User Management: Configuring Authentication 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 7-4
- Configuring Authentication Cache Timeout (Optional), page 7-28
- Authenticating Against a Backend Active Directory, page 7-28
- Map Users to Roles Using Attributes or VLAN IDs, page 7-31
- Auth Test, page 7-39
- RADIUS Accounting, page 7-41

For details on AD SSO, see the “Configuring Active Directory Single Sign-On (AD SSO)” chapter in the Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x).

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 and administrator 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.

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
- Agent requirements
- Attribute-based auth mapping rules

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 Agent).

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 for both users and Cisco NAC Appliance administrators. 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 5-17.

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 Agent to allow users to choose the domain in which to be authenticated.

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.

FIPS 140-2 Compliance

For LDAP over GSSAPI and Kerberos functions with FIPS-compliant CAMs/CASs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

You can configure a FIPS 140-2 compliant external RADIUS Authentication Provider type by setting up a secure IPSec tunnel between your Cisco NAC Appliance system and Cisco ACS 4.x in a Windows environment running Windows Server 2003 or 2008.
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.

- Click the Edit icon next to the auth server to modify settings.
- Click the Mapping icon 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 7-5
- RADIUS, page 7-6
- Windows NT, page 7-15
- LDAP, page 7-16
- Active Directory Single Sign-On (SSO), page 7-22
- Windows NetBIOS SSO, page 7-22
- Cisco VPN SSO, page 7-24
- Allow All, page 7-26
- Guest, page 7-26

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

- Authenticating Against a Backend Active Directory, page 7-28

---

*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

Note
In Cisco NAC Appliance, you can configure one Kerberos auth provider and one LDAP auth provider using the GSSAPI authentication method, but only one of the two can be active at any time. See LDAP, page 7-16 for more information.

Note
For Kerberos functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

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

Step 2
From the Authentication Type dropdown menu, choose Kerberos.

Figure 7-3 Add Kerberos Auth Server

Step 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.

Step 4
Domain Name—The domain name for your Kerberos realm in UPPER CASE, such as CISCO.COM.

Step 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.

Step 6
Server Name—The fully qualified host name or IP address of the Kerberos authentication server, such as auth.cisco.com.

Step 7
Description—Enter an optional description of this auth server for reference.

Step 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.
Chapter 7  User Management: Configuring Authentication Servers

Adding an Authentication Provider

While running Windows 2008 AD Server at 2003 Server functional level, if you face issues, try the following:

Run KTPass to allow multiple algorithms for new service account.

```
 ktpass -princ newadsso[@adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

**Note** Before performing the following step, Cisco strongly recommends making a backup copy of the CAM’s `/perfigo/control/tomcat/conf/krb.txt` file.

After running the `ktpass` command above, manually modify two files on the CAM as follows:

- In the CAM CLI, navigate to `/perfigo/control/tomcat/conf/krb.txt` and add the following lines:

```ini
[libdefaults]
kdc_timeout = 20000
default_tkt_enctypes = RC4-HMAC
default_tgs_enctypes = RC4-HMAC
permitted_enctypes = RC4-HMAC
```

- Navigate to `/perfigo/control/bin/starttomcat`.

Search for `CATALINA_OPTS`.

Add `-DKRB_OVERRIDE=true` to the value of `CATALINA_OPTS`.

For example:

```
Old value: CATALINA_OPTS="-server ...
New Value: CATALINA_OPTS="-server ... -DKRB_OVERRIDE=true"
```

**Note** If you are applying this change to an existing HA pair, you must perform the above update on both the HA-Primary and HA-Secondary CAM just as you would upgrade a pair of HA-enabled CAMs. For more information, see the corresponding Release Notes for Cisco NAC Appliance.

Restart the CAM by entering the `service perfigo stop` and `service perfigo start` commands. See also Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x) for complete details.

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.

**Note** To configure an IPSec tunnel required to connect Cisco NAC Appliance with an external RADIUS server, refer to Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server, page 7-8. This configuration procedure specifies what you need to set up to connect the CAM with an ACS server to perform RADIUS authentication in a FIPS 140-2 compliant network deployment.

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

**Figure 7-4    Add RADIUS Auth Server**

**Step 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.

**Step 4**  **Server Name**—The fully qualified host name (e.g., auth.cisco.com) or IP address of the RADIUS authentication server.

**Step 5**  **Server Port**—The port number on which the RADIUS server is listening.

**Step 6**  **Radius Type**—The RADIUS authentication method. Supported methods include: EAPMD5, PAP, CHAP, MSCHAP, and MSCHAP2.

**Step 7**  **Timeout (sec)**—The timeout value for the authentication request.

**Step 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.

**Step 9**  **Shared Secret**—The RADIUS shared secret bound to the specified client’s IP address.

**Step 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.

**Step 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.
Adding an Authentication Provider

**Note** If your CAM is deployed as a member of an HA failover pair, be sure you specify the service IP address for the HA pair to ensure the RADIUS authentication server receives the proper RADIUS accounting packets from the CAM. Regardless of whether the HA-Primary or HA-Standby CAM sends the accounting packets it will show up in the accounting packets as the pair. You must also configure the RADIUS authentication server to accept authentication packets from both the HA-Primary and HA-Secondary CAM eth0 IP addresses to ensure that the RADIUS server accepts the packets regardless of which CAM in the HA pair sends them. This is done in Cisco Secure ACS under AAA Clients.

**Step 12** NAS-Port—The NAS-Port value to be sent with all RADIUS authentication packets.

**Step 13** NAS-Port-Type—The NAS-Port-Type value to be sent with all RADIUS authentication packets.

**Step 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.

**Step 15** Failover Peer IP—The IP address of the failover RADIUS authentication server.

**Step 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.

**Step 17** For a FIPS 140-2 compliant deployment, activate the Enable IPsec checkbox to ensure you can establish a secure IPsec tunnel for authentication traffic. See also, Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server, page 7-8.

**Step 18** Description—Enter an optional description of this auth server for reference.

**Step 19** Click Add Server.

**Note** If you have configured a RADIUS server, the RADIUS Session Timeout for user login is automatically enabled. The timeout duration therefore occurs on a per user basis, depending on the user profile configured on the RADIUS server. See Session Timer, page 8-15 for more details on timers.

Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server

You can configure a FIPS 140-2 compliant external RADIUS Auth Provider type by setting up IPSec communication between your Cisco NAC Appliance system and Cisco ACS 4.x in a Windows environment running Windows Server 2003 or 2008. There are two primary stages to this task:

- Import Certificates in Windows
- Set Up the IPsec Tunnel

**Import Certificates in Windows**

**Step 1** In Windows, choose Start > Run and enter mmc to open the certificates console window.

**Step 2** Select File > Add/Remove Snap-in and click Add.

**Step 3** Click Certificates.
Step 4  Under Console Root, click **Certificates (Local Computer)**. A list of PKI objects appears at the right pane.

Step 5  Go to Action > All Tasks > Import and click Next.

Step 6  Click **Browse**, select the server certificate, and click Next.

Step 7  Select **Place all certificates in the following store**.

Step 8  Click **Browse**, specify the appropriate certificate, and click Next.

Step 9  Click Next.

Step 10  Click Finish.

Step 11  After installing the certificate in Windows, verify the certificate by double-clicking on the certificate. The General tab should display “You have a private key that corresponds to this certificate.” If not, you can use the following OpenSSL command to convert separate key/certificate files into a single .p12 format:

