it keeps track of how many sessions each user has and denies the user a new session after the configured limit has been reached
- **Home-Agent**—manages a pool of on-demand IP addresses
- **USR-VPN**—manages Virtual Private Networks (VPNs) that use USR NAS Clients.
- **Home-Agent-IPv6**—manages a pool of on-demand IPv6 addresses
- **Remote-IP-Dynamic**—manages a pool of IP addresses that allows you to dynamically allocate IP addresses from a pool of addresses. It internally works with a remote ODBC database.
- **Remote-User-Session-Limit**—manages per-user concurrent sessions; that is, it keeps track of how many sessions each user has and denies the user a new session after the configured limit has been reached. It internally works with a remote ODBC database.
- **Remote-Group-Session-Limit**—manages concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions after the configured limit has been reached. It internally works with a remote ODBC database.
- **Session Cache**—allows you to define the RADIUS attributes to store in cache.
- **Dynamic-DNS**—manages the DNS server.
- **Remote-Session-Cache**—allows you to define the RADIUS attributes to store in cache. It should be used with session manager of type 'remote'.
- **3GPP**—allows you to define the attribute for 3GPP authorization.

Each Resource Manager is responsible for examining the request and deciding whether to allocate a resource for the user, do nothing, or cause Cisco Prime Access Registrar to reject the request.

Table 2-47 lists and describes the fields in the Resource Manager Details page.

Table 2-47 Resource Manager Properties

Fields	Description
Resource Manager Name	Required; must be unique in the Resource Managers list.

Table 2-47 Resource Manager Properties (continued)

Fields	Description
Description (optional)	Optional; description of the Resource Manager.
Type	Required; must be either **Dynamic-DNS**, **IP-Dynamic**, **IP-Per-NAS-Port**, **IPX-Dynamic**, **Session Cache, Subnet-Dynamic, Group-Session-Limit**, **Home-Agent**, **User-Session-Limit**, **USR-VPN, Home-Agent-IPv6, Remote-IP-Dynamic, Remote-User-Session-Limit, Remote-Group-Session-Limit, Remote-Session-Cache,** or **3GPP**. Based on the option selected, the fields displayed in the Resource Manager Details page varies.

The fields displayed in the Resource Manager Details page changes based on the option selected in the Type field. The following tables describe the fields in the Resource Manager Details page.

DYNAMIC-DNS

Table 2-48 lists and describes the fields in the Resource Manager Details page.

Table 2-48 DYNAMIC-DNS Properties

Fields	Description
General tab	
Max DNS TTLS	Set the maximum TTL of the DNS record.
DNS Host bytes	Set the number of bytes to be used to construct the reverse zone entry.
Forward Zone Name	Set the name of the forward zone. For a given Resource Manager you must decide which forward zone you will be updating for sessions the resource manager will manage.
Reverse Zone Name	Set the name of the reverse zone.
Forward Zone Server	Set the Server IP of the forward zone
Reverse Zone Server	Set the Server IP of the reverse zone
Forward Zone TSIG KeyS	Server-wide security key to process all forward zone dynamic DNS updates. This is used if a ForwardZoneTSIGKey was not specified on the Resource Manager.
Reverse Zone TSIG Keys	Server-wide security key to process all reverse zone dynamic DNS updates. This is used if a ReverseZoneTSIGKey was not specified on the Resource Manager

GROUP-SESSION-LIMIT

Table 2-49 lists and describes the fields in the Resource Manager Details page.

Table 2-49 GROUP-SESSION-LIMIT Properties

Fields	Description
Group Session Limit	Set the GroupSessionLimit property to the maximum number of concurrent sessions for all users.

REMOTE-GROUP-SESSION-LIMIT

Table 2-50 lists and describes the fields in the Resource Manager Details page.

Table 2-50 REMOTE-GROUP-SESSION-LIMIT Properties

Fields	Description
Group Session Limit	Set the GroupSessionLimit property to the maximum number of concurrent sessions for all users.

HOME-AGENT

Table 2-51 lists and describes the fields in the Resource Manager Details page.

Table 2-51 HOME-AGENT Properties

Fields	Description
HomeAgentIPAddresses tab	
Start	Required; must be an IP address.
End	Required; must be an IP address.

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

HOME-AGENT-IPv6

Table 2-52 lists and describes the fields in the Resource Manager Details page.

Table 2-52 HOME-AGENT-IPv6 Properties

Fields	Description
HomeAgentIPv6Addresses tab	
Start	Required; must be an IPv6 address.
End	Required; must be an IPv6 address.

Click the **Add** button to save the details and list it in Start and End IPv6 list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

IP-DYNAMIC

Table 2-53 lists and describes the fields in the Resource Manager Details page.

Table 2-53 IP-DYNAMIC Properties

Fields	Description
General tab	
Reuse IP for same SessionKey and User	When set to TRUE, this property supports overlapping IP addresses between session managers for VPN users. Default value is FALSE.
Net Mask	Required; must be set to a valid net mask.

Table 2-53 IP-DYNAMIC Properties (continued)

Fields	Description
Allow Overlapped IP Addresses	When set to TRUE, this property supports overlapping IP addresses between session managers for VPN users. Default value is FALSE.
IP Addresses tab	
Start	Required; must be an IP address.
End	Required; must be an IP address.

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

REMOTE-IP-DYNAMIC

Table 2-54 lists and describes the fields in the Resource Manager Details page.

Table 2-54 REMOTE-IP-DYNAMIC Properties

Fields	Description
General tab	
Reuse IP for same SessionKey and User	When set to TRUE, this property supports overlapping IP addresses between session managers for VPN users. Default value is FALSE.
Net Mask	Required; must be set to a valid net mask.
Allow Overlapped IP Addresses	When set to TRUE, this property supports overlapping IP addresses between session managers for VPN users. Default value is FALSE.
IP Addresses tab	
Start	Required; must be an IP address.
End	Required; must be an IP address.

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

IP-PER-NAS-PORT

Table 2-55 lists and describes the fields in the Resource Manager Details page.

Table 2-55 IP-PER-NAS-PORT Properties

Fields	Description
General tab	
Net Mask	Required; if used, must be set to a valid net mask.
Allow Overlapped IP Addresses	When set to TRUE, this property supports overlapping IP addresses between session managers for VPN users. Default value is FALSE.
NAS	Required; must be the name of a known Client.This value must be the same as the NAS-Identifier attribute in the Access-Request packet.

Table 2-55 IP-PER-NAS-PORT Properties (continued)

Fields	Description
IP Config tab	
Start	Required; must be an IP address.
End	Required; must be an IP address.
Port Config tab	
Start	Required; set the NAS port
End	Required; set the NAS port

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

IPX-DYNAMIC

Table 2-56 lists and describes the fields in the Resource Manager Details page.

Table 2-56 IPX-DYNAMIC Properties

Fields	Description
Networks tab	
Start	Required; must be an IP address.
End	Required; must be an IP address.

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

SESSION-CACHE

Table 2-57 lists and describes the fields in the Resource Manager Details page.

Table 2-57 SESSION-CACHE Properties

Fields	Description
General tab	
Overwrite Attributes	Specifies whether to overwrite the existing attributes if there are any in the session record.
Query Key	Required; set the QueryKey to the a RADIUS attribute you want to key on, such as Framed-IP-Address. A change made in Prime Access Registrar requires that this attribute not be an XML attribute, even if this session-cache resource manager is being used for an XML query. **Note** Any existing session-cache resource managers using an XML attribute for the Query Key must be changed to a RADIUS attribute that this XML attribute is mapped to under Query-Mappings.

Table 2-57 SESSION-CACHE Properties (continued)

Fields	Description
Pending Removal Delay	Required; length of time information remains in the cache after the session ends (defaults to 10 seconds)
Query Mapping tab	
XML Attribute	Set the QueryKey property to the XML attribute you want to key on such as XML-Address-format-IPv4 and list all attributes to be cached in the AttributesToBeCached subdirectory.
Radius Attribute	Required; list of attribute pairs, mapping the XML attributes on the left-hand side to the RADIUS attribute on the right-hand side.
AttributeToBeCached tab	
RADIUS	Optional; set Radius, if the attribute needs to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute needs to be defined for Vendor. If Vendor is selected, specify the vendor type from the drop-down list.
Attribute Name	Required; use this subdirectory to provide a list of RADIUS attributes you want to store in cache

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

SUBNET-DYNAMIC

Table 2-58 lists and describes the fields in the Resource Manager Details page.

Table 2-58 SUBNET-DYNAMIC Properties

Fields	Description
Subnet Dynamic tab	
Net Mask	Required; must be set to the size of the managed subnets
Start	Required; must be an IP addresses
End	Required; must be an IP addresses

Click the **Add** button to save the details and list it in Start and End IP list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

USER-SESSION-LIMIT

Table 2-59 lists and describes the fields in the Resource Manager Details page.

Table 2-59 USER-SESSION-LIMIT Properties

Fields	Description
User Session Limit	Set the user session limit property to the maximum number of concurrent sessions for a particular user

REMOTE-USER-SESSION-LIMIT

Table 2-60 lists and describes the fields in the Resource Manager Details page.

Table 2-60 REMOTE-USER-SESSION-LIMIT Properties

Fields	Description
User Session Limit	Set the user session limit property to the maximum number of concurrent sessions for a particular user

USR-VPN

Table 2-61 lists and describes the fields in the Resource Manager Details page.

Table 2-61 USR-VPN Properties

Fields	Description
General tab	
Identifier	Required; must be set to the VPN ID the USR NAS will use to identify a VPN.
Neighbor	Optional; if set, should be the IP address of the next hop router for the VPN.
Framed Routing	Optional; if set, should be **RIP V2 Off** or **RIP V2 On** if the USR NAS is to run RIP Version 2 for the user.
Gateway tab	
Name of Gateway	Required; name of the gateway.
Description (optional)	Optional; description of the gateway.
IP Address	Required; IP address of the gateway
Shared Secret	Required; must match the shared secret of the gateway.
Tunnel Refresh	Optional; if specified it is the number of seconds the tunnel stays active before a secure "keepalive" is exchanged between the tunnel peers in order to maintain the tunnel open.
Location ID	Optional; if specified it is a string indicating the physical location of the gateway. Click the **Save** button, to save the details.

To edit the gateway details, check the appropriate check box and click the **Edit** button. Enter new information in the editable fields and click the **Save** button. You can also delete the record using **Delete** button.

REMOTE-SESSION-CACHE

Table 2-62 lists and describes the fields in the Resource Manager Details page.

Table 2-62 REMOTE-SESSION-CACHE Properties

Fields	Description
General tab	
Overwrite Attributes	Specifies whether to overwrite the existing attributes if there are any in the session record.

Table 2-62 REMOTE-SESSION-CACHE Properties (continued)

Fields	Description
Query Key	Required; set the QueryKey to the a RADIUS attribute you want to key on, such as Framed-IP-Address. A change made in Prime Access Registrar requires that this attribute not be an XML attribute, even if this session-cache resource manager is being used for an XML query. **Note** Any existing session-cache resource managers using an XML attribute for the Query Key must be changed to a RADIUS attribute that this XML attribute is mapped to under Query-Mappings.
Pending Removal Delay	Required; length of time information remains in the cache after the session ends (defaults to 10 seconds)
Remote Query Mapping tab	
XML Attribute	Set the QueryKey property to the XML attribute you want to key on such as XML-Address-format-IPv4 and list all attributes to be cached in the AttributesToBeCached subdirectory.
Radius Attribute	Required; list of attribute pairs, mapping the XML attributes on the left-hand side to the RADIUS attribute on the right-hand side.
RemoteAttributeToBeCached tab	
RADIUS	Optional; set Radius, if the attribute needs to be defined for RADIUS.
VENDOR	Optional; set Vendor, if the attribute needs to be defined for Vendor. If Vendor is selected, specify the vendor type from the drop-down list.
Attribute Name	Required; use this subdirectory to provide a list of RADIUS attributes you want to store in cache

3GPP

Table 2-63 lists and describes the 3GPP properties in the Resource Manager Details page.

Table 2-63 3GPP Properties

Fields	Description
EnableRegistrationFlow	Check the box to enable initiation of a Server-Assignment-Request (SAR) registration message when a session is created and a SAR deregistration message when a session is deleted.
EnableSessionTermination	Check the box to enable initiation of a Server-Termination-Request (STR) message when a session is deleted.
ReuseExistingSession	If selected, SAR registration will not be initiated for an existing session.

Table 2-63 3GPP Properties (continued)

Fields	Description
HSSProxyService	Required; a service of type Diameter used to group a list of HSS/Diameter servers towards which the SAR and STR messages need to be initiated in the 3GPP authorization flow.
EnableNon3GPPUserData-Caching	Check this box to cache all Access Point Names (APNs). By default, this option is checked. Uncheck this box to cache only specific APNs based on the requirement.

You can use the Resource Manager List page for the following:

- Filtering Records
- Adding Resource Manager Details
- Network Resources
- Editing Records
- Deleting Records

Adding Resource Manager Details

To add new resource manager details:

Step 1 Choose **Configuration > Resource Manager**. The Resource Manager List page is displayed.

Step 2 Click **Add**. The Resource Manager Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Submit** to save the specified details in the Resource Manager Details page. Otherwise click **Cancel** to return to the Resource Manager List page without saving the details.

The Resource Manager List page is displayed with the newly added details or a respective error message is displayed.

Note Resource Manager supports the following remote type session managers: remote-ip-dynamic, remote-session-cache, home-agent, remote-user-session-limit, home-agent-ipv6 and remote-group-session-limit.

Network Resources

Network Resources constitutes the maintenance and management of the details of the clients and remote servers. The clients IP address and shared secret details are maintained under clients, The management of server directory with use of remote server protocols details are maintained in remote server.

