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 two options:

- Local User Authentication—Create sponsor accounts directly on the Cisco NAC Guest Server. See Configuring Local Sponsor Authentication
- AD Authentication—Authenticate sponsors against an existing Active Directory (AD) implementation. See Configuring Active Directory (AD) Authentication.

Configuring Local Sponsor Authentication

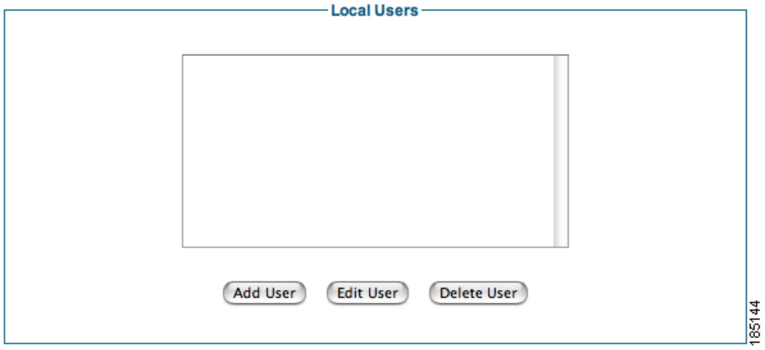
Local authentication allows you to set up sponsor user accounts directly on the Cisco NAC Guest Server. Local authentication allows you to do the following:

- Add New Local User Account
- Edit Existing User Account
- Delete Existing User Account

Add New Local User Account

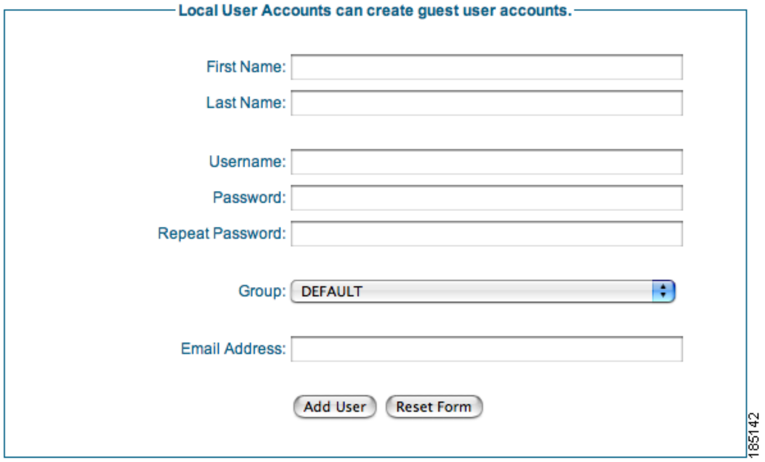
Step 1 From the administration interface select **Authentication > Local Users** from the left hand menu (Figure 4-1).

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


Local User Accounts can create guest user accounts.

Group: DEFAULT

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.

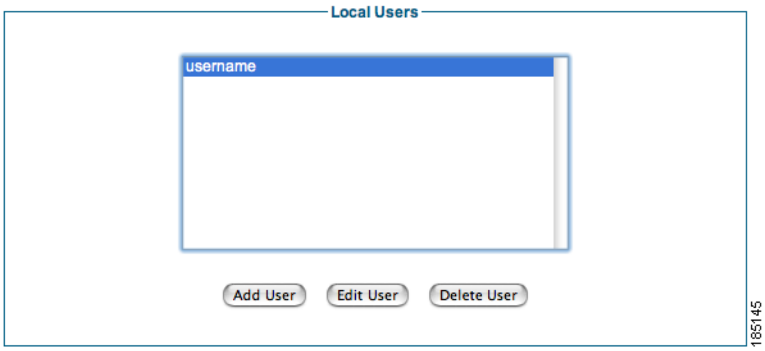
- If successfully added, a success message displays at the top of the page and you can add additional user accounts.

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 > Local Users** from the left hand menu (Figure 4-3).

