



CHAPTER 4

Configuring Sponsor Authentication

Sponsors are the people who use Cisco NAC Guest Server to create guest accounts. Sponsor authentication is the method used to authenticate sponsor users on the Guest Server. There are four options available:

- Local User Authentication—Create sponsor accounts directly on the Cisco NAC Guest Server. See [Configuring Local Sponsor Authentication](#)
- Active Directory Authentication—Authenticate sponsors against an existing Active Directory (AD) implementation. See [Configuring Active Directory \(AD\) Authentication](#).
- LDAP Authentication—Authenticate sponsors against a Lightweight Directory Access Protocol (LDAP) server. See [Configuring LDAP Authentication](#).
- RADIUS Authentication—Authenticate sponsors against a RADIUS server. See [Configuring RADIUS Authentication](#).

You may specify multiple authentication services for authenticating sponsors to the Cisco NAC Guest Server and then specify the order in which you want to authenticate sponsors. For details see [Configuring Sponsor Authentication Settings](#).

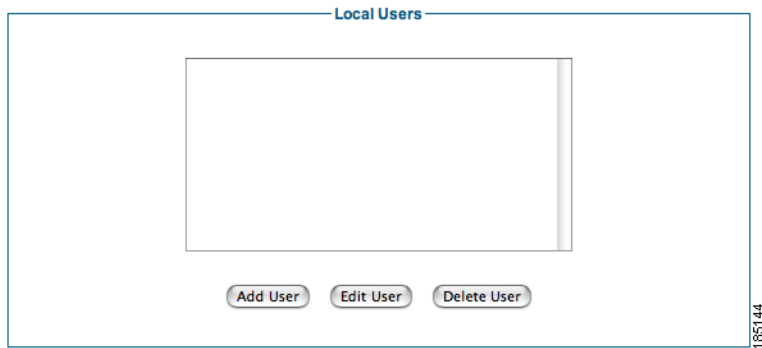
Configuring Local Sponsor Authentication

Local authentication allows you to set up sponsor user accounts directly on the Cisco NAC Guest Server. Local authentication allows you to do the following:

- [Add New Local User Account](#)
- [Edit Existing User Account](#)
- [Delete Existing User Account](#)

Add New Local User Account

-
- Step 1** From the administration interface select **Authentication > Sponsors > Local User Database** from the menu ([Figure 4-1](#)).

Figure 4-1 Local Users

Step 2 Click the **Add User** button to bring up the local sponsor configuration page (Figure 4-2).

Figure 4-2 Add Local User

Step 3 In the Add a Local User Account page, enter all the sponsor user credentials:

- First Name—Type the first name of the sponsor.
- Last Name—Type the last name of the sponsor.
- Username—Type the user name for the sponsor account.
- Password—Type the password for the sponsor account.
- Repeat Password—Retype the password for the sponsor account
- Groups—Select the group for the sponsor account from the dropdown. [Chapter 5, “Configuring User Group Permissions”](#) provides further details on groups.
- Email Address—Type email address of the sponsor.

Step 4 Click the **Add User** button.

- If there are any errors, the account is not added and an error message displays at the top of the page.

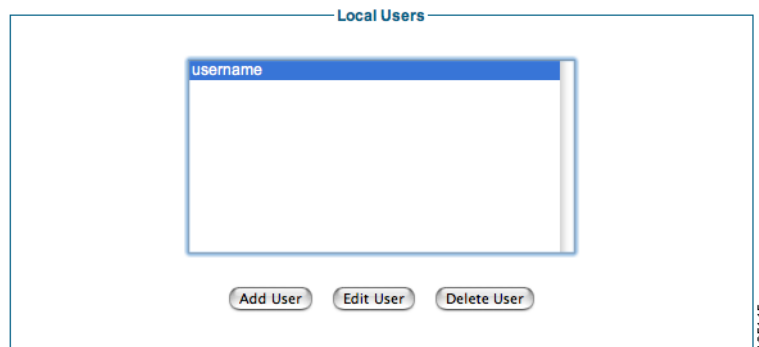
- If successfully added, a success message displays at the top of the page and you can add additional user accounts.

Edit Existing User Account

You can modify the settings of local user accounts that are already created.

- Step 1** From the administration interface select **Authentication > Sponsors > Local User Database** from the menu (Figure 4-3).

Figure 4-3 Local Users to Edit



- Step 2** Select the user from the list and click the **Edit User** button.
- Step 3** In the Edit a Local User Account page, edit the user credentials (Figure 4-4).

