



CHAPTER 7

User Management: Configuring Auth Servers

This chapter describes how to set up external authentication sources, configure Active Directory Single Sign-On (SSO), VLAN ID or attribute-based auth server mapping rules, and RADIUS accounting. Topics are as follows:

- [Overview, page 7-1](#)
- [Adding an Authentication Provider, page 7-3](#)
- [Configuring Authentication Cache Timeout \(Optional\), page 7-13](#)
- [Authenticating Against a Backend Active Directory, page 7-14](#)
- [Map Users to Roles Using Attributes or VLAN IDs, page 7-16](#)
- [Auth Test, page 7-24](#)
- [RADIUS Accounting, page 7-26](#)

For details on AD SSO, see the “Configuring Active Directory Single Sign-On (AD SSO)” chapter in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)*.

For details on creating and configuring the web user login page, see [Chapter 5, “Configuring User Login Page and Guest Access.”](#)

For details on configuring user roles and local users, see [Chapter 6, “User Management: Configuring User Roles and Local Users.”](#)

For details on configuring traffic policies for user roles, see [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule.”](#)

Overview

By connecting the Clean Access Manager to external authentication sources, you can use existing user data to authenticate users in the untrusted network. Cisco NAC Appliance supports several authentication provider types for the following two cases:

- When you want to work with an existing backend authentication server(s)
- When you want to enable any of the transparent authentication mechanisms provided by Cisco NAC Appliance

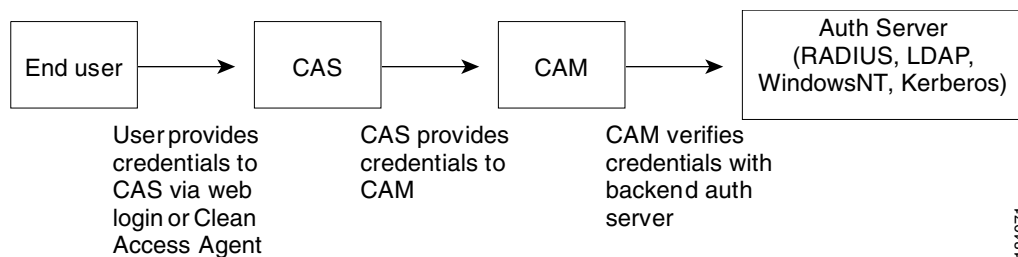
Working with Existing Backend Authentication Servers

When working with existing backend authentication servers, Cisco supports the following authentication protocol types:

- Kerberos
- RADIUS (Remote Authentication Dial-In User Service)
- Windows NT (NTLM Auth Server)
- LDAP (Lightweight Directory Access Protocol)

When using this option, the CAM is the authentication client which communicates with the backend auth server. [Figure 7-1](#) illustrates the authentication flow.

Figure 7-1 Cisco NAC Appliance Authentication Flow with Backend Auth Server



Currently, it is required to use RADIUS, LDAP, Windows NT, or Kerberos auth server types if you want to enable Cisco NAC Appliance system features such as:

- Network scanning policies
- Clean Access Agent requirements
- Attribute-based auth mapping rules



Note

For Windows NT only, the CAM must be on the same subnet as the domain controllers.

Working with Transparent Auth Mechanisms

When using this option, Cisco supports the following authentication protocol types:

- Active Directory SSO
- Cisco VPN SSO
- Windows NetBIOS SSO (formerly known as “Transparent Windows”)
- S/Ident (Secure/Identification)

Depending on the protocol chosen, the Clean Access Server sniffs traffic relevant to the authentication source flowing from the end user machine to the auth server (for example, Windows logon traffic for the Windows NetBIOS SSO auth type). The CAS then uses or attempts to use that information to authenticate the user. In this case, the user does not explicitly log into the Cisco NAC Appliance system (via web login or Clean Access Agent).



Note

S/Ident and Windows NetBIOS SSO can be used for authentication only—posture assessment, quarantining, and remediation do not currently apply to these auth types.

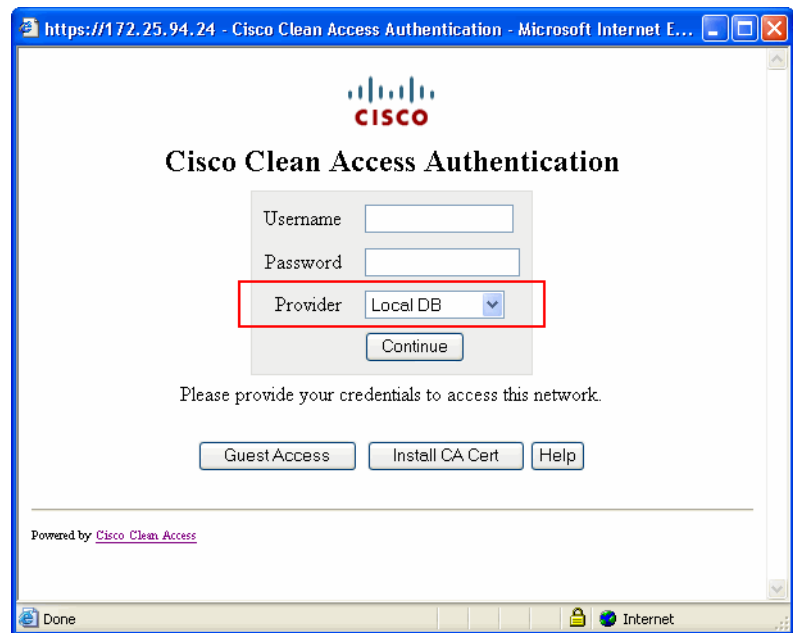
Local Authentication

You can set up any combination of local and external authentication mechanisms. Typically, external authentication sources are used for general users, while local authentication (where users are validated internally to the CAM) is used for test users, guests, or other types of users with limited network access. For details on using local authentication for guest access, see [Guest User Access](#), page 5-16.

Providers

A provider is a configured authentication source. You can configure the providers you set up to appear in the **Provider** dropdown menu of the web login page (Figure 7-2) and Clean Access Agent to allow users to choose the domain in which to be authenticated.

