



CHAPTER 4

Configuring Sponsor Authentication

Sponsors are the people who use Cisco NAC Guest Server to create guest accounts. Sponsor authentication authenticates sponsor users to the Sponsor interface of the Guest Server. There are five options available:

- Local User Authentication—Create local sponsor accounts directly on the Cisco NAC Guest Server. See [Configuring Local Sponsor Authentication, page 4-1](#).
- Active Directory Authentication—Authenticate sponsors against an existing Active Directory (AD) implementation. See [Configuring Active Directory \(AD\) Authentication, page 4-6](#).
- LDAP Authentication—Authenticate sponsors against a Lightweight Directory Access Protocol (LDAP) server. See [Configuring LDAP Authentication, page 4-10](#).
- RADIUS Authentication—Authenticate sponsors against a RADIUS server. See [Configuring RADIUS Authentication, page 4-16](#).
- Active Directory Single Sign-On—This option uses Kerberos between the client’s web browser and the Cisco NAC Guest Server to automatically authenticate a sponsor against an Active Directory Domain Controller. See [Configuring Active Directory Single Sign-On, page 4-20](#).

You can configure multiple authentication servers in the Cisco NAC Guest Server as well as the order in which the authentication servers are used to authenticate sponsors. For details, see [Configuring Sponsor Authentication Settings, page 4-19](#).

Configuring Local Sponsor Authentication

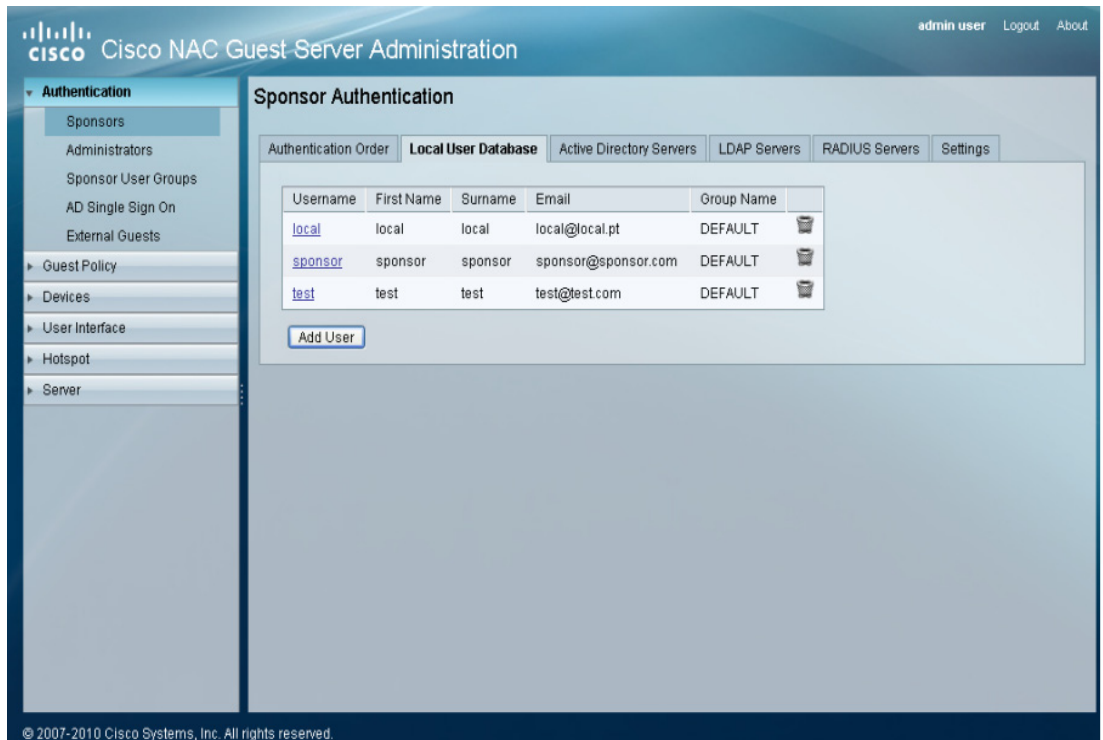
Local authentication allows you to set up sponsor user accounts directly on the Cisco NAC Guest Server. You can do the following with local authentication:

- [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 as shown in [Figure 4-1](#).

Figure 4-1 Local Users



Step 2 Click the **Add User** button to bring up the local sponsor configuration page as shown in [Figure 4-2](#).

Figure 4-2 Add Local User

Add A Local User Account

Local User Database

Local User Accounts can create guest user accounts

First Name:

Last Name:

Email:

Group:

Username:

Password: Confirm:

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.
- **Email**—Type email address of the sponsor.
- **Group**—Select the group for the sponsor account from the dropdown. [Chapter 5, “Configuring Sponsor User Groups”](#) provides further details on groups.