Figure 4-4 Edit Local Sponsor Account

The screenshot shows the "Edit the local user account details" form. It includes the following fields and controls:

- Username: username
- First Name: first
- Last Name: last
- Password: [empty field]
- Repeat Password: [empty field]
- Group: DEFAULT (dropdown menu)
- Email Address: firstlast@cisco.com
- Buttons: Save Settings, Reset Form

A note below the password fields states: "If you don't wish to change the password please keep the entry empty."

- First Name—Edit the first name for the sponsor account.
- Last Name—Edit the last name for the sponsor account.



Note Leaving the Password and Repeat Password fields empty keeps the existing password.

- Password—Change the password for the sponsor account.
- Repeat Password—Retype the changed password for the sponsor account.
- Groups—Select the group for the sponsor account from the dropdown. [Chapter 5, “Configuring User Group Permissions”](#) provides further details on groups.
- Email Address—Edit the email address of the sponsor.

Step 4 Click the **Save Settings** button.

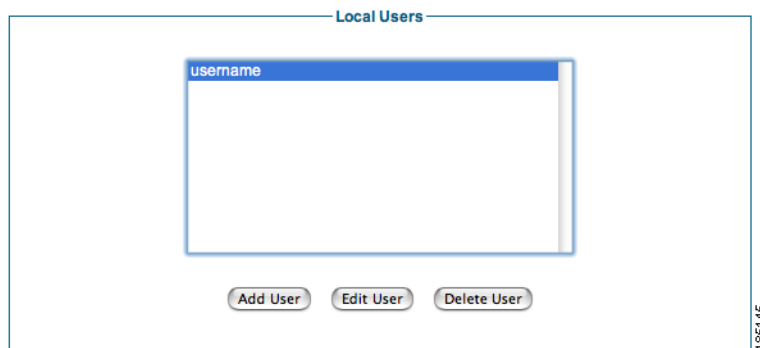
- If there are any errors, the account is not changed and an error message displays at the top of the page.
- If successfully changed, a success message displays at the top of the page and you can make additional changes to the same user account.

Delete Existing User Account

You can delete existing sponsor user accounts from the administration interface.

Step 1 From the administration interface select **Authentication > Sponsors > Local User Database** from the menu ([Figure 4-5](#)).

Figure 4-5 Select User to Delete



Step 2 Select the user from the list and click the **Delete User** button.

Step 3 Confirm deletion of the user at the prompt.

- If successfully deleted, a success message displays at the top of the page and you can perform additional local user account operations.

Configuring Active Directory (AD) Authentication

Active Directory Authentication authenticates sponsor users to the Guest Server using their existing AD user accounts. This keeps sponsors from having to remember another set of user names and passwords just to authenticate to the Guest Server. It also enables the administrator to quickly roll out Guest Access because there is no need to create and manage additional sponsor accounts. Active Directory authentication allows you to do the following:

- [Add Active Directory Domain Controller](#)
- [Edit Existing Domain Controller](#)
- [Delete Existing Domain Controller Entry](#)

AD authentication supports authentication against multiple domain controllers. The domain controllers can be part of the same Active Directory to provide resilience, or they can be in different Active Directories so that the Guest Server can authenticate sponsor users from separate domains, even where no trust relationship is configured.

All Active Directory Authentication is performed against individual domain controller entries. A domain controller entry consists of 6 items:

- **Server Name**—A text description to identify the domain controller. As a best practice, Cisco recommends identifying the domain controller and the account suffix in this field (although it can be set to anything that you choose.)
- **User Account Suffix**—Every user in Active Directory has a full user logon name which appears as “username@domain.” Typing the @domain suffix (including the @ symbol) in this field allows sponsor users not to have to enter their full user logon name.
- **Domain Controller IP Address**—The IP address of the domain controller that the sponsor user authenticates against.
- **Base DN**—The root of the Active Directory. This allows an LDAP search to be performed to find the user group of the sponsor.
- **AD Username**—The user account that has permissions to search the AD. This allows an LDAP search for the user group of the sponsor.
- **AD Password**—The password for the user account that has permissions to search the AD.

To allow you to authenticate different user account suffixes against the same domain controller, you can create multiple domain controller entries with the same IP address and different user Account suffixes. All that needs to be different in each entry is the Server Name, User Account Suffix and Base DN.

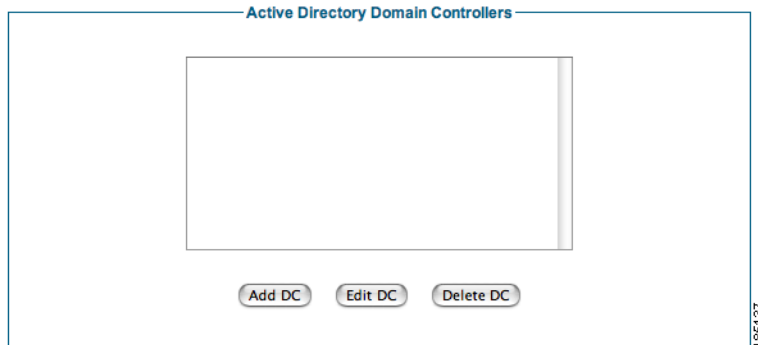
To provide resilience in the event of a domain controller failure, you can enter multiple entries for the same User Account Suffix with different Domain Controller IP Addresses. All that needs to be different in each entry is the Server Name.