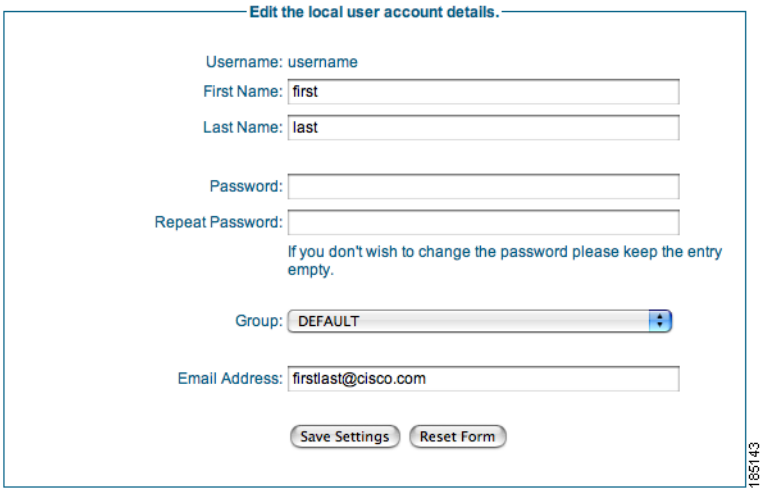
Figure 4-3 Local Users to Edit



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



Edit the local user account details.

Username: username

First Name: first

Last Name: last

Password:

Repeat Password:

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

Group: DEFAULT

Email Address: firstlast@cisco.com

- 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.

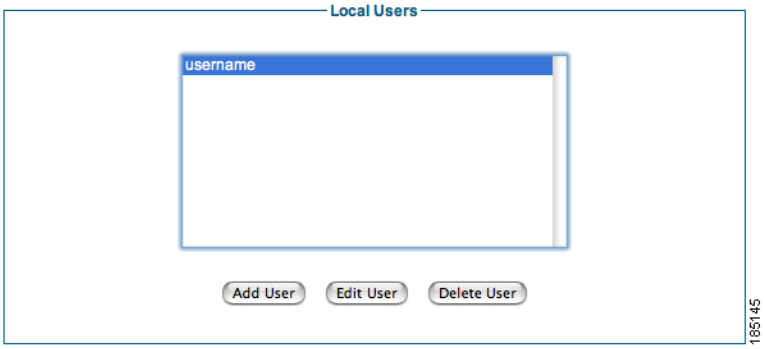
- If there are any errors, the account is not changed and an error message displays at the top of the page.
- If successfully changed, a success message displays at the top of the page and you can make additional changes to the same user account.

Delete Existing User Account

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

Step 1 From the administration interface select **Authentication > Local Users** from the left hand 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 (Lightweight Directory Access Protocol) 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.

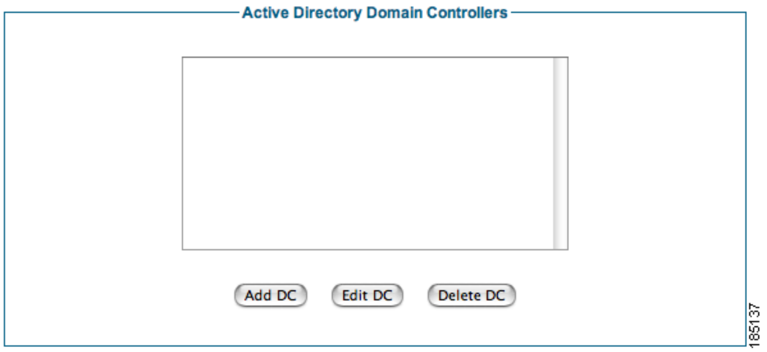
To provide resilience in the event of a domain controller failure, you can enter multiple entries for the same User Account Suffix with different Domain Controller IP Addresses. All that needs to be different in each entry is the Server Name.

The Guest Server attempts to authenticate sponsors against each Domain Controller entry in turn.

Add Active Directory Domain Controller

Step 1 From the administration interface select **Authentication > AD Authentication** from the left hand menu. (Figure 4-6).

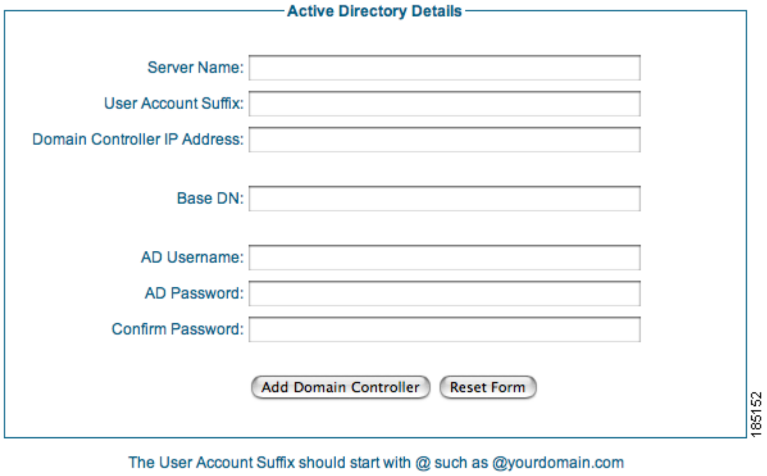
Figure 4-6 Active Directory Authentication



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 IP Address—Type the IP address 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.

