CHAPTER 3

Using the Graphical User Interface

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

- Microsoft Internet Explorer 6.0 SP1 (Windows 2000 & Windows XP)
- Netscape 7.02 (Windows 2000 & Windows XP)

This chapter contains the following sections:

Note Replication is not supported when using the GUI. If you plan to use replication, use the **aregcmd** command-line interface to make configuration changes to the Cisco AR server.

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

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

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 logout of the system.

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

The Overview page is the top-level of the Cisco AR server GUI and provides links to the Configure page and the Monitor page.

Configure Page

The Configure page enables you to configure the following:

- Administrators
- Clients

- Profiles
- Userlists and Users

Note Replication is not supported when you use the GUI to configure the Cisco AR server.

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

Administrators

The Administrators page 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.

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

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.

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.

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

Editing Administrators

The Edit Administrator page enables you to modify administrator attributes.

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 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

The Clients page 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.

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

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.

After you successfully add a new client, Cisco AR returns you to the Clients page. If the add is not successful, Cisco AR displays 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, **NAS-Identifier**. The name must be unique within the Clients list.
Description	Optional description of the client.

Table 3-2 Client Properties (continued)

Property	Description
IPAddress	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 **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.
SharedSecret	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. Cisco AR provides five Scripts you can use: one for Ascend, Cisco, Cabletron, Altiga, and one for USR. You can also provide your own Script.
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.
EnableDynamicAuthorization	Optional; when set to TRUE, this property enables Change of Authorization (CoA) and Packet of Disconnect (PoD) features.
DynamicAuthorizationServer	This subdirectory is only present in a client with EnableDynamicAuthorization set to TRUE and contains properties required for CoA and PoD requests.
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.
DynamicAuthSharedSecret	Located under the DynamicAuthorizationServer subdirectory, this is the shared secret used for communicating CoA and PoD packets with the client.
PODAttributeGroup	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**.

Table 3-2 Client Properties (continued)

Property	Description
COAAttributeGroup	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**.
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).
EnableNotifications	Required; the default value is FALSE and indicates the client is not capable of receiving Accounting-Stop notifications from the Cisco AR server. When set to TRUE, the client can receive Accounting-Stop notifications from the Cisco AR server and additional properties must be configured under a new sub-directory named NotificationProperties.
NotificationProperties	When the EnableNotifications property is set to TRUE, this subdirectory contains additional properties required to support the Query-Notify feature.
Port	Located under the NotificationProperties subdirectory, specifies the port used by the Cisco AR server to receive Accounting-Stop packets. Required when EnableNotifications is set to TRUE; the default value is 1813.
InitialTimeout	Located under the NotificationProperties subdirectory, specifies the timeout value in milliseconds the Cisco AR 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.
MaxTries	Located under the NotificationProperties subdirectory, specifies the number of times the Cisco AR server sends an Accounting-Stop packet to a client. Required when EnableNotifications is set to TRUE; the default value is 3.
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.

Editing Clients

The Edit Client page 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.

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 an error message and a link back to the Edit Client page.

Profiles

The Profiles page 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.

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

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

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

Click Add to add AV pairs to the 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

To modify an 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 an error message and a link back to the Edit Profile page.

Userlists and Users

The UserLists page 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.

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

The List Users page 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.

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

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.
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.

Table 3-4 Users Properties (continued)

Property	Description
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

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

Editing Users

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 an error message and a link back to the Edit User page.

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

The Monitor page provides subareas where you can click to monitor the trace level and server status, view server logs, and monitor and release sessions.

The subareas of Monitor page are:

- Trace Level
- Logs
- Status and Sessions

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.

Related Topics

- Logs

AAA Server Trace Level

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: • Which services and session managers are used to process a packet • Which client and vendor objects are used to process a packet • Detailed remote server information for LDAP and RADIUS, such as sending a packet and timing out • Details about poorly formed packets • Details included in trace level 1
3	Indicates the following: • Error traces in TCL scripts when referencing invalid RADIUS attributes. • Which scripts have been executed • Details about local UserList processing • Details included in trace levels 1 and 2

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

Trace Level	Information Returned by Trace Command
4	Indicates the following: • Information about advanced duplication detection processing • Details about creating, updating, and deleting sessions • Trace details about all scripting APIs called • Details included in trace levels 1, 2, and 3
5	Indicates the following: • Details about use of the policy engine including: – Which rules were run – What the rules did – If the rule passed or failed – Detailed information about which policies were called • Details included in trace levels 1, 2, 3, and 4

View AAA Server Trace

The Server Trace log shows a sequence of significant events logged by the Cisco AR server.

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

The Server Log page displays the server log of events with dates, timestamps, and a short description of the event.

Server Accounting Log Page

The Server Accounting Log page shows the accounting log history with dates, timestamps, and accounting status types.

Server CLI aregcmd Log Page

The Server CLI **aregcmd** log page displays a log of **aregcmd** events with dates and timestamps.

Server Statistics Log Page

The Server Statistics log page displays the current global statistics for the Cisco AR server.

Status and Sessions

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

- AAA Server Status and Sessions Page
- Sessions List and Query Page

The default TOC entry is Server Status.

AAA Server Status and Sessions Page

The AAA Server Status and Sessions page lists the status of the AR Server Agent, the AR GUI, and the health of the server.

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.

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

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.