The Guest Server attempts to authenticate sponsors against each Domain Controller entry according to the Authentication Order specified in [Configuring Sponsor Authentication Settings, page 4-18](#).

Add Active Directory Domain Controller

- Step 1** From the administration interface select **Authentication > Sponsors > Active Directory Servers** from the menu. (Figure 4-6).

Figure 4-6 Active Directory Authentication



- Step 2** Click the **Add DC** button.
- Step 3** In the Add Active Directory Domain Controller page, enter all the details for authenticating against a specific AD Domain Controller (Figure 4-7).

Figure 4-7 Add Active Directory Domain Controller

The User Account Suffix should start with @ such as @yourdomain.com

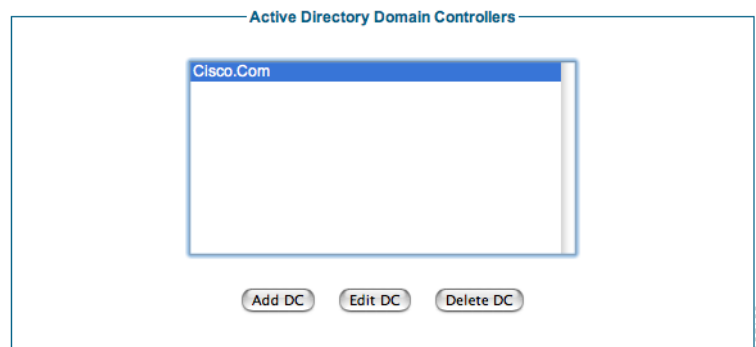
- **Server Name**—Type a text description of the AD Server Name and account suffix for the domain controller, for example: CCA.CISCO.COM.
- **User Account Suffix**—Type the User Account Suffix and include the leading @, for example: @cca.cisco.com. Every AD user has a full user logon name that appears as “username@domain.” To allow sponsors not to have to type their full user logon name, type the @domain part (including the @ symbol) in this field.
- **Domain Controller** —Type the IP address or DNS name for the domain controller. This is the IP address of the DC against which the sponsor authenticates.

- **Base DN**—Type the Base Distinguished Name (DN) of the domain controller. This is the name of the root of the directory tree. It is used so that when group searches are performed, the Guest Server knows from where to start. An example of the base DN for the domain cca. cisco.com is DC=cca,DC=cisco,DC=com.
 - **AD Username**—Type a username that has permissions to search the Active Directory using LDAP. This allows the Guest Server find out details about users such as the list of groups to which they belong.
 - **AD Password**—In addition to the AD Username, type the password for that account.
 - **Confirm AD Password**— Retype the password to make sure it is correct.
 - **Status**—Select the status of the Domain Controller. If it is set to **Active**, the Guest Server will use it for authenticating sponsors. If it is set to **Disabled**, it will not be used.
- Step 4** Optionally click the **Test Connection** button to verify the settings are correct for the domain controller. The Test Connection will authenticate with the specified AD Username and Password to verify the settings.
- Step 5** Click the **Add Domain Controller** button.

Edit Existing Domain Controller

- Step 1** From the administration interface select **Authentication > Sponsor > Active Directory Servers** from the menu.
- Step 2** Select the Active Directory Domain Controller from the list and click the **Edit DC** button (Figure 4-8).

Figure 4-8 Select Domain Controller to Edit



- Step 3** In the Active Directory Domain Controller page (Figure 4-9), edit the details for authenticating against this AD domain controller.

Figure 4-9 Edit DC Settings

Edit Active Directory Domain Controller

Server Name: Cisco.Com

User Account Suffix: @cisco.com

Domain Controller IP Address: 1.1.1.1

Base DN: DN=cisco,DN=com

AD Username: administrator

AD Password:

Confirm Password:

If you don't wish to change the password please keep the entry empty.

