



## Using the Graphical User Interface

---

This chapter describes how to use the stand-alone graphical user interface (GUI) to configure Cisco AR. Cisco AR requires you to use the following browser versions:

- IE 6.0.28 for Windows
- Netscape 7.02 for Windows, Solaris, or Linux

This chapter contains the following sections:

- [Launching the GUI](#)
- [Login Page](#)
- [Overview Page](#)
- [Configure Page](#)
- [Monitor Page](#)
- [Read-Only GUI](#)

### Launching the GUI

You start the GUI by pointing your browser to the Cisco AR server and port 8080, as in the following:

**`http://ar_server_name:8080`**

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

**`https://ar_servr_name:8443`**

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

- [Disabling HTTP](#)
- [Disabling HTTPS](#)

### Disabling HTTP

To disable HTTP access, you must edit the **server.xml** file in the **/cisco-ar/jakarta-tomcat-4.0.6/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 59-62. Use the **<!--** character sequence to begin a comment. Use the **-->** character sequence to end a comment.

The following are lines 57-62 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 className="org.apache.catalina.connector.http.HttpConnector"
  port="8080" minProcessors="5" maxProcessors="75"
  enableLookups="true" redirectPort="8443"
  acceptCount="10" debug="0" connectionTimeout="60000"/>
```

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 Cisco AR 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/jakarta-tomcat-4.0.6/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 69-77. Use the **<!--** character sequence to begin a comment. Use the **-->** character sequence to end a comment.

The following are lines 66-77 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 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>
```

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>
-->
```

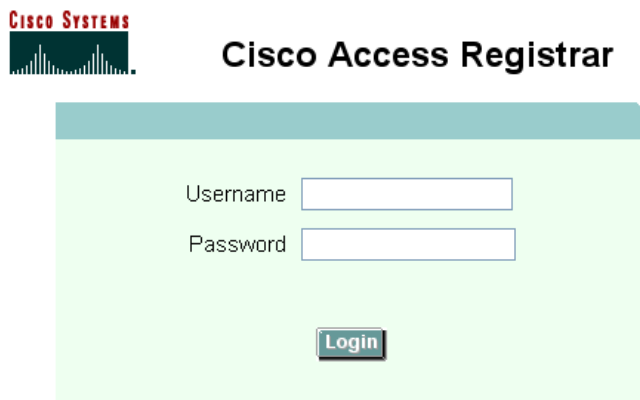
After you modify the **server.xml** file, you must restart the Cisco AR server for the changes to take effect. Use the following command line to restart the server:

```
/opt/CSCOAr/bin/arserver restart
```

## Login Page

Figure 3-1 shows the login page with fields for your username and password. This page displays when you first log into the system, if a session times out, or after you logout of the system.

Figure 3-1 Login Page



This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/ww/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

## Logging In

Only users who are configured as administrators can log into the Cisco AR server. To log into the Cisco AR GUI, enter a username and password for a configured administrator in the fields provided, then click **Login**.

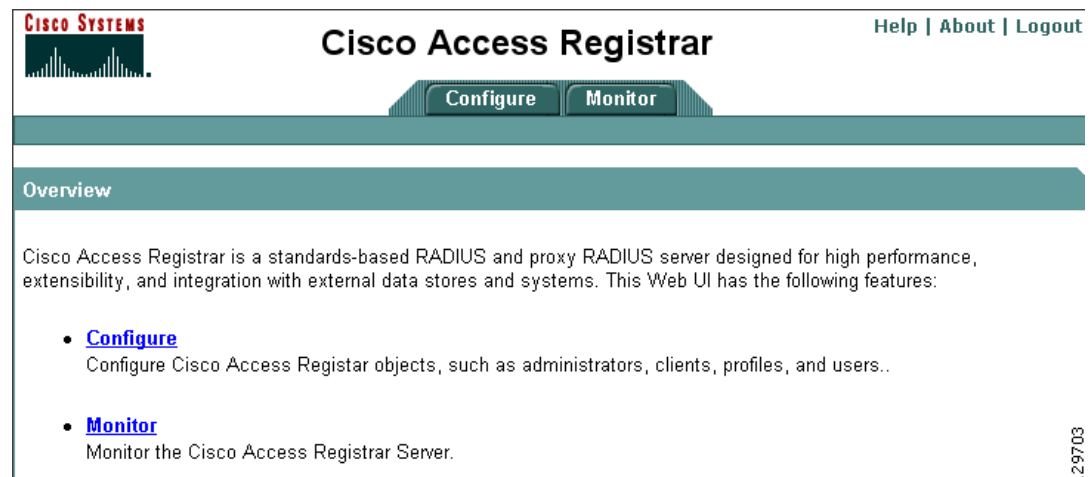
## Logging Out

To log out of the Cisco AR GUI, click **Logout** in the upper right portion of the Cisco AR GUI window.

## Overview Page

Figure 3-2 shows the top-level Overview page, the default page to load for the Cisco AR server.

Figure 3-2 Overview Page



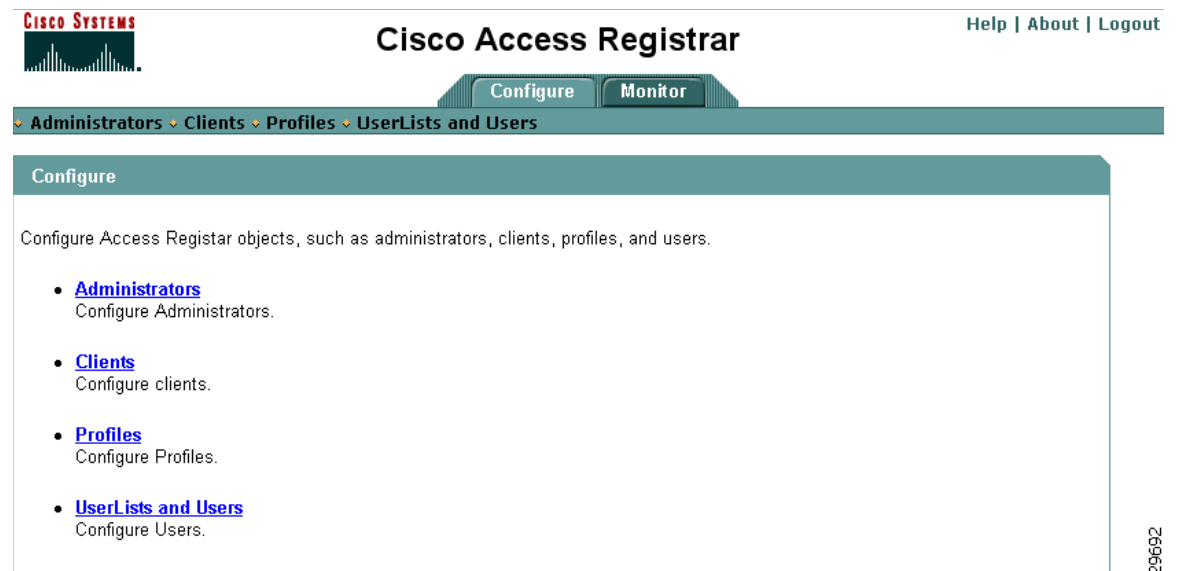
## Configure Page

Figure 3-3 shows the default Configure page. The Configure tab takes you to the Configure page where you can configure any of the following:

- [Administrators](#)
- [Clients](#)
- [Profiles](#)
- [Userlists and Users](#)

The Configure page shows subareas where you can click to configure administrators, Clients, Profiles, UserLists, and Users.

Figure 3-3 Configure Page

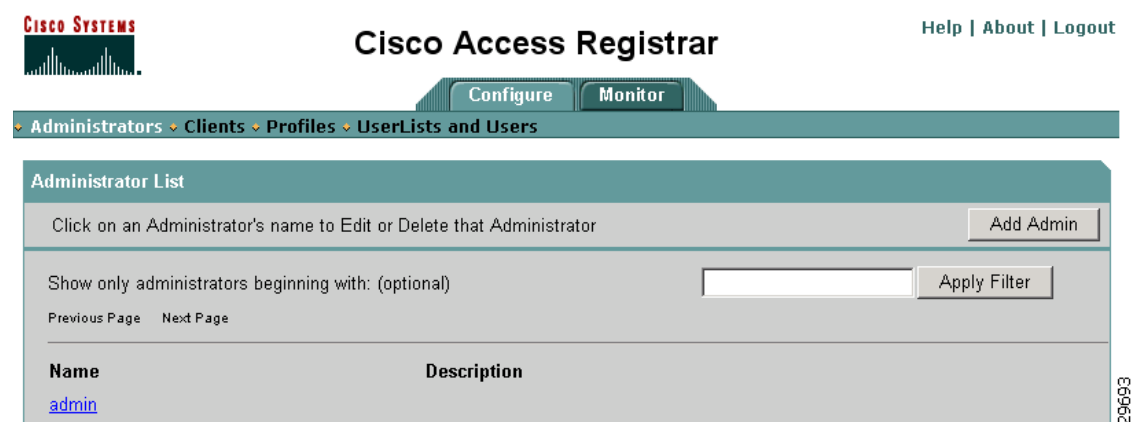


129692

## Administrators

Figure 3-4 shows the Administrators page which displays an alphabetical list of names and descriptions of the administrators known to the system. Click **Add Admin** to add a new administrator. Click on an administrator's name to edit or delete that administrator.

Figure 3-4 Administrators Page



129693

To locate an administrator, enter a partial name in the field provided, then click **Apply Filter**. The **Previous Page** and **Next Page** links take you to a previous page or the next page of administrators if available. Each administrator's name in the list is a link to the Edit page for that administrator.

## Adding Administrators

Figure 3-5 shows the Add Administrator page. Enter the attributes of a new administrator in the available fields and click **Submit** to add the new administrator. Click **Cancel** to return to the Administrators page without adding the administrator.

Figure 3-5 Add Administrator Page

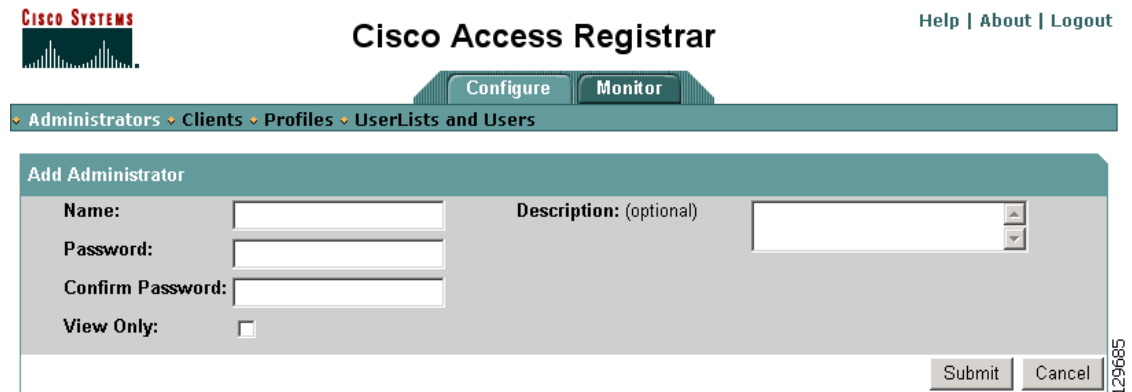


Table 3-1 provides the administrator properties and their descriptions.

Table 3-1 Administrator Properties

Property	Description
Name	Required; administrator’s user ID
Password	Required; encrypted password of the administrator
Confirm Password	Required; encrypted password of the administrator and must match Password
Description	Optional description of the administrator
ViewOnly	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.

If you successfully add a new administrator, Cisco AR returns you to the Administrators page. If the add is not successful, Cisco AR displays a page with an error message and a link back to the Add Administrator page.

## Editing Administrators

Figure 3-6 shows the Edit Administrator page which provides fields for the administrator attributes you can modify.

Figure 3-6 Edit Administrator Page

To modify administrator attributes, enter new information in the editable fields and click **Submit**. If the modification is successful, Cisco AR returns you to the Administrators page. If the modification is not successful, Cisco AR displays a page with an error message and a link back to the Edit Administrator page.

Click **Delete** to remove an administrator from the list of administrators. Click **Cancel** to return to the Administrators page.

## Clients

Figure 3-7 shows the Clients page which displays an alphabetical list of names of the clients known to the system and includes the client's IP address and shared secret. Click **Add Client** to add a new client.

Figure 3-7 Clients Page

Name	IP Address	Shared Secret
<a href="#">localhost</a>	127.0.0.1	secret

To locate a client, enter a partial name in the field provided, then click **Apply Filter**. The **Previous Page** and **Next Page** links take you to a previous page or the next page of data if available. Each client's name in the list is a link to the Edit page for that client.

## Adding Clients

Figure 3-8 shows the Add Client page.

Figure 3-8 Add Client Page

Enter the required attributes of a new client in the Name, IP Address, and Shared Secret fields. If you check the **Enable Dynamic Auth Server** check box, provide values for Dynamic Auth Shared Secret, Max Tries, Port, Initial Timeout, and COA Attribute. Use the pull-down menus to select Incoming and Outgoing scripts and to select a Vendor type. Click **Submit** to add the new client. Click **Cancel** to return to the Clients page without adding the client.