Figure 7-2 Provider Field in Web Login Page



Mapping Rules

You can set up role assignment for users based on the authentication server. For all auth server types, you can create mapping rules to assign users to roles based on VLAN ID. For LDAP and RADIUS auth servers, you can additionally map users into roles based on attribute values passed from the authentication server.

Adding an Authentication Provider

The following are the general steps to add an authentication server to the Clean Access Manager:

- Step 1** Go to **User Management > Auth Servers > New**.
- Step 2** From the **Authentication Type** list, choose the authentication provider type.
- Step 3** For **Provider Name**, type a name that is unique for authentication providers. If you intend to offer your users the ability to select providers from the login page, be sure to use a name that is meaningful or recognizable for your users, since this name will be used.

- Step 4** Choose the **Default Role** (user role) to be assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address. The default role is also assigned in the case that LDAP/RADIUS mapping rules do not result in a successful match.
- Step 5** Enter an optional **Description** for the authentication server.
- Step 6** Complete the fields specific to the authentication type you chose, as described in the following sections.
- Step 7** When finished, click **Add Server**.

The new authentication source appears under **User Management > Auth Servers > List of Servers**.

- Click the **Edit** button next to the auth server to modify settings.
- Click the **Mapping** button next to the auth server to configure VLAN-based mapping rules for any server type, or attribute-based mapping rules for LDAP, RADIUS, and Cisco VPN SSO auth types.

Specific parameters to add each auth server type are described in the following sections:

- [Kerberos, page 7-4](#)
- [RADIUS, page 7-5](#)
- [Windows NT, page 7-7](#)
- [LDAP, page 7-8](#)
- [Active Directory Single Sign-On \(SSO\), page 7-9](#)
- [Windows NetBIOS SSO, page 7-9](#)
- [Cisco VPN SSO, page 7-11](#)
- [Allow All, page 7-12](#)

Specific parameters to add each auth server type are described in the following sections:

- [Authenticating Against a Backend Active Directory, page 7-14](#)



Note

To set a default auth provider for users configure the **Default Provider** option under **Administration > User Pages > Login Page > Edit > Content**. See [Chapter 5, “Configuring User Login Page and Guest Access.”](#)

Kerberos

1. Go to **User Management > Auth Servers > New**.
2. From the **Authentication Type** dropdown menu, choose **Kerberos**.

Figure 7-3 Add Kerberos Auth Server

User Management > Auth Servers

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

List · New

Authentication Type: Kerberos (dropdown) Provider Name:

Domain Name: CISCO.COM Default Role: TestRole (dropdown)

Server Name: auth.cisco.com

Description:

Add Server Cancel

183844

3. **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Domain Name**—The domain name for your Kerberos realm in UPPER CASE, such as **CISCO.COM**.
5. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
6. **Server Name**—The fully qualified host name or IP address of the Kerberos authentication server, such as auth.cisco.com.
7. **Description**—Enter an optional description of this auth server for reference.
8. Click **Add Server**.

**Note**

When working with Kerberos servers, keep in mind that Kerberos is case-sensitive and that the realm name must be in UPPER CASE. The clock must also be synchronized between the CAM and DC.

RADIUS

The RADIUS authentication client in the Clean Access Manager can support failover between two RADIUS servers. This allows the CAM to attempt to authenticate against a pair of RADIUS servers, trying the primary server first and then failing over to the secondary server if it is unable to communicate with the primary server. See the **Enable Failover** and **Failover Peer IP** field descriptions below for details.

1. Go to **User Management > Auth Servers > New**.
2. From the **Authentication Type** dropdown menu, choose **Radius**.

Figure 7-4 Add RADIUS Auth Server

3. **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Server Name**—The fully qualified host name (e.g., auth.cisco.com) or IP address of the RADIUS authentication server.
5. **Server Port**—The port number on which the RADIUS server is listening.
6. **Radius Type**—The RADIUS authentication method. Supported methods include: EAPMD5, PAP, CHAP, MSCHAP, and MSCHAP2.
7. **Timeout (sec)**—The timeout value for the authentication request.
8. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if RADIUS mapping rules do not result in a successful match.
9. **Shared Secret**—The RADIUS shared secret bound to the specified client's IP address.
10. **NAS-Identifier**—The NAS-Identifier value to be sent with all RADIUS authentication packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
11. **NAS-IP-Address**—The NAS-IP-Address value to be sent with all RADIUS authentication packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to send the packets.
12. **NAS-Port**—The NAS-Port value to be sent with all RADIUS authentication packets.
13. **NAS-Port-Type**—The NAS-Port-Type value to be sent with all RADIUS authentication packets.
14. **Enable Failover**—This enables sending a second authentication packet to a RADIUS failover peer IP if the primary RADIUS authentication server's response times out.
15. **Failover Peer IP**—The IP address of the failover RADIUS authentication server.

16. **Accept RADIUS packets with empty attributes from some old RADIUS servers**—This option enables the RADIUS authentication client to allow RADIUS authentication responses that are malformed due to empty attributes, as long as the responses contain a success or failure code. This may be required for compatibility with older RADIUS servers.
17. **Description**—Enter an optional description of this auth server for reference.
18. Click **Add Server**.

RADIUS Challenge-Response Impact On the Clean Access Agent

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user Clean Access Agent login session can accommodate extra authentication challenge-response dialogs not available in other dialog sessions—beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

For details, refer to:

- [Example Windows RADIUS Challenge-Response User Login Session Dialogs, page 11-72](#)
- [Example Mac OS X RADIUS Challenge-Response User Login Session Dialogs, page 11-75](#)

Windows NT



Note

- If the CAM is not in the same subnet as the domain controllers, then the CAM DNS settings must be able to resolve the DCs.
- Currently, only NTLM v1 is supported.

1. Go to **User Management > Auth Servers > New**.
2. From the **Authentication Type** dropdown menu, choose **Windows NT**.