This section describes the following:

- Clients
- Remote Servers

Clients

All NASs and proxy clients that communicate directly with Prime Access Registrar must have an entry in the Clients list. This is required because NAS and proxy clients share a secret with the RADIUS server which is used to encrypt passwords and to sign responses.

Table 2-64 lists and describes the fields in the Client Details page.

Table 2-64 Client Properties

Fields	Description
Name	Required and should match the Client identifier specified in the standard RADIUS attribute, **NAS-Identifier**. The name must be unique within the Clients list.
IncomingScript	Optional; you can use this property to specify a Script you can use to determine the services to use for authentication, authorization, and/or accounting.
OutgoingScript	Optional; you can use this property to specify a Script you can use to make any Client-specific modifications when responding to a particular Client.
Protocol	Required; set it to **Radius**, **Diameter**, **Radius-TLS**, or **Tacacs-and-Radius**.
Description	Optional description of the client.
Vendor	Optional; displayed when the protocol is set to Diameter. When set, must be the name of a known Vendor.
Server Identity	Optional; displayed when the protocol is set to Diameter. While exchanging the CER information in the client, Prime Access Registrar sends the configured server identity value as the origin-host value. When set, it takes precedence over the /Radius/Advance/Diameter/TransportManagement configuration.
HostName	Required; hostname or IP address of the Diameter client.
Port	Required; port on which client connects with the Prime Access Registrar server.
SCTP-Enabled	Required; displays when the protocol is set to Diameter and indicates whether the connection will be an SCTP. If set to TRUE, SCTP will be used. If set to FALSE, TCP will be used.
Advertised-Realm	Optional; displays when the protocol is set to Diameter. While exchanging the CER information in the client, Prime Access Registrar sends the configured server realm value as the origin-realms value. It takes precedence over the /Radius/Advance/Diameter/TransportManagement configuration.
WatchDogTimeout	Time interval between watch dog messages.
MaxIncomingRequestRate	Maximum number of incoming requests allowed per second.
KeepAliveTime	Time interval, in milliseconds, to keep an idle session active.
InitialTimeout	Timeout value, in milliseconds, the Prime Access Registrar server waits for a response before dropping the packet.

Table 2-64 Client Properties (continued)

Fields	Description
TLS-Enabled	Check this box to enable TLS security mechanism for the Diameter client.
Advertised-HostName	Optional; specifies the local hostname address that will be advertised by the Prime Access Registrar server to other peers during CER/CEA exchange.
AuthSession-StateInASR	When EnableAuthSessionState is set to: • No-State-Maintained—When RTR is received from HSS , Auth-Session-State AVP should be set with No-State-Maintained on sending ASR to the client; and the session is deleted. • State-Maintained—When RTR is received from HSS , Auth-Session-State AVP should be set with State-Maintained on sending ASR to client. The session is deleted only on reception of STR from client.
UserLogEnabled	This field is available for protocol of type **Diameter**. Check this box to display the user information in the log file for example username, AAAID, client identifier, result-code, and diameter-message-type. If this option is enabled, Prime Access Registrar stores all subscriber messages including Diameter request and response in a separate log file called subscriber_log in the $INSTALLPATH/logs folder.
TCP-ReadBuffer	Allows you to configure read buffer socket options for TCP connections.
TCP-WriteBuffer	Allows you to configure write buffer socket options for TCP connections.
Note The above two parameters are available only for Diameter client. When these values are set to zero, default kernel settings will take effect.	
EnableMulti-ProxyMode	This field is available for protocol of type **Diameter**. Check this box to enable Diameter client configurations in multiple proxy mode. If this option is enabled, client-based Diameter connections can be established from multiple peers with the same IP address but with different source ports and origin-hosts.
EnableDiaDynamicAuthorization	This field is available for protocol of type **Diameter**. Check this box to enable Diameter dynamic authorization for the client.
EnableDOIC	This field is available for protocol of type **Diameter**. Check this box to enable D Overload Indication Conveyance (DOIC) for the client. For more details about the DOIC feature, see DOIC Priorities, page 2-106.
MaximumTLS-Connections	This field is available for protocol of type **radius-tls**. Maximum number of TLS connections that the client can establish with Prime Access Registrar. Default value is one. Maximum number of TLS connections allowed per client is 50.
SCTPParameters Section	
This section is available if the SCTP-Enabled option is checked.	
SourcePort	Client source port. Default value is 3868.
DestinationPort	Client destination port. Default value is 3868.
PathMaxRetrans	Maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive. Default value is 5.

Table 2-64 Client Properties (continued)

Fields	Description
RTOInitial	Initial value of RTO (retransmission timeout) that is used in RTO calculations. Measured in milliseconds and default value is 3 seconds.
RTOCookieLife	Maximum lifespan of the cookie sent in an INIT ACK chunk. Measured in milliseconds and default value is 60 secs.
RTOMin	Minimum value of RTO. Measured in milliseconds and default value is 1 second.
HBInterval	Interval when a HEARTBEAT chunk is sent to a destination transport address to monitor the reachability of an idle destination transport address. Measured in milliseconds and default is 30 seconds.
RTOMax	Maximum value of RTO. Measured in milliseconds and default value is 60 seconds.
SACKTimeout	Delayed SACK timeout. Default value is 200 msecs.
MaxInitRetransmits	Maximum number of times an INIT chunk or a COOKIE ECHO chunk is retransmitted before an endpoint aborts the initialization process and closes the association. Default value is 8.
InitNumOStreams	Initial number of streams per socket.
AssociationMaxRetrans	Maximum number of consecutive retransmissions to a peer before an endpoint considers that the peer is unreachable and closes the association. Default value is 10.
InitMaxInStreams	Maximum number of inbound streams per socket.
SCTPAdvertisedHostName	Displays set of IP addresses for local and remote hosts.
TLSOptions / RTLS Options This section is available if the protocol is set to one of the following: • Diameter and TLS-Enabled option is checked • radius-tls	
PrivateKeyPassword	The password used to protect the server's private key.
ServerKeyFile	The full pathname of the file containing the server's RSA private key. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The valid encoding prefix is "PEM". If an encoding prefix is not present, the file is assumed to be in PEM format. The following example assumes that the subdirectory **pki** under **/cisco-ar** contains the server's certificate file. The file **server-key.pem** is assumed to be in PEM format. The file extension ***.pem*** is not significant. **set ServerKeyFile PEM:/cisco-ar/pki/server-key.pem**
ServerCertificateFile	The full pathname of the file containing the server's certificate or certificate chain used during the TLS exchange. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The valid encoding prefix is PEM. If an encoding prefix is not present, the file is assumed to be in PEM format.

Table 2-64 Client Properties (continued)

Fields	Description
CACertificateFile	The full pathname of the file containing trusted CA certificates used for client verification. The file can contain more than one certificate, but all certificates must be in PEM format. DER encoding is not allowed.
CACertificatePath	The name of a directory containing trusted CA certificates (in PEM format) used for client verification. This parameter is optional, and if it is used there are some special preparations required for the directory it references. Each certificate file in this directory must contain exactly one certificate in PEM format. The server looks up the certificate files using the MD5 hash value of the certificate's subject name as a key. The directory must therefore also contain a set of symbolic links each of which points to an actual certificate file. The name of each symbolic link is the hash of the subject name of the certificate. For example, if a certificate file named **ca-cert.pem** is located in the CACertificatePath directory, and the MD5 hash of the subject name contained in **ca-cert.path.pem** is 1b96dd93, then a symbolic link named 1b96dd93 must point to **ca-cert.pem**. If there are subject name collisions such as multiple certificates with the same subject name, each link name must be indexed with a numeric extension as in 1b96dd93.0 and 1b96dd93.1.
PeerVerificationMode	Select one of the following options: • None—If the peer verification certificate must not be requested. • Optional—If peer verification certificate can be requested; but, verification is not required. • RequireCertificate—If peer certificate must be requested and verified.
Verification-Depth	Specifies the maximum length of the certificate chain used for client verification.
EnableAuto-Chaining	When set to TRUE, Prime Access Registrar sends its server certificate chain (Server-Cert -> IntermediateCA -> RootCA) while presenting the server certificate to the client for server side authentication. When set to FALSE, Prime Access Registrar sends only the server certificate (Server-Cert) to the client.
DOICOptions Section	
This section is available if the **EnableDOIC** option is checked.	
OverloadReductionPercentage	Percentage indicating the traffic that the reacting node should throttle, which could be between 0 and 100.

Table 2-64 Client Properties (continued)

Fields	Description
OLRValidityIn-Seconds	Indicates the time of expiry (in seconds) of the overload report (OLR) sent by the reporting node. Value could be between 1 and 86,400.
General Properties tab The tabs are available if the protocol is set to Radius or Tacacs-and-Radius.	
IPAddress	Required; must be a valid IP address and unique in the Clients list. Prime Access Registrar uses this property to identify the Client that sent the request, either using the source IP address to identify the immediate sender or using the **NAS-IP-Address** attribute in the Request dictionary to identify the NAS sending the request through a proxy. When a range is configured for a Client's IPAddress property, any incoming requests whose source address belongs to the range specified, will be allowed for further processing by the server. Similarly when a wildcard (an asterisk '*' in this case) is specified, any incoming requests whose source address matches the wildcard specification will be allowed. In both the cases, the configured client properties like SharedSecret, and Vendor are used to process the requests. You can specify a range of IP addresses using a hyphen as in: 100.1.2.11-20 You can use an asterisk wildcard to match all numbers in an IP address octet as in: 100.1.2.* You can specify an IPAddress and a subnet mask together using Classless Inter-Domain Routing (CIDR) notation as in: 100.1.2.0/24 You can use the IPAddress property to set a base address and use the NetMask property to specify the number of clients in the subnet range.
Shared Secret	Required; must match the secret configured in the Client.
Type	Required; accept the default (NAS), or set it to ATM, Proxy, or NAS+Proxy.
Vendor	Optional; you can use this property when you need special processing for a specific vendor's NAS. To use this property, you must configure a **Vendor** object and include a script. Prime Access Registrar provides five Scripts you can use: one for Ascend, Cisco, Cabletron, Altiga, and one for USR. You can also provide your own Script.
NetMask	Specifies the subnet mask used with the network address setting configured for the IPAdress property when configuring a range of IP addresses. This property is not used for a single client with an IP address only. The NetMask property is used to configure multiple clients when you configure a base IP address in the IPAddress property. You can set the NetMask property for a range of 256 clients using the following example: **set NetMask 255.255.255.0** **Note** If you set the NetMask property, validation will fail if you attempt to specify a subnet mask using CIDR notation with the IPAddress property (described above).

Table 2-64 Client Properties (continued)

Fields	Description
Enforce Traffic Throttling	By default, the value is set to FALSE. When set to TRUE, the traffic throttling check for the packet will be executed.
3GPP-Teardown-Indicator	This field is available only for the protocol of type Radius. Set it to 0 or 1 to add in the disconnect packet.
Dynamic Authorization tab	
Enable Dynamic Authorization	Optional; when set to TRUE, this property enables Change of Authorization (CoA) and Packet of Disconnect (PoD) features.
Shared Secret	Located under the DynamicAuthorizationServer subdirectory, this is the shared secret used for communicating CoA and PoD packets with the client.
Port	Located under the DynamicAuthorizationServer subdirectory, the default port is 3799.
InitialTimeout	Located under the DynamicAuthorizationServer subdirectory, the default is 5000.
MaxTries	Located under the DynamicAuthorizationServer subdirectory, the default is 3.
COA Attribute	This property is found under the DynamicAuthorizationServer subdirectory and points to a group of attributes to be included in a CoA request sent to this client. These attribute groups are created and configured under the AttributeGroups subdirectory in **/Radius/Advanced**.
POD Attribute	This property is found under the DynamicAuthorizationServer subdirectory and points to a group of attributes to be included in a POD request sent to this client. These attribute groups are created and configured under the AttributeGroups subdirectory in **/Radius/Advanced**.
Notification Properties tab	
Enable Notifications	Required; the default value is FALSE and indicates the client is not capable of receiving Accounting-Stop notifications from the Prime Access Registrar server. When set to TRUE, the client can receive Accounting-Stop notifications from the Prime Access Registrar server and additional properties must be configured under a new sub-directory named NotificationProperties.
InitialTimeout	Located under the NotificationProperties subdirectory, specifies the timeout value in milliseconds the Prime Access Registrar server waits for an Accounting-Response packet before attempting a retry (sending another Accounting-Stop packet to the client). Required when EnableNotifications is set to TRUE; the default value is 5000.
Port	Located under the NotificationProperties subdirectory, specifies the port used by the Prime Access Registrar server to receive Accounting-Stop packets. Required when EnableNotifications is set to TRUE; the default value is 1813.
MaxTries	Located under the NotificationProperties subdirectory, specifies the number of times the Prime Access Registrar server sends an Accounting-Stop packet to a client. Required when EnableNotifications is set to TRUE; the default value is 3.
Notification-Properties	When the EnableNotifications property is set to TRUE, this subdirectory contains additional properties required to support the Query-Notify feature.

Table 2-64 Client Properties (continued)

Fields	Description
NotificationAttributeGroup	Located under the NotificationProperties subdirectory, specifies the name of an attribute group under **/Radius/Advanced/AttributeGroups** that contains the attributes to be included when sending an the Accounting-Stop packet to this client. Required when EnableNotifications is set to TRUE; there is no default value. You must provide the name of a valid AttributeGroup and the named AttributeGroup must contain at least one valid attribute, or validation will fail.
TCP Options This section is available if the protocol is set to **radius-tls**.	
KeepAliveIntervalTime	Time interval in seconds between individual keepalive probes.
TCPConnectionIdleTime	Time (in seconds) the connection can remain idle before TCP starts sending keepalive probes.
KeepAliveMaxtries	Maximum number of keepalive probes TCP can send before dropping the connection.