- **Username**—Type the user name for the sponsor account.
- **Password**—Type the password for the sponsor account.
- **Confirm** —Retype the password for the sponsor account

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

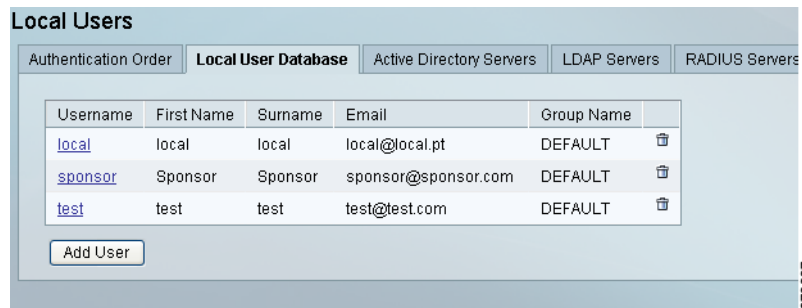
- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional user accounts.

Edit Existing User Account

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

Step 1 From the administration interface, select **Authentication > Sponsors** and click the **Local User Database** tab as shown in [Figure 4-3](#).

Figure 4-3 Local Users to Edit



The screenshot shows the 'Local Users' interface with the 'Local User Database' tab selected. It contains a table with the following data:

Username	First Name	Surname	Email	Group Name	
<u>local</u>	local	local	local@local.pt	DEFAULT	
<u>sponsor</u>	Sponsor	Sponsor	sponsor@sponsor.com	DEFAULT	
<u>test</u>	test	test	test@test.com	DEFAULT	

Below the table is an 'Add User' button. The interface also shows tabs for 'Authentication Order', 'Active Directory Servers', 'LDAP Servers', and 'RADIUS Servers'.

Step 2 Select the user from the list and click the underlined username.

Step 3 In the Edit a Local User Account page, edit the user credentials as shown in [Figure 4-4](#).

Figure 4-4 Edit Local User Account

- **First Name**—Edit the first name for the sponsor account.
- **Last Name**—Edit the last name for the sponsor account.
- **Email** —Edit the email address of the sponsor.
- **Group**—Select the group for the sponsor account from the dropdown. [Chapter 5, “Configuring Sponsor User Groups”](#) provides further details on groups.



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

- **Password**—Change the password for the sponsor account.
- **Confirm** —Retype the changed password for the sponsor account.

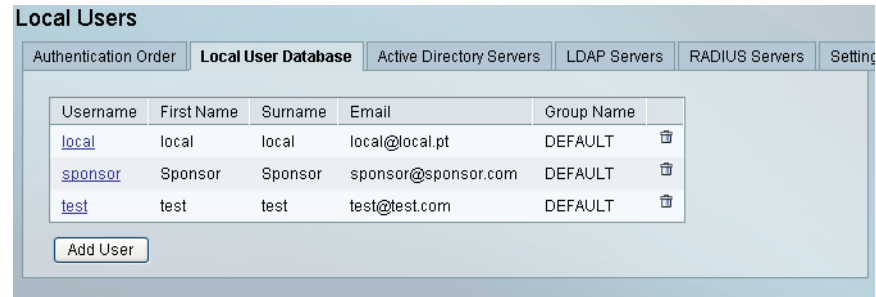
Step 4 Click the **Save Settings** button.

- If there are any errors, the account is not changed and an error message is displayed at the top of the page.
- If successfully changed, a success message is displayed 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** and then click the **Local User Database** tab as shown in [Figure 4-5](#).

Figure 4-5 Select User to Delete

- Step 2** A list of local users appears on the page. Choose the user you wish to delete by clicking the bin icon to the right of the **Group Name** field.
- Step 3** Confirm deletion of the user at the prompt.
- If successfully deleted, a success message is displayed 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. The sponsors need not have another set of user names and passwords 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 local 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. 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 authenticated by the sponsor user.
- **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. The Server Name, User Account Suffix, and Base DN need to be different in each entry.

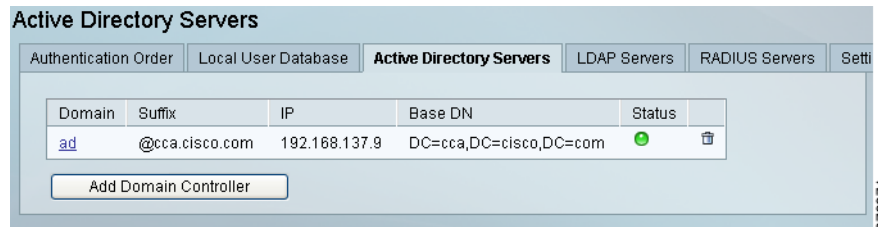
To provide resilience in the event of a domain controller failure, you can enter multiple entries for the same User Account Suffix with different Domain Controller IP Addresses. The Server Name needs to be different in each entry.

The Guest Server attempts to authenticate sponsors against each Domain Controller entry according to the Authentication Order specified in [Configuring Sponsor Authentication Settings, page 4-19](#).