```
openssl pkcs12 -export -in cert.pem -inkey key.pem -out ACSCert.p12
```

Step 12  Enter any password when prompted.

You will also need to use this password when you import the ACS certificate on in Windows.

Step 13  Ensure that the CA from the CAM and ACS are the same (or that the CAM trusts the ACS CA and vice-versa).

Step 14  Go to Action > All Tasks > Import and click Next.

Step 15  Click **Browse**, select the root CA certificate, and click Next.

Step 16  Select **Place all certificates in the following store**.

Step 17  Click **Browse**, select the “Trusted Root Certification Authorities” folder, and click Next.

Step 18  Click Next.

Step 19  Click Finish.

---

**Set Up the IPSec Tunnel**

**Note** Before going through the following procedure, ensure you have disabled the “Use Add Wizard” option for ACS.

---

Step 1  Go to Start > Programs > Administrative Tools > Local Security Policy.

Step 2  Click IP Security Policies on Local Computer from the left navigation menu.

Step 3  Go to Action > Create IP Security Policy (Figure 7-5).
Step 4  On the wizard, click **Next**.
Step 5  Enter a name for the policy (for example, “IPSec rules for CAM-ACS”) and click **Next**.
Step 6  Uncheck (disable) the **Activate the default responses rule** option and click **Next**.
Step 7  Leave the **Edit properties** box checked (enabled) and click **Finish**.
Step 8  In the properties dialog, click **Add**.
Step 9  Select the IP Filter List tab and click Add (Figure 7-6).

Figure 7-6  IP Filter List

Step 10 Specify a name for the IP address filter list (for example, “CAM to ACS Filter List”).

Step 11 Click Add to add filter.

Step 12 Select the Addresses tab.

Step 13 Specify A Specific IP address as the Source address and enter the CAM IP address.

Step 14 Specify A Specific IP address as the Destination address and enter the ACS server IP address.

Step 15 Check (enable) the Mirrored option and click OK.

Step 16 If you have deployed your CAMs in an HA configuration, repeat Step 12 through Step 15 for the IP-secondary CAM IP address and service IP address.

Step 17 Click OK.

Step 18 In the Filter lists, choose the radio button of the list you just created.
**Step 19** Select the **Filter Action** tab and click **Add** to add a new filter action (*Figure 7-7*).

*Figure 7-7  New Filter Action*

**Step 20** Select the **General** tab and enter a name (for example, “NAC IPSec Filter Action”).

**Step 21** Select the **Security Methods** tab.

**Step 22** Choose the **Negotiate security** option and click **Add**.

**Step 23** Specify **Integrity and encryption** as the security method and click **OK**.

**Step 24** Ensure that the following settings are defined:
- **AH Integrity** is `<None>`
- **ESP Confidentiality** is 3DES
- **ESP Integrity** is SHA1

**Step 25** Check (enable) the **Use session key perfect forward secrecy (PFS)** option and click **OK**.

**Step 26** Choose the **NAC IPsec Filter Action** option.
Step 27  Select the **Authentication Methods** tab and remove all authentications methods that are displayed (Figure 7-8).

![Authentication Methods](image)

**Figure 7-8  Authentication Methods**

Step 28  Click **Add**.
Step 29 Select Use a certificate from this certification authority (CA) (Figure 7-9).

Figure 7-9 Use a certificate from this certification authority (CA)

Step 30 Click Browse, select the entry corresponding to your root certificate authority, and click OK.

Step 31 Click OK.

Step 32 Select the Tunnel Setting tab and ensure that the This rule does not specify and IPSec tunnel option is specified. This option specifies that the system should use transport mode and not tunnel mode.

Step 33 Select the Connection Type tab and ensure that the All network connections option is enabled.

Step 34 Click OK.

Step 35 Click on the rule you created in the right pane and go to Action > Assign.

Step 36 Ping the ACS server IP address from the CAM to ensure they can see on another on the network.

Step 37 Navigate to the User Management > Auth Servers > Auth Test CAM web console page and perform an Auth Test for this RADIUS server to verify connectivity, as described in Auth Test, page 7-39.

RADIUS Challenge-Response Impact On the Agent

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user 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 RADIUS Challenge-Response Cisco NAC Agent Dialogs, page 10-22.

**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 7-10 Add Windows NT 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. **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**.
Chapter 7  User Management: Configuring Authentication Servers

Adding an Authentication Provider

LDAP

Note
This section describes the general steps to configure an LDAP authentication provider. You can also use these steps to configure SIMPLE or GSSAPI authentication for an LDAP Lookup Server, which is used for authorization when configuring AD SSO. For details on configuring AD SSO, refer to the Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x).

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 7-28 for details. You can configure the LDAP server to use one of two authentication mechanisms:

- **SIMPLE**—The CAM and LDAP server pass user ID and password information between themselves without encrypting the data. See Configure LDAP Server with Simple Authentication, page 7-17.
- **GSSAPI**—(Generic Security Services Application Programming Interface) Provides an option to encrypt user ID and password information passed between the CAM and the specified LDAP server to help ensure privacy. See Configure LDAP Server with GSSAPI Authentication, page 7-18.

Note
To ensure complete DNS capability when using GSSAPI, you must ensure that all Domain Controllers, child domains, and hosts conform to strict DNS naming conventions and that you have the ability to perform both forward- and reverse-DNS.

In Cisco NAC Appliance, you can configure one LDAP auth provider using the GSSAPI authentication method and one Kerberos auth provider, but only one of the two can be active at any time. See Kerberos, page 7-5 for more information.

For LDAP over GSSAPI functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

Note
Cisco NAC Appliance performs standard search and bind authentication. For LDAP, if Search(Admin) Username/Search(Admin) Password is not specified, Cisco NAC Appliance attempts anonymous bind.
Configure LDAP Server with Simple Authentication

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

**Step 2** From the Authentication Type dropdown menu, choose LDAP.

**Figure 7-11 Add LDAP Auth Server—SIMPLE Authentication Mechanism**

**Step 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.

**Step 4** Description—Enter an optional description of this auth server for reference.

**Step 5** 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.

**Note**

When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of all directory partitions in both single and multi domain environments.

You can add redundancy for LDAP Authentication servers by entering multiple LDAP URLs in the Server URL field separated by a space, for example:

```
ldap://ldap1.abc.com ldap://ldap2.abc.com ldap://ldap3.abc.com
```

If the first LDAP server listed does not respond within 15 seconds, the CAM then attempts to authenticate using the alternate LDAP server(s) in the list. Every LDAP authentication request is passed to the first server specified in the list by default. You can only input 128 characters in this field, thus limiting the number of redundant servers you can specify.
Adding an Authentication Provider

Step 6  **Server version**—The LDAP version. Supported types include Version 2 and Version 3. Leave as **Auto** (default) to have the server version automatically detected.

Step 7  **Search Base Context**—The root of the LDAP tree in which to perform the search for users (e.g. `dc=cisco, dc=com`).

Step 8  **Search Filter**—The attribute to be authenticated (e.g., `uid=$user$, or `sAMAccountName=$user$`).

Step 9  **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).

Step 10  **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.

Step 11  **DerefAlias**—Options are Always (default), Never, Finding, Searching.

Step 12  **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 using the *Import Certificate* option on the **Administration > CCA Manager > SSL > X509 Certificate** page.

Step 13  **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.

Step 14  Specify the **Authentication Mechanism** to be SIMPLE.

Step 15  **Search(Admin) Full DN**—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. (See Figure 7-11.)

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

Step 16  **Search(Admin) Password**—The password for the LDAP user.

Step 17  Click **Add Server**.

---

**Configure LDAP Server with GSSAPI Authentication**

- **Note**  In Cisco NAC Appliance, you can configure one LDAP auth provider using the GSSAPI authentication method and one Kerberos auth provider, but only one of the two can be active at any time. See [Kerberos](#), page 7-5 for more information.

- **Note**  For LDAP over GSSAPI functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.
**Chapter 7  User Management: Configuring Authentication Servers**

**Adding an Authentication Provider**

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

**Step 2**  From the Authentication Type dropdown menu, choose LDAP.

**Figure 7-12  Add LDAP Auth Server—GSSAPI Authentication Mechanism**

**Step 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.

**Step 4**  **Description**—Enter an optional description of this auth server for reference.

**Step 5**  **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.

**Note**

When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of all directory partitions in both single and multi domain environments.

You can add redundancy for LDAP Authentication servers by entering multiple LDAP URLs in the Server URL field separated by a space, for example:

```
ldap://ldap1.abc.com ldap://ldap2.abc.com ldap://ldap3.abc.com
```
Adding an Authentication Provider

If the first LDAP server listed does not respond within 15 seconds, the CAM then attempts to authenticate using the alternate LDAP server(s) in the list. Every LDAP authentication request is passed to the first server specified in the list by default. You can only input 128 characters in this field, thus limiting the number of redundant servers you can specify.

Step 6  **Server version**—The LDAP version. Supported types include Version 2 and Version 3. Leave as Auto (default) to have the server version automatically detected.

Step 7  **Search Base Context**—The root of the LDAP tree in which to perform the search for users (e.g. dc=cisco, dc=com).

Step 8  **Search Filter**—The attribute to be authenticated (e.g., uid=$user$, or sAMAccountName=$user$).

Step 9  **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).

Step 10  **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.

Step 11  **DerefAlias**—Options are Always (default), Never, Finding, Searching.

Step 12  **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 using the *Import Certificate* option on the Administration > CCA Manager > SSL > X509 Certificate page.

If you choose SSL, ensure that you provide the details in the Multiple Domain SSL tab as well. See Multiple Domain SSL, page 7-21.

Step 13  **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.

Step 14  Specify the **Authentication Mechanism** to be GSSAPI.

**Note**  For LDAP over GSSAPI functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

Step 15  **Search(Admin) Username**—If access to the directory is controlled, this field is automatically populated with the LDAP user ID used to connect to the server (“admin” in the example illustrated in Figure 7-12).

Step 16  **Search(Admin) Password**—The password for the LDAP user.

Step 17  **Default Realm**—The realm with which the LDAP server is most commonly associated.

Step 18  **KDC Timeout (in seconds)**—The period of time the CAM keeps trying to connect before declaring the specified KDC server unreachable.

Step 19  **KDC/Realm Mapping**—You can specify one or more mappings between LDAP server IP address/port specifications and LDAP realms.
Note: You can also specify “failover” or “redundant” mappings in the KDC/Realm Mapping field. For example, if you specify an LDAP server IP address-to-realm mapping, but use a redundant LDAP server in your network, you can also enter the backup LDAP server’s IP address immediately after the primary IP address-to-realm mapping to ensure the CAM also checks with the redundant server in case the first one is unreachable.

Step 20 Domain/Realm Mapping—You can specify one or more mappings between LDAP server domains and LDAP realms.

Step 21 Base/Realm Mapping—You can specify a different LDAP Search Base depending on which Kerberos Realm is being authenticated.

Step 22 Click Add Server.

Multiple Domain SSL

When you choose the LDAP server to use SSL, you need to provide the details in the Multiple Domain SSL tab as well.

Step 1 Go to User Management > Auth Servers > Lookup Servers > Multiple Domain SSL.

Figure 7-13 Multiple Domain SSL

Step 2 Choose the appropriate LDAP provider name from the Provider drop-down.

Step 3 Enter the other details according to the provider you have selected as follows:

a. **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.

b. **Search(Admin) Full DN**—Enter the distinguished name(DN) of an AD user account and the first CN (common name) entry should be an AD user with read privileges.

c. **Domain Name**—Enter the domain name for your LDAP server in upper case, such as CISCO.COM.
Adding an Authentication Provider

1. **Search(Admin) Password**—The password for the LDAP user.
2. **Search Base Context**—The root of the LDAP tree to perform the search for users (e.g. dc=cisco, dc=com).

**Step 4** Click Add.

**Step 5** The bottom pane displays the details of the servers you have added.

**Step 6** You can click the Edit icon to modify the details and the Delete icon to remove a server.

**Note** If a domain has child domains, you must add the server details for each child domain separately.

---

**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 Configuration Guide, Release 4.9(x)* for complete details.

---

**Windows NetBIOS SSO**


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 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 7-23**).

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.


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 7-14 Add Windows NetBIOS SSO Auth Server**

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 NAC Appliance enables administrators to deploy the CAS In-Band behind a VPN concentrator, or router, or multiple routers. Cisco NAC Appliance supports multi-hop Layer 3 In-Band deployment by allowing the CAM and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. With Layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before.

