

|  |
|--|
| <b>Contents</b>  |
| <a href="#">Introduction</a>   |
| <b><a href="#">Prerequisites</a></b>                                   |
| <a href="#">Requirements</a>   |
| <a href="#">Components Used</a>  |
| <a href="#">Conventions</a>  |
| <b><a href="#">Authentication Against Backend Active Directory</a></b> |
| <a href="#">AD/LDAP Configuration Example</a>                          |
| <b><a href="#">Map Users to Roles Using Attributes or VLAN IDs</a></b> |
| <a href="#">Configure Mapping Rule</a>                                 |
| <a href="#">Edit Mapping Rules</a>                                     |
| <b><a href="#">Troubleshoot</a></b>                                    |
| <b><a href="#">Cisco Support Community - Featured</a></b>              |
| <b><a href="#">Conversations</a></b>                                   |
| <b><a href="#">Related Information</a></b>                             |

## Introduction

This document describes the Lightweight Directory Access Protocol (LDAP) mapping feature in order to map the users to certain roles in Network Admission Control (NAC) Appliance or Cisco Clean Access (CCA).

Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed NAC product that uses the network infrastructure to enforce security policy compliance on all devices that seek to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines before network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network.

## Prerequisites

### Requirements

This document assumes that CCA Manager, CCA Server and LDAP Server are installed and work properly.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco NAC Appliance 3300 Series - Clean Access Manager 4.0
- Cisco NAC Appliance 3300 Series - Clean Access Server 4.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

## Authentication Against Backend Active Directory

Several types of authentication providers in the Clean Access Manager can be used to authenticate users against an Active Directory (AD) server, Microsoft's proprietary directory service. These include Windows NT(NTLM), Kerberos and LDAP (preferred).

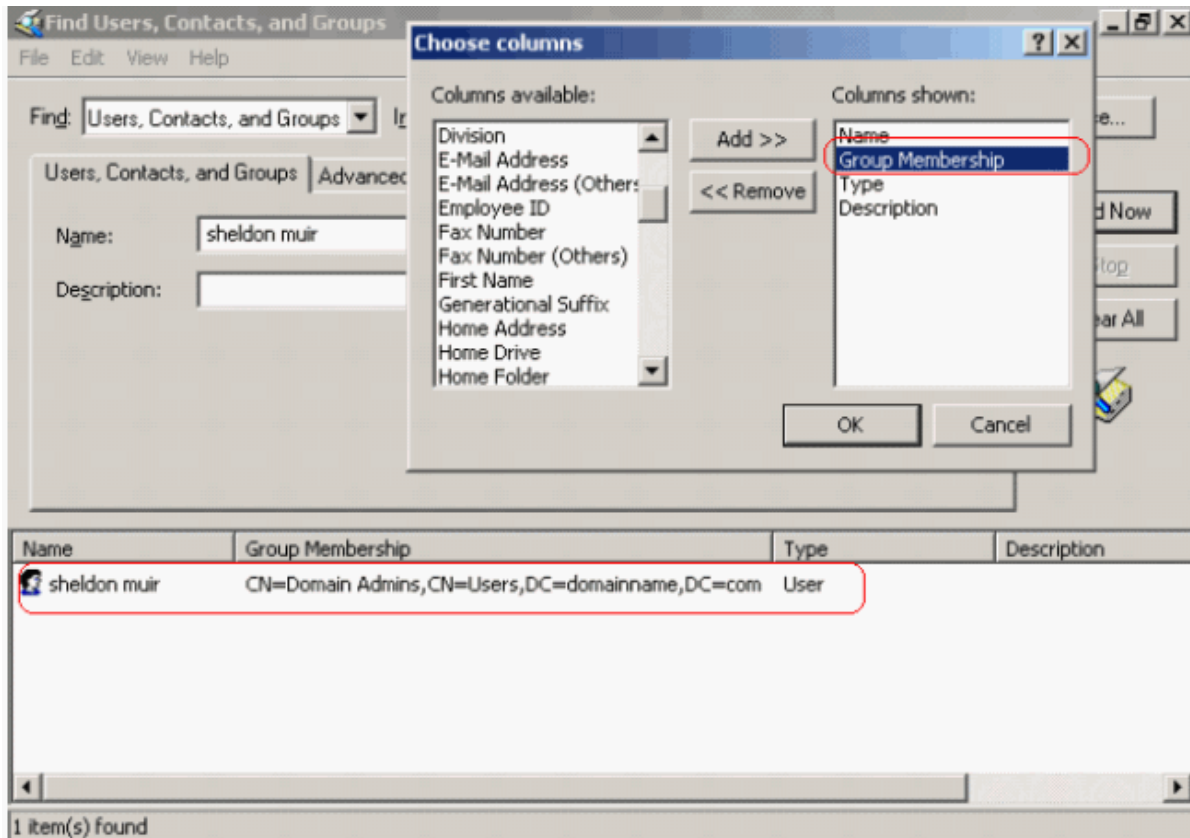
If you use LDAP to connect to the AD, the Search(Admin) Full distinguished name (DN) typically has to be set to the DN of an account with either administrative privileges or basic user privileges. The first common name (CN) entry should be an administrator of the AD, or a user with read privileges. Note that the search filter, SAMAccountName, is the user login name in the default AD schema.