Add Active Directory Domain Controller

- Step 1** From the administration interface, select **Authentication > Sponsors > Active Directory Servers** from the menu as shown in [Figure 4-6](#).

Figure 4-6 Active Directory Authentication



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

Figure 4-7 Add Active Directory Domain Controller

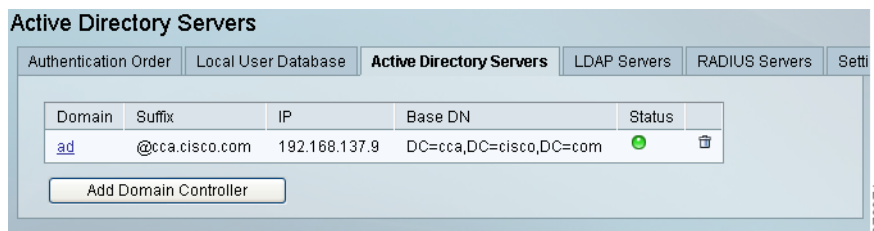
- **Server Name**—Type a text description of the AD Server Name and account suffix for the domain controller. For example: CCA.CISCO.COM.
- **User Account Suffix**—Type the User Account Suffix and include the leading @. For example: @cca.cisco.com. Every AD user has a full user logon name that appears as “username@domain”. To allow sponsors to type their user logon name alone, 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 authenticated by the sponsor.

- **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.
 - **Username**—Type a username that has permissions to search the Active Directory using LDAP. This allows the Guest Server to find out details about users such as the list of groups to which they belong.
 - **Password**—In addition to the AD Username, type the password for that account.
 - **Confirm**—Retype the password for confirmation.
 - **Enabled**—Check the checkbox to enable the Guest Server to use this AD server to authenticate sponsors. If not checked, the AD server will not be used.
- Step 4** Click the **Test Connection** button to verify that the settings are correct for the domain controller. Test Connection authenticates with the specified AD Username and Password to verify the settings. Success or failure status is returned by “Active Directory Connection Successful” or “Active Directory Connection Failed” messages.
- Step 5** Click the **Add Domain Controller** button to add the Domain Controller button. If successfully added, a confirmation message is displayed at the top of the page.

Edit Existing Domain Controller

- Step 1** From the administration interface, select **Authentication > Sponsor > Active Directory Servers** from the menu as shown in [Figure 4-6](#).
- Step 2** Select the Active Directory Domain Controller from the list and click the underlined domain name to select and edit the domain controller as shown in [Figure 4-8](#).

Figure 4-8 Select Domain Controller to Edit



- Step 3** In the Edit Active Directory Domain Controller page as shown in [Figure 4-9](#), edit the details for authenticating against this AD domain controller.

Figure 4-9 Edit Active Directory Domain Controller

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**—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, leave the Password and Confirm fields empty to retain the existing password.

- **Password**—Edit the password for that AD user account that has search permissions.
- **Confirm** —Retype the password to make sure it is correct.
- **Enabled**—Check this checkbox to enable the Guest Server to use this AD server to authenticate sponsors. If not checked, the AD server will not be used.

Step 5 Click the **Test Connection** button to verify that the settings are correct for the domain controller. Test Connection authenticates with the specified AD Username and Password to verify the settings. Success or failure status is returned by “Active Directory Connection Successful” or “Active Directory Connection Failed” messages.

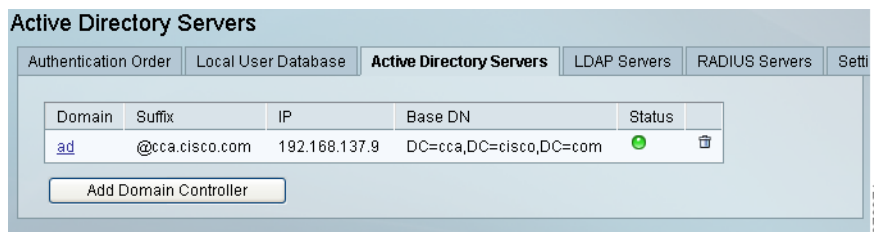
Step 6 Click the **Save Settings** button.

Delete Existing Domain Controller Entry

Step 1 From the administration interface, select **Authentication > Sponsor > Active Directory Servers** from the menu.

Step 2 Click the underlined name of the domain controller from the list as shown in [Figure 4-10](#).

Figure 4-10 Delete Domain Controller entries



Step 3 Delete the domain controller by clicking the bin icon to the right of the **Status** field.

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 is displayed at the top of the page. If successfully deleted, a success message is displayed 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. The sponsors need not have another set of user names and passwords 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 local 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`.
- 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 to which the user belongs. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups of which the user is a member.
 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 for which you want to match the user.

To determine the method to be used, Cisco recommends checking the LDAP documentation for your server or using an LDAP browser 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. The Server name and URL need to be different in each entry.