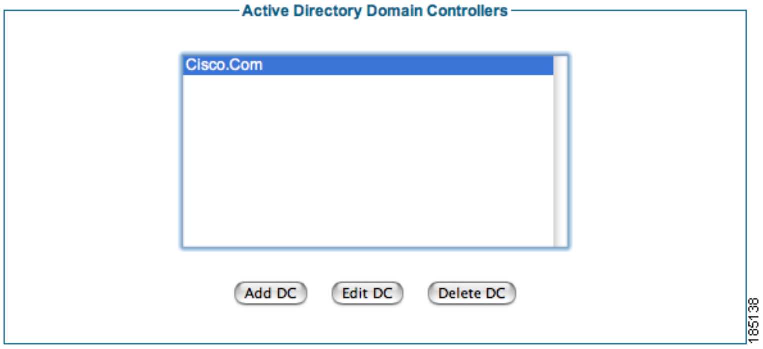
Step 4 Click the Add Domain Controller button.

Edit Existing Domain Controller

Step 1 From the administration interface select **Authentication > AD Authentication** from the left hand menu.

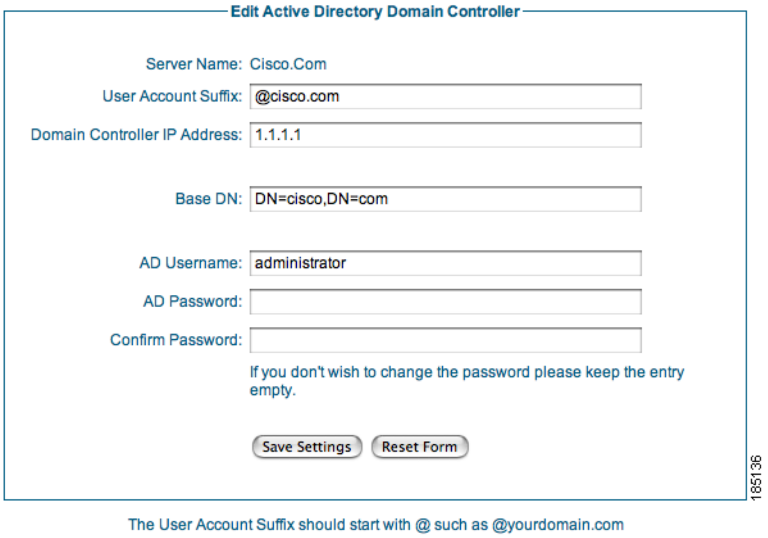
Step 2 Select the Active Directory Domain Controller from the list and click the Edit DC button (Figure 4-8).

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.

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.

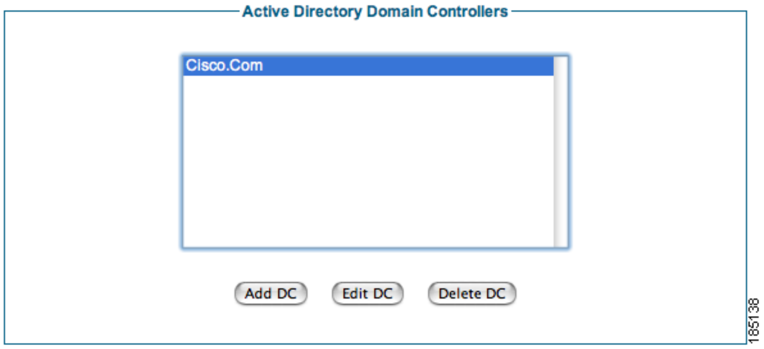
Step 5 Click the Save Settings button.

Delete Existing Domain Controller Entry

Step 1 From the administration interface select **Authentication > AD Authentication** from the left hand 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.