## AD/LDAP Configuration Example

This illustrates a sample configuration using LDAP to communicate with the backend Active Directory:

1. Create a Domain Admin user within Active Directory Users and Computers. Place this user into the Users folder.
2. Within Active Directory Users and Computers, select **Find** from the Actions menu.

Make sure that your results show the Group Membership column for the created user. Your search results should show the **user** and the associated **Group Membership** within Active Directory. This is the information you will need to transfer into the Clean Access Manager.



3. From the Clean Access Manager web console, go to the **User Management > Auth Servers > New Server** form.
4. Choose **LDAP** as the Server Type.
5. For the **Search(Admin) Full DN** and **Search Base Context** fields, input the results from the Find within Active Directory Users and Computers.

User Management > Auth Servers

Auth Servers | Lookup Servers | Mapping Rules | Auth Test | Accounting

List · New

|                       |                           |                        |                        |
|-----------------------|---------------------------|------------------------|------------------------|
| Authentication Type   | LDAP                      | Provider Name          | Laptop-ActiveDirectory |
| Server URL            | ldap://192.168.137.10:389 | Server version         | Auto                   |
| Search(Admin) Full DN | CN=sheldon muir, CN=L     | Search(Admin) Password | NOT SET                |
| Search Base Context   | DC=domainname, DC=c       | Search Filter          | SAMAccountName=\$us    |
| Referral              | Manage (ignore)           | DerefLink              | OFF                    |
| DerefAlias            | Always                    | Security Type          | None                   |
| Default Role          | Role1                     |                        |                        |
| Description           | DEMO                      |                        |                        |

Add Server Cancel

6. These fields are all that is necessary to properly set up this auth server within the CAM:

- **ServerURL:** ldap://192.168.137.10:389 - This is the domain controller IP address and LDAP listening port.
- **Search(Admin) Full DN:** CN=sheldon muir, CN=Users, DC=domainname, DC=com
- **Search Base Context:** DC=domainname, DC=com
- **Default Role:** Select the default role a user will be put into once authenticated.
- **Description:** Used just for reference.
- **Provider Name:** This is the name of the LDAP server used for User Page setup on the CAM.
- **Search Password:** sheldon muir's domain password
- **Search Filter:** SAMAccountName=\$user\$

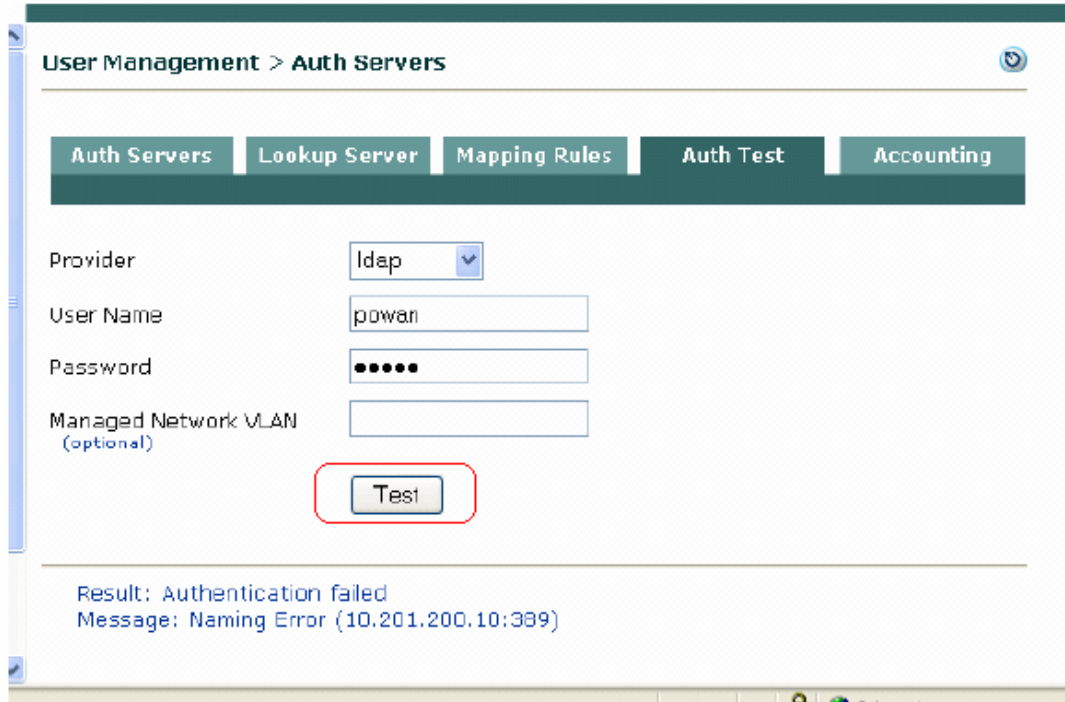
7. Click **Add Server**.