Figure 7-5 Add Windows NT Auth Server

The screenshot shows the 'User Management > Auth Servers' interface. The 'Auth Servers' tab is active, and the 'New' button is highlighted. The form contains the following fields:

- Authentication Type:** A dropdown menu set to 'Windows NT'.
- Provider Name:** An empty text input field.
- Domain Name:** A text input field containing 'CISCO.COM'.
- Default Role:** A dropdown menu set to 'TestRole'.
- Description:** An empty text input field.

At the bottom of the form are two buttons: 'Add Server' and 'Cancel'.

183647

3. **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Domain Name**—The host name of the Windows NT environment.
5. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
6. **Description**—Enter an optional description of this auth server for reference.
7. Click **Add Server**.

LDAP

An LDAP auth provider in the Clean Access Manager can be used to authenticate users against a Microsoft Active Directory server. See [Authenticating Against a Backend Active Directory, page 7-14](#) for details.



Note

Cisco NAC Appliance performs standard search and bind authentication. For LDAP, if Search(Admin) Full DN/Search(Admin) Password is not specified, Cisco NAC Appliance attempts anonymous bind.

1. Go to **User Management > Auth Servers > New**.
2. From the **Authentication Type** dropdown menu, choose **LDAP**.

Figure 7-6 Add LDAP Auth Server

3. **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Server URL**—Type the URL of the LDAP server, in the form:

```
ldap://<directory_server_name>:<port_number>
```

If no port number is specified, 389 is assumed.

5. **Server version**—The LDAP version. Supported types include Version 2 and Version 3. Leave as **Auto** (default) to have the server version automatically detected.
6. **Search(Admin) Full DN**—If access to the directory is controlled, the LDAP user ID used to connect to the server in this field in the form:


```
cn= jane doe, cn=users, dc=cisco, dc=com
```

The Search(Admin) user can be an LDAP administrator or a basic user. If using LDAP to connect to an AD server, the Search(Admin) Full DN (distinguished name) must be the DN of an AD user account and the first CN (common name) entry should be an AD user with read privileges.
7. **Search(Admin) Password**—The password for the LDAP user.
8. **Search Base Context**—The root of the LDAP tree in which to perform the search for users (e.g. dc=cisco, dc=com).
9. **Search Filter**—The attribute to be authenticated (e.g., uid=\$user\$, or sAMAccountName=\$user\$).
10. **Referral**—Whether referral entries are managed (in which the LDAP server returns referral entries as ordinary entries) or returned as handles (Handle(Follow)). The default is Manage(Ignore).
11. **DerefLink**—If **ON**, object aliases returned as search results are de-referenced, that is, the actual object that the alias refers to is returned as the search result, not the alias itself. The default is OFF.
12. **DerefAlias**—Options are Always (default), Never, Finding, Searching.
13. **Security Type**—Whether the connection to the LDAP server uses SSL. The default is None.



Note If the LDAP server uses SSL, be sure to import the certificate from the SSL Certificate tab of the **Administration > Clean Access Manager** page.

14. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if LDAP mapping rules do not result in a successful match.
15. **Description**—Enter an optional description of this auth server for reference.
16. Click **Add Server**.

Active Directory Single Sign-On (SSO)

See the “Configuring Active Directory Single Sign-On (AD SSO)” chapter in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)* for complete details.

Windows NetBIOS SSO



Note

The Windows NetBIOS SSO authentication feature is deprecated. Cisco recommends the “Configuring Active Directory Single Sign-On (AD SSO)” chapter in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)* instead.

In Windows NetBIOS SSO authentication (formerly known as “Transparent Windows”), the CAS sniffs relevant Windows login packets from the end-user machine to the domain controller to determine whether or not the user is logged in successfully. If Windows NetBIOS SSO authentication is enabled and the CAS successfully detects login traffic, the user is logged into the Cisco NAC Appliance system without having to explicitly login through the web login page or Clean Access Agent.

With Windows NetBIOS SSO, only authentication can be done—posture assessment, quarantining, remediation, do not apply. However, the user only needs to perform Ctrl-Alt-Dlt to login.

**Note**

For Windows NetBIOS SSO login, it is not required for the CAM to be on the same subnet as the domain controller. The list of Windows NetBIOS SSO DC is published from the CAM.

Implementing Windows NetBIOS SSO

Implementing Windows NetBIOS SSO login involves the following steps:

1. Add a **Windows NetBIOS SSO** auth server through **User Management > Auth Servers > New Server** (see [Add Windows NetBIOS SSO Auth Server, page 7-10](#)).
2. From **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > NetBIOS SSO**:
 - a. Click the option for **Enable Transparent Windows Single Sign-On with NetBIOS** on the specific CAS and click **Update**.
 - b. Enter each **Windows Domain Controller IP** and click **Add Server**.

See section “Enable Windows NetBIOS SSO” of the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(2\)](#) for details.

3. Add IP traffic control policies for the Unauthenticated role to allow users on the untrusted side access to the domain controllers on the trusted network. Typical policies may include allowing TCP, and UDP traffic for each controller (IP address and 255.255.255.255 mask) for ports 88(Kerberos), 135 (DCE endpoint resolution), 139 (netbios-ssn), 389 (LDAP), 445(smb-tcp). See [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule.”](#)

**Note**

Because the CAS attempts to authenticate the user by sniffing Windows logon packets on the network, if the end device does not send such traffic (i.e. authenticates from cache) the CAS cannot authenticate the user. In order to cause such login traffic to be generated, you can use a login script to establish network shares/shared printers. You can also login as a different user from the same machine to cause the machine to communicate to the domain controller (typically a different user’s credentials will not be cached).

Add Windows NetBIOS SSO Auth Server

1. Go to **User Management > Auth Servers > New Server**.
2. From the **Authentication Type** dropdown menu, choose **Windows NetBIOS SSO**.

Figure 7-7 Add Windows NetBIOS SSO Auth Server

User Management > Auth Servers

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

List · New

Authentication Type: Windows NetBIOS SSO Provider Name: ntlm

(Note: This feature has been deprecated. Use "Windows Kerberos SSO" if applicable.)