You can use the Clients page for the following:

- Filtering Records
- Adding Client Details
- Editing Records
- Deleting Records

Adding Client Details

To add new Client details:

Step 1 Choose **Network Resources > Clients**. The Clients page is displayed.

Step 2 Click **Add** to add new client details. The Client Details page is displayed.

Step 3 Enter the required details in the General Properties, Dynamic Authorization, and Notification Properties tabs.

Step 4 Click **Save** to save the specified details in the Client Details page. Otherwise click **Cancel** to return to the Client page without saving the details.

The Client page is displayed with the newly added details or a respective error message is displayed.

Remote Servers

You can use the RemoteServers object to specify the properties of the remote servers to which Services proxy requests.

Prime Access Registrar provides the following RemoteServer protocol types:

- LDAP
- LDAP Accounting
- ODBC/OCI
- ODBC/OCI-Accounting
- Diameter
- REST
- Others

Note You must not configure a remote server with an IP address, which is same as that of the client. This is applicable for all types of remote servers.

LDAP

Specify the **ldap** service type when you want to use a particular LDAP remote server for authentication and/or authorization.When using LDAP for authentication and a local database for authorization, ensure that the usernames in both locations are identical with regard to case-sensitivity.

Table 2-65 lists and describes the fields in the Add LDAP-RemoteServers Details page.

Table 2-65 LDAP Server Properties

Fields	Description
LDAP Properties tab	
Name	Required; name of the LDAP server.
Host Name	Required; the LDAP server's hostname or IP address. Prime Access Registrar supports IPv4 and IPv6 addresses for the hostname. **Note** To use IPv6 addresses, you must have Next Generation (NG) license of Prime Access Registrar. For LDAP, IPv6 addresses must be enclosed in square brackets, as in [2001:420:27c1:420:250:56ff:fe99:3dfd].
Port	Required; defaults to port 389.
Description	Description of the LDAP server.
Timeout	Required; the default is 15. The timeout property indicates how many seconds the RADIUS server will wait for a response from the LDAP server. **Note** Use InitialTimeout from above as a template, except this is timeout is specified in seconds.
Reactivate Time Interval	Required; the amount of time (in milliseconds) to wait before retrying a remote server that was offline. You must specify a number greater than zero. The default is 300,000 (5 minutes).

Table 2-65 LDAP Server Properties (continued)

Fields	Description
MaxReferrals	Required; must be a number equal to or greater than zero. This property indicates how many referrals are allowed when looking up user information. When you set this property to zero, no referrals are allowed. Cisco Prime Access Registrar manages referrals by allowing the RADIUS server's administrator to indicate an LDAP "referral attribute," which might or might not appear in the user information returned from an LDAP query. When this information is returned from a query, Cisco Prime Access Registrar assumes it is a referral and initiates another query based on the referral. Referrals can also contain referrals. **Note** This is an LDAP v2 referral property.
Referral Attribute	Required when you have specified a **MaxReferrals** value. This property specifies which LDAP attribute, returned from an LDAP search, to check for referral information. **Note** This is an LDAP v2 referral property.
Referral Filter	Required when you have specified a **MaxReferral** value. This is the filter Cisco Prime Access Registrar uses when processing referrals. When checking referrals, the information Cisco Prime Access Registrar finds in the referral itself is considered to be the search path and this property provides the filter. The syntax is the same as that of the **Filter** property. **Note** This is an LDAP v2 referral property.
Bind Name	Optional; the distinguished name (dn) to use when establishing a connection between the LDAP and RADIUS servers.
Bind Password	Optional; the password associated with the **BindName**.
Search Path	Required; the path that indicates where in the LDAP database to start the search for user information.
Limit Outstanding Requests	Required; the default is FALSE. Cisco Prime Access Registrar uses this property in conjunction with the **MaxOutstandingRequests** property to tune the RADIUS server's use of the LDAP server. When you set this property to TRUE, the number of outstanding requests for this RemoteServer is limited to the value you specified in **MaxOutstandingRequests**. When the number of requests exceeds this number, Cisco Prime Access Registrar queues the remaining requests, and sends them as soon as the number of outstanding requests drops to this number.
User Password Attribute	Required; this specifies which LDAP field the RADIUS server should check for the user's password.
Escape Spl.Character in UserName	FALSE by default.
Datasource Connections	Specifies the number of concurrent connections to the LDAP server. The default value is 8.

Table 2-65 LDAP Server Properties (continued)

Fields	Description
Use SSL	A boolean field indicating whether you want Cisco Prime Access Registrar to use SSL (Secure Socket Layer) when communicating with this RemoteServer. When you set it to TRUE, be sure to specify the **CertificateDBPath** field in the **Advanced** section, and be sure the port you specified for this RemoteServer is the SSL port used by the LDAP server.
EnableKeepAlive	Default is FALSE. This is enabled to send a TCP keepalive to keep the idle connection active.
Filter	Required; this specifies the search filter Cisco Prime Access Registrar uses when querying the LDAP server for user information. When you configure this property, use the notation "%s" to indicate where the user ID should be inserted. For example, a typical value for this property is "(uid=%s)," which means that when querying for information about user `joe`, use the filter `uid=joe`.
Max Outstanding Requests	Required when you have set the **LimitOutstandingRequests** to TRUE. The number you specify, which must be greater than zero, determines the maximum number of outstanding requests allowed for this remote server.
Password Encryption Style	The default is **None**. You can also specify **crypt, dynamic, SHA-1, and SSHA-1**.
DNSLookup and LDAP RebindInterval	Specifies the timeout period after which the Prime Access Registrar server will attempt to resolve the LDAP hostname to IP address (DNS resolution); 0 by default
Search Scope	Specifies how deep to search within a search path; default is *SubTree* which indicates a search of the base object and the entire subtree of which the base object distinguished name is the highest object. *Base* indicates a search of the base object only. *OneLevel* indicates a search of objects immediately subordinate to the base object, but does not include the base object.
Use Binary Password Comparison	A boolean field that enables binary password comparison for authentication. This property when set to TRUE, enables binary password comparison. By default, this property is set to FALSE.
Use Bind Based Authentication	A boolean field that enables bind-based authentication with LDAP server. By default, this property is set to FALSE. When set to FALSE, it uses existing legacy authentication method. On setting this property to TRUE, the mappings LDAPToRadius, LDAPToEnvironment, and LDAPToCheckItem will not work.
LDAPToRadiusMappings tab	
LDAPAttribute	Set the value for the LDAP attribute

Table 2-65 LDAP Server Properties (continued)

Fields	Description
RadiusAttribute	A list of name/value pairs in which the name is the name of the **ldap** attribute to retrieve from the user record, and the value is the name of the RADIUS attribute to set to the value of the **ldap** attribute retrieved. For example, when the **LDAPToRadiusMappings** has the entry: **FramedIPAddress = Framed-IP-Address**, the RemoteServer retrieves the **FramedIPAddress** attribute from the **ldap** user entry for the specified user, uses the value returned, and sets the Response variable **Framed-IP-Address** to that value. Click the **Add** button to save the details and list it in the attribute list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
LDAPToCheckItems Mappings tab	
Attribute Type	Select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list.
LDAPAttribute	Set the value for the LDAP attribute
CheckedItems	A list of LDAP *attribute/value* pairs which must be present in the RADIUS access request and must match, both name and value, for the check to pass. For example, when the **LDAPToCheckItemMappings** has the entry: **group = User-Group**, the Access Request must contain the attribute **group**, and it must be set to **User-Group**. Click the **Add** button to save the details and list it in the attribute list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
LDAPToEnvironmentalMappings tab	
LDAPAttribute	Set the value for the LDAP attribute
EnvironmentalAttribute	A list of name/value pairs in which the name is the name of the **ldap** attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the **ldap** attribute retrieved. For example, when the **LDAPToEnvironmentMappings** has the entry: **group = User-Group**, the RemoteServer retrieves the **group** attribute from the **ldap** user entry for the specified user, uses the value returned, and sets the Environment variable **User-Group** to that value. Click the **Add** button to save the details and list it in the attribute list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the LDAP-RemoteServers page for the following:

- Filtering Records
- Adding LDAP Details
- LDAP Accounting
- Editing Records
- Deleting Records

Adding LDAP Details

To add new LDAP details:

Step 1 Choose **Network Resources > RemoteServers > LDAP**. The LDAP-RemoteServers page is displayed.

Step 2 Click **Add** to add LDAP details. The LDAP-RemoteServers Details page is displayed.

Step 3 Enter the required details in the tabs.

Step 4 Click **Save LDAP Server** to save the specified details in the LDAP-RemoteServers Details page. The LDAP-RemoteServers page is displayed with the newly added details or a respective error message is displayed. Otherwise click **Cancel** to return to the LDAP-RemoteServers page without saving the details.

LDAP Accounting

Previous releases of Prime Access Registrar supported accessing user data from an LDAP server, but this feature was limited to performing authentication and authorization (AA). You could only write the accounting records to local file or oracle database or proxy to another RADIUS server.
Prime Access Registrar supports writing accounting records into LDAP server enabling integration between billing systems and LDAP.

Table 2-66 lists and describes the fields in the LDAPAcct RemoteServer Details page.

Table 2-66 LDAP Accounting Server Properties

Fields	Description
LDAP Acct Properties tab	
Name	Name of the remote server; this property is mandatory, and there is no default.
Description	Optional description of server.
HostName	Required; the LDAP server's hostname or IP address.
Port	Required; the default value is 389. Port the LDAP server is listening on.
Timeout	Mandatory time interval (in seconds) to wait for LADP-write operation to complete; defaults to 15 seconds.
ReactivateTimerInterval	Mandatory time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms.

Table 2-66 LDAP Accounting Server Properties (continued)

Fields	Description
BindName	Optional; the distinguished name (dn) to use when establishing a connection between the LDAP and RADIUS servers.
BindPassword	Optional; the password associated with the BindName.
EnableKeepAlive	Required; default is FALSE. This is enabled to send a TCP keepalive to keep the idle connection active.
Delimiter	Character used to separate the values of the attributes given in AttributeList property.
LDAPEnvironmentMultiValueDelimiter	Optional; allows you to specify a character that separates multi-valued attribute lists when using ldap-accounting.
DnPath	Required; the path that indicates where in the LDAP database to start the write for user information.
EntryName	Required; this specifies the write entry name Prime Access Registrar uses when insetting the LDAP server for user information. When you configure this property, use the notation "%s" to indicate where the user ID should be inserted. For example, a typical value for this property is "(uid=%s)," which means that when insetting for information about user joe, use the fentry name uid=joe.
LimitOutstandingRequests	Required; the default is FALSE. Prime Access Registrar uses this property in conjunction with the **MaxOutstandingRequests** property to tune the RADIUS server's use of the LDAP server. When you set this property to TRUE, the number of outstanding requests for this RemoteServer is limited to the value you specified in **MaxOutstandingRequests**. When the number of requests exceeds this number, Prime Access Registrar queues the remaining requests, and sends them as soon as the number of outstanding requests drops to this number.
MaxOutstandingRequests	Required when you have set the **LimitOutstandingRequests** to TRUE. The number you specify, which must be greater than zero, determines the maximum number of outstanding requests allowed for this remote server.
ObjectClass	Required; list of object classes which are all schemas defined in LDAP server. These schemas define required attributes and allowed attributes for an entry which is inserted from Prime Access Registrar.
DNSLookup and LDAPAcct RebindInterval	Specifies the timeout period after which the Prime Access Registrar server will attempt to resolve the LDAP hostname to IP address (DNS resolution).
Escape Spl.Character in UserName	FALSE by default.
AttributeList	List of comma-separated attribute names.
Datasource Connections	Mandatory number of connections to be established; defaults to 8.
UseLocalTimeZone	Optional; the default is FALSE. It determines the timezone of accounting records TimeStamp.

Table 2-66 LDAP Accounting Server Properties (continued)

Fields	Description
UseSSL	A boolean field indicating whether you want Prime Access Registrar to use SSL (Secure Socket Layer) when communicating with this RemoteServer. When you set it to TRUE, be sure to specify the **CertificateDBPath** field in the **Advanced** section, and be sure the port you specified for this RemoteServer is the SSL port used by the LDAP server.
AttributestoWrite tab	
LDAPAcctAttribute	Set the LDAP Accounting attribute.
EnvironmentalAttribute	A list of name and value pairs in which the name is the name of the data store attribute to retrieve from the user record, and the value is the name of the RADIUS attribute to set to the value of the data store attribute retrieved. The data store attributes must match those defined in the external SQL file. Click the **Add** button to save the details and list it in the Attributes list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the LDAP Acct-RemoteServers page for the following:

- Filtering Records
- Adding LDAP Accounting Details
- Editing Records
- Deleting Records

Adding LDAP Accounting Details

To add new LDAP accounting details:

Step 1 Choose **Network Resources > RemoteServers > LDAP Accounting**. The LDAPAcct-RemoteServers page is displayed.

Step 2 Click **Add** to add LDAP accounting details. The LDAPAcct RemoteServer Details page is displayed.

Step 3 Enter the required details in the tabs.

Step 4 Click **Save LDAP Acct Server** to save the specified details in the LDAPAcct RemoteServer Details page. Otherwise click **Cancel** to return to the LDAPAcct-RemoteServers page without saving the details.

The LDAPAcct-RemoteServers page is displayed with the newly added details or a respective error message is displayed.

ODBC/OCI

Specify **odbc** or **oci** when you want to use an ODBC or OCI service for authentication, authorization and accounting through an ODBC or OCI data store respectively. Use an ODBC or OCI service to authenticate and authorize an access requests by querying user information through ODBC or OCI and to insert accounting records into a data store through ODBC or OCI.