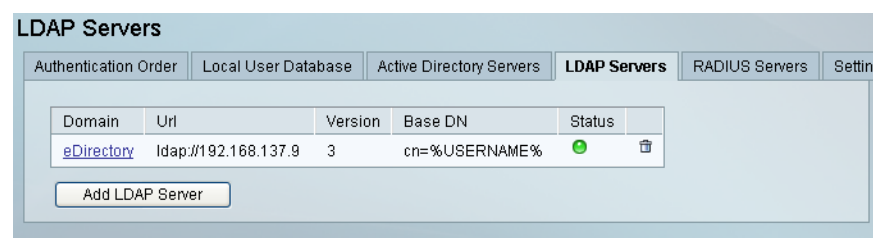
The Guest Server attempts to authenticate sponsors against each LDAP server entry in the order specified by Authentication Order, as detailed in [Configuring Sponsor Authentication Settings, page 4-19](#).

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

Add an LDAP Server

- Step 1** From the administration interface, select **Authentication > Sponsors > LDAP Servers** from the menu as shown in [Figure 4-11](#).

Figure 4-11 LDAP Authentication



- Step 2** Click the **Add LDAP Server** button.
- Step 3** In the Add LDAP Server page, enter all the details for authenticating against a specific LDAP server as shown in [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.
- **Version**—The version of LDAP supported by the server (version 1, 2 or 3).
- **Base DN**—This is the Distinguished Name of the container object from which an LDAP search to find the user is started, 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 of which the user is a member. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups of which the user is a member. 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 to which you want to match the user.

To determine the method to be used, 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.

192565

- **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**—Repeat the password for confirmation.
- **Enabled**—Check the checkbox to enable the Guest Server to use this LDAP server to authenticate sponsors. If not checked, the LDAP server will not be used.

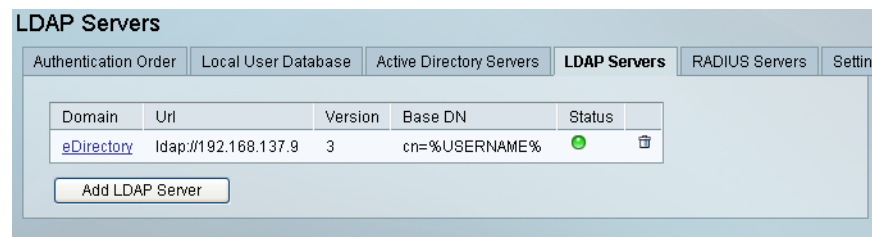
Step 4 Click the **Add LDAP Server** button to successfully save the settings.

Edit an Existing LDAP Server

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

Step 2 Select the LDAP Server you wish to edit from the list and click the underlined domain of that server as shown in [Figure 4-13](#).

Figure 4-13 Select LDAP Server to Edit



Step 3 In the LDAP Server page as shown in [Figure 4-14](#), edit the details for authenticating against this LDAP server.

Figure 4-14 Edit LDAP Server Settings

Edit LDAP Server

LDAP Servers

LDAP Server Details

LDAP Server Name: eDirectory

LDAP Server URL:

Version:

Base DN:

Use Search Filter:
e.g. uid=%USERNAME% or cn=%USERNAME%

Group Mapping: Use group object specified under user Groups settings
 Use username attribute

Username:

Password: Confirm:
If you don't wish to change the password please keep the entry empty

Enabled:

To test the LDAP Server connection, enter the details into the form and then click the 'Test Connection' button. Items marked * are required for connection test.

192540

Step 4 Modify settings as needed:

- **LDAP Server URL**—Enter the URL for accessing the LDAP server, such as ldap://ldap.cisco.com or ldaps://ldap.cisco.com.
- **Version**—The version of LDAP supported by the server (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 of which the user is a member. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups of which the user is a member. 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 to which you want to match the user.

To determine the method to be used, 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**—Repeat the password for confirmation.



Note If you do not want to change the password, leave the Password and Confirm fields empty to retain the existing password.

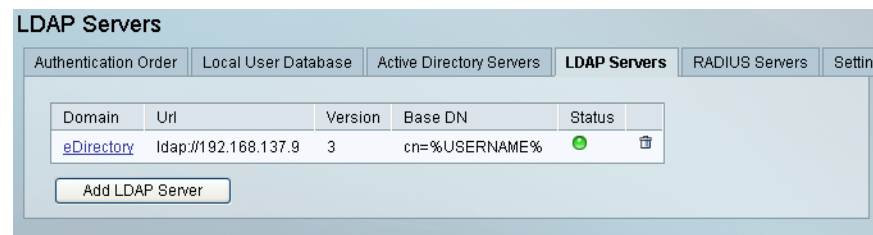
- **Enabled**—Check the checkbox to enable the Guest Server to use this LDAP server to authenticate sponsors. If not checked, the LDAP server will not be used.