Default Role: TestRole

Description:

Add Server Cancel

184142

3. **Provider Name**—The **Provider Name** value defaults to **ntlm**.
4. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
5. **Description**—Enter an optional description of this auth server for reference.
6. Click **Add Server**.

Cisco VPN SSO



Note

Cisco NAC Appliance supports Single Sign-On (SSO) for the following:

- Cisco VPN Concentrators
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Aireospace Wireless LAN Controllers
- Cisco SSL VPN Client (Full Tunnel)
- Cisco VPN Client (IPSec)

Cisco NAC Appliance provides integration with Cisco VPN concentrators and can enable SSO capability for VPN users, using RADIUS Accounting information. The Clean Access Server can acquire the client's IP address from either Framed_IP_address or Calling_Station_ID RADIUS attributes for SSO purposes.

- Single Sign-On (SSO) for Cisco VPN concentrator users—VPN users do not need to login to the web browser or the Clean Access Agent because the RADIUS accounting information sent to the CAS/CAM by the VPN concentrator provides the user ID and IP address of users logging into the VPN concentrator (RADIUS Accounting Start Message).
- Single Sign-On (SSO) for Cisco Aireospace Wireless LAN Controller users—For SSO to work, the Cisco Aireospace Wireless LAN Controller must send the Calling_Station_IP attribute as the client's IP address (as opposed to the Framed_IP_address that the VPN concentrator uses).
- Accurate Session Timeout/Expiry—Due to the use of RADIUS accounting, the VPN concentrator informs the Clean Access Server exactly when the user has logged out (RADIUS Accounting Stop Message). See [OOB \(L2\) and Multihop \(L3\) Sessions](#), page 8-16 for additional details.

Add Cisco VPN SSO Auth Server

To enable SSO for Cisco VPN concentrator users, add a Cisco VPN SSO auth server:

1. Go to **User Management > Auth Servers > New**.
2. From the **Authentication Type** dropdown menu, choose **Cisco VPN SSO**.

Figure 7-8 Add Cisco VPN Auth Server

3. **Provider Name**—The **Provider Name** value defaults to **CiscoVPN**.
4. **Default Role**—Choose the user role assigned to users authenticated by the Cisco VPN concentrator. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if RADIUS mapping rules do not result in a successful match.
5. **Description**—Enter an optional description of the Cisco VPN concentrator for reference.
6. Click **Add Server**.

Make sure you have completed configuration under **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth**. For complete details on configuring the Clean Access Server for VPN concentrators, see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(2\)](#).

Allow All

The **AllowAll** option is a special authentication type that provides an alternative to the Guest Access login button feature. It allows users to type in any credential to login (e.g., an email address for user name and/or password) but does not validate the credentials. This option can be used when administrators want to capture limited information on who is logging in (such as a list of email addresses). The identifier the user submits in the login page will appear as the **User Name** in the Online Users page while the user is logged in. In this case, administrators should also modify the **Username Label** button label on the login page to reflect the type of value they want users to enter as a credential. See [Guest User Access, page 5-16](#) for additional details.



Note

The AllowAll auth type can be applied to users other than “guest.” Any normal login role (e.g. one configured for posture assessment) can be specified as the Default Role for the AllowAll auth type.

1. Go to **User Management > Auth Servers > New**.

- From the **Authentication Type** dropdown menu, choose **Allow All**.

Figure 7-9 Allow All Auth Server Type

User Management > Auth Servers

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

List · New

Authentication Type: Allow All (dropdown) | Provider Name:

Default Role: TestRole (dropdown)

Description:

Add Server | Cancel

184143

- Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
- Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
- Description**—Enter an optional description of this auth server for reference.
- Click **Add Server**.

Configuring Authentication Cache Timeout (Optional)

For performance reasons, the Clean Access Manager caches the authentication results from user authentication for 2 minutes by default. The **Authentication Cache Timeout** control on the Auth Server list page allows administrators to configure the number of seconds the authentication result will be cached in the CAM. When a user account is removed from the authentication server (LDAP, RADIUS, etc.), administrators can restrict the time window a user can login again into CCA by configuring the Authentication Cache Timeout.

- Go to **User Management > Auth Servers > Auth Servers > List**.

Figure 7-10 List Auth Servers

User Management > Auth Servers

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

List · New

Authentication Cache Timeout (seconds): 120 | Update

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			
Idap	Idap				
ntlm	netbios sso				
Cisco VPN	vpn sso				
WindowsSSO	active directory sso				

183840

2. Type the number of seconds you want user authentication results to be cached in the CAM. The default is 120 seconds; minimum is 1 second, maximum is 86400 seconds,
3. Click **Update**.

Authenticating Against a Backend Active Directory

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

If using LDAP to connect to the AD server, the Search(Admin) Full DN (distinguished name) can be the DN of an AD administrator or user account and the first CN (common name) entry should be an AD user with read privileges.



Note

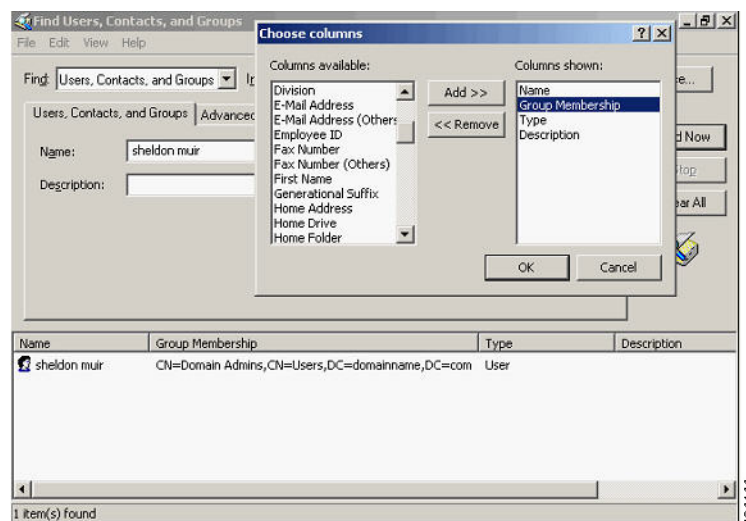
The search filter, "sAMAccountName," is the user login name in the default AD schema.