Table 2-67 lists and describes the fields in the ODBC/OCI-RemoteServers Details page.

Table 2-67 ODBC/OCI Server Properties

Fields	Description
Name	Required; name of the ODBC/OCI Server.
Protocol	The type of remote server. You select the option ODBC or OCI from the drop-down list.
Datasource Connections	Required; default is 8. This represents the total number of connections Prime Access Registrar can open with the ODBC server; total number of threads Prime Access Registrar can create for the ODBC server.
ODBC Datasource Name	Required; name of the ODBCDataSource to use and must refer to one entry in the list of ODBC datasources configured under **/Radius/Advanced/ODBCDataSources**.
User Password Attribute	Set the user password.
SNMPTrapIP	The SNMP trap IP for the remote servers. Prime Access Registrar supports IPv4 and IPv6 addresses for the SNMP trap IP. **Note** To use IPv6 addresses, you must have Next Generation (NG) license of Prime Access Registrar.
Description	Description of the ODBC Server
Timeout	Required; the default is 15. The timeout property indicates how many seconds the RADIUS server will wait for a response from the ODBC server. **Note** Use InitialTimeout from above as a template, except this is timeout is specified in seconds.
Reactivate Time Interval	Required; default is 300,000 milliseconds. Length of time to wait before attempting to reconnect if a thread is not connected to a data source.
Keep Alive Timer Interval	Mandatory time interval (in milliseconds) to send a keepalive to keep the idle connection active; defaults to zero (0) meaning the option is disabled
SNMPTrapPort	The SNMP trap port for the remote server; defaults to 1521.
OCITimeOutCount	This and the following fields appear when you select **oci** from the **Protocol** drop-down list. Required; continuous timeout count to disconnect the selected connection. Default value is 10.
OCIConnectionReactivationInterval	Required; time interval for attempting to reconnect the disconnected OCI remote server session. Default value is 3000 ms.

Table 2-67 ODBC/OCI Server Properties (continued)

Fields	Description
OCIActiveConnectionThreshold-Count	Required; threshold count of disconnections after which Prime Access Registrar will mark the remote server as down and try to reactivate it. Default value is 4.
SQL Definitions tab	
Name	SQLDefinition properties define the SQL you want to execute.
Description	Description of the SQL
Type	Prime Access Registrar supports only type **query**.
SQL	SQL query used to add, update or delete a record from a database
Execution SequenceNumber	Sequence number for SQLStatement execution, must be greater than zero (mandatory, no default)
Marker List	Defines all markers for the query. MarkerList uses the format UserName/SQL_DATA_TYPE.
RadiusMappings tab	
ODBC/OCI Attribute	Set the ODBC or OCI attribute
RADIUS Attribute	A list of name and value pairs in which the name is the name of the data store attribute to retrieve from the user record, and the value is the name of the RADIUS attribute to set to the value of the data store attribute retrieved. The data store attributes must match those defined in the external SQL file. Click the **Add** button to save the details and list it in the Attributes list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
CheckItemsMappings tab	
Attribute Type	Select either **RADIUS** or **VENDOR**. If Vendor is selected, specify the vendor type from the drop-down list.
ODBC/OCI Attribute	Set the ODBC or OCI attribute
CheckItem	A list of ODBC attribute/value pairs. Click the **Add** button to save the details and list it in the Attributes list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.
EnvironmentalMappings tab	

Table 2-67 ODBC/OCI Server Properties (continued)

Fields	Description
ODBC/OCI Attribute	Set the ODBC or OCI attribute
Environmental Attribute	A list of name/value pairs in which the name is the name of the data store attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the ODBC attribute retrieved. Click the **Add** button to save the details and list it in the Attributes list. To navigate between the listed attributes, use the navigation option available adjacent to the list. See Relocating Records for more details. To delete the available attributes, select the relevant attribute and click the **Delete** button below.

You can use the ODBC/OCI-RemoteServers page for the following:

- Filtering Records
- Adding ODBC/OCI Details
- ODBC/OCI-Accounting
- Editing Records
- Deleting Records

Adding ODBC/OCI Details

To add new ODBC or OCI details:

Step 1 Choose **Network Resources > RemoteServers > ODBC/OCI**. The ODBC/OCI-RemoteServers page is displayed.

Step 2 Click **Add** to add ODBC or OCI details. The ODBC/OCI-RemoteServers Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Add** to enter the SQL details in the **SQL Definitions** tab.

Step 5 Click **Save** to save the specified details in the **SQL Definitions** tab or click **Cancel** to cancel the action.

Step 6 Enter the required details in the tabs.

Step 7 Click **Add Server** to save the specified details in the ODBC/OCI-RemoteServers Details page. Otherwise click **Cancel** to return to the ODBC/OCI-RemoteServers page without saving the details.

The ODBC/OCI-RemoteServers page is displayed with the newly added details or a respective error message is displayed.

ODBC/OCI-Accounting

If you use the Oracle Accounting feature, you must configure an ODBC/OCI-Accounting RemoteServer object.

Table 2-68 lists and describes the fields in the Add ODBC/OCI Accounting-RemoteServers page.

Table 2-68 ODBC/OCI Accounting Server Properties

Fields	Description
General Properties tab	
Name	Name of the remote server; this property is mandatory, and there is no default.
Protocol	The type of Accounting remote server. You can select the option odbc-accounting or oci-accounting from the drop-down list.
Datasource Connections	Mandatory number of connections to be established; defaults to 8
ODBC Datasource Name	Name of the ODBCDataSource to use and must refer to one entry in the list of ODBC datasources configured under **/Radius/Advanced/ODBCDataSources**. Mandatory; no default
Buffer Accounting Packets	Mandatory, TRUE or FALSE, determines whether to buffer the accounting packets to local file, defaults to TRUE which means that packet buffering is enabled. **Note** When set to TRUE, a constant flow of incoming accounting packets can fill the buffer backing store files in **/cisco-ar/data/odbc** beyond the size configured in MaximumBufferFileSize. Configure BackingStoreDiscThreshold in **/Radius/Advanced** when using ODBC accounting.
Max. Buffer Filesize	Mandatory if BufferAccountingPackets is set to TRUE, determines the maximum buffer file size, defaults to 10 Megabyte)
Backing Store Environment Variables	Optional; when BufferAccountingPackets is set to TRUE, contains a comma-separated list of environment variable names to be stored into a local file along with buffered packet. No default. BackingStoreEnvironmentVariables can also be specified in scripts using the BackingStoreEnvironmentVariables environment variable.
Attribute List	List of comma-separated attribute names.
SNMPTrapIP	Optional; when set to a valid IP address, the traps (responding/not responding traps) for the ODBC/OCI Accounting server will have this IP address. This is used to identify the server. If the value is not set, SNMP traps use 255.255.255.255 as the IP address.
Description	Optional; description of server.
Timeout	Mandatory time interval (in seconds) to wait for SQL operation to complete; defaults to 15 seconds.
Reactivate Time Interval	Mandatory time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms.
Keep Alive Timer Interval	Mandatory time interval (in milliseconds) to send a keepalive to keep the idle connection active; defaults to zero (0) meaning the option is disabled.
No. of Retries for Buffered Packet	Mandatory if BufferAccountingPackets is set to TRUE. A number greater than zero determines the number of attempts to be made to insert the buffered packet into Oracle. Defaults to 3.

Table 2-68 ODBC/OCI Accounting Server Properties (continued)

Fields	Description
Use Local Timezone	Set to TRUE or FALSE, determines the timezone of accounting records' TimeStamp (defaults to FALSE).
Delimiter	Character used to separate the values of the attributes given in AttributeList property.
SNMPTrapPort	Optional; when set to a valid port, the traps (responding/not responding traps) for the ODBC/OCI Accounting server will have this port. If the value is not set, SNMP traps use 1521 as the IP port.
OCIAutoCommit	This and the following fields appear when you select **oci-accounting** from the **Protocol** drop-down list. Required; check this box to let the OCI remote server connections auto commit the Oracle database transactions. Prime Access Registrar will not execute the Commit query explicitly to commit the Oracle database transactions. Auto Commit flag is enabled while establishing the connection itself.
OCITransactionCount	Required; default value is zero. Number of transactions per connection after which Prime Access Registrar can execute the Commit query in the Oracle database instead of committing the transactions after each Oracle query.
OCITimeOutCount	Required; continuous timeout count to disconnect the selected connection. Default value is 10.
OCIConnectionReactivationInterval	Required; time interval for attempting to reconnect the disconnected OCI remote server session. Default value is 3000 ms.
OCIActiveConnectionThresholdCount	Required; threshold count of disconnections after which Prime Access Registrar will mark the remote server as down and try to reactivate it. Default value is 4.
SQL Definitions tab	
Name	Required; SQLDefinition properties define the SQL you want to execute.
Description	Description of the SQL
Type	Required; Prime Access Registrar supports insert, update and delete options.
SQL	Required; SQL query used to acquire the password
Execution SequenceNumber	Required; sequence number for SQLStatement execution, must be greater than zero (mandatory, no default)
Marker List	Required; defines all markers for the query. MarkerList uses the format UserName/SQL_DATA_TYPE.

You can use the ODBC/OCI Accounting-RemoteServers page for the following:

- Filtering Records
- Adding ODBC/OCI Accounting Details
- Others
- Editing Records

- Deleting Records

Adding ODBC/OCI Accounting Details

To add new ODBC or OCI accounting details:

Step 1 Choose **Network Resources > RemoteServers > ODBC/OCI Accounting**. The ODBC/OCI Accounting-RemoteServers page is displayed.

Step 2 Click **Add** to add ODBC or OCI accounting details. The ODBC/OCI Accounting-RemoteServers Details page is displayed.

Step 3 Enter the required details in the tabs.

Step 4 Click **Add Accounting Server** to save the specified details in the ODBC/OCI Accounting-RemoteServers Details page. The ODBC/OCI Accounting-RemoteServers page is displayed with the newly added details or a respective error message is displayed. Otherwise click **Cancel** to return to the ODBC/OCI Accounting-RemoteServers page without saving the details.

Diameter

Diameter is a networking protocol which is derived from RADIUS protocol.

You can click the **Add** button in the Diameter-RemoteServers page to add a new Diameter remote server. Table 2-69 lists and describes the Diameter remote server properties.

Table 2-69 Diameter Remote Server Properties

Fields	Description
Name	Required; name of the Diameter server.
Description	Optional; description of the Diameter server.
Protocol	Required; protocol used by the Diameter server.
MaxTries	Number of retry attempts to be made by the Diameter server for request and response.
Host Name	Host name of the server.
Initial Timeout	Specifies the timeout value in milliseconds the Prime Access Registrar server waits for an Accounting-Response packet before attempting a retry. This value must be less than the DWatchDogTimeout value.
DestinationPort	Port used by the server.
DWatchDogTimeout	Time interval between watch dog messages.
IncomingScript	Optional; if there is a script, it is the first script Prime Access Registrar runs when it receives a request from any client and/or for any service.

Table 2-69 Diameter Remote Server Properties (continued)

Fields	Description
OutgoingScript	Optional; if there is a script, it is the last script Prime Access Registrar runs before it sends a Diameter packet to the remote server. You can choose to configure block listing as part of the outgoing script for Diameter remote server. For more information about block listing, see the “Using Extension Points” chapter of the *Cisco Prime Access Registrar 9.2 Administrator Guide*.
SCTP-Enabled	Indicates whether the connection will be an SCTP. If set to TRUE, SCTP will be used. If set to FALSE, TCP will be used.
AdvertiseHostName	Optional; specifies the local hostname address that will be advertised by the Prime Access Registrar server to other peers during CER/CEA exchange.
AdvertiseRealm	Advertising realm.
ReactivateTimerInterval	Mandatory time interval, in milliseconds, to reactivate an inactive server.
Vendor	Select a valid vendor.
LimitOutstandingRequests	Check this box to limit the number of outstanding requests. If you enable this option, the number of outstanding requests for the Diameter remote server is limited to the value specified in the MaxOutstandingRequests field.
UserLogEnabled	Check this box to log user details of the specified remote server. If this option is enabled, Prime Access Registrar stores all subscriber messages including Diameter request and response in a separate log file called subscriber_log in the $INSTALLPATH/logs folder.
MaxOutstandingRequests	Maximum number of outstanding requests allowed for the Diameter remote server
MaxPendingPackets	Maximum number of packets that can be pending for the Diameter remote server.
DestinationRealm	Required. Destination realm to send Diameter packets to the remote server. The role of the remote server should be Relay.
TLS-Enabled	Check this box to enable TLS security mechanism for the Diameter remote server.
EnableDOIC	This field is available for protocol of type **Diameter**. Check this box to enable DOIC for the remote server. For more details about the DOIC feature, see DOIC Priorities, page 2-106.
MaxTPSLimit	Maximum number of requests allowed per second for the Diameter remote server.
MaxSessionLimit	Maximum number of sessions allowed for the Diameter remote server.
DisconnectBasedOn-Threshold	Check this box if the remote server’s TCP connections are to be disconnected based on a threshold value.
DisconnectThreshold	This field appears only when the DisconnectBasedOnThreshold box is checked. Threshold count to disconnect the remote server’s TCP connections, which indicates the total number of failed requests that are not answered even after MaxTries is reached for each of those requests.