If Enable Dynamic Auth Server check box is unchecked (disabled), the fields to enter Dynamic Auth Shared Secret, Port, Initial Timeout, Max Tries, and DOA Attribute are grayed out and you cannot enter values. If Enable Dynamic Auth Server check box is checked, you must enter appropriate values in these fields.

If you successfully add a new client, Cisco AR returns you to the Clients page. If the add is not successful, Cisco AR displays a page with an error message and a link back to the Add Client page.

Table 3-2 provides the **Client** object properties.

Table 3-2 Client Properties

Property	Description
Name	Required and should match the client identifier specified in the standard RADIUS attribute, <b>NAS-Identifier</b> . The name must be unique within the clients list.
Description	Optional description of the client.

Table 3-2 Client Properties (continued)

Property	Description
IP Address	<p>Required; must be a valid IP address and unique in the clients list. Cisco AR 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 <b>NAS-IP-Address</b> attribute in the Request dictionary to identify the NAS sending the request through a proxy.</p> <p>You can specify a range of IP addresses using a hyphen as in:</p> <p style="padding-left: 40px;">100.1.2.11-20</p> <p>You can use an asterisk wildcard to match all numbers in an IP address octet as in:</p> <p style="padding-left: 40px;">100.1.2.*</p> <p>You can specify an IP address and a subnet mask together using Classless Inter-Domain Routing (CIDR) notation as in:</p> <p style="padding-left: 40px;">100.1.2.0/24</p>
SharedSecret	Required; must match the secret configured in the client.
Type	Required; accept the default (NAS), or set it to Proxy or NAS+Proxy.
Enable Dynamic Auth Server	Check to enable the Dynamic Authorization Server feature.
Dynamic Auth Shared Secret	The property Dynamic Auth Shared Secret is initially set to the same value as the client's SharedSecret property when you check the Enable Dynamic Auth Server check box. You can use this location to configure a different Dynamic Auth Shared Secret.
Port	The default port is 3799.
InitialTimeout	Represents the number of milliseconds used as a timeout for the first attempt to send a POD packet to a remote server. For each successive retry on the same packet, the previous timeout value used is doubled. You must specify a number greater than zero, and the default value is 5000 (or 5 seconds).
MaxTries	Represents the number of times to send a proxy request to a remote server before deciding the server is offline. You must specify a number greater than zero, and 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 <b>/Radius/Advanced</b> .
Vendor	Use this property when you need special processing for a specific vendor's NAS. To use this property, you must configure a <b>Vendor</b> object and include a Script. Cisco AR provides scripts you can use for Ascend, Cisco, Cabletron, Altiga, and USR, or you can also provide your own script. This field is optional for the CLI, but required for the GUI. Use the menu to select a vendor other than the default None.
IncomingScript	Use this property to specify a script you can use to determine the services to use for authentication, authorization, and/or accounting. This field is optional for the CLI, but required for the GUI. Use the menu to select an IncomingScript other than the default None.
OutgoingScript	Use this property to specify a script you can use to make any client-specific modifications when responding to a particular client. This field is optional for the CLI, but required for the GUI. Use the menu to select an OutgoingScript other than the default None.

## Editing Clients

Figure 3-9 shows the Edit Client page which provides fields for the client attributes you can modify. Click **Delete** to remove a client from the list of administrators. Click **Cancel** to return to the Client page.

Figure 3-9 Edit Client Page

The screenshot shows the Cisco Access Registrar web interface. At the top, there is a navigation bar with 'Configure' and 'Monitor' tabs. Below that is a breadcrumb trail: Administrators > Clients > Profiles > UserLists and Users. The main content area is titled 'Edit Client' and contains a form with the following fields:

- Name:** localhost
- IP Address:** 127.0.0.1
- Shared Secret:** secret
- Enable Dynamic Auth Server:**
- Dynamic Auth Shared Secret:** (empty text box)
- Max Tries:** (empty text box)
- Incoming Script:** ParseServiceHints
- Vendor:** None
- Description: (optional):** (empty text box)
- Type:** NAS
- Port:** (empty text box)
- Initial Timeout:** (empty text box)
- COA Attribute:** None
- Outgoing Script:** None

At the bottom right of the form, there are three buttons: Submit, Delete, and Cancel. A vertical label '129695' is visible on the right side of the form area.