185136

The User Account Suffix should start with @ such as @yourdomain.com

Step 4 Modify settings as needed:

- **User Account Suffix**—Edit the User Account Suffix and include the leading @, for example: @cca.cisco.com. Every AD user has a full user logon name that appears as “username@domain.” To allow sponsors not to have to type their full user logon name, type the @domain part (including the @ symbol) in this field.
- **Domain Controller IP Address**—Edit the IP address for the domain controller. This is the IP address of the DC against which the sponsor authenticates.
- **Base DN**—Edit the Base Distinguished Name (DN) of the domain controller. This is the name of the root of the directory tree. It is used so that when group searches are performed, the Guest Server knows from where to start. An example of the base DN for the domain cca. cisco.com is DC=cca,DC=cisco,DC=com.
- **AD Username**—Edit the username that has permissions to search the Active Directory using LDAP. This allows the Guest Server find out details about users such as the list of groups to which they belong.



Note If you do not want to change the password, leaving both password entries empty preserves the existing password.

- **AD Password**—Edit the password for that AD user account that has search permissions.
- **Confirm AD Password**—Retype the password to make sure it is correct.
- **Status**—Select the status of the Domain Controller. If it is set to **Active**, the Guest Server will use it for authenticating sponsors. If it is set to **Disabled**, it will not be used.

Step 5 Optionally click the **Test Connection** button to verify the settings are correct for the domain controller. The Test Connection will authenticate with the specified AD Username and Password to verify the settings.

Step 6 Click the **Save Settings** button.

Delete Existing Domain Controller Entry

- Step 1** From the administration interface, select **Authentication > Sponsor > Active Directory Servers** from the menu.
- Step 2** Select the domain controller from the list (Figure 4-10).

Figure 4-10 Delete Domain Controller entries



- Step 3** Click the **Delete DC** button.
- Step 4** Confirm deletion of the Domain Controller at the prompt.

If there are any errors, the DC is not changed and an error message displays at the top of the page. If successfully deleted, a success message displays at the top of the page and you can perform additional Domain Controller operations.

Configuring LDAP Authentication

LDAP Authentication authenticates sponsor users to the Guest Server using their existing LDAP user accounts. This keeps sponsors from having to remember another set of user names and passwords just to authenticate to the Guest Server. It also enables the administrator to quickly roll out Guest Access because there is no need to create and manage additional sponsor accounts. LDAP authentication allows you to do the following:

- [Add an LDAP Server](#)
- [Edit an Existing LDAP Server](#)
- [Delete an Existing LDAP Server Entry](#)

LDAP authentication supports authentication against multiple LDAP Servers.

An LDAP server entry consists of multiple items:

- LDAP Server Name—A text description to identify the LDAP Server.
- LDAP Server URL—This is the URL to access the LDAP server such as `ldap://ldap.cisco.com`.
- Port—The TCP port used to contact the LDAP server, such as port 389.
- Version—The LDAP version to use (version 1, 2 or 3).

- Base DN—This is the Distinguished Name of the container object where an LDAP search to find the user begins, such as OU=Engineering,O=Cisco.
- User Search Filter—The User Search Filter defines how user entries are named in the LDAP server. For example, you can define them as uid (uid=%USERNAME%) or cn (cn=%USERNAME%).
- Group Mapping—There are two main methods that LDAP servers use for assigning users to groups:
 1. Storing the group membership in an attribute of the user object. With this method the user object has one or more attributes that list the groups that the user is a member of. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups the user is a member of.
 2. Storing the user membership in an attribute of the group object. With this method there is a group object that contains a list of the users who are members of the group. If your LDAP server uses this method, you need to specify the group to check under the LDAP mapping section of a User Group you want to match the user to.

To determine which method to use, Cisco recommends checking the LDAP documentation for your server or using an LDAP browser like the one available at <http://www.ldapbrowser.com/> to check the attributes of the server.

- Username—The user account that has permissions to search the LDAP server. This is needed so that the Cisco NAC Guest Server can search for the user account and group mapping information.
- Password—The password for the user account that has permissions to search the LDAP server.

To provide resilience in the event of an LDAP server failure, you can enter multiple entries for high availability LDAP servers pointing to the same database. All that needs to be different in each entry is the Server name and URL.

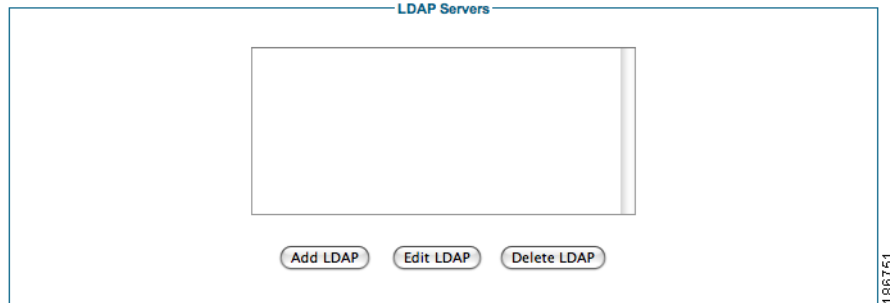
The Guest Server attempts to authenticate sponsors against each LDAP server entry in the order specified by Authentication Order detailed in the [Configuring Sponsor Authentication Settings](#) section.