Table 2-69 Diameter Remote Server Properties (continued)

Fields	Description
Host	Destination host to send the packets (default is localhost).
TCP-ReadBuffer	Allows you to configure read buffer socket options for TCP connections initiated to the remote server.
TCP-WriteBuffer	Allows you to configure write buffer socket options for TCP connections initiated to the remote server.
Note When the above two parameters are set to zero, default kernel settings will take effect.	
SCTPParameters Section	
This section is available if the SCTP-Enabled option is checked.	
SourcePort	Remote server source port. Default value is 3868.
DestinationPort	Remote server destination port. Default value is 3868.
PathMaxRetrans	Maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive. Default value is 5.
RTOInitial	Initial value of RTO (retransmission timeout) that is used in RTO calculations. Measured in milliseconds and default value is 3 seconds.
RTOCookieLife	Maximum lifespan of the cookie sent in an INIT ACK chunk. Measured in milliseconds and default value is 60 secs.
RTOMin	Minimum value of RTO. Measured in milliseconds and default value is 1 second.
HBInterval	Interval when a HEARTBEAT chunk is sent to a destination transport address to monitor the reachability of an idle destination transport address. Measured in milliseconds and default is 30 seconds.
RTOMax	Maximum value of RTO. Measured in milliseconds and default value is 60 seconds.
SACKTimeout	Delayed SACK timeout. Default value is 200 msecs.
MaxInitRetransmits	Maximum number of times an INIT chunk or a COOKIE ECHO chunk is retransmitted before an endpoint aborts the initialization process and closes the association. Default value is 8.
InitNumOStreams	Initial number of streams per socket.
AssociationMaxRetrans	Maximum number of consecutive retransmissions to a peer before an endpoint considers that the peer is unreachable and closes the association. Default value is 10.
InitMaxInStreams	Maximum number of inbound streams per socket.
SCTPAdvHostName Section	
This section is available if the SCTP-Enabled option is checked.	
Local	SCTP advertising host name of the local server.
Remote	SCTP advertising host name of the remote server.
TLSEnabled Section	
This section is available if the TLS-Enabled option is checked.	
PrivateKeyPassword	The password used to protect the server’s private key.

Table 2-69 Diameter Remote Server Properties (continued)

Fields	Description
ServerKeyFile	The full pathname of the file containing the server's RSA private key. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The valid encoding prefix is "PEM". If an encoding prefix is not present, the file is assumed to be in PEM format. The following example assumes that the subdirectory **pki** under **/cisco-ar** contains the server's certificate file. The file **server-key.pem** is assumed to be in PEM format. The file extension ***.pem*** is not significant. **set ServerKeyFile PEM:/cisco-ar/pki/server-key.pem**
ServerCertificateFile	The full pathname of the file containing the server's certificate or certificate chain used during the TLS exchange. The pathname can be optionally prefixed with a special string that indicates the type of encoding used for the certificate. The valid encoding prefix is PEM. If an encoding prefix is not present, the file is assumed to be in PEM format.
CACertificateFile	The full pathname of the file containing trusted CA certificates used for client verification. The file can contain more than one certificate, but all certificates must be in PEM format. DER encoding is not allowed.
CACertificatePath	The name of a directory containing trusted CA certificates (in PEM format) used for client verification. This parameter is optional, and if it is used there are some special preparations required for the directory it references. Each certificate file in this directory must contain exactly one certificate in PEM format. The server looks up the certificate files using the MD5 hash value of the certificate's subject name as a key. The directory must therefore also contain a set of symbolic links each of which points to an actual certificate file. The name of each symbolic link is the hash of the subject name of the certificate. For example, if a certificate file named **ca-cert.pem** is located in the CACertificatePath directory, and the MD5 hash of the subject name contained in **ca-cert.path.pem** is 1b96dd93, then a symbolic link named 1b96dd93 must point to **ca-cert.pem**. If there are subject name collisions such as multiple certificates with the same subject name, each link name must be indexed with a numeric extension as in 1b96dd93.0 and 1b96dd93.1.
PeerVerificationMode	Select one of the following options: • None—If Prime Access Registrar is not required to provide its certificate; but, the peer's certificate must be verified. • Optional—If Prime Access Registrar can provide its certificate optionally; but, the peer's certificate must be verified. • RequireCertificate—If Prime Access Registrar must provide its certificate and the peer's certificate must also be verified.
VerificationDepth	Specifies the maximum length of the certificate chain used for client verification.

Table 2-69 Diameter Remote Server Properties (continued)

Fields	Description
EnableAutoChaining	When set to TRUE, Prime Access Registrar sends its server certificate chain (Server-Cert -> IntermediateCA -> RootCA) while presenting the server certificate to the client for server side authentication. When set to FALSE, Prime Access Registrar sends only the server certificate (Server-Cert) to the client.
DOIC Options This section is available if the **EnableDOIC** option is checked.	
ForwardAbatement	Abatement action to be taken based on priorities during active overload condition.
ForwardPriorityList	Priority list for implementing forward abatement. You can set up the priority list from P0 - P4 under **Configuration** > **Advanced** > **DOICPriorities**; e.g. Priority0
DivertAbatement	Abatement action to be taken based on priorities during active overload condition.
DivertPriorityList	Priority list for implementing divert abatement. You can set up the priority list from P0 - P4 under **Configuration** > **Advanced** > **DOICPriorities;** e.g. Priority2,Priority3.
DivertHost	IP address of the remote server to which the incoming requests should get diverted under active overload conditions. This IP has to be configured under Remoteservers in Prime Access Registrar configuration. If **DOICPriorityList** is specified, **DivertHost** must be given some value.

Adding Diameter Remote Server Details

To add new Diameter remote server details:

Step 1 Choose **Network Resources > RemoteServers > Diameter**. The Diameter-Remote Servers page is displayed.

Step 2 Click **Add** to add Diameter remote server details.

Step 3 Enter the required details as described in Table 2-69.

Step 4 Click **Add Diameter Server** to save the details. Click **Cancel** to return to the previous page without saving the details.

The Diameter-Remote Servers page is displayed with the newly added details or a respective error message is displayed.

REST

Prime Access Registrar allows you to configure a REST remote server for extended-EAP service. Extended-EAP is used as an authorization service to retrieve authorization information from the remote web server using the REST interface. Prime Access Registrar processes all EAP requests and extends through extended EAP service. Extended-EAP is supported for the following EAP protocols:

- EAP-AKA
- EAP-AKA-PRIME
- EAP-SIM

You can click the **Add** button in the **REST-RemoteServers** page to add a new REST remote server. Table 2-70 lists and describes the REST remote server properties.

Table 2-70 REST Remote Server Properties

Fields	Description
RESTRemoteServerProperties Tab	
Name	Required; name of the REST server.
Description	Optional; description of the REST server.
Protocol	Indicates the protocol, which is REST.
ReactivateTimerInterval	Required; time interval, in milliseconds, to reactivate an inactive REST server. Default value is 300000.
RequestTimeout	Required; timeout value, in milliseconds, the REST server can wait for a request or response before attempting a retry. Default value is 2000. We recommend that you set the value to 1000.
MaxTimeOuts	Maximum number of timeouts allowed for the remote server.
RESTSourceConnections	Mandatory number of connections to be established towards the REST server; default value is eight.
RequestURL	Required; URL of the REST web server including port number. Ensure that you enter IMSI keyword in the URL.
UserName	Required; user name of the REST web server.
Password	Required; password of the REST web server.
KeepAliveTimerInterval	Mandatory time interval, in milliseconds, to send a keepalive to keep the idle connection active; defaults to zero (0) meaning the option is disabled.

You can use the REST RemoteServer page for the following:

- Filtering Records
- Editing Records
- Deleting Records

Adding REST Remote Server Details

To add new REST remote server details:

Step 1 Choose **Network Resources > RemoteServers > REST**. The **REST-RemoteServers** page is displayed.

Step 2 Click **Add** to add REST remote server details.

Step 3 Enter the required details as described in Table 2-70.

Step 4 Click **Save REST Server** to save the details. Click **Cancel** to return to the previous page without saving the details.

The REST-RemoteServers page is displayed with the newly added details or a respective error message is displayed.

Others

This feature of GUI allows you to set other specifications. The various types of protocols are:

- Radius
- Dynamic DNS
- Map-Gateway
- Prepaid-CRB
- Prepaid IS 835C
- Sigtran
- Sigtran-m3ua

Table 2-71 lists and describes the fields in the Remote Server Details page. The fields listed below are the entire list of all the available protocols. The fields are displayed based on the type of protocol selected.

Table 2-71 Other Server Properties

Fields	Description
Remote Server Details	
Name	Required; name of the server.
Description	Optional; description of the server.
Protocol	Required; type of the remote server. Choose from one of the following options: • Radius • Dynamic DNS • Map-Gateway • Prepaid-CRB • Prepa-IS835C • Sigtran • Sigtran-m3ua
IP Address	Required; this property specifies where to send the proxy request. It is the address of the remote server. You must set it to a valid IP address.

Table 2-71 Other Server Properties (continued)

Fields	Description
Port	By default, Prime Access Registrar listens on ports 1812 and 1813.
ReactivateTimerInterval	Mandatory time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms.
MaxTries	Number of times the server tries to send dynamic updates to a server.
Initial Timeout	Time, in milliseconds, that the server waits for a response before retrying a request.
SharedSecret	Required; the secret shared between the remote server and the RADIUS server.
Vendor	Optional; when set, must be the name of a known Vendor.
IncomingScript	Optional; when set, must be the name of a known incoming script. Prime Access Registrar runs the IncomingScript after it receives the response.
OutGoingScript	Optional; when set, must be the name of a known outgoing script. Prime Access Registrar runs the OutgoingScript just before it sends the proxy request to the remote server.
AccountingPort	Port where the RADIUS server sends accounting packets.
AcknowledgeAccounting	When ACKAccounting is TRUE, the Prime Access Registrar server waits for the Accounting-Response from the remote RADIUS server before sending the corresponding Accounting-Response to the client. When ACKAccounting is FALSE, the Prime Access Registrar server returns an Accounting-Response to the client without waiting for a response from the remote server.
SendandForget	This field is available if the AcknowledgeAccounting option is disabled. After forwarding a proxy packet to the remote server and an initial response to the client, Prime Access Registrar maintains a buffer of the original request and a copy of the proxy request until it receives a response from the remote server or packet timeout is triggered. If SendandForget is enabled, Prime Access Registrar deletes the original and proxy requests from the buffer after sending the response to the client. This helps in reducing buffer pool exhaustion in case of a low-responding remote server.
Accept Dynamic Authorization Requests	The value is set to False, by default.
MaxRename Retries	Number of times that the resource managers can try to add a host even if it detects that the host's name is already present. This controls the number of times Prime Access Registrar tries to modify a host's name to resolve a conflict on each failed update.

Table 2-71 Other Server Properties (continued)

Fields	Description
MaxTPSLimit	Maximum number of requests allowed per second for the remote server. This field is available only for RADIUS remote server.
MaxSessionLimit	Maximum number of sessions allowed for the remote server. This field is available only for RADIUS and Sigtran-m3ua remote servers.
Trim HostName	Controls whether Prime Access Registrar trims the hostname string to the first period character. If this attribute is enabled, the hostname is truncated before the period. If disabled, the server retains the period characters in the hostname.
FwdZoneTSIG	Server-wide security key to process all forward zone dynamic DNS updates. This is used if a ForwardZoneTSIGKey was not specified on the Resource Manager.
ReverseZoneTSIG	Server-wide security key to process all reverse zone dynamic DNS updates. This is used if a ReverseZoneTSIGKey was not specified on the Resource Manager.
File Name	Name of the shared library provided by the billing server vendor, such as **libprepaid.so**
Connections	Number of threads the prepaid service and billing server can each use (default is 8).
HostName	Required; hostname of the remote server.
Local Sub System Number	Required; the default value for this property is 0. This represents the subsystem number used by SUA user.
CgPA Global Title Address	Required; represents the Global Title Address of CallingPartyAddress.
Set OPC In CgPA	Required; if it is set to TRUE, OPC will be used in CallingPartyAddress.
CdPANumberingPlan	Required; used to specify the numbering plan of the called party. The default value is 7.
CgPANumberingPlan	Required; used to specify the numbering plan of the calling party. The default value is 7.
Global Title Translation Script	This is used to specify the name of the script which is responsible for translating IMSI to GTA. You can choose to configure block listing as part of the global title translation script for SIGTRAN-M3UA remote server. For more information about block listing, see the “Using Extension Points” chapter of the *Cisco Prime Access Registrar 9.2 Administrator Guide*.
SUA Configuration Filename	Required; used to specify the name of configuration file for SUA stack initialization.
Max Outstanding Requests	This represents the maximum outstanding request to HLR.

Table 2-71 Other Server Properties (continued)

Fields	Description
Timeout	Required; represents the how long the remote server should wait before marking the request as timedout.
Limit Outstanding Requests	Limits the outstanding request to HLR when it is set to TRUE.
SourceIPAddress	Required; name of the local IP address.
SourcePort	Required; specify the port number in which Prime Access Registrar is installed for M3UA transactions.
LocalSubSystemNumber	Required; the local sub system number is set as 149 by default.
DestinationPort	Required; specify the destination port number to which Prime Access Registrar connects.
IMSITranslationScript	Specify the scripting point that is used to modify the IMSI based on the requirement before sending the request to STP/HLR.
Timeout	Required; specify the time (in seconds) to wait before an authentication request times out; defaults to 120.
ReactivateTimerInterval	Required; specify the time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms (which is 5 minutes).
Limit Outstanding Requests	Prime Access Registrar uses this property in conjunction with the MaxOutstandingRequests property to tune the RADIUS server's use of the HLR. The default is FALSE. When you set this property to TRUE, the number of outstanding requests for this RemoteServer is limited to the value you specified in MaxOutstandingRequests. When the number of requests exceeds this number, Prime Access Registrar queues the remaining requests, and sends them as soon as the number of outstanding requests drops to this number.
MaxOutstandingRequests	Required; specify the maximum number of outstanding requests allowed for this remote server.
MAP-Version	Required; specify the MAP version as 2 or 3 that HLR supports.
NetworkVariant	Required for SIGTRAN-M3UA remote server; Choose **ITU** or **ANSI** to represent the standard that SIGTRAN-M3UA remote server supports.
SubServiceField	Required; specify the type of network to which this SAP belongs. The possible options are INT and NAT which represents international network and national network respectively.
TCAPVariant	Required; specify the name of the TCAP network variant switch. The possible options are ITU88, ITU92, or ITU96.
NetworkAppearance	Required; specify the network appearance code which ranges from 0-2147483647. This field is optional for SIGTRAN-M3UA remote servers as per the RFC 4666 (http://tools.ietf.org/html/rfc4666.) You can set the value to 0 to remove network appearance from the data packet.
NetworkIndicator	Required; specify the network indicator used in SCCP address. The possible options are NAT and INT which represents international network and national network respectively.