At this point, your Auth Test should work.

8. In order to test authentication:

- a. From **User Management > Auth Servers > Auth Test** tab, select the provider against which you want to test credentials in the **Provider** list. If the provider does not appear, make sure it is correctly configured in the **List of Servers** tab.
- b. Enter the username and password for the user and if needed a VLAN ID value.
- c. Click **Authenticate**.

The test results appear at the bottom of the window.



#### Authentication Successful:

For any provider type, Result: Authentication successful and Role of the user are displayed when the auth test succeeds.

For LDAP/RADIUS servers, when authentication is successful and mapping rules are configured, the attributes/values specified in the mapping rule are also displayed if the auth server (LDAP/RADIUS) returns those values. For example:

```
Result: Authentication successful
Role: <role name>
Attributes for Mapping:
<Attribute Name>=<Attribute value>
```

#### Authentication Failed:

When authentication fails, a message displays along with the Authentication failed result as shown.

| Message  | Description  |
|--|--|
| Message: Invalid User Credential   | Correct user name, incorrect password  |
| Message: Unable to find the full DN for user <User Name>                     | Correct password, incorrect user name (LDAP provider)  |
| Message: Client Receive Exception: Packet Receive Failed (Receive timed out) | Correct password, incorrect user name (RADIUS provider)  |
| Message: Invalid Admin(Search) Credential                                    | Correct user name, correct password, incorrect value configured in the Search (Admin) Full DN field of the Auth provider (e.g. incorrect CN configured for LDAP) |

|                                    |   |
|------------------------------------|---|
|                                    | Server)   |
| Message: Naming Error (x.x.x.x: x) | Correct user name, correct password, incorrect value configured in the Server URL field of the Auth provider (e.g. incorrect port or URL configured for LDAP) |

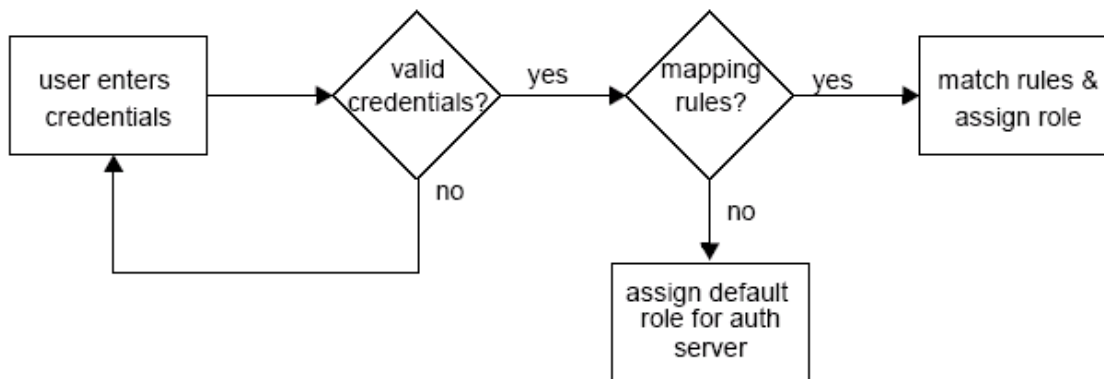
## Map Users to Roles Using Attributes or VLAN IDs

The **Mapping** Rules forms can be used to map users into user role(s) based on these parameters:

- The VLAN ID of user traffic that originates from the untrusted side of the CAS (all auth server types)
- Authentication attributes passed from LDAP and RADIUS auth servers (and RADIUS attributes passed from Cisco VPN Concentrators)

For example, if you have two sets of users on the same IP subnet but with different network access privileges, such as wireless employees and students, you can use an attribute from an LDAP server to map one set of users into a particular user role. You can then create traffic policies to allow network access to one role and deny network access to other roles.