**Cisco VPN SSO**

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

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

You can configure Cisco NAC Appliance to perform VPN SSO via a Cisco ASA in a FIPS-compliant network deployment. For detailed configuration information, see the “Configure VPN SSO in a FIPS 140-2 Compliant Deployment” section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

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 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).

  **Note** A CAS deployed as a Real-IP gateway supporting VPN SSO opens the Accounting port only on the trusted (eth0) interface. For configuration information, see the “Integrating with Cisco VPN Concentrators” chapter of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

- Single Sign-On (SSO) for Cisco Airespace Wireless LAN Controller users—For SSO to work, the Cisco Airespace 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.

Figure 7-15 illustrates the login and posture assessment process for a VPN user using the Agent with Single Sign-On. Note that the initial download of the Agent must be performed via the VPN connection.
Add Cisco VPN SSO Auth Server

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

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

**Step 2**  
From the Authentication Type dropdown menu, choose Cisco VPN SSO.

**Figure 7-16 Add Cisco VPN Auth Server**

**Step 3**  
Provider Name—The Provider Name value defaults to CiscoVPN.

**Step 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.

**Step 5**  
Description—Enter an optional description of the Cisco VPN concentrator for reference.

**Step 6**  
Click Add Server.

Allow All

The **Allow All** 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 5-17 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.

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

**Step 2**
From the Authentication Type dropdown menu, choose **Allow All**.

**Figure 7-17 Allow All Auth Server Type**

**Step 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.

**Step 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.

**Step 5**
Description—Enter an optional description of this auth server for reference.

**Step 6**
Click **Add Server**.

Guest

The **Guest** option is very similar in implementation and application to the **Allow All** auth server type and it serves as a useful alternative to guest users simply logging in via the existing guest access button on the web login page. Like the **Allow All** auth server type, the **Guest** option 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, but also enables you to collect other required or optional information not available in the
Allow All function. For example, you can require users to supply a contact phone number and birth date before they are allowed to access the network as a guest user. The identifier a user submits in the login page appears in the Online Users and User Management > Local Users > Guest Users pages while the user is logged in.

Note
You can only configure one “Guest” Auth Server type in the Cisco NAC Appliance system at a time.

To configure a Guest authentication server type:

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

Step 2 From the Authentication Type dropdown menu, choose Guest.

Figure 7-18 Guest Auth Server Type

Step 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.

Step 4 Default Role—Choose the user role assigned to guest 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 value is 30 days.

Step 5 Max Token Validity (in days)—Enter the number of days a guest user account remains valid in the NAC Appliance system. The default value is 7 days.

Step 6 Remove Invalid Guest Users After (in days)—Once a guest user account has been “Invalid” for the specified number of days, the NAC Appliance system reserves the right to remove that guest user account from the NAC Appliance system database.

Tip
If your NAC Appliance system provides guest access to a very large number of different guest users on a regular basis, you might want to consider changing the Remove Invalid Guest Users After (in days) setting to a smaller number to help minimize the number of invalid/legacy user IDs in the database.

Step 7 Description—Enter an optional description of this guest authentication server for reference.

Step 8 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 Cisco NAC Appliance by configuring the Authentication Cache Timeout.

Step 1  Go to User Management > Auth Servers > Auth Servers > List.

Figure 7-19  List Auth Servers

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Authentication Type</th>
<th>Description</th>
<th>Mapping</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local DB</td>
<td>local</td>
<td>Cisco local authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap</td>
<td>ldap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntnt</td>