Table 2-71 Other Server Properties (continued)

Fields	Description
RoutingIndicator	Required; specify the routing indicator. The possible options are RTE_GT or RTE_SSN which is used to route the packets for HLR.
MLCNumber	Required; specify the MLC number which is required for M3UA service for fetching the MSISDN from the HLR. This is the map layer network node number by which the HLR identifies the Prime Access Registrar in the network. The MLC number is configured in E.164 format. **Note** MLC is a max-15 digit number.
TrafficMode	Required; specify the traffic mode values for the HLR.
LoadShareMode	Required; specify the load share mode for the HLR. When there is more than one associations with HLR, then the load sharing is set as Signaling Link Selection (SLS). SLS is done based on a simple round-robin basis.
SCCPVariant	The Signaling Connection Control Part (SCCP) variant of the Global Title: • Select **ITU88**, **ITU92**, or **ITU96**, if NetworkVariant is set to ITU. • Select **ANS88**, **ANS92**, or **ANS96**, if NetworkVariant is set to ANS.
MaxTimeOuts	Maximum number of timeouts allowed for the remote server.
RoutingParameters	
OriginPointCode	Required; specify the originating point of a message in a signalling network. The value ranges from 0 - 16777215.
DestinationPointCode	Required; specify the destination address of a signalling point in a SS7 network.
RemoteSubSystemNumber	Required; specify the sub system number of the remote server. The RemoteSubSystemNumber is set as 6 by default.
OPCMask	Required; specify the wild card mask for the origin point code. The value ranges from 0 - 16777215.
DPCMask	Specify the wild card mask for the destination point code. The value ranges from 0 - 16777215.
ServiceIndicatorOctet	Specify the service identifier octet. The value ranges from 0 - 255.
RoutingContext	Required; specify the routing context which ranges from 0 - 16777215.
Source & Destination IP Addresses	

Table 2-71 Other Server Properties (continued)

Fields	Description
SourceIPAddresses	Applicable only for Sigtran-m3ua protocol type. Enter the source IP address to be configured on the remote server and then click **Add**. The entered IP address is displayed in the SourceIPAddresses list box. Click **Delete** to remote the IP address from the list.
DestinationIPAddresses	Applicable only for Sigtran-m3ua protocol type. Enter the destination IP address to be configured on the remote server and then click **Add**. The entered IP address is displayed in the DestinationIPAddresses list box. Click **Delete** to remote the IP address from the list.

You can use the RemoteServers page allows for the following:

- Filtering Records
- Setting Other Specifications
- Editing Records
- Deleting Records

Setting Other Specifications

To set up other specifications:

Step 1 Select **Network Resources > RemoteServers > Others**. The RemoteServers page is displayed.

Step 2 Click **Add** to add other specifications. The Remote Server Details page is displayed.

Step 3 Enter the required details.

Step 4 Click **Add Radius Server** to save the specified details in the Remote Server Details page. Otherwise click **Cancel** to return to the RemoteServers page without saving the details.

The RemoteServers page is displayed with the newly added details or a respective error message is displayed.

Administration

Administration constitutes the maintenance and management of details specific administrator, various statistical data respective to the administrators, backing up and restoring server details, and license management of the server.

This section describes the following:

- Administrators
- Statistics
- DiameterStatistics
- TACACSStatistics

- Back Up and Restore
- LicenseUpload
- HealthMonitor

Administrators

Prime Access Registrar provided *super-user* administrative access in which administrator can perform all tasks including starting and stopping the system and changing the configuration.
Prime Access Registrar also provides view-only administrative access. View-only access restricts an administrator to only being able to observe the system and prevents that user from making changes.

Table 2-72 lists and describes the fields in the Administrator Details page.

Table 2-72 Administrator Properties

Fields	Description
Name	Required; administrator's user ID.
Description	Optional; description of the administrator.
New Password	Required; encrypted password of the administrator.
Confirm New Password	Required; encrypted password of the administrator and must match Password.
View Only	Default value (FALSE) indicates that the administrator is able to modify the configuration. When set to TRUE, the administrator can only view the server configuration and set the change the server trace level.

You can use the Administrators page for the following:

- Filtering Records
- Adding Administrator Details
- Statistics
- Editing Records
- Deleting Records

Adding Administrator Details

To add new Administrator details:

Step 1 Choose **Administration** > **Administrators**. The Administrators page is displayed.

Step 2 Click **Add** to add administrator details. The Administrator Details page is displayed.

Step 3 Specify the required details.

Step 4 Click **Submit** to save the specified details in the Administrator Details page. Otherwise click **Cancel** to return to the Administrators page without saving the details.

The Administrators page is displayed with the newly added details or a respective error message is displayed.

Statistics

This feature provides statistical information on the specified RADIUS server.

Table 2-73 lists the statistics information of the RADIUS server.

Table 2-73 aregcmd stats Information for RADIUS server

Stats Value	Meaning
serverStartTime	Indicates the start time of the server.
serverResetTime	Indicates the time when the server was reloaded.
serverStat	Indicates if the server is running or stopped.
totalCPUUtilizationOfRadiusProcess	Indicates the CPU utilization for RADIUS process.
totalMemoryLimitForRadiusProcess	Indicates the total memory for RADIUS process.
totalUsedMemoryByRadiusProcess	Indicates the used memory for RADIUS process.
totalAvailableMemoryForRadiusProcess	Indicates the free memory for RADIUS process.
totalPacketsInPool	Number of packets that can be accommodated in the pool.
totalPacketsReceived	Number of packets that are received by RADIUS server.
totalPacketsSent	Number of packets that are sent by RADIUS server.
totalRequests	Number of requests received by RADIUS server. This includes access requests and accounting requests.
totalResponses	Number of responses sent by RADIUS server. This includes access accepts/rejects and accounting responses.
totalAccessRequests	Number of access requests received/processed by RADIUS server.
totalAccessAccepts	Number of access accepts sent by RADIUS server.
totalAccessChallenges	Number of access challenges sent by RADIUS server.

Table 2-73 aregcmd stats Information for RADIUS server (continued)

Stats Value	Meaning
totalAccessRejects	Number of access rejects sent by RADIUS server.
totalAccessResponses	Number of access responses sent by RADIUS server.
totalAccountingRequests	Number of accounting requests received by RADIUS server.
totalAccountingResponses	Number of accounting responses sent by RADIUS server.
totalStatusServerRequests	Number of status server request received by RADIUS server.
totalAscendIPAAllocateRequests	Number of requests received related to Ascend IP address allocation.
totalAscendIPAAllocateResponses	Number of responses sent related to Ascend IP Address Allocation.
totalAscendIPAReleaseRequests	Number of requests received related to Ascend IP Address release.
totalAscendIPAReleaseResponses	Number of responses sent related to Ascend IP Address release.
totalUSRNASRebootRequests	Number of user NAS reboot request received by RADIUS server.
totalUSRNASRebootResponses	Number of user NAS reboot response sent by RADIUS server.
totalUSRResourceFreeRequests	Number of user resource free request received by RADIUS server.
totalUSRResourceFreeResponses	Number of user resource free response sent by RADIUS server.
totalUSRQueryResourceRequests	Number of user query resource request received by RADIUS server.
totalUSRQueryResourceResponses	Number of user query resource response sent by RADIUS server.
totalUSRQueryReclaimRequests	Number of user query reclaim request received by RADIUS server.
totalUSRQueryReclaimResponses	Number of user query reclaim response sent by RADIUS server.
totalPacketsInUse	Number of packets that are being used.
totalPacketsDrained	Number of packets that are drained.
totalPacketsDropped	Number of packets that are dropped.
totalPayloadDecryptionFailures	Number of failures due to payloads decryption.
totalEAPSIMDecryptionFailures	Number of IMSI decryption failures for EAP-SIM services.

Table 2-73 aregcmd stats Information for RADIUS server (continued)

Stats Value	Meaning
totalEAPSIMDecryptionSuccess	Number of IMSI decryption success for EAP-SIM services.
totalEAPAKADecryptionFailures	Number of IMSI decryption failures for EAP-AKA services.
totalEAPAKADecryptionSuccess	Number of IMSI decryption success for EAP-AKA services.
totalEAPAKAPRIMEDecryptionFailures	Number of IMSI decryption failures for EAP-AKA’ services.
totalEAPAKAPRIMEDecryptionSuccess	Number of IMSI decryption success for EAP-AKA’ services.
OCIActiveConnectionCount	Number of active OCI connections from Prime Access Registrar to the Oracle database.
TotalRESTErrorResponses	Number of error responses from REST server.
TotalRequestsAcknowledged	Number of responses received since last server restart.
TotalResponsesDroppedForNotInCache	Number of responses dropped because their ID did not match the ID of any Pending requests.
TotalResponsesDroppedForSignatureMismatch	Number of responses dropped because their response authenticator did not decode to the correct shared secret.
TotalRequestsDroppedAfterMaxTries	Number of requests dropped because no response was received after retrying the configured number of times. This value is different from totalRequestsTimedOut because using the default configuration values, no response within 2000 ms bumps the TimedOut counter, but it waits 14000 ms (2000 + 4000 + 8000) to bump this counter.
LastRequestTime	Date and time of last proxy request.
LastAcceptTime	Date and time of last ACCEPT response to a client.
The following fields appear when you select a RADIUS client from the Clients drop-down list box at the bottom of the page.	
RADIUS Client statistics for:	Provides client’s IP address, name, and IP address type
TLSActiveConnectionCount	Number of active TLS connections established for the RADIUS client.
totalAuthAccessRequests	Number of authentication access requests that are received by Prime Access Registrar from the client.

Table 2-73 aregcmd stats Information for RADIUS server (continued)

Stats Value	Meaning
totalAuthDupAccessRequests	Number of duplicate authentication access requests that are received by Prime Access Registrar from the client.
totalAuthAccessAccepts	Number of authentication access requests from the client that are accepted by Prime Access Registrar.
totalAuthAccessRejects	Number of authentication access requests from the client that are rejected by Prime Access Registrar.
totalAuthAccessChallenges	Number of authentication challenges that are faced by Prime Access Registrar for the requests raised by the client.
totalAuthMalformedAccessRequests	Number of malformed authentication access requests that are received by Prime Access Registrar from the client.
totalAuthBadAuthenticators	Number of bad authentication access requests that are received by Prime Access Registrar from the client.
totalAuthPacketsDropped	Number of authentication access requests received from the client that are dropped by Prime Access Registrar. The packets, which are invalid and do not fulfill the parsing conditions, are dropped.
totalAuthUnknownTypes	Number of unknown authentication access requests that are received by Prime Access Registrar from the client.
totalAccPacketsDropped	Number of accounting access requests received from the client that are dropped by Prime Access Registrar. The packets, which are invalid and do not fulfill the parsing conditions, are dropped.
totalAccRequests	Number of accounting access requests received by Prime Access Registrar from the client.
totalAccDupRequests	Number of duplicate accounting access requests that are received by Prime Access Registrar from the client.
totalAccResponses	Number of accounting response sent by Prime Access Registrar to the client
totalAccBadAuthenticators	Number of bad accounting access requests that are received by Prime Access Registrar from the client.
totalAccMalformedRequests	Number of malformed accounting access requests that are received by Prime Access Registrar from the client.

Table 2-73 aregcmd stats Information for RADIUS server (continued)

Stats Value	Meaning
totalAccNoRecords	Number of accounting access requests that are received with no records by Prime Access Registrar from the client.
totalAccUnknownTypes	Number of unknown accounting access requests that are received by Prime Access Registrar from the client.

Resetting Server Statistics

To reset server statistics:

Step 1 Choose **Administration** > **Statistics**. The Radius Server Statistics page is displayed.

Step 2 Click **Reset** to reset all the RADIUS server statistics.

DiameterStatistics

Prime Access Registrar supports statistic of Diameter messages through the CLI/GUI and SNMP. The existing ‘stats’ module has been extended to include additional counters related to Diameter. The Diameter statistics includes peer statistics and global summary statistics details on the specified server.

Table 2-74 lists the statistics information of the Diameter server. The statistical information in Table 2-75 is displayed based on the Diameter peer selected. Table 2-76 is displayed based on the Diameter remote server selected.

Table 2-74 Diameter Stats Information

Metric	Value
Diameter Statistics	
serverStartTime	The start time of the server.
serverResetTime	The reset time of the server.
serverState	The state of the server.
cdbpLocalStatsTotalUpTime	The total time for which the Diameter server is up.
cdbpLocalResetTime	The time elapsed since a server was reset.
cdbpLocalStatsTotalNumberOfDiameterPackets	Total number of allocated Diameter packets.
cdbpLocalStatsTotalAvailableDiameterPackets	Total number of available Diameter packets.
cdbpLocalStatsTotalPacketsIn	The total number of packets received by a Diameter Base protocol.
cdbpLocalStatsTotalPacketsOut	The total number of packets transmitted by a Diameter Base protocol.