AD/LDAP Configuration Example

The following 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 information is what you will need to transfer into the Clean Access Manager.

Figure 7-11 Find Group Membership within Active Directory



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.

Figure 7-12 Example New LDAP Server for AD

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. The following fields are all that is necessary to properly set up this auth server within the CAM:
 - a. **ServerURL:** ldap://192.168.137.10:389 – This is the domain controller IP address and LDAP listening port.
 - b. **Search(Admin) Full DN:** CN=sheldon muir, CN=Users, DC=domainname, DC=com
 - c. **Search Base Context:** DC=domainname, DC=com
 - d. **Default Role:** Select the default role a user will be put into once authenticated.
 - e. **Description:** Used just for reference.
 - f. **Provider Name:** This is the name of the LDAP server used for User Page setup on the CAM.
 - g. **Search Password:** sheldon muir’s domain password
 - h. **Search Filter:** SAMAccountName=\$user\$
7. Click **Add Server**.
8. At this point, an authentication test using the **Auth Test** feature should work (see [Auth Test](#), page 7-24).



Note

You can also use an LDAP browser (e.g. <http://www.tucows.com/preview/242937>) to validate your search credentials first.

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 the following parameters:

- The VLAN ID of user traffic originating 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)



Note

You cannot reliably use the “memberOf” attribute to determine the user’s Primary Group in an LDAP Active Directory group membership query. You must use a workaround method to be able to map the user’s Primary Group VLAN ID, based on Active Directory group membership.

For more information, see the following Microsoft Knowledge Base articles:

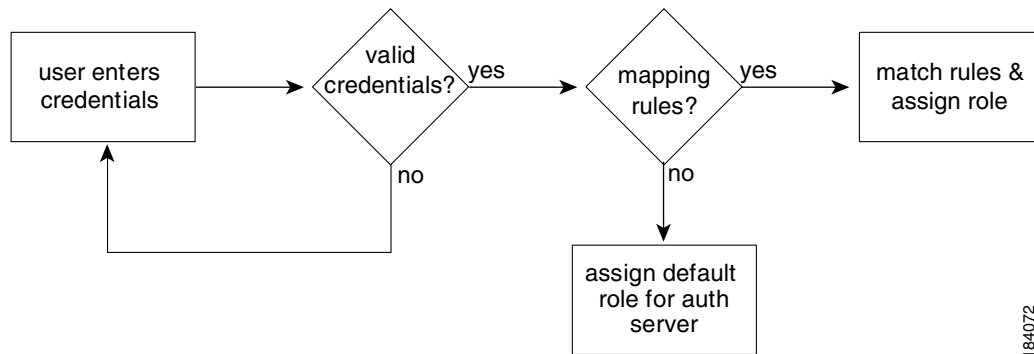
<http://support.microsoft.com/kb/275523>

<http://support.microsoft.com/kb/321360>

For example, if you have two sets of users on the same IP subnet but with different network access privileges (e.g. 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. (See [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule”](#) for details on traffic policies.)

Cisco NAC Appliance performs the mapping sequence as shown in [Figure 7-13](#).

Figure 7-13 Mapping Rules



184072



Note

For an overview of how mapping rules fit into the scheme of user roles, see [Figure 6-1 Normal Login User Roles, page 6-2](#).

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 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.

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

- Do one of the following:
 - Go to **User Management > Auth Servers > Mapping Rules** and click the **Add Mapping Rule** link for the authentication server,
 - Click the **Mapping** button for the auth server under **User Management > Auth Servers > List of Servers** (Figure 7-14), then click the **Add Mapping Rule** link for the auth server (Figure 7-15).

Figure 7-14 List of Auth Servers

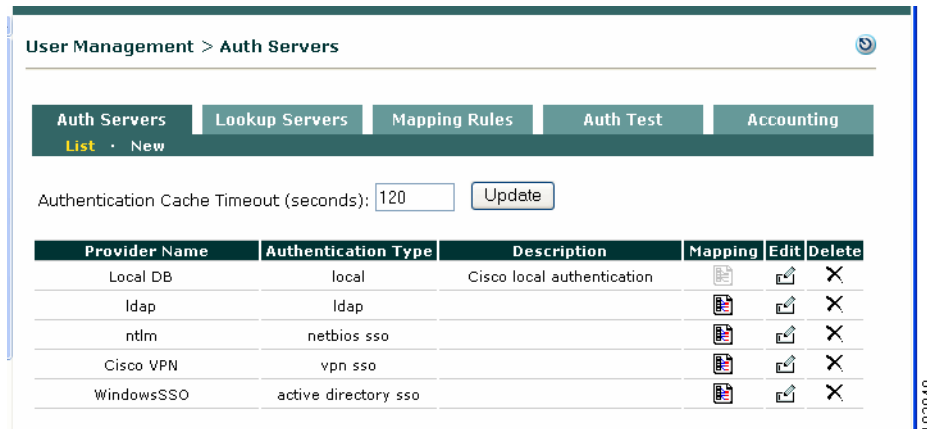
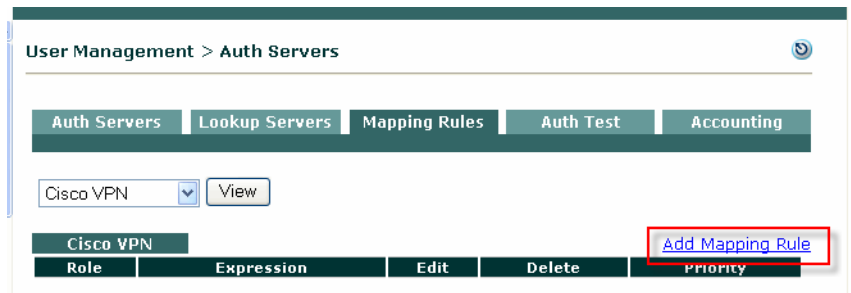


Figure 7-15 Mapping for Cisco VPN Auth Type



- The **Add Mapping Rule** form appears.