Cisco NAC Appliance performs the mapping sequence as shown:



Cisco NAC Appliance allows the administrator to specify complex boolean expressions when defining mapping rules for Kerberos, LDAP and RADIUS authentication servers. Mapping rules are broken down into conditions and you can use boolean expressions to combine multiple user attributes and multiple VLAN IDs in order to map users into user roles. Mapping rules can be created for a range of VLAN IDs, and attribute matches can be made case-insensitive. This allows multiple conditions to be flexibly configured for a mapping rule.

A mapping rule comprises an auth provider type, a rule expression, and the user role into which to map the user. The rule expression comprises one or a combination of conditions the user parameters must match to be mapped into the specified user role. A condition is comprised of a condition type, a source attribute name, an operator, and the attribute value against which the particular attribute is matched.

In order to create a mapping rule, you first add (save) conditions to configure a rule expression. Then, once a rule expression is created, you can add the mapping rule to the auth server for the specified user role.

Mapping rules can be cascading. If a source has more than one mapping rule, the rules are evaluated in the order in which they appear in the mapping rules list. The role for the first positive mapping rule is used. Once a rule is met, other rules are not tested. If no rule is true, the default role for that authentication source is used.

## Configure Mapping Rule

Complete these steps:

1. Go to **User Management > Auth Servers > Mapping Rules** and click the **Add Mapping Rule** link for the authentication server.

The **Add Mapping Rule** form appears.

The screenshot shows the 'User Management -> Auth Servers' interface. The 'Mapping Rules' tab is active. The form includes the following fields and buttons:

- Provider Name:** LDAP-SRVR
- Role Name:** Role2
- Priority:** 1
- Description:** (empty text box)
- Rule Expression:** <Configure conditions>
- Add Mapping:** (button, circled in red with label B)
- Condition Type:** Attribute (dropdown menu)
- Operator:** equals (dropdown menu)
- Attribute Name:** (text box, currently empty)
- Attribute Value:** (text box)
- Add Condition:** (button, circled in red with label A)
- Cancel:** (button)

At the bottom, there is a table with the following columns: #, Type, Left Operand, Operator, Right Operand, Edit, Del.

2. Configure Conditions for Mapping Rule (A):

- **Provider Name**—The Provider Name sets the fields of the Mapping Rules form for that authentication server type. For example, the form only allows VLAN ID mapping rule configuration for Kerberos, Windows NT, Windows NetBIOS SSO, and S/Ident auth server types. The form allows VLAN ID or Attribute mapping rule configuration for RADIUS, LDAP, and Cisco VPN SSO auth types.
- **Condition Type**—Configure and add conditions first (step A in figure) before adding the mapping rule. Choose one of these from the dropdown menu in order to set the fields of the Condition form:
  - **Attribute**—For LDAP, RADIUS, Cisco VPN SSO auth providers only.
  - **VLAN ID**—All auth server types.

For a condition type of VLAN ID (see the figure), this field is called **Property Name**. By default, this is populated with "VLAN ID" (and disabled for editing).
- **Attribute Name**—For LDAP servers (see the figure), **Attribute Name** is a text field into which you enter the source attribute you want to test. The name must be identical (case-sensitive) to the name of the attribute passed by the authentication source, unless you choose the **equals ignore case** operator to create the condition.
- **Attribute Value**—Enter the value to be tested against the source **Attribute Name**.
- **Operator (Attribute)**—Choose the operator that defines the test of the source attribute string:
  - **equals**—True if the value of the **Attribute Name** matches the **Attribute Value**.
  - **not equals**—True if the value of the **Attribute Name** does not match the **Attribute Value**.
  - **contains**—True if the value of the **Attribute Name** contains the **Attribute Value**.
  - **starts with**—True if the value of the **Attribute Name** begins with the **Attribute Value**.
  - **ends with**—True if the value of the **Attribute Name** ends with the **Attribute Value**.

- **equals ignore case**—True if the value of the **Attribute Name** matches the **Attribute Value** string. It does not matter whether the string is uppercase or lowercase.
  - **Operator (VLAN ID)**—If you choose VLAN ID as the **Condition Type**, choose one of these operators to define a condition that tests against VLAN ID integers:
    - **equals**—True if the VLAN ID matches the VLAN ID in the **Property Value** field.
    - **not equals**—True if the VLAN ID does not match the VLAN ID in the **Property Value** field.
    - **belongs to**—True if the VLAN ID falls within the range of values configured for the **Property Value** field. The value should be one or more comma separated VLAN IDs. Ranges of VLAN IDs can be specified by hyphen (-), for example, [2,5,7,100-128,556-520]. Only integers can be entered, not strings. Note that brackets are optional.