To modify client attributes, enter new information in the editable fields. If you uncheck the Enable Dynamic Auth Server check box, Cisco AR clears the Port, Dynamic Auth Shared Secret, Initial Timeout, Max Tries, and COA Attribute fields.

Click **Submit** to modify the client. If the modification is successful, Cisco AR returns you to the Clients page. If the modification is not successful, Cisco AR displays a page with an error message and a link back to the Edit Client page.

## Profiles

Figure 3-10 shows the Profiles page which displays an alphabetical list of names and descriptions of the profiles known to the system. Click **Add Profile** to add a new profile. Click **Delete** to remove a profile from the list of profiles. Click **Cancel** to return to the Profiles page.

Figure 3-10 Profiles Page

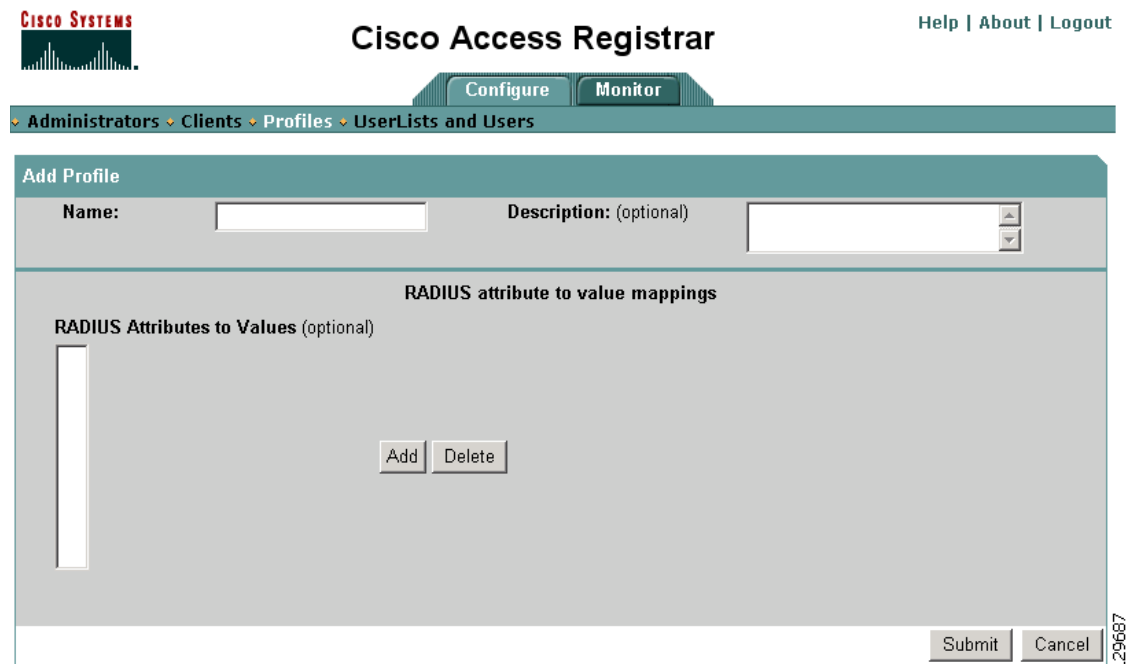


To locate an profile, enter a partial name in the field provided, then click **Apply Filter**. The **Previous Page** and **Next Page** links take you to a previous page or the next page of data if available. Each profile name in the list is a link to the Edit page for that profile.

## Adding Profiles

Figure 3-11 shows the Add Profile page.

Figure 3-11 Add Profile Page



Enter the name of a new profile in the Name field and an optional description. In the RADIUS Attribute to Value Mappings area, click **Add** to provide an attribute value (AV) pair.

The Add Profile page then displays fields for the **RADIUS Attribute** and **Maps To Attribute Value**. Click **Apply** to add the AV pair, or click **Cancel** to hide the fields without adding the AV pair. You can add as many AV pairs as is required. Click **Submit** to add the new profile. Click **Cancel** to return to the Profiles page without adding the profile.

Table 3-3 provides the profile properties and their definitions.

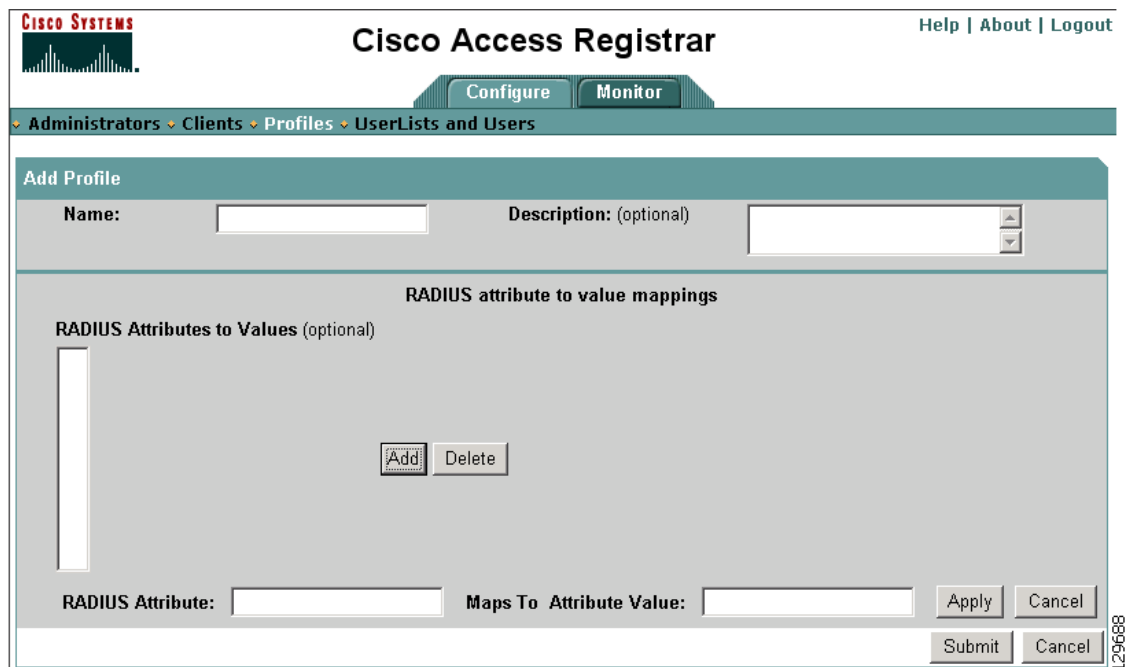
**Table 3-3 Profile Properties**

Property	Description
Name	Required profile name
Description	Optional description of the profile
RADIUS Attributes to Value	Optional list of attribute/value pairs

If you successfully add a new profile, Cisco AR returns you to the Profiles page. If the add is not successful, Cisco AR displays a page with an error message and a link back to the Add Profiles page.

Click Add to add AV pairs to the profile, as shown in Figure 3-12.

**Figure 3-12 Adding AV Pairs to a Profile**



The Submit button submits the new profile and the Cancel button returns the user to the Profiles page without submitting the information. When the new profile is submitted, you are returned to the Profiles page on a successful submit or taken to an error page with an error message and a link back to the Add Profile page.

## Editing Profiles

Figure 3-13 shows the Edit Profile page. To modify a profile's attributes, enter new information in the editable fields and click **Submit**. If the modification is successful, Cisco AR returns you to the Profiles page. If the modification is not successful, Cisco AR displays a page with an error message and a link back to the Edit Profile page.

Figure 3-13 Edit Profiles Page

The screenshot displays the Cisco Access Registrar web interface. At the top, the Cisco logo and 'Cisco Access Registrar' title are visible, along with 'Help | About | Logout' links. Below the title bar are 'Configure' and 'Monitor' tabs. A breadcrumb trail shows 'Administrators > Clients > Profiles > UserLists and Users'. The main content area is titled 'Edit Profile' and contains the following elements:

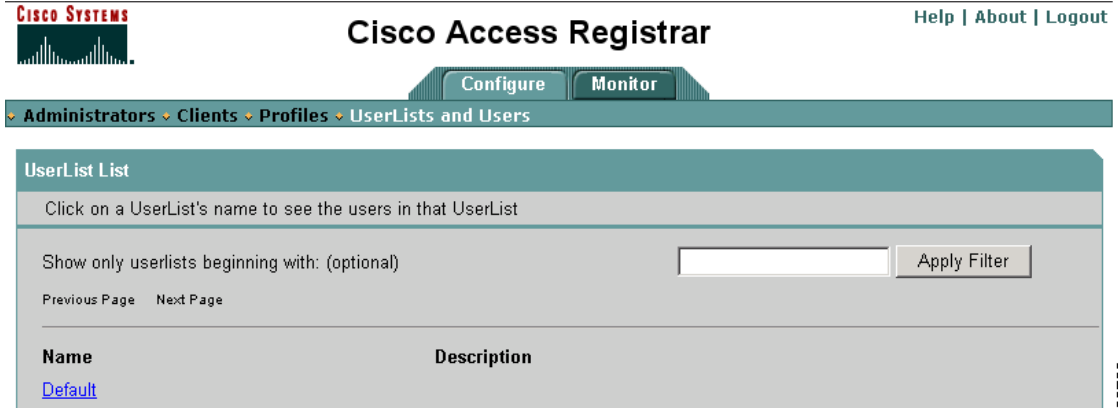
- Name:** A text input field containing 'default-PPP-users'.
- Description: (optional):** A text input field with a dropdown arrow.
- RADIUS attribute to value mappings:** A section containing a list of mappings:
  - Framed-Compression <--> VJ TCP/IP header compression
  - Service-Type <--> Framed
  - Framed-Protocol <--> PPP
  - Framed-MTU <--> 1500
  - Framed-Routing <--> None
  - Ascend-Idle-Limit <--> 1800
- Buttons:** 'Add' and 'Delete' buttons are positioned to the right of the mappings list. At the bottom right of the form are 'Submit', 'Delete', and 'Cancel' buttons.

A vertical ID number '129696' is visible on the right edge of the screenshot.

## Userlists and Users

Figure 3-14 shows the UserLists page which displays an alphabetical list of all UserLists and descriptions of the UserLists known to the system. The Cisco AR GUI does not support adding, editing, or deleting UserLists; you must use the CLI to add new UserLists.

Figure 3-14 UserLists Page

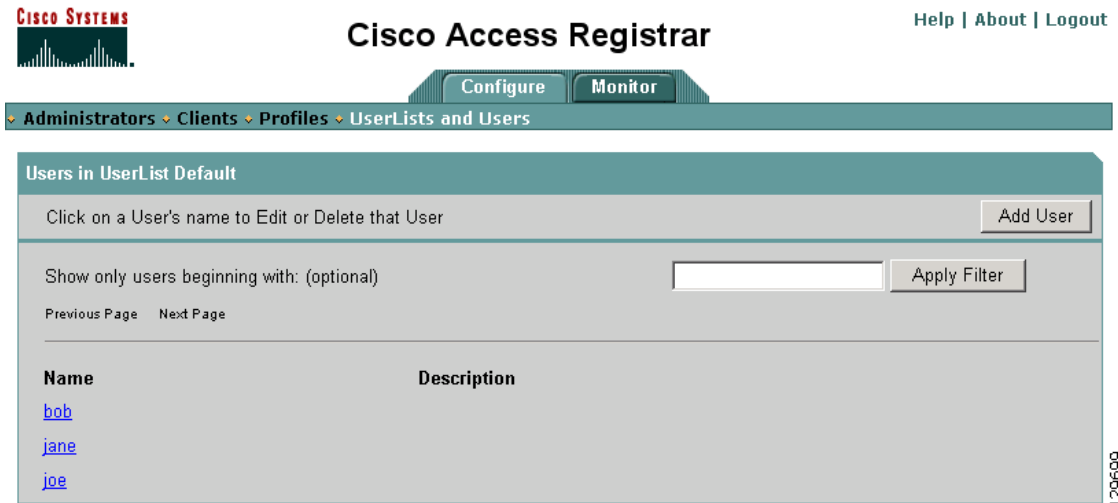


To locate a UserList, enter a partial name in the field provided, then click **Apply Filter**. The **Previous Page** and **Next Page** links take you to a previous page or the next page of data if available. Each UserList name in the list is a link to the Edit page for that UserList.