To verify that you have the correct LDAP credentials for connecting to your LDAP server, Cisco recommends testing an LDAP browser like the one available at <http://www.ldapbrowser.com/>.

Add an LDAP Server

- Step 1** From the administration interface select **Authentication > Sponsors > LDAP Servers** from the menu (Figure 4-11).

Figure 4-11 LDAP Authentication



- Step 2** Click the **Add LDAP** button.

- Step 3** In the Add LDAP Server page, enter all the details for authenticating against a specific LDAP server (Figure 4-12).

Figure 4-12 Add LDAP Server

- LDAP Server Name—Type a text description of the LDAP Server Name. For example: Cisco LDAP - ldap.cisco.com.
- LDAP Server URL—Enter the URL for accessing the LDAP server, such as ldap://ldap.cisco.com or ldaps://ldap.cisco.com.
- Port—Enter the TCP port used to connect to the LDAP server. The common port for LDAP is 389.
- Version—The version of LDAP that the server supports (version 1, 2 or 3).
- Base DN—This is the Distinguished Name of the container object where an LDAP search to find the user will be started from, such as OU=Users,O=Cisco.com or OU=Engineering,O=Cisco.
- User Search Filter—The User Search Filter defines how user entries are named in the LDAP server. For example you can define them to be uid (uid=%USERNAME%) or cn (cn=%USERNAME%). The %USERNAME% should be placed where the username will be inserted in a search.
- Group Mapping—There are two main methods that LDAP servers use for assigning users to groups:
 1. Storing the group membership in an attribute of the user object. With this method the user object has one or more attributes that list the groups that the user is a member of. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups the user is a member of. This attribute may be called something like groupMembership, memberOf, or group.
 2. Storing the user membership in an attribute of the group object. With this method there is a group object that contains a list of the users who are members of the group. If your LDAP server uses this method, you need to specify the group to check under the LDAP mapping section of a User Group you want to match the user to.

To determine which method to use, Cisco recommends checking the LDAP documentation for your server or using an LDAP browser like the one available at <http://www.ldapbrowser.com/> to check the attributes of the server.

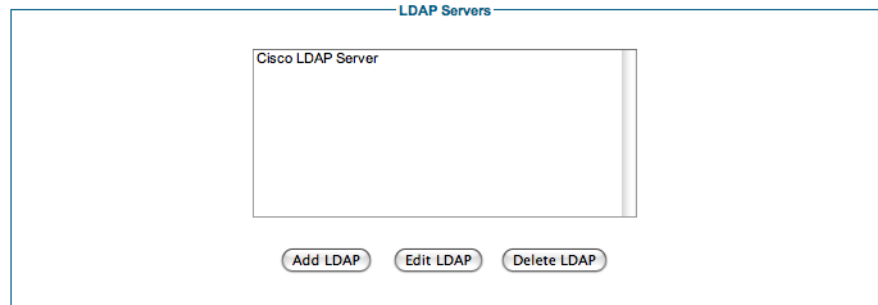
- Username—The user account that has permissions to search the LDAP server. This is needed so that the Cisco NAC Guest Server can search for the user account and group mapping information.
- Password—The password for the user account that has permissions to search the LDAP server.
- Confirm Password—Repeat the password to make sure it matches.
- Status—Select the status of the LDAP server. If it is set to Active the Guest Server will use it for authenticating sponsors. If it is set to Disabled it will not be used.

Step 4 Optionally click the **Test Connection** button to verify the settings are correct for the LDAP server. The Test Connection will bind with the username and password specified to the LDAP server to verify that it can bind successfully.

Step 5 Click the **Add LDAP Server** button.

Edit an Existing LDAP Server

- Step 1** From the administration interface select **Authentication > Sponsor > LDAP Servers** from the menu.
- Step 2** Select the Active Directory Domain Controller from the list and click the **Edit DC** button (Figure 4-13).

Figure 4-13 Select LDAP Server to Edit

Step 3 In the LDAP Server page (Figure 4-14), edit the details for authenticating against this LDAP server.

Figure 4-14 Edit LDAP Server Settings

 The screenshot shows the "Edit LDAP Server" configuration page. Fields include:

- LDAP Server Name: Cisco LDAP Server
- LDAP Server URL: ldap://ldap.cisco.com
- Port: 389
- Version: LDAP Version 3 (dropdown)
- Base DN: OU=users,O=cisco.com
- User Search Filter: uid=%USERNAME% (with example: e.g. uid=%USERNAME% or cn=%USERNAME%)
- Use Username attribute for Group mapping:
 - Use attribute: groupMembership
 - Use group object specified under User Groups settings
- LDAP Username: ldapadmin (Full administrator DN)
- LDAP Password: (empty)
- Confirm Password: (empty)
- Status: Active (dropdown)

 At the bottom, there are buttons for "Save Settings", "Reset Form", and "Test Connection". A note says: "To test the Active Directory connection, save the settings and then click the 'Test Connection' button." A vertical label "186742" is on the right side.