Figure 7-16 Example Add Mapping Rule (Cisco VPN)

User Management -> Auth Servers

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

Provider Name: Cisco VPN Priority: 1

Role Name: Employee Description: Employee

Rule Expression: <Configure conditions>

B Add Mapping

Condition Type: Attribute Operator: equals ignore case

Vendor: Standard Attribute Value: employee

Attribute Name: Class Add Condition Cancel

A

#	Type	Left Operand	Operator	Right Operand	Edit	Del
---	------	--------------	----------	---------------	------	-----

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 7-16) before adding the mapping rule. Choose one of the following from the dropdown menu to set the fields of the Condition form:
 - **Attribute**—For LDAP, RADIUS, Cisco VPN SSO auth providers only.
 - **VLAN ID**—All auth server types.
 - **Compound**—This condition type only appears after you have at least one condition statement already added to the mapping rule (see Figure 7-20 on page 7-22). It allows you to combine individual conditions using boolean operators. You can combine VLAN ID conditions with operators: equals, not equals, belongs to. You can combine Attribute conditions alone, or mixed VLAN ID and Attribute conditions with operators: AND, OR, or NOT. For compound conditions, instead of associating attribute types to attribute values, you choose two existing conditions to associate together, which become Left and Right Operands for the compound statement.
- 3. **Attribute Name**—Depending on the context, this field appears as follows:
 - For a **VLAN ID** condition type (Figure 7-17), this field is called **Property Name** and is populated by default with “VLAN ID” (and disabled for editing).
 - For LDAP servers (Figure 7-18), **Attribute Name** is a text field into which you type 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.



Note You cannot reliably use the “memberOf” attribute to determine the user’s Primary Group in an LDAP Active Directory Group membership query. Therefore, you must use a workaround method to be able to map the user’s Primary Group VLAN ID, based on Active Directory group membership.

For more information, see the following Microsoft Knowledge Base articles:

<http://support.microsoft.com/kb/275523>

<http://support.microsoft.com/kb/321360>

- For Cisco VPN servers, **Attribute Name** is a dropdown menu (Figure 7-21) with the following options: Class, Framed_IP_Address, NAS_IP_Address, NAS_Port, NAS_Port_Type, User_Name, Tunnel_Client_Endpoint, Service_Type, Framed_Protocol, Acct_Authentic
4. For RADIUS servers (Figure 7-19), the Condition fields are populated differently:
 - **Vendor**—Choose Standard, Cisco, Microsoft, or WISPr (Wireless Internet Service Provider roaming) from the dropdown menu.
 - **Attribute Name**—Choose from the set of attributes for each **Vendor** from the dropdown menu. For example, Standard has 253 attributes (Figure 7-22), Cisco has 30 attributes (Figure 7-23), Microsoft has 32 attributes (Figure 7-24), and WISPr has 11 attributes (Figure 7-24).



Note For RADIUS servers, only attributes returned in the “access-accept” packet are used for mapping.

- **Data Type**—(Optional) You can optionally specify Integer or String according to the value passed by the **Attribute Name**. If no data type is specified, **Default** is used.
5. **Attribute Value**—Type the value to be tested against the source **Attribute Name**.
 6. **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, regardless of whether the string is uppercase or lowercase.
 7. **Operator (VLAN ID)**—If you choose VLAN ID as the **Condition Type**, choose one of the following 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.



Note For the Cisco VPN SSO type, VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.

8. **Add Condition (Save Condition)**—Make sure to configure the condition, then click **Add Condition** to add the condition to the rule expression (otherwise your configuration is not saved).

Add Mapping Rule to Role (B)

Add the mapping rule (step **B** in [Figure 7-16](#)) after you have configured and added the condition(s).

9. **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.
10. **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.
11. **Rule Expression**—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** to save all the conditions to the rule.
12. **Description**—An optional description of the mapping rule.
13. **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.

Figure 7-17 Example Add VLAN ID Mapping Rule

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

Figure 7-18 Example Add LDAP Mapping Rule (Attribute)

User Management -> Auth Servers

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

Provider Name: LDAP-SRVR | Priority: 1

Role Name: Role2 | Description:

Rule Expression: <Configure conditions>

Add Mapping

Condition Type: Attribute | Operator: equals

Attribute Name: Attribute | Attribute Value:

Add Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del

183633

Figure 7-19 Example Add RADIUS Mapping Rule (Attribute)

User Management -> Auth Servers

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

Provider Name: Radius | Priority: 1

Role Name: Role3 | Description:

Rule Expression: <Configure conditions>

Add Mapping

Condition Type: Attribute | Operator: equals

Vendor: Standard | Attribute Name: Acct_Authentic | Data Type: Default | Attribute Value:

Add Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del

183635

Figure 7-20 Example Compound Condition Mapping Rules

User Management -> Auth Servers

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

Provider Name: Cisco VPN | Priority: 1

Role Name: CiscoVPNclients | Description: Map users to CiscoVPNclients rol

Rule Expression: (((0,6 equals Login) AND (0,45 equals RADIUS)) AND (VLAN ID belongs to 100-128))

Add Mapping

Condition Type: Compound | Operator: AND

Left Operand: Condition # 3 | Right Operand: Condition # 4

Add Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,6	equals	Login		
2	Attribute	0,45	equals	RADIUS		
3	Compound	#1	AND	#2		
4	VLAN ID	VLAN ID	belongs to	100-128		
5	Compound	#3	AND	#4		

Editing Mapping Rules

Priority—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 below it (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. To delete an individual condition, you have to delete the compound condition first.