## List User Page

Figure 3-15 shows the List Users page which displays an alphabetic list of the Users of a selected UserList. The name of the displayed UserList displays in white at the top of the content area. Click **Add User** to add a new user to this list.

Figure 3-15 List Users Page



To locate a user in this list, enter a partial name in the field provided, then click **Apply Filter**. The **Previous Page** and **Next Page** links take you to a previous page or the next page of data if available. Each username in the list is a link to the Edit page for that user.

## Adding Users

Figure 3-16 shows the Add User page.

Figure 3-16 Add User Page

The screenshot shows the 'Add User' page in the Cisco Access Registrar GUI. The page has a header with the Cisco logo and 'Cisco Access Registrar' text, along with 'Help | About | Logout' links. Below the header are 'Configure' and 'Monitor' tabs. A navigation breadcrumb shows 'Administrators > Clients > Profiles > UserLists and Users'. The main form area is titled 'Add User' and contains the following fields:

- Name:** Text input field.
- Description: (optional):** Text input field with a scroll bar.
- Enabled:** Check box, checked.
- Password:** Text input field.
- Confirm Password:** Text input field.
- Allow No Password:** Check box, unchecked.
- Profile:** Drop-down menu, set to 'None'.
- Authentication Script:** Drop-down menu, set to 'None'.
- Authorization Script:** Drop-down menu, set to 'None'.
- User Group:** Drop-down menu, set to 'None'.

Below the form is a section titled 'RADIUS attribute to value mappings' with a sub-section 'RADIUS Attributes to Values (optional)'. It contains a vertical list box and two buttons: 'Add' and 'Delete'. At the bottom right of the form are 'Submit' and 'Cancel' buttons. The page number '129689' is printed vertically on the right side.

Table 3-4 lists and describes the **Users** fields the GUI provides to add a new user. Enter values for the new user in the appropriate fields. In the RADIUS Attribute to Value Mappings area, click **Add** to provide one or more AV pairs.

Table 3-4 Users Properties

Property	Description
Name	Required; must be unique.
Description	Optional description of the user.
Password	Required; length must be between 0-253 characters.
Confirm Password	Required; must match Password
Enabled	Required; must be checked to allow user access. If Enabled is not checked, user is denied access.
UserGroup	Use pull-down menu to select a UserGroup and use the properties specified in the UserGroup to authenticate and/or authorize the user. The default is none.

Table 3-4 Users Properties (continued)

Property	Description
Profile	Use pull-down menu to select a Profile. If the service-type is not equal to Authenticate Only, Cisco AR 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.
AuthenticationScript	Use pull-down menu 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 AuthenticationScript other than the default None.
AuthorizationScript	Use pull-down menu 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 AuthorizationScript other than the default None.
RADIUS attribute to value mappings	RADIUS attributes and their assigned value that Cisco AR returns in the Access-Accept response packet.

The Add User page then displays fields for the **RADIUS Attribute** and **Maps To Attribute Value**. Click **Apply** to add the AV pair, or click **Cancel** to hide the fields without adding the AV pair. You can add as many AV pairs as is required.

Click Add to provide RADIUS Attributes and their values, as shown in [Figure 3-17](#).

Figure 3-17 Adding AV Pairs to a User

Click **Submit** to add the new user. Click **Cancel** to return to the UserLists page without adding the user. If you successfully add a new user, Cisco AR returns you to the UserLists page. If the add is not successful, Cisco AR displays a page with an error message and a link back to the Add User page.

## Editing Users

[Figure 3-18](#) shows the Edit User page. To modify user attributes, enter new information in the editable fields. Use the Edit User page to provide additional AV pairs. Click **Submit** to change the user attributes. If the modification is successful, Cisco AR returns you to the Users page. If the modification is not successful, Cisco AR displays a page with an error message and a link back to the Edit User page.

Figure 3-18 Edit User Page

The screenshot shows the 'Edit User' page in the Cisco Access Registrar GUI. The page title is 'Cisco Access Registrar' with a navigation bar containing 'Configure' and 'Monitor' tabs. The breadcrumb trail is 'Administrators > Clients > Profiles > UserLists and Users'. The 'Edit User' form contains the following fields:

- Name: bob
- Description: (optional) [empty]
- Enabled:
- Change Password:
- New Password: [empty]
- Confirm New Password: [empty]
- Allow No Password:
- Profile: None
- Authentication Script: None
- Authorization Script: None
- User Group: PPP-users

Below the form is a section titled 'RADIUS attribute to value mappings' with a sub-section 'RADIUS Attributes to Values' containing an empty list and 'Add' and 'Delete' buttons. At the bottom right of the form are 'Submit', 'Delete', and 'Cancel' buttons. A vertical ID '129697' is visible on the right side of the form.

Click **Delete** to delete the selected user. If the delete is successful, Cisco AR displays the Users page. If the delete is unsuccessful, Cisco AR displays an error message and a link back to the Edit User page.

Click **Cancel** to return to the previous UserList page.

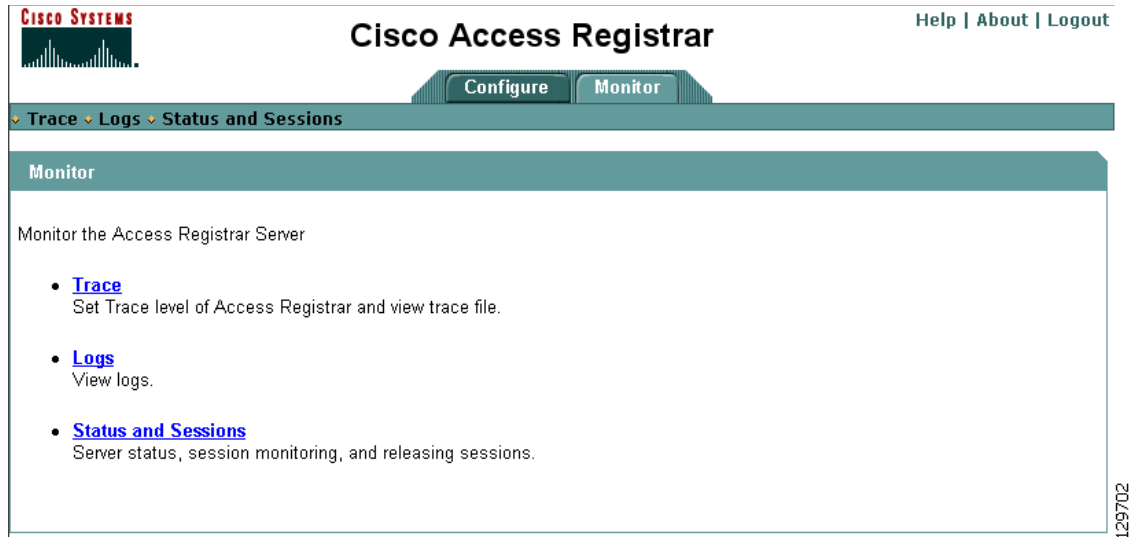
## Monitor Page

Figure 3-19 shows the default Monitor page. The Monitor page shows subareas where you can click to monitor the trace level, view server logs, and monitor server status and sessions and release sessions.

The subareas of Monitor page are:

- [Trace Level](#)
- [Logs](#)
- [Status and Sessions](#)

Figure 3-19 Monitor Page



129702

## Trace Level

The Cisco AR GUI provides two options in the Table of Contents (TOC) under **Monitor > Trace**:

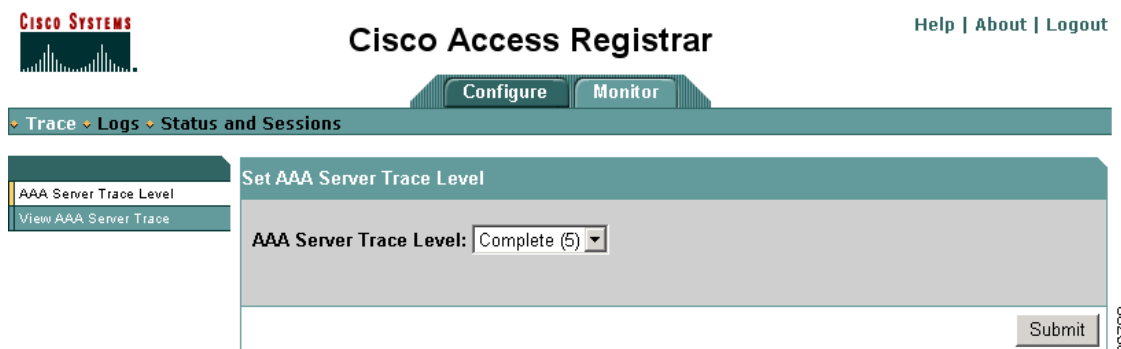
- [AAA Server Trace Level](#)
- [View AAA Server Trace](#)

The Set AAA Server Trace Level page is the default view.

## AAA Server Trace Level

Figure 3-20 shows the default Trace Level page.

Figure 3-20 Server Trace Level Page



129708

The AAA Server Trace Level page displays the current trace level for the Cisco AR server and provides a pull-down menu that enables you to change the trace level. Cisco AR provides six levels of tracing from zero to five (0-5).

The trace level determines how much information is displayed about the contents of a packet. When the trace level is zero, no tracing is performed. The higher the trace level, the more information displayed. The highest trace level currently used by the Cisco AR server is trace level 5.

The **trace** levels are inclusive, meaning that if you set **trace** to level 3, you will also get the information reported for **trace** levels 1 and 2. If you set trace level 4, you also get information reported for **trace** levels 1, 2, and 3.

Use the pull-down menu to select a trace level, then click **Submit** to set the new trace level. After you set a new trace level, the Cisco AR server returns the AAA Server Trace Level page and displays the selected value.

If an error occurs, the Cisco AR server displays an error page with the error message and a link back to the AAA Server Trace Level page.

[Table 3-5](#) lists the different **trace** levels and the information returned.

**Table 3-5 Trace Levels and Information Returned**

Trace Level	Information Returned by Trace Command
0	No trace performed
1	Reports when a packet is sent or received or when there is a change in a remote server's status.
2	Indicates the following: <ul style="list-style-type: none"> <li>• Which services and session managers are used to process a packet</li> <li>• Which client and vendor objects are used to process a packet</li> <li>• Detailed remote server information for LDAP and RADIUS, such as sending a packet and timing out</li> <li>• Details about poorly formed packets</li> <li>• Details included in trace level 1</li> </ul>
3	Indicates the following: <ul style="list-style-type: none"> <li>• Error traces in TCL scripts when referencing invalid RADIUS attributes.</li> <li>• Which scripts have been executed</li> <li>• Details about local UserList processing</li> <li>• Details included in trace levels 1 and 2</li> </ul>

Table 3-5 Trace Levels and Information Returned (continued)

Trace Level	Information Returned by Trace Command
4	<p>Indicates the following:</p> <ul style="list-style-type: none"> <li>• Information about advanced duplication detection processing</li> <li>• Details about creating, updating, and deleting sessions</li> <li>• Trace details about all scripting APIs called</li> <li>• Details included in trace levels 1, 2, and 3</li> </ul>
5	<p>Indicates the following:</p> <ul style="list-style-type: none"> <li>• Details about use of the policy engine including: <ul style="list-style-type: none"> <li>– Which rules were run</li> <li>– What the rules did</li> <li>– If the rule passed or failed</li> <li>– Detailed information about which policies were called</li> </ul> </li> <li>• Details included in trace levels 1, 2, 3, and 4</li> </ul>

## View AAA Server Trace

Figure 3-21 shows the Server Trace page.

Figure 3-21 Server Trace Page

The screenshot displays the Cisco Access Registrar interface. At the top, there is a navigation bar with 'Configure' and 'Monitor' tabs. Below this is a breadcrumb trail: 'Trace > Logs > Status and Sessions'. The main content area is titled 'View Server Trace Log' and contains the following log entries:

```

03/24/2005 15:03:55: Log: Trace level set to 3
03/24/2005 15:04:06: Log: Trace level set to 4
03/24/2005 15:04:46: Log: Stopping Server
03/24/2005 15:04:46: Log: Replication Manager Stopped.
03/24/2005 15:04:46: P788: Cisco Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:46: P789: Altiga Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:46: P790: USR Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:46: P791: Cisco Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:46: P792: Cabletron Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:46: P793: Ascend Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: Log: Closing interface 127.0.0.1, port 1812 (RADIUS Access)
03/24/2005 15:04:47: Log: Closing interface 127.0.0.1, port 1813 (RADIUS Accounting)
03/24/2005 15:04:47: Log: Closing interface 10.1.9.247, port 1812 (RADIUS Access)
03/24/2005 15:04:47: Log: Closing interface 10.1.9.247, port 1813 (RADIUS Accounting)
03/24/2005 15:04:47: P794: Cisco Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: P795: Altiga Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: P796: USR Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: P797: Cisco Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: P798: Cabletron Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: P799: Ascend Vendor filter InitEntryPoint function Initialize called with iScriptingPoint = 0x201
03/24/2005 15:04:47: Log: Closing configuration database
03/24/2005 15:04:47: Log: Trace output is being sent to file name_radius_1_trace
03/24/2005 15:04:47: Log: Opening configuration database

```

The sidebar on the left contains the following items:

- AAA Server Trace Level
- View AAA Server Trace

The vertical ID '129707' is located on the right side of the screenshot.

## Logs

The Table of Contents for the Log subarea provides four options:

- [Server Log Page](#)
- [Server Accounting Log Page](#)
- [Server CLI aregcmd Log Page](#)
- [Server Statistics Log Page](#)

The default TOC entry is Server Log.

## Server Log Page

Figure 3-22 shows the Server Log page.

Figure 3-22 Server Log Page

**CISCO SYSTEMS** Help | About | Logout

### Cisco Access Registrar

Configure Monitor

Trace > Logs > Status and Sessions

Log Category	View Server Log
Server Log	02/18/2005 1:01:17 name/radius/1 Info System 0 Cisco Access Registrar 4.0.0.3
Server Accounting Log	02/18/2005 1:01:17 name/radius/1 Info System 0 name/radius (Radius Server) startup
Server CLI ARegCmd Log	02/18/2005 1:01:17 name/radius/1 Info System 0 version 4.0.0.3, build 0; built 2005-02-17_02:40:19 [1108636819] by twieland@cn
Server Stats Log	02/18/2005 1:01:17 name/radius/1 Info System 0 threads=0, memory=0, disk=0, nlogs=0, logsize=0, console=0, interact=0
	02/18/2005 1:01:18 name/radius/1 Info System 0 Trace output is being sent to file name_radius_1_trace
	02/18/2005 1:01:18 name/radius/1 Info Server 0 Opening configuration database
	02/18/2005 1:01:18 name/radius/1 Info Server 0 Backing Store: No map file found ("opt/CSC0ar/data/radius/LogFileSessionBackingS
	02/18/2005 1:01:18 name/radius/1 Info Server 0 Backing Store: No map file found ("opt/CSC0ar/data/odbc/LogFilePacketBackingS
	02/18/2005 1:01:19 name/radius/1 Info Server 0 RollingEncryption using newkey 0 and aging key 1
	02/18/2005 1:01:26 name/radius/1 Info Server 0 Session Backing Store: Resurrected 0 sessions.
	02/18/2005 1:01:26 name/radius/1 Info Server 0 Starting Server
	02/18/2005 1:01:27 name/radius/1 Info Server 0 Starting Interface 127.0.0.1, port 1645 (RADIUS Access)
	02/18/2005 1:01:27 name/radius/1 Info Server 0 Starting Interface 127.0.0.1, port 1646 (RADIUS Accounting)
	02/18/2005 1:01:27 name/radius/1 Info Server 0 Starting Interface 10.1.9.212, port 1645 (RADIUS Access)
	02/18/2005 1:01:27 name/radius/1 Info Server 0 Starting Interface 10.1.9.212, port 1646 (RADIUS Accounting)

129711

## Server Accounting Log Page

Figure 3-23 shows the Server Accounting log page.

**Figure 3-23** Server Accounting Log Page



```
View Accounting Log

Thu, 24 Mar 2005 18:15:08
  User-Name = user1
  NAS-Port = 1
  NAS-Identifier = localhost
  Acct-Status-Type = Start
  Acct-Session-Id = 1

Thu, 24 Mar 2005 18:15:33
  User-Name = user1
  NAS-Port = 1
  NAS-Identifier = localhost
  Acct-Status-Type = Stop
  Acct-Session-Id = 1

Thu, 24 Mar 2005 18:16:18
  User-Name = user2
  NAS-Port = 1
  NAS-Identifier = localhost
  Acct-Status-Type = Start
  Acct-Session-Id = 1