- Step 5** Click the **Test Connection** button to verify that 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. Success or failure status is returned by “LDAP Connection Successful” or “LDAP Connection Failed” messages.
- 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 as shown in [Figure 4-15](#).

Figure 4-15 Delete LDAP Server entries



- Step 3** A list of LDAP Servers appears on the choose the server you wish to delete by clicking the bin icon to the right of the **Status** field.
- 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 is displayed at the top of the page. If successfully deleted, a success message is displayed at the top of the page and you can perform additional LDAP Server operations.

Configuring RADIUS Authentication

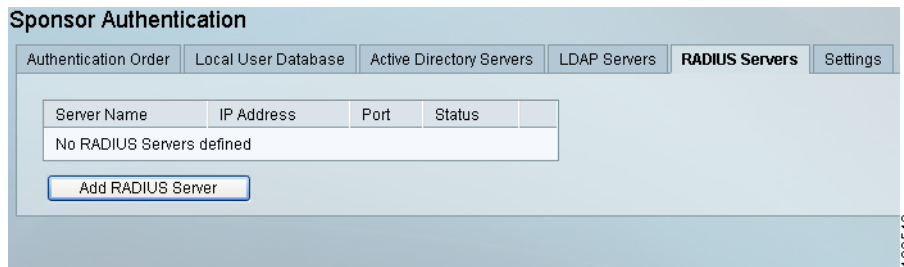
RADIUS authentication authenticates sponsor users to the Cisco NAC Guest Server using their existing RADIUS user accounts. The sponsors need not have another set of user names and passwords to authenticate to the Guest Server. It also enables the administrator to quickly roll out Guest Access because there is no need to create and manage additional local 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](#)

Add a RADIUS Server

Step 1 From the administration interface, select **Authentication > Sponsors > RADIUS Servers** from the menu as shown in [Figure 4-16](#).

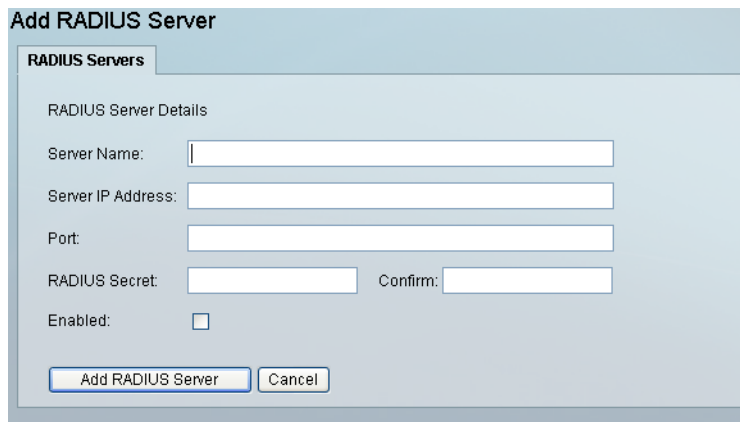
Figure 4-16 RADIUS Authentication



Step 2 Click the **Add RADIUS Server** button.

Step 3 In the Add RADIUS Server page, enter all the details for authenticating against a specific RADIUS server as shown in [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.

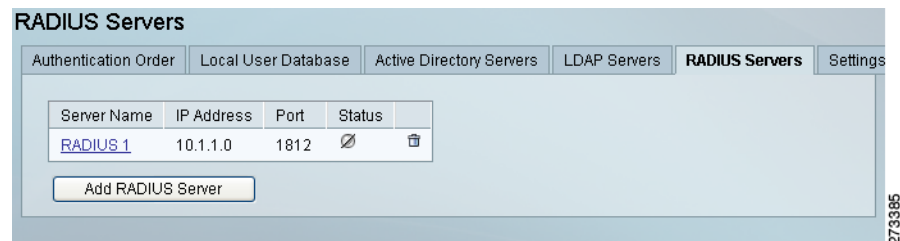
- **Server IP Address**—Enter the IP address or domain name of the RADIUS server.
- **Port**—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
- **RADIUS Secret**—The shared secret used to secure the communications between the Cisco NAC Guest Server and the RADIUS server.
- **Confirm**—Repeat the shared secret for confirmation.
- **Enabled**—Check the checkbox to enable the Guest Server to use this RADIUS server to authenticate sponsors. If not checked, the RADIUS server will not be used.

Step 4 Click the **Save** button.