Figure 7-21 CiscoVPN—Standard Attribute Names

Condition Type: Attribute

Vendor: Standard

Attribute Name: Class

#	Type
Class	
Framed_IP_Address	
NAS_IP_Address	
NAS_Port	
NAS_Port_Type	
User_Name	
Tunnel_Client_Endpoint	
Service_Type	
Framed_Protocol	
Acct_Authentic	

Figure 7-22 RADIUS—Standard Attribute Names

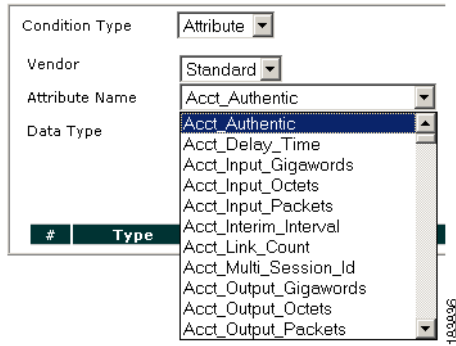


Figure 7-23 RADIUS—Cisco Attribute Names

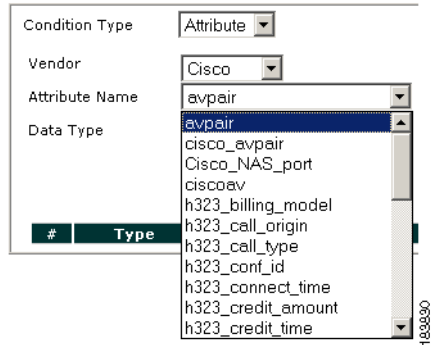


Figure 7-24 RADIUS—Microsoft Attribute Names

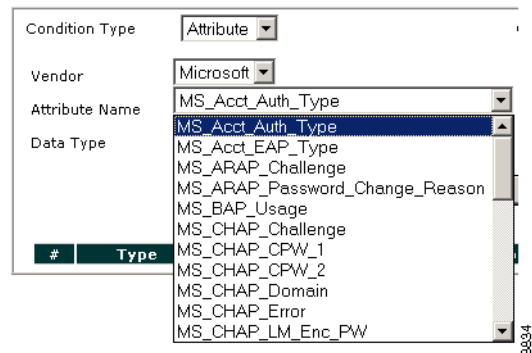


Figure 7-25 RADIUS—WISPr (Wireless Internet Service Provider roaming) Attribute Names

Condition Type: Attribute

Vendor: WISPr

Attribute Name: Bandwidth_Max_Down

Data Type: Bandwidth_Max_Down

#	Type
	Bandwidth_Max_Down
	Bandwidth_Max_Up
	Bandwidth_Min_Down
	Bandwidth_Min_Up
	Billing_Class_Of_Service
	Location_ID
	Location_Name
	Logoff_URL
	Redirection_URL
	Session_Terminate_End_Of_Day
	Session_Terminate_Time

Auth Test

The **Auth Test** tab is intended to allow you to test Kerberos, RADIUS, Windows NT, and LDAP authentication providers you configured against actual user credentials, and will list the role assigned to the user. Error messages are provided to assist in debugging authentication sources, particularly LDAP and RADIUS servers.



Tip

When creating or making changes to an existing authentication provider, create a new Auth Server entry that points to the staging or development setup. You can then use **Auth Test** to test the setup prior to production deployment.



Note

You cannot use Auth Test to test SSO. A client machine is needed to test SSO.

To test authentication:

1. 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.
2. Type the username and password for the user and if needed a VLAN ID value.
3. Click **Authenticate**. The test results appear at the bottom of the page.

Figure 7-26 Auth Test

Authentication Successful

For any provider type, the **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. [Table 7-1](#) illustrates some example authentication test failure messages.

Table 7-1 Example “Authentication Failed” Results

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)

**Note**

The **Auth Test** feature does not apply to S/Ident, Windows NetBIOS SSO, and Cisco VPN SSO authentication provider types.

RADIUS Accounting

The Clean Access Manager can be configured to send accounting messages to a RADIUS accounting server. The CAM sends a **Start** accounting message when a user logs into the network and sends a **Stop** accounting message when the user logs out of the system (or is logged out or timed out). This allows for the accounting of user time and other attributes on the network.

You can also customize the data to be sent in accounting packets for login events, logout events, or shared events (login and logout events).

Enable RADIUS Accounting

1. Go to **User Management > Auth Servers > Accounting > Server Config**.

Figure 7-27 RADIUS Accounting Server Config Page

User Management > Auth Servers

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

Server Config | Login Event | Logout Event | Shared Events

Enable RADIUS Accounting

Server Name * Server Port *

Timeout (sec) * Shared Secret *

NAS-Identifier NAS-IP-Address

(Either a NAS-Identifier or NAS-IP-Address must be specified)

NAS-Port NAS-Port-Type ▼

Enable Failover Failover Peer IP

(* Asterisks indicate required fields.)

2. Select **Enable RADIUS Accounting** to enable the Clean Access Manager to send accounting information to the named RADIUS accounting server.
3. Enter values for the following form fields:
 - **Server Name**—The fully qualified host name (e.g. auth.cisco.com) or IP address of the RADIUS accounting server.
 - **Server Port**—The port number on which the RADIUS server is listening. The Server Name and Server Port are used to direct accounting traffic to the accounting server.
 - **Timeout(sec)**—Specifies how long to attempt to retransmit a failed packet.
 - **Shared Secret**—The shared secret used to authenticate the Clean Access Manager accounting client with the specified RADIUS accounting server.

- **NAS-Identifier**—The NAS-Identifier value to be sent with all RADIUS accounting packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
 - **NAS-IP-Address**—The NAS-IP-Address value to be sent with all RADIUS accounting packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to send the packets.
 - **NAS-Port**—The NAS-Port value to be sent with all RADIUS accounting packets.
 - **NAS-Port-Type**—The NAS-Port-Type value to be sent with all RADIUS accounting packets.
 - **Enable Failover**—This enables sending a second accounting packet to a RADIUS failover peer IP if the primary RADIUS accounting server's response times out.
 - **Failover Peer IP**—The IP address of the failover RADIUS accounting server.
4. Click **Update** to update the server configuration.

Restore Factory Default Settings

The Clean Access Manager can be restored to the factory default accounting configuration as follows:

1. Go to **Administration > Backup** to backup your database before restoring default settings.
2. Go to **User Management > Auth Servers > Accounting > Server Config**
3. Click the **Reset Events to Factory Default** button to remove the user configuration and replace it with the Clean Access Manager default accounting configuration.
4. Click OK in the confirmation dialog that appears.