Step 4 Modify settings as needed:

- LDAP Server URL—Enter the URL for accessing the LDAP server, such as ldap://ldap.cisco.com or ldap://ldap.cisco.com.
- Port—Enter the TCP port used to connect to the LDAP server. The common port for LDAP is 389.
- Version—The version of LDAP that the server supports (version 1, 2 or 3).
- Base DN—This is the Distinguished Name of the container object where an LDAP search to find the user will be started from, such as OU=Users,O=Cisco.com or OU=Engineering,O=Cisco.

- **User Search Filter**—The User Search Filter defines how user entries are named in the LDAP server. For example you can define them to be uid (uid=%USERNAME%) or cn (cn=%USERNAME%). The %USERNAME% should be placed where the username will be inserted in a search.
- **Group Mapping**—There are two main methods that LDAP servers use for assigning users to groups:
 1. Storing the group membership in an attribute of the user object. With this method the user object has one or more attributes that list the groups that the user is a member of. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups the user is a member of. This attribute may be called something like groupMembership, memberOf, or group.
 2. Storing the user membership in an attribute of the group object. With this method there is a group object that contains a list of the users who are members of the group. If your LDAP server uses this method, you need to specify the group to check under the LDAP mapping section of a User Group you want to match the user to.

To determine which method to use, Cisco recommends checking the LDAP documentation for your server or using an LDAP browser like the one available at <http://www.ldapbrowser.com/> to check the attributes of the server.

- **Username**—The user account that has permissions to search the LDAP server. This is needed so that the Cisco NAC Guest Server can search for the user account and group mapping information.
- **Password**—The password for the user account that has permissions to search the LDAP server.
- **Confirm Password**—Repeat the password to make sure it matches.



Note If you do not want to change the password, leaving both password entries empty preserves the existing password.

- **Status**—Select the status of the LDAP Server. If it is set to Active the Guest Server will use it for authenticating sponsors. If it is set to Disabled it will not be used.

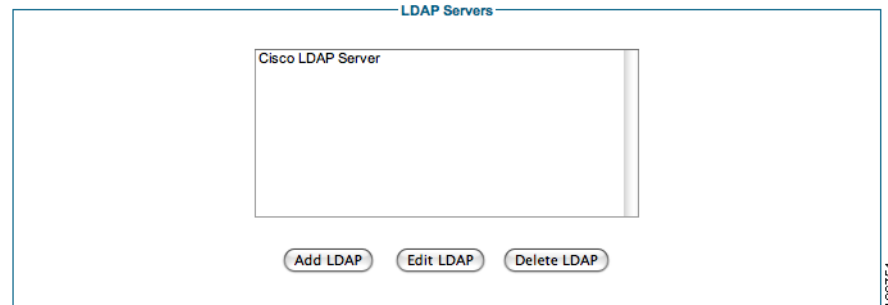
Step 5 Optionally click the **Test Connection** button to verify the settings are correct for the LDAP server. The Test Connection will bind with the username and password specified to the LDAP server to verify that it can bind successfully.

Step 6 Click the **Save Settings** button.

Delete an Existing LDAP Server Entry

Step 1 From the administration interface select **Authentication > Sponsor > LDAP Servers** from the menu.

Step 2 Select the LDAP Server from the list ([Figure 4-15](#)).

Figure 4-15 Delete LDAP Server entries

Step 3 Click the **Delete LDAP** button.

Step 4 Confirm deletion of the LDAP Server at the prompt.

If there are any errors, the LDAP Server is not changed and an error message displays at the top of the page. If successfully deleted, a success message displays at the top of the page and you can perform additional LDAP Server operations.