**Example:**

| # | Type    | Left Operand | Operator   | Right Operand         | Edit | Del |
|---|---------|--------------|------------|-----------------------|------|-----|
| 1 | VLAN ID | VLAN ID      | belongs to | 2,5,7,100-128,556-520 |      | X   |

- **Add Condition (Save Condition)**—Make sure to configure the condition, then click **Add Condition** in order to add the condition to the rule expression (otherwise your configuration is not saved).
- 3. Add Mapping Rule to Role (B): Add the mapping rule (step **B** in [figure](#)) after you have configured and added the condition(s).
  - **Role Name**—After you have added at least one condition, choose the user role to which you will apply the mapping from the dropdown menu.
  - **Priority**—Select a priority from the dropdown to determine the order in which mapping rules are tested. The first rule that evaluates to true is used to assign the user a role.
  - **Rule Expression**—In order to aid in configuring conditional statements for the mapping rule, this field displays the contents of the last Condition to be added. After adding the condition(s), you must click **Add Mapping Rule** in order to save all the conditions to the rule.
  - **Description**—An optional description of the mapping rule.
  - **Add Mapping (Save Mapping)**—Click this button when done adding conditions to create the mapping rule for the role. You have to Add or Save the mapping for a specified role, or your configuration and your conditions will not be saved.

## Edit Mapping Rules

- **Priority**—In order to change the priority of a mapping rule later, click the up/down arrow next to the entry in the **User Management > Auth Servers > List of Servers**. The priority determines the order in which the rules are tested. The first rule that evaluates to true is used to assign the user to a role.
- **Edit**—Click the Edit button next to the rule to modify the mapping rule, or delete conditions from the rule. Note that when editing a compound condition, the conditions underneath (created later) are not displayed. This is to avoid loops.
- **Delete**—Click the delete button next to the Mapping Rule entry for an auth server to delete that individual mapping rule. Click the delete button next to a condition on the Edit mapping rule form to remove that condition from the Mapping Rule. Note that you cannot remove a condition that is dependent on another rule in a compound statement. In order to delete an individual condition, you have to delete the compound condition first.

## Troubleshoot

If mapping of AD user to CCA user role is not working, then make sure that you map users to a role based on attributes with Attribute Names= memberof, Operator=contains, and Attribute Value=(group name).

## Cisco Support Community - Featured Conversations

[Cisco Support Community](#) is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Below are just some of the most recent and relevant conversations happening right now.

|   |
|---|
|   |
| Want to see more? Join us by clicking <a href="#">here</a>  |
| <a href="#">Cisco NAC V4.7 LDAP Mapping users to...</a> <a href="#">yasmena_adel</a> 1 Reply 1 month, 2 weeks ago     |
| <a href="#">Roles for Users in via LDAP</a> <a href="#">leighharrison</a> 1 Reply 10 months, 4 weeks ago              |
| <a href="#">WPA2 802.1x with MS RADIUS, LDAP, Clean...</a> <a href="#">bcarneva</a> 1 Reply 2 months, 1 day ago       |
| <a href="#">NAC and Novell LDAP authentication</a> <a href="#">bhouston</a> 2 Replies 3 years, 3 days ago             |
| <a href="#">Map users into user roles on Cisco NAM</a> <a href="#">hebaelshahat</a> 2 Replies 12 months, 4 days ago   |
| <a href="#">ACS LDAP authentication - restrict to...</a> <a href="#">greg.fuller</a> 1 Reply 2 years, 1 month ago     |
| <a href="#">Need Suggestions on upgrading from CCM...</a> <a href="#">akin.utku</a> 0 Replies 10 months, 2 days ago   |
| <a href="#">RDP access for certain global ip's</a> <a href="#">sudhakar.itengineer</a> 0 Replies 5 months, 3 days ago |
| <a href="#">using LDAP group to autenticate users...</a> <a href="#">luisborges</a> 6 Replies 2 years, 6 months ago   |
| <a href="#">Cisco NAC users don't get IP address</a> <a href="#">a7med_magdy</a> 5 Replies 3 weeks, 2 days ago        |
| <a href="#">Start A New Discussion</a> <a href="#">Subscribe</a>  |

## Related Information

- [Cisco NAC Appliance Support Page](#)
- [Technical Support & Documentation - Cisco Systems](#)