Add Data to Login, Logout or Shared Events

For greater control over the data that is sent in accounting packets, you can add or customize the RADIUS accounting data that is sent for login events, logout events, or shared events (data sent for both login and logout events).

Data Fields

The following data fields apply to all events (login, logout, shared):

- **Current Time (Unix Seconds)**—The time the event occurred
- **Login Time (Unix Seconds)**—The time the user logged on.
- **CA Manager IP**—IP address of the Clean Access Manager
- **Current Time (DTF)**—Current time in date time format (DTF)
- **OS Name**—Operating system of the user
- **Vlan ID**—VLAN ID with which the user session was created.
- **User Role Description**—Description of the user role of the user
- **User Role Name**—Name of the user role of the user
- **User Role ID**—Role ID that uniquely identifies the user role.
- **CA Server IP**— IP of the Clean Access Server the user logged into.
- **CA Server Description**—Description of the Clean Access Server the user logged into.
- **CA Server Key**—Key of the Clean Access Server.
- **Provider Name**—Authentication provider of the user

- Login Time (DTF)—Login time of the user in date time format (DTF)
- User MAC—MAC address of the user
- User IP—IP address of the user
- User Key—Key with which the user logged in.



Note For out-of-band users only, user_key= IP address.

- User Name—User account name.

Logout Event Data Fields

The following four data fields apply to logout events only and are not sent for login or shared events:

- Logout Time (Unix Seconds)—Logout time of the user in Unix seconds.
- Logout Time (DTF)—Logout time of the user in date time format.
- Session Duration (Seconds)—Duration of the session in seconds.
- Termination Reason—Output of the Acct_Terminate_Cause RADIUS attribute.

Add New Entry (Login Event, Logout Event, Shared Event)

To add new data to a RADIUS attribute for a shared event:

The following steps describe how to configure a RADIUS attribute with customized data. The steps below describe a shared event. The same process applies for login and logout events.

1. Go to **User Management > Auth Servers > Accounting**.
2. Click the **Shared Event** (or **Login Event, Logout Event**) link to bring up the appropriate page.
3. Click the **New Entry** link at the right-hand side of the page to bring up the add form.

Figure 7-28 New Shared Event

User Management > Auth Servers

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

Server Config · Login Event · Logout Event · **Shared Events**

Data sent when User Logs in or Logs out

Send RADIUS Attribute:

RADIUS Attribute type: Integer

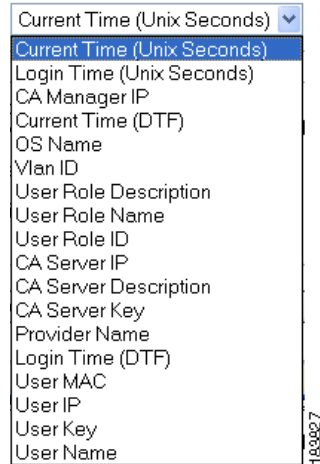
Data to send thus far: ""

Sample of data to be sent: ""

Selecting dynamic data from the drop-down list and clicking "Add Data" will cause that data to be sent with the associated RADIUS Attribute.

Static data can be entered via "Add Text"

Dynamic and static data can be combined to create human-readable strings by adding data and text. Each added entry will be appended on to the end of the last.

Figure 7-29 RADIUS Attribute Dropdown Menu

4. From the **Send RADIUS Attribute** dropdown menu, choose a RADIUS attribute.
5. Click the **Change Attribute** button to update the **RADIUS Attribute type**. The type, such as “String” or “Integer,” will display in this field.
6. Configure the type of data to send with the attribute. There are three options:
 - Send static data—In this case, type the text to be added in the **Add Text** text box and click the **Add Text** button. Every time a user logs in/logs out, the RADIUS attribute selected will be sent with the static data entered.
 - Send dynamic data—In this case, select one of the 18 dynamic data variables (or 22 for logout events) from the dropdown menu and click the **Add Data** button. Every time a user logs in/logs out, the dynamic data selected will be replaced with the appropriate value when sent.
 - Send static and dynamic data—In this case, a combination of static and dynamic data is sent. For example:

User: [User Name] logged in at: [Login Time DTF] from CA Server [CA Server Description]

See also [Figure 7-30](#), [Figure 7-31](#), and [Figure 7-32](#) show examples of Login, Logout, and Shared events, respectively, for additional details.

7. As data is added, the **Data to send thus far:** field displays all the data types selected to be sent with the attribute, and the **Sample of data to be sent:** field illustrates how the data will appear.
8. Click **Commit Changes** to save your changes.
9. Click the **Reset Element** button to reset the form.
10. Click **Undo Last Addition** to remove the last entry added to the **Data to send thus far:** field.

[Figure 7-30](#), [Figure 7-31](#), and [Figure 7-32](#) show examples of Login, Logout, and Shared events, respectively.

Figure 7-30 Login Events

User Management > Auth Servers

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

Server Config | Login Event | Logout Event | Shared Events

Data sent when User Logs in only [New Entry...](#)

Attribute Name	Data	Sample	Edit	Delete
Acct_Status_Type	1	1		

Figure 7-31 Logout Events

User Management > Auth Servers

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

Server Config | Login Event | Logout Event | Shared Events

Data sent when User Logs out only [New Entry...](#)

Attribute Name	Data	Sample	Edit	Delete
Acct_Status_Type	2	2		
Service_Type	1	1		
Acct_Terminate_Cause	[Termination Reason]	4		
Acct_Session_Time	[Session Duration (Seconds)]	4546		

Figure 7-32 Shared Events

User Management > Auth Servers

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

Server Config | Login Event | Logout Event | Shared Events

Data sent when User Logs in or Logs out [New Entry...](#)

Attribute Name	Data	Sample	Edit	Delete
User_Name	[User Key][User MAC]	192.168.151.200_X5OQRDGDGTANKNVW3_0A:0B:DB:1F:05:E1		
Login_IP_Host	[CA Server IP]	192.168.151.1		
Framed_IP_Address	[User IP]	192.168.151.200		
Event_Timestamp	[Current Time (Unix Seconds)]	1107558172		