Configuring RADIUS Authentication

RADIUS Authentication authenticates sponsor users to the Guest Server using their existing RADIUS user accounts. This keeps sponsors from having to remember another set of user names and passwords just to authenticate to the Guest Server. It also enables the administrator to quickly roll out Guest Access because there is no need to create and manage additional sponsor accounts. RADIUS authentication allows you to do the following:

- [Add a RADIUS Server](#)
- [Edit an Existing RADIUS Server](#)
- [Delete an Existing RADIUS Server Entry](#)

RADIUS authentication supports authentication against multiple RADIUS servers, you can

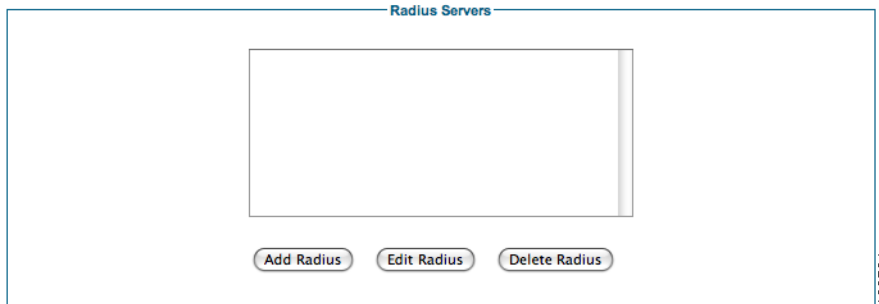
A RADIUS server entry consists of multiple items:

- **RADIUS Server Name**—A text description to identify the LDAP Server.
- **Server IP Address**—This is the IP Address of the RADIUS Server.
- **Port**—The UDP port to contact the ldap server, commonly either 1645 or 1812.
- **Secret**—The shared secret used to secure communications between the RADIUS server and the Cisco NAC Guest Server.

Add a RADIUS Server

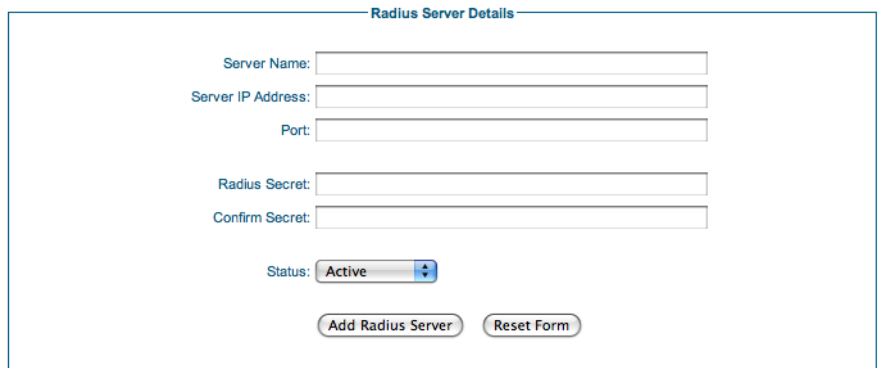
- Step 1** From the administration interface select **Authentication > Sponsors > RADIUS Servers** from the menu (Figure 4-16).

Figure 4-16 RADIUS Authentication



- Step 2** Click the **Add Radius** button.
- Step 3** In the Add RADIUS Server page, enter all the details for authenticating against a specific RADIUS server (Figure 4-17).

Figure 4-17 Add RADIUS Server



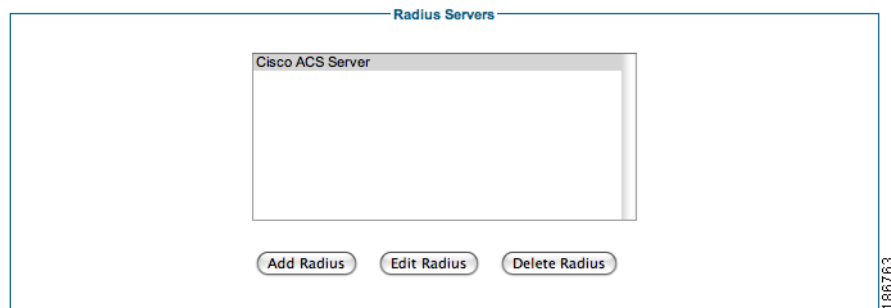
- **Server Name**—Type a text description of the RADIUS Server Name, for example: Cisco RADIUS - radius.cisco.com.
- **Server IP Address**—Enter the IP address or domain name of the RADIUS server.
- **Port**—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
- **Radius Secret**—The shared secret used to secure the communications between the Cisco NAC Guest Server and the RADIUS server.
- **Status**—Select the status of the RADIUS Server. If it is set to **Active**, the Guest Server will use it for authenticating sponsors. If it is set to **Disabled**, it will not be used.

- Step 4** Click the **Add Radius Server** button.

Edit an Existing RADIUS Server

- Step 1** From the administration interface select **Authentication > Sponsor > Radius Servers** from the menu.
- Step 2** Select the RADIUS server from the list and click the **Edit Radius** button (Figure 4-18).

Figure 4-18 Select RADIUS Server to Edit



- Step 3** In the RADIUS Server Details page (Figure 4-19), edit the details for authenticating against this RADIUS server.