Table 2-74 Diameter Stats Information (continued)

Metric	Value
cdbpLocalStatsTotalPacketsInUse	The total number of packets used.
cdbpLocalStatsTotalnumberofStaleSessions	The total number of Diameter stale sessions in Prime Access Registrar. The stale sessions will be released during the stale session removal process that runs at the specified purge time (/Radius/Advanced/ Diameter-StaleSessionPurgeTime).
cdbpLocalStatsTotalnumberofSessions	The total number of Diameter sessions in Prime Access Registrar.
Peer	The name of the peer. You can select a peer from the drop-down list.

Table 2-75 Diameter Peer Stats Information

Metric	Value
Diameter Peers: To view the following fields, select a Diameter peer from the **Peer** drop-down list box and then click **Show Peer Stats**. Click **Reset**, to reset all the Diameter statistics of the peer.	
Stats for the Remote Server	The name of the selected peer.
ipaddress	The IP address of the peer.
port	The port of the peer.
cdbpPeerStatsState	Indicates the connection state in the Peer State Machine of the peer with which the Diameter server is communicating.
cdbpPeerStatsASAsOut	Number of Abort-Session-Answer messages that are sent to the peer.
cdbpPeerStatsACRsIn	Number of Accounting-Request messages that are received from the peer
cdbpPeerStatsACRsOut	Number of Accounting-Request messages that are sent to the peer.
cdbpPeerStatsACAsIn	Number of Accounting-Answer messages that are received from the peer.
cdbpPeerStatsACAsOut	Number of Accounting-Answer messages that are sent to the peer.
cdbpPeerStatsCERsIn	Number of Capabilities-Exchange-Request messages received from the peer.
cdbpPeerStatsCERsOut	Number of Capabilities-Exchange-Request messages sent to the peer.
cdbpPeerStatsCEAsIn	Number of Capabilities-Exchange-Answer messages received from the peer.
cdbpPeerStatsCEAsOut	Number of Capabilities-Exchange-Answer messages sent to the peer.

Table 2-75 Diameter Peer Stats Information (continued)

Metric	Value
cdbpPeerStatsDWRsIn	Number of Device-Watchdog-Request messages received from the peer.
cdbpPeerStatsStateDuration	Represents the Peer state duration.
cdbpPeerStatsDWRsOut	Number of Device-Watchdog-Request messages sent to the peer.
cdbpPeerStatsDWAsIn	Number of Device-Watchdog-Answer messages received from the peer.
cdbpPeerStatsDWAsOut	Number of Device-Watchdog-Answer messages sent to the peer.
cdbpPeerStatsDPRsIn	Number of Disconnect-Peer-Request messages received from the peer.
cdbpPeerStatsDPRsOut	Number of Disconnect-Peer-Request messages sent to the peer.
cdbpPeerStatsDPAsIn	Number of Disconnect-Peer-Answer messages received from the peer.
cdbpPeerStatsDPAsOut	Number of Disconnect-Peer-Answer messages sent to the peer.
cdbpPeerStatsRARsIn	Number of Re-Auth-Request messages that are received from the peer.
cdbpPeerStatsRARsOut	Number of Re-Auth-Request messages that are sent to the peer.
cdbpPeerStatsRAAsIn	Number of Re-Auth-Answer messages that are received from the peer.
PeerStatsRstRARsOut	Number of Reset (RST) Re-Auth-Request messages triggered during the session restoration process.
PeerStatsRstRAAsIn	Number of RST Re-Auth-Answer messages received from the peer during the session restoration process.
PeerStatsRstFailedRARs	Number of failed Re-Auth-Request messages during the session restoration process.
cdbpPeerStatsLastDiscCause	The last cause for a peer’s disconnection.
cdbpPeerStatsRAAsOut	Number of Re-Auth-Answer messages that are sent to the peer.
cdbpPeerStatsSTRsIn	Number of Session-Termination-Request messages that are received from the peer.
cdbpPeerStatsSTRsOut	Number of Session-Termination-Request messages that are sent to the peer.
cdbpPeerStatsSTAsIn	Number of Session-Termination-Answer messages that are received from the peer.
cdbpPeerStatsSTAsOut	Number of Session-Termination-Answer messages that are sent to the peer.
cdbpPeerStatsDWReqTimer	The interval between the packets that are sent to the peers.

Table 2-75 ***Diameter Peer Stats Information (continued)***

Metric	Value
cdbpPeerstatsRedirectEvents	Number of redirects that are sent from a peer.
cdbpPeerStatsAccDupRequests	Number of duplicate Diameter Accounting-Request packets.
cdbpPeerStatsMalformedReqsts	Number of malformed Diameter packets that are received.
cdbpPeerStatsAccsNotRecorded	Number of Diameter Accounting-Request packets that are received and responded but not recorded.
cdbpPeerStatsWhoInitDisconnect	Indicates whether the host or peer initiated the disconnect.
cdbpPeerStatsAccRetrans	Number of Diameter Accounting-Request packets that are retransmitted to the Diameter server.
cdbpPeerStatsTotalRetrans	Number of Diameter packets that are retransmitted to the Diameter server. This does not include the Diameter Accounting-Request packets that are retransmitted.
cdbpPeerStatsAccPendReqstsOut	Number of Diameter Accounting-Request packets that are sent to the peer which have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent to the server and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
cdbpPeerStatsAccReqstsDropped	Number of Accounting-Requests to the server that are dropped.
cdbpPeerStatsHByHDropMessages	An answer message that is received with an unknown hop-by-hop identifier. This does not include the accounting requests that are dropped.
cdbpPeerStatsEToEDupMessages	The duplicate answer messages that are locally consumed. This does not include duplicate accounting requests that are received.
cdbpPeerStatsUnknownTypes	Number of Diameter packets of unknown type that are received from the peer.
cdbpPeerStatsProtocolErrors	Number of protocol errors that are returned to peer, but not including the redirects.
cdbpPeerStatsTransientFailures	Indicates the transient failure count.
cdbpPeerStatsPermanentFailures	Indicates the permanent failure count.
cdbpPeerStatsDWCurrentStatus	Indicates the connection status of the peer.
cdbpPeerStatsTransportDown	Number of unexpected transport failures.
cdbpPeerStatsTimeoutConnAtmpts	Number of times the server attempts to connect to a peer when there is no transport connection with the peer. This is reset on disconnection.
cdbpPeerStatsASRsIn	Number of Abort-Session-Request messages that are received from the peer.
cdbpPeerStatsASRsOut	Number Abort-Session-Request messages that are sent to the peer.

Table 2-75 Diameter Peer Stats Information (continued)

Metric	Value
cdbpPeerStatsASAsIn	Number of Abort-Session-Answer messages that are received from the peer.
cdbpPeerStatsDERsIn	Number of Diameter-EAP-Request (DER) messages that are received from the peer.
cdbpPeerStatsDERsOut	Number of DER messages that are sent to the peer.
cdbpPeerStatsDEAsIn	Number of Diameter-EAP-Answer (DEA) messages that are received from the peer.
cdbpPeerStatsDEAsOut	Number of DEA messages that are sent to the peer.
cdbpPeerStats5GIndicatorDEAsIn	Number of DEA messages with Interworking-5GS-Indicator AVP that are received from the peer. The Interworking-5GS-Indicator AVP is present in the DEA packet to differentiate it as a 5G packet. This will help in understanding the 5G DEA message flow in Prime Access Registrar.
cdbpPeerStats5GIndicatorDEAsOut	Number of DEA messages with Interworking-5GS-Indicator AVP that are sent to the peer. **Note** If the environment variable **EnableMatchingServiceSelection5GFlag** is set to 1, the **cdbpPeerStats5GIndicatorDEAsOut** counter is updated only if the Interworking-5GS-Indicator AVP is present in the APN configuration of matching Service-Selection. For more details about the environment variable, see “Environment Variable” chapter of the *Cisco Prime Access Registrar 9.2 Reference Gui de*.
cdbpPeerStatsAARsIn	Number of AA-Request messages that are received from the peer.
cdbpPeerStatsAARsOut	Number of AA-Request messages that are sent to the peer.
cdbpPeerStatsAAAsIn	Number of AA-Answer messages that are received from the peer.
cdbpPeerStatsAAAsOut	Number of AA-Answer messages that are sent to the peer.
cdbpPeerStatsMARsIn	Number of Multimedia-Authentication-Request messages that are received from the peer.
cdbpPeerStatsMARsOut	Number of Multimedia-Authentication-Request messages that are sent to the peer.
cdbpPeerStatsMAAsIn	Number of Mutlimedia-Authentication-Answer messages that are received from the peer.
cdbpPeerStatsMAAsOut	Number of Mutlimedia-Authentication-Answer messages that are sent to the peer.
cdbpPeerStatsSARsIn	Number of Server-Assignment-Request messages that are received from the peer.

Table 2-75 Diameter Peer Stats Information (continued)

Metric	Value
ccdbpPeerStatsSARsOut	Number of Server-Assignment-Request messages that are sent to the peer.
cdbpPeerStatsSAAsIn	Number of Server-Assignment-Answer messages that are received from the peer.
cdbpPeerStatsSAAsOut	Number of Server-Assignment-Answer messages that are sent to the peer.
cdbpPeerStatsRTRsIn	Number of Registration-Termination-Request messages that are received from the peer.
cdbpPeerStatsRTRsOut	Number of Registration-Termination-Request messages that are sent to the peer.
cdbpPeerStatsRTAsIn	Number of Registration-Termination-Answer messages that are received from the peer.
cdbpPeerStatsRTAsOut	Number of Registration-Termination-Answer messages that are sent to the peer.
cdbpPeerStatsPPRsIn	Number of Push-Profile-Request messages that are received from the peer.
cdbpPeerStatsPPRsOut	Number of Push-Profile-Request messages that are sent to the peer.
cdbpPeerStatsPPAsIn	Number of Push-Profile-Answer messages that are received from the peer.
cdbpPeerStatsPPAsOut	Number of Push-Profile-Answer messages that are sent to the peer.
cdbpPeerStatsCoreNetRestrictionDEAsIn	Number of DEA messages with Core-Network-Restrictions AVP that are received from the peer. The Core-Network-Restrictions AVP is present in the DEA packet to indicate the various types of core networks that are not allowed for a given user.
cdbpPeerStatsCoreNetRestrictionDEA-sOut	Number of DEA messages with Core-Network-Restrictions AVP that are sent to the peer.

Table 2-76 Diameter Remote Server Stats Information

Metric	Value
Diameter RemoteServers: To view the following fields, select a remote server from the **RemoteServers** drop-down list box and then click **Show RemoteServer Stats**. Click **Reset**, to reset all the Diameter statistics of the remote server.	
Stats for the Remote Server	The name of the selected remote server.
ipaddress	The IP address of the remote server.
port	The port of the remote server.
cDiaRemSvrActive	Indicates whether the server was active (not in a down state).

Table 2-76 Diameter Remote Server Stats Information (continued)

Metric	Value
cDiaRemSvrRTTAverage	Average round trip time since the last server restart.
cDiaRemSvrRTTDeviation	Indicates a standard deviation of the RTTAverage.
cDiaRemSvrServerType	Indicates the remote server type.
cDiaRemSvrTotalRequestsPending	Number of requests currently queued.
cDiaRemSvrTotalRequestsOutstanding	Number of requests currently proxied that have not yet returned
cDiaRemSvrTotalRequestsAcknowledged	Number of responses received since last server restart.
cDiaRemSvrStatsState	Indicates the connection state of the Diameter remote server.
cDiaRemSvrStatsASRsIn	Number of Abort-Session-Request messages that are received by the remote server.
cDiaRemSvrStatsASRsOut	Number Abort-Session-Request messages that are sent by the remote server.
cDiaRemSvrStatsASAsIn	Number of Abort-Session-Answer messages that are received by the remote server.
cDiaRemSvrStatsASAsOut	Number of Abort-Session-Answer messages that are sent by the remote server.
cDiaRemSvrStatsACRsIn	Number of Accounting-Request messages that are received by the remote server.
cDiaRemSvrStatsACRsOut	Number of Accounting-Request messages that are sent by the remote server.
cDiaRemSvrStatsACAsIn	Number of Accounting-Answer messages that are received by the remote server.
cDiaRemSvrStatsACAsOut	Number of Accounting-Answer messages that are sent by the remote server.
cDiaRemSvrStatsCERsIn	Number of Capabilities-Exchange-Request messages received by the remote server.
cDiaRemSvrStatsCERsOut	Number of Capabilities-Exchange-Request messages sent by the remote server.
cDiaRemSvrStatsCEAsIn	Number of Capabilities-Exchange-Answer messages received by the remote server.
cDiaRemSvrStatsCEAsOut	Number of Capabilities-Exchange-Answer messages sent by the remote server.
cDiaRemSvrStatsDWRsIn	Number of Device-Watchdog-Request messages received by the remote server.
cDiaRemSvrStatsDWRsOut	Number of Device-Watchdog-Request messages sent by the remote server.
cDiaRemSvrStatsDWAsIn	Number of Device-Watchdog-Answer messages received by the remote server.