Edit an Existing RADIUS Server

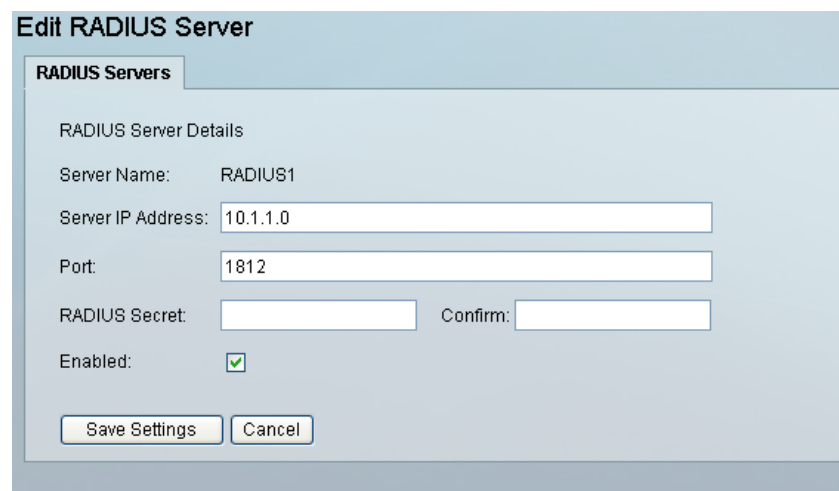
- Step 1** From the administration interface, select **Authentication > Sponsor > RADIUS Servers** from the menu.
- Step 2** Select the RADIUS server from the list and click the underlined name of the server you wish to edit as shown in [Figure 4-18](#).

Figure 4-18 Select RADIUS Server to Edit



- Step 3** In the Edit RADIUS Server Details page as shown in [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, leave the Secret and Confirm fields to retain the existing shared secret.

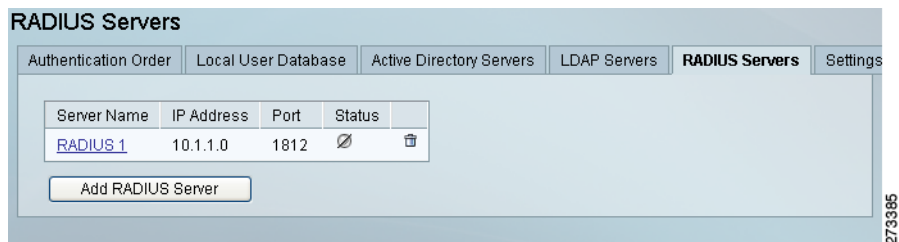
- **Enabled**—Check the checkbox to enable the Guest Server to use this RADIUS server to authenticate sponsors. If not checked, the RADIUS server will not be used.

- 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 as shown in [Figure 4-20](#).

Figure 4-20 Delete RADIUS Server Entries



- Step 3** A list of RADIUS Servers appears on the page. Click the bin icon to the right of the **Status** field to delete the server.
- 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 is displayed at the top of the page. If successfully deleted, a success message is displayed at the top of the page and you can perform additional RADIUS operations.

Configuring Sponsor Authentication Settings

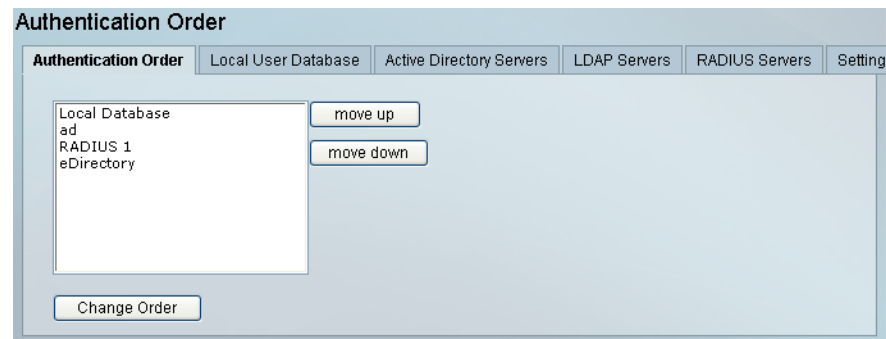
Changing the Order of Authentication Servers

When a sponsor authenticates against the Cisco NAC Guest Server, the Guest Server 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 you want on a server-by-server basis.

- Step 1** From the administration interface, select **Authentication > Sponsor > Authentication Order** from the menu as shown in [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 one 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.

Session Timeouts

A sponsor that logs in to the Cisco NAC Guest Server is logged out after a period of inactivity. You can set the inactivity period through the Session Timeout Settings page.



Note

The Session Timeout defined here applies to both the Sponsor and Administration interfaces. See [Admin Session Timeout, page 3-19](#).

- Step 1** From the administration interface, select **Authentication > Sponsor > Settings** from the menu as shown in [Figure 4-22](#).

Figure 4-22 Session Timeout

- Step 2** Enter the Session Timeout value in minutes (default is 10 minutes). When sponsors are inactive for this amount of time, their sessions 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.

Configuring Active Directory Single Sign-On

The Active Directory Single Sign-On (AD SSO) feature uses Kerberos between the client's web browser and the Cisco NAC Guest Server to automatically authenticate a sponsor against an Active Directory Domain Controller.

An Active Directory Domain Controller in the same domain as the single sign on configuration must have been previously configured as described in [Configuring Active Directory \(AD\) Authentication, page 4-6](#).