Figure 4-19 Edit RADIUS Server Settings

- Step 4** Modify settings as needed:
- Server IP Address—Enter the IP address or domain name of the RADIUS server.
 - Port—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
 - Radius Secret—The shared secret used to secure the communications between the Cisco NAC Guest Server and the RADIUS server.



Note If you do not want to change the shared secret, leaving both secret entries empty preserves the existing shared secret.

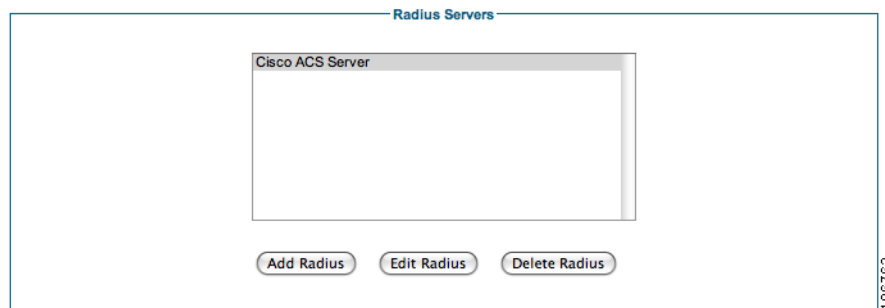
- Status —Select the status of the RADIUS Server. If it is set to **Active**, the Guest Server will use it for authenticating sponsors. If it is set to **Disabled**, it will not be used.

Step 5 Click the **Save Settings** button.

Delete an Existing RADIUS Server Entry

- Step 1** From the administration interface select **Authentication > Sponsor > Radius Servers** from the menu.
- Step 2** Select the RADIUS server from the list (Figure 4-20).

Figure 4-20 Delete RADIUS Server Entries



- Step 3** Click the **Delete Radius** button.
- Step 4** Confirm deletion of the RADIUS server at the prompt.

If there are any errors, the RADIUS server is not changed and an error message displays at the top of the page. If successfully deleted, a success message displays at the top of the page and you can perform additional RADIUS operations.

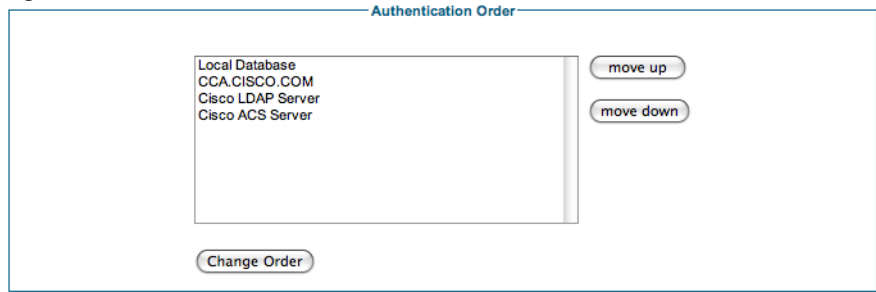
Configuring Sponsor Authentication Settings

Changing the Order of Authentication Servers

When a sponsor authenticates against the Cisco NAC Guest Server it tries each authentication server that has been defined in order until it successfully authenticates a sponsor. If none of the authentication servers can authenticate the sponsor an error message is returned.

As you can define many different authentication servers of different kinds you can order them in any way that you want on a server-by-server basis.

- Step 1** From the administration interface select **Authentication > Sponsor > Authentication Order** from the menu (Figure 4-21).

Figure 4-21 Authentication Order.

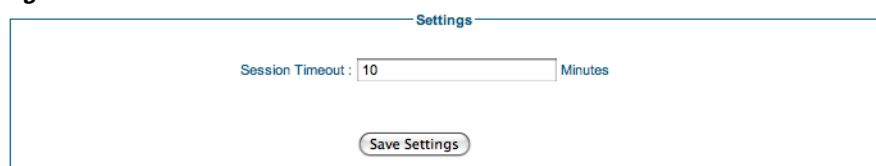
The first server to be authenticated against is at the top of the list and the last at the bottom.

- Step 2** Select the server that you want to re-order from the list and click either the **move up** or **move down** button. Perform this action with all the servers until they are in the correct order.
- Step 3** To save the authentication order click the **Change Order** button.

Sponsor Timeouts

When a sponsor is logged in to the Cisco NAC Guest Server they should be logged out after a period of inactivity. You can set the inactivity period through the sponsor settings page.

- Step 1** From the administration interface select **Authentication > Sponsor > Settings** from the menu (Figure 4-22).

Figure 4-22 Session Timeouts.

- Step 2** Enter the session timeout value (in minutes). When a sponsor has been inactive for this amount of time, their session expire and the next action they perform takes them to the login page.
- Step 3** Click the **Save Settings** button to save the session timeout.