Thu, 24 Mar 2005 18:16:18
  User-Name = user2
  NAS-Port = 1
  NAS-Identifier = localhost
  Acct-Status-Type = Stop
  Acct-Session-Id = 1
```

129684

## Server CLI aregcmd Log Page

Figure 3-24 shows the Server CLI **aregcmd** log page.

Figure 3-24 Server CLI **aregcmd** Log Page

The screenshot displays the Cisco Access Registrar web interface. At the top left is the Cisco Systems logo. The main title is "Cisco Access Registrar". On the right, there are links for "Help | About | Logout". Below the title, there are two tabs: "Configure" and "Monitor". A breadcrumb trail shows "Trace > Logs > Status and Sessions". On the left, a sidebar menu lists "Server Log", "Server Accounting Log", "Server CLI ARegCmd Log" (which is highlighted), and "Server Stats Log". The main content area is titled "View CLI Log" and contains a list of log entries. Each entry follows the format: `02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7721 "" TRUE Default`. The entries are numbered from 1 to 19. On the right side of the log area, the number "129710" is displayed vertically.

Log Entry
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7721 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7722 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7723 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7724 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7725 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7726 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7727 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7728 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7729 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7730 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7731 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7732 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7733 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7734 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7735 "" TRUE Default
02/20/2005 22:17:54 aregcmd Info Configuration 0 [localhost admin] --> add /Radius/UserLists/Default/user7736 "" TRUE Default

## Server Statistics Log Page

Figure 3-25 shows the Server Statistics log page.

Figure 3-25 Server Statistics Log

The screenshot shows the Cisco Access Registrar web interface. At the top left is the Cisco Systems logo. The main title is 'Cisco Access Registrar'. To the right are links for 'Help | About | Logout'. Below the title are two tabs: 'Configure' and 'Monitor'. A breadcrumb trail reads 'Trace > Logs > Status and Sessions'. On the left is a sidebar menu with the following items: 'Server Log', 'Server Accounting Log', 'Server CLI ARegCmd Log', and 'Server Stats Log'. The main content area is titled 'Global Statistics for Radius:' and contains the following text:

```

serverStartTime = Wed Feb 23 09:29:44 2005
serverResetTime = Wed Mar 2 07:07:59 2005
serverStat = Running
totalPacketsInPool = 1024
totalPacketsReceived = 4522
totalPacketsSent = 4372
totalRequests = 12
totalResponses = 12
totalAccessRequests = 12
totalAccessAccepts = 11
totalAccessChallenges = 0
totalAccessRejects = 1
totalAccessResponses = 12
totalAccountingRequests = 0
totalAccountingResponses = 0
totalStatusServerRequests = 0

```

129712

## Status and Sessions

The Table of Contents for the Status and Sessions subarea provides two options:

- [AAA Server Status Page](#)
- [Sessions List and Query Page](#)

The default TOC entry is Server Status.

## AAA Server Status Page

The AAA Server Status page lists the status of the Access Registrar Server Agent, the Access Registrar GUI, and the health of the server. [Figure 3-26](#) shows the AAA Server Status page.

**Figure 3-26** AAA Server Status Page

The screenshot shows the Cisco Access Registrar interface. At the top left is the Cisco Systems logo. The main title is 'Cisco Access Registrar'. To the right are links for 'Help | About | Logout'. Below the title are two buttons: 'Configure' and 'Monitor'. A navigation bar contains 'Trace > Logs > Status and Sessions'. On the left, a sidebar shows 'AAA Server Status' and 'Sessions'. The main content area is titled 'AAA Server Status' and contains the following text:

```

AAA server running : (pid: 16343)
AAA daemon manager running : (pid: 16327)
AAA database lock manager running : (pid: 16334)
AAA database running : (pid: 16333)
AR GUI running : (pid: 16344)
Server is Running, its health is 10 out of 10
  
```

129705

## Sessions List and Query Page

The Session List and Query page lists currently running sessions and provides fields where you can specify a username or Session ID for which to query. Use the **Release All** button to release all sessions. [Figure 3-27](#) shows the Session List and Query page.

**Figure 3-27** Session List and Query Page

The screenshot shows the Cisco Access Registrar interface. At the top left is the Cisco Systems logo. The main title is 'Cisco Access Registrar'. To the right are links for 'Help | About | Logout'. Below the title are two buttons: 'Configure' and 'Monitor'. A navigation bar contains 'Trace > Logs > Status and Sessions'. On the left, a sidebar shows 'AAA Server Status' and 'Sessions'. The main content area is titled 'Session List and Query' and contains the following form:

UserName to query for:

SessionID to query for:

Release all Sessions:

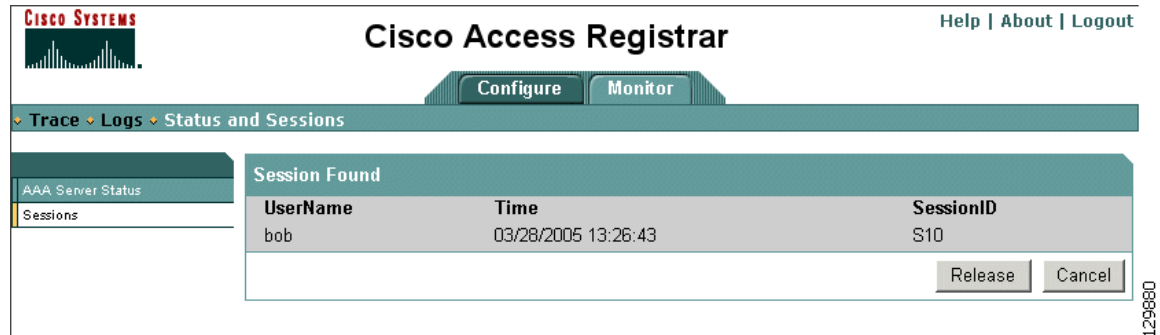
UserName	Time	SessionID
bob	03/24/2005 10:30:01	S1
joe	03/24/2005 10:31:07	S2
jane	03/24/2005 10:31:18	S3

129698

## Query Session

After you provide a username or SessionID on the Session List and Query page and click **Submit**, the GUI displays the Query Session Result page as shown in [Figure 3-28](#).

**Figure 3-28** Query Session Results Page



The Query Session Result page displays the username, Time, and SessionID of the session found during the query. A message displays to indicate if no sessions were found. Click **Release** to release the session and return to the Sessions page. Click **Cancel** to return to the Session page without releasing the session.

## Read-Only GUI

Cisco AR 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 Monitor section displays the same as a fully-enabled administrator, but the Release and Release All buttons do not display. The Configure section displays the same as a fully-enabled administrator, but the Add buttons do not display. When you click the name links, the edit pages display, but in text format without forms or controls.