Starting from NAC Guest Server 2.0.4, the following environments are supported:

- Windows 2003 Server
- Windows 2008 R2 Server
- Microsoft Windows 2003 client with Internet Explorer 6, 7, 8, and 9

Requirements for Active Directory Single Sign-On

The following requirements must be met for Active Directory Single Sign-On to be configured successfully:

- DNS must be configured and working on the Cisco NAC Guest Server
- DNS must be configured and working on the Domain Controller.
- Both of the following DNS entries for the Cisco NAC Guest Server must be defined:
 - “A” record
 - “PTR” record
- Both of the following DNS entries for the Domain Controller must be defined:
 - “A” record
 - “PTR” record
- Cisco NAC Guest Server time settings must be synchronized with the Active Directory Domain.

If any of these setting are not met, then AD SSO configuration will fail.

**Note**

Cisco strongly recommends to configure NTP so that time is synchronized with the Active Directory Domain. Single Sign-On will fail if the time on the Cisco NAC Guest Server time differs by more than 5 minutes from the client or the domain.

- Step 1** Configure an Active Directory Server as described in [Configuring Active Directory \(AD\) Authentication, page 4-6](#). An Active Directory Server is needed so that users performing Single Sign-On can be correctly mapped against a sponsor group. The Active Directory Server must be in the same domain as the Single Sign-On configuration.
- Step 2** From the administration interface, select **Authentication > AD Single Sign-On** from the left menu as shown in [Figure 4-23](#).

Figure 4-23 Active Directory Single Sign-On

- Step 3** Check the **Enable AD Single Sign On** checkbox to enable AD SSO.
- Step 4** Type the Active Directory Domain Name for the domain for which you want to enable SSO.
- Step 5** Type the Fully Qualified Domain Name of the Active Directory Domain Controller. The Cisco NAC Guest Server needs to be able to resolve both A and PTR records for the Domain Controller.
- Step 6** Type the Fully Qualified Domain Name of the NAC Guest Server. The NAC Guest Server needs to be able to resolve both A and PTR records for itself with DNS.
- Step 7** Type an AD Administrator Username for the Domain, this account is used for adding the NAC Guest Server to the domain and creating its computer account.
- Step 8** Type the Password for the AD Administrator and retype it in the Confirm field.
- Step 9** Click **Save**. The NAC Guest Server will join to the domain, create a computer account and turn on Active Directory Single Sign on.

Mapping User Group with AD SSO

To map a user group with AD SSO, you need to configure the Active Directory Server as Auth Server and then map the AD group with Sponsor User Group.

-
- Step 1** Choose **Authentications > Sponsors > Active Directory Servers**.
 - Step 2** Add a new domain controller.
 - Step 3** Click **Test Connection** to ensure that have configured the domain controller.
 - Step 4** Add a new user group as described in [Adding Sponsor User Groups, page 5-2](#).
 - Step 5** Select **No** in the **Create Bulk Accounts** dropdown.
 - Step 6** In the Active Directory Mapping, ensure that you are selecting the right user group as described in [Mapping to Active Directory Groups, page 5-10](#).
 - Step 7** You can verify that the user is placed in the Sponser group by checking the Audit Logs as described in [Audit Logs, page 15-5](#).
-

Configuring AD SSO on Multiple Domains

Starting from NAC Guest Server Release 2.0.4, you can configure AD SSO on multiple domains.

In the following example, the NAC Guest Server is already present in the domain **cca.cisco.com**. This section explains how to enable AD SSO for a different domain **child.cca.cisco.com** present in the same forest, **cca.cisco.com**.

Before configuring the SSO section, ensure that the "A" and "PTR" records exist for the domain controller and NAC Guest Server.

-
- Step 1** From the administration interface, select **Authentication > AD Single Sign-On** from the left menu as shown in [Figure 4-24](#).

Figure 4-24 Server Settings for Multiple Domain

Server Settings

Enable AD Single Sign On:

AD Domain: CHILD.CCA.CISCO.COM

Domain Controller FQDN: acsdev-w2k3.child.cca.cisco.com

This Server's Hostname FQDN: ngs.cca.cisco.com

Active Directory Credentials

This password is only used to join this server to the Domain. It is not saved.

AD Administrator Username: Administrator

Password: ●●●●●● Confirm: ●●●●●●

Save Cancel

302003

- Step 2** Check the **Enable AD Single Sign On** checkbox to enable AD SSO.
- Step 3** Type the Active Directory Domain Name as **CHILD.CCA.CISCO.COM**.
- Step 4** Type the Fully Qualified Domain Name of the Active Directory Domain Controller.
- Step 5** Type the Fully Qualified Domain Name of the NAC Guest Server as **ngs.cca.cisco.com**.
- Step 6** Type an AD Administrator Username for the Domain.
- Step 7** Type the Password for the AD Administrator and retype it in the Confirm field.
- Step 8** Click **Save**.
- Step 9** Once the domain is configured, you get a success message as shown in [Figure 4-25](#).