Table 2-76 Diameter Remote Server Stats Information (continued)

Metric	Value
cDiaRemSvrStatsDWAsOut	Number of Device-Watchdog-Answer messages sent by the remote server.
cDiaRemSvrStatsDPRsIn	Number of Disconnect-Peer-Request messages received by the remote server.
cDiaRemSvrStatsDPRsOut	Number of Disconnect-Peer-Request messages sent by the remote server.
cDiaRemSvrStatsDPAsIn	Number of Disconnect-Peer-Answer messages received by the remote server.
cDiaRemSvrStatsDPAsOut	Number of Disconnect-Peer-Answer messages sent by the remote server.
cDiaRemSvrStatsRARsIn	Number of Re-Auth-Request messages that are received by the remote server.
cDiaRemSvrStatsRARsOut	Number of Re-Auth-Request messages that are sent by the remote server.
cDiaRemSvrStatsRAAsIn	Number of Re-Auth-Answer messages that are received by the remote server.
cDiaRemSvrStatsRAAsOut	Number of Re-Auth-Answer messages that are sent by the remote server.
cDiaRemSvrStatsSTRsIn	Number of Session-Termination-Request messages that are received by the remote server.
cDiaRemSvrStatsSTRsOut	Number of Session-Termination-Request messages that are sent by the remote server.
cDiaRemSvrStatsSTAsIn	Number of Session-Termination-Answer messages that are received by the remote server.
cDiaRemSvrStatsSTAsOut	Number of Session-Termination-Answer messages that are sent by the remote server.
cDiaRemSvrStatsRedirectEvents	Number of redirects that are sent from the remote server.
cDiaRemSvrStatsAccDupRequests	Number of duplicate Diameter Accounting-Request packets.
cDiaRemSvrStatsMalformedRequests	Number of malformed Diameter packets that are received.
cDiaRemSvrStatsAccsNotRecorded	Number of Diameter Accounting-Request packets that are received and responded but not recorded.
cDiaRemSvrStatsWhoInitDisconnect	Indicates whether the host or remote server initiated the disconnect.
cDiaRemSvrStatsAccRetrans	Number of Diameter Accounting-Request packets that are retransmitted by the Diameter remote server.
cDiaRemSvrStatsTotalRetrans	Number of Diameter packets that are retransmitted by the Diameter server. This does not include the Diameter Accounting-Request packets that are retransmitted.

Table 2-76 Diameter Remote Server Stats Information (continued)

Metric	Value
cDiaRemSvrStatsAccPendRequestsOut	Number of Diameter Accounting-Request packets that are sent by the remote server which have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent by the server and decremented due to receipt of an Accounting-Response, a timeout or a re-transmission.
cDiaRemSvrStatsAccReqstsDropped	Number of Accounting-Requests that are dropped.
cDiaRemSvrStatsHByHDropMessages	An answer message that is received with an unknown hop-by-hop identifier. This does not include the accounting requests that are dropped.
cDiaRemSvrStatsEToEDupMessages	The duplicate answer messages that are locally consumed. This does not include duplicate accounting requests that are received.
cDiaRemSvrStatsUnknownTypes	Number of Diameter packets of unknown type that are received by the remote server.
cDiaRemSvrStatsProtocolErrors	Number of protocol errors that are returned by the remote server, but not including the redirects.
cDiaRemSvrStatsTransientFailures	Indicates the transient failure count.
cDiaRemSvrStatsPermanentFailures	Indicates the permanent failure count.
cDiaRemSvrStatsDWCurrentStatus	Indicates the connection status of the remote server.
cDiaRemSvrStatsTransportDown	Number of unexpected transport failures.
cDiaRemSvrStatsTimeoutConnAtmpts	Number of times the remote server attempts to reconnect when there is no transport connection. This is reset on disconnection.
cDiaRemSvrStatsMARsIn	Number of Multimedia-Authentication-Request messages that are received by the remote server.
cDiaRemSvrStatsMARsOut	Number of Multimedia-Authentication-Request messages that are sent by the remote server.
cDiaRemSvrStatsMAAsIn	Number of Mutlimedia-Authentication-Answer messages that are received by the remote server.
cDiaRemSvrStatsMAAsOut	Number of Mutlimedia-Authentication-Answer messages that are sent by the remote server.
cDiaRemSvrStatsSARsIn	Number of Server-Assignment-Request (SAR) messages that are received by the remote server.
cDiaRemSvrStatsSARsOut	Number of SAR messages that are sent by the remote server.
cDiaRemSvrStatsSAAsIn	Number of Server-Assignment-Answer (SAA) messages that are received by the remote server.
cDiaRemSvrStatsSAAsOut	Number of SAA messages that are sent by the remote server.

Table 2-76 Diameter Remote Server Stats Information (continued)

Metric	Value
cDiaRemSvrStats5GIndicatorSAAsIn	Number of SAA messages with Interworking-5GS-Indicator AVP that are received by the remote server. The Interworking-5GS-Indicator AVP is present in the SAA packet to differentiate it as a 5G packet. This will help in understanding the 5G SAA message flow in Prime Access Registrar. **Note** If the environment variable **EnableMatchingServiceSelection5GFlag** is set to 1, the **cDiaRemSvrStats5GIndicatorSAAsIn** counter is updated only if the Interworking-5GS-Indicator AVP is present in the APN configuration of matching Service-Selection. For more details about the environment variable, see “Environment Variable” chapter of the *Cisco Prime Access Registrar 9.2 Reference Guide* .
cDiaRemSvrStats5GIndicatorSAAsOut	Number of SAA messages with Interworking-5GS-Indicator AVP that are sent by the remote server.
cDiaRemSvrStats5GIndicatorFailedSARs	Number of failed SAR messages with Interworking-5GS-Indicator AVP that are received by the remote server.
cDiaRemSvrStats5GIndicatorFailedDERs	Number of failed DER messages with Interworking-5GS-Indicator AVP that are received by the remote server.
cDiaRemSvrStatsUDRsIn	Number of User-Data-Request (UDR) messages that are received by the remote server.
cDiaRemSvrStatsUDRsOut	Number of UDR messages that are sent by the remote server.
cDiaRemSvrStatsUDAsIn	Number of User-Data-Answer (UDA) messages that are received by the remote server.
cDiaRemSvrStatsUDAsOut	Number of UDA messages that are sent by the remote server.
cDiaRemSvrStatsRTRsIn	Number of Registration-Termination-Request messages that are received by the remote server.
cDiaRemSvrStatsRTRsOut	Number of Registration-Termination-Request messages that are sent by the remote server.
cDiaRemSvrStatsRTAsIn	Number of Registration-Termination-Answer messages that are received by the remote server.
cDiaRemSvrStatsRTAsOut	Number of Registration-Termination-Answer messages that are sent by the remote server.
cDiaRemSvrStatsPPRsIn	Number of Push-Profile-Request messages that are received by the remote server.
cDiaRemSvrStatsPPRsOut	Number of Push-Profile-Request messages that are sent by the remote server.

Table 2-76 Diameter Remote Server Stats Information (continued)

Metric	Value
cDiaRemSvrStatsPPAsIn	Number of Push-Profile-Answer messages that are received by the remote server.
cDiaRemSvrStatsPPAsOut	Number of Push-Profile-Answer messages that are sent by the remote server.
cDiaRemSvrStatsDERsIn	Number of Diameter-EAP-Request messages that are received by the remote server.
cDiaRemSvrStatsDERsOut	Number of Diameter-EAP-Request messages that are sent by the remote server.
cDiaRemSvrStatsDEAsIn	Number of Diameter-EAP-Answer messages that are received by the remote server.
cDiaRemSvrStatsDEAsOut	Number of Diameter-EAP-Answer messages that are sent by the remote server.
cDiaRemSvrStatsAARsIn	Number of AA-Request messages that are received by the remote server.
cDiaRemSvrStatsAARsOut	Number of AA-Request messages that are sent by the remote server.
cDiaRemSvrStatsAAAsIn	Number of AA-Answer messages that are received by the remote server.
cDiaRemSvrStatsAAAsOut	Number of AA-Answer messages that are sent by the remote server.
cDiaRemSvrStatsCoreNetRestriction-SAAsIn	Number of SAA messages with Core-Network-Restrictions AVP that are received by the remote server. The Core-Network-Restrictions AVP is present in the Non-3GPP-User-Data of SAA packet and contains a bitmask indicating the types of core networks that are not allowed for a given user.
cDiaRemSvrStatsCoreNetRestriction-SAAsOut	Number of SAA messages with Core-Network-Restrictions AVP that are sent by the remote server.
cDiaRemSvrStatsCoreNetRestriction-FailedSARs	Number of failed SAR messages with Core-Network-Restrictions AVP that are received by the remote server.
cDiaRemSvrStatsCoreNetRestriction-FailedDERs	Number of failed DER messages with Core-Network-Restrictions AVP that are received by the remote server.

Prime Access Registrar allows you to view the Diameter peer statistics at the interface level. Applicable statistics will be listed for interfaces such as SWm, S6b, STa, SWx, NASREQ, and so on. For more details on interface-level KPI counters, refer to the *Cisco Prime Access Registrar 9.2 Reference Guide*.

TACACSStatistics

Prime Access Registrar supports CISCO-AAA-SERVER-MIB to describe the statistics of TACACS+ protocol. This is supported through CLI/GUI and SNMP.

Table 2-77 lists the statistics information and the meaning of the values.

Table 2-77 TACACS Stats Information

Metric	Value
TACACS Statistics	
serverStartTime	The start time of the server.
serverResetTime	The reset time of the server.
serverState	The state of the server.
totalPacketsReceived	Number of packets that are received by a TACACS+ protocol irrespective of the type of Authentication and Accounting.
totalPacketsSent	Number of packets that are sent by a TACACS+ protocol irrespective of the type of Authentication and Accounting.
totalRequests	Number of packet requests that are received by a TACACS+ protocol irrespective of the type of Authentication and Accounting.
totalResponses	Number of packet responses that are sent by a TACACS+ protocol irrespective of the type of Authentication and Accounting.
totalAuthenticationRequests	Number of authentication requests that are received by Prime Access Registrar.
totalAuthenticationAccepts	Number of authentication requests that are accepted by Prime Access Registrar.
totalAuthenticationRejects	Number of authentication requests that are rejected by Prime Access Registrar.
totalAuthenticationChallenges	Number of authentication challenges that are faced by Prime Access Registrar.
totalAuthenticationResponses	Number of authentication responses that are sent by Prime Access Registrar.
totalAuthorizationRequests	Number of authorization requests that are received by Prime Access Registrar.
totalAuthorizationAccepts	Number of authorization requests that are accepted by Prime Access Registrar.
totalAuthorizationRejects	Number of authorization requests that are rejected by Prime Access Registrar.
totalAuthorizationResponses	Number of authorization responses that are sent by Prime Access Registrar.
totalAccountingRequests	Number of accounting requests that are received by Prime Access Registrar.
totalAccountingAccepts	Number of accounting requests that are accepted by Prime Access Registrar.
totalAccountingRejects	Number of accounting requests that are rejected by Prime Access Registrar.

Table 2-77 TACACS Stats Information (continued)

Metric	Value
totalAccountingResponses	Number of accounting requests that are sent by Prime Access Registrar.
totalPayloadDecryptionFailures	Number of packets that are not decrypted by Prime Access Registrar.
totalPacketsDropped	Number of packets that are dropped by Prime Access Registrar. The packets are dropped, which are invalid and do not fulfill the parsing conditions.

Back Up and Restore

To back up and restore the server details, Choose **Administration** > **Backup&Restore**. The Backup page is displayed with the list of recently backed up details of the server with the date and time. This option allows you to take a backup of the database, sessions, and scripts, and stores it in **/cisco-ar/backup** directory.

Backup Server Details

To back up the server details:

Step 1 Choose **Administration** > **Backup & Restore**. The Backup page is displayed.

Step 2 Click **Backup** to take a backup of the database, sessions, and scripts, and stores it in /cisco-ar/backup directory. The details will be backed up and appended to the backup list and displayed in the Backup page.

Restoring Server Details

To restore the backed-up server details:

Step 1 Choose **Administration** > **Backup & Restore**. The Backup page is displayed.

Step 2 Choose the record from the backup list.

Step 3 Click **Restore**. The details of the selected back up file will be restored successfully.

LicenseUpload

Prime Access Registrar license information are uploaded using the Upload feature. To upload the license file:

Uploading License File

To upload the Prime Access Registrar license file:

Step 1 Choose **Administration** > **LicenseUpload**. The Prime Access Registrar License-Upload page is displayed.

Step 2 Click **Browse** to locate the license file. The File Upload dialog box is displayed.

Step 3 Choose the required file.

Step 4 Click **Upload**. The selected file will be uploaded in **/cisco-ar/license** directory.

Note You need to ensure that the license file that you want to upload should be in **.lic** format.

Step 5 Click **Reset** to clear the text in the Select the File field, if you want to clear the selected path.

HealthMonitor

The Health Monitor statistics displays the health condition of the monitoring parameters based on the warning and threshold values set up earlier. For more details, see Health Monitor, page 2-107.

The status of the health monitoring parameters are displayed as one of the following:

- GOOD—If the parameter is within the limits.
- REDUCING—If the parameter is hitting the warning threshold value.
- CRITICAL—If the parameter is dropping below the error threshold value.
- UNMONITORED—If the parameter is unmonitored (no threshold values are set for the parameter).

Table 2-77 lists RADIUS and Diameter health detailed report.

Table 2-78 Health Monitoring Statistics

Metric	**Value**
Diameter Health Detailed Report / RADIUS Health Detailed Report	
CPU Utilization Health	Status of CPU utilization.
Memory Health	Status of Prime Access Registrar memory.
Packet Buffer Health	Status of packet buffer.
Worker Threads Health	Status of worker threads.
Packet Rejects Health	Status of packet rejects.
Packet Drops Health	Status of packet drops.
Packets TimedOuts Health	Status of packet timeouts.
Peer Connectivity Health	Status of peer connectivity.

Read-Only GUI

Prime Access Registrar provides a read-only GUI that enables an administrator to observe the system but prevents that administrator from making changes.

When you configure a user to be an administrator, check the View-Only check box to limit the administrator to view-only operation. You can also use the CLI by setting the View-Only property to TRUE under /Administrator/admin_name.

When using the Read-Only GUI, the Configuration, Network Resources and Administration sections are displayed as same as a fully-enabled administrator. The details of these sections are displayed in text format and cannot be edited.