Figure 4-25 Configuration Successful for Multi-Domain Setup

Configuration Created

Server Settings

Enable AD Single Sign On:

AD Domain: CHILD.CCA.CISCO.COM

Domain Controller FQDN: acsdev-w2k3.child.cca.cisco.com

This Server's Hostname FQDN: ngs.cca.cisco.com

302003

Verifying the Configuration for Multiple Domain

From the user machine, log into the domain. In this example, this machine is part of the **child.cca.cisco.com** domain. Ensure that the NAC Guest Server is part of local intranet and auto-login is turned on.

In the web browser, enter the domain name. You should be automatically logged in to the domain with the credentials.

**Note**

Use the FQDN for the NAC Guest Server to test SSO from the browser. The IP address does not work.

Configuring AD SSO on Multiple Forests

Starting from NAC Guest Server Release 2.0.4, you can configure AD SSO on multiple forests.

In the following example, the NAC Guest Server is already present in the forest **cca.cisco.com**. This section explains how to enable AD SSO for a different domain **chn-acpdev.com** present in a different forest.

Before configuring the SSO section, ensure that the "A" and "PTR" records exist for the domain controller and NAC Guest Server.

**Note**

AD SSO is supported in cross-forest configurations with two-way trust established between the forests.

Step 1

From the administration interface, select **Authentication > AD Single Sign-On** from the left menu as shown in [Figure 4-26](#).

Figure 4-26 Server Settings for Multiple Forest

Server Settings

Enable AD Single Sign On:

AD Domain: CHN-ACSDEV.COM

Domain Controller FQDN: acs-aantonim.chn-acsdev.com

This Server's Hostname FQDN: ngs.cca.cisco.com

Active Directory Credentials

This password is only used to join this server to the Domain. It is not saved.

AD Administrator Username: Administrator

Password: ●●●●●● Confirm: ●●●●●●

Save Cancel

902001

- Step 2** Check the **Enable AD Single Sign On** checkbox to enable AD SSO.
- Step 3** Type the Active Directory Domain Name as **CHN-ACSDEV.COM**.
- Step 4** Type the Fully Qualified Domain Name of the Active Directory Domain Controller.
- Step 5** Type the Fully Qualified Domain Name of the NAC Guest Server as **ngs.cca.cisco.com**.
- Step 6** Type an AD Administrator Username for the Domain.
- Step 7** Type the Password for the AD Administrator and retype it in the Confirm field.
- Step 8** Click **Save**.
- Step 9** Once the domain is configured, you get a success message as shown in [Figure 4-27](#).

Figure 4-27 Configuration Successful for Multi-Forest Setup

The screenshot shows a configuration window with a green checkmark and the text "Configuration Created". Below this, under the heading "Server Settings", there are four fields:

- Enable AD Single Sign On:
- AD Domain: CHN-ACSDEV.COM
- Domain Controller FQDN: acs-aantonim.chn-acsdev.com
- This Server's Hostname FQDN: ngs.cca.cisco.com

A vertical ID number "302004" is visible on the right side of the configuration box.

Verifying the Configuration for Multiple Forest

From the user machine, log into the domain. In this example, the machine is part of the **chn-acsdev.com** domain. Ensure that the NAC Guest Server is part of local intranet and auto-login is turned on.

In the web browser, enter the domain name. You should be automatically logged in to the domain with the credentials.



Note

Use the FQDN for the NAC Guest Server to test SSO from the browser. The IP address does not work.

Troubleshooting the AD SSO Configuration

This section describes the error messages in the logs and tips to troubleshoot the issues that may occur during the configuration.

Error: Domain format incorrect / Domain Controller must be a FQDN, not an IP address

The domain has not been entered in a correct format, for example: CCA.CISCO.COM.

Error: Hostname must be a FQDN, not an IP address

The hostname of the NAC Guest server cannot be an IP address it must be a Fully Qualified Domain Name, example: nac.cca.cisco.com.

Error: Cannot determine IP address for Domain Controller

Error: Cannot get DNS A record for Domain Controller

Error: Cannot get DNS A record for hostname

Error: Cannot get DNS PTR record for Domain Controller IP address

Error: Cannot get DNS PTR record for hostname IP address

The above errors occur when there is an issue with DNS configuration.

Error: Failed to create computer account for this server on the Domain Controller. See application log for details

Error: Invalid username/password

The administrator username or password is not correct. View the application log for full details of the error.

Error: Invalid Domain or cannot resolve network address for DC

There is a DNS problem on the AD server.

Error: Domain Controller time does not match this server's time

Ensure that the server times match. It is recommended to use NTP to synchronize server times.

Error: The DC cannot determine the hostname for the Guest server by reverse lookup. There may be an issue with your DNS configuration.

The above error may be due to DNS configuration issue on the AD server.