<td>netsrc sso</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CiscoVLAN</td>
<td>vlan sso</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WindowsSSO</td>
<td>active directory sso</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Authentication Cache Timeout (seconds): [120]  Update

Step 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.

Note  If you set this timeout value to 0, the CAM does not cache user authentication results although this method may affect performance due to increased authentication traffic for multiple users logging into Cisco NAC Appliance.

Step 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.

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.
6. The following fields are all that is necessary to properly set up this auth server within the CAM:
   a. **Description**: Used just for reference.
   b. **Server URL**: ldap://192.168.137.10:3268 – This is the domain controller IP address and default Microsoft Global Catalog port for AD.

   **Note**  
   When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments.

e. **Search(Admin) Full DN**: CN=sheldon muir, CN=Users, DC=domainname, DC=com
   d. **Search Base Context**: DC=domainname, DC=com
   e. **Default Role**: Select the default role a user will be put into once authenticated.
   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 7-39).
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)
  
  **Note** Only Layer 2 Adjacency mode is supported.

- 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 7-22.

![Figure 7-22 Mapping Rules](image)

For an overview of how mapping rules fit into the scheme of user roles, see Figure 6-1 Normal Login User Roles, page 6-3.

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**

1. 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** icon for the auth server under **User Management > Auth Servers > List** (Figure 7-23), then click the **Add Mapping Rule** link for the auth server (Figure 7-24).

**Figure 7-23 List of Auth Servers**

<table>
<thead>
<tr>
<th>User Management &gt; Auth Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Servers List - New</td>
</tr>
<tr>
<td>Lookup Servers</td>
</tr>
<tr>
<td>Mapping Rules</td>
</tr>
<tr>
<td>Auth Test</td>
</tr>
<tr>
<td>Accounting</td>
</tr>
</tbody>
</table>

Authentication Cache Timeout (seconds): 120

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Authentication Type</th>
<th>Description</th>
<th>Mapping</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local DB</td>
<td>local</td>
<td>Cisco local authentication</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap</td>
<td>ldap</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mitm</td>
<td>mitm</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco VPN</td>
<td>vlp sso</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WindowsSSO</td>
<td>active directory sso</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OL-28003-01
2. The Add Mapping Rule form appears.

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 7-25) 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 7-29 on page 7-37). 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 7-26), this field is called **Property Name** and is populated by default with “VLAN ID” (and disabled for editing).
   - For LDAP servers (Figure 7-27), **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/275523)
   - [http://support.microsoft.com/kb/321360](http://support.microsoft.com/kb/321360)

   - For Cisco VPN servers, **Attribute Name** is a dropdown menu (Figure 7-30) 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 7-28), 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 7-31), Cisco has 30 attributes (Figure 7-32), Microsoft has 32 attributes (Figure 7-33), and WISPr has 11 attributes (Figure 7-33).

   **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 7-25) 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 7-26  Example Add VLAN ID Mapping Rule

#### Map Users to Roles Using Attributes or VLAN IDs

The figure illustrates how to map users to roles using attributes or VLAN IDs. The user management context is shown with options for Action Servers, Lookup Servers, Mapping Rules, Auth Test, and Accounting.

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>AllowAllGuest</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Name</td>
<td>Guest</td>
<td>Description</td>
</tr>
<tr>
<td>Rule Expression</td>
<td>( VLAN ID belongs to 2,5,7,100-128,556-520 )</td>
<td></td>
</tr>
</tbody>
</table>

![Map VLAN ID to Roles](image)

**Figure 7-26 Example Add VLAN ID Mapping Rule**

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>VLAN ID</th>
<th>Operator</th>
<th>Property Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property Name</td>
<td>VLAN ID</td>
<td></td>
<td>2,5,7,100-128,556-520</td>
</tr>
</tbody>
</table>

**Value must be one or more comma separated VLAN IDs. Example: (2, 5, 7, 100-128, 556-520)**

<table>
<thead>
<tr>
<th>#</th>
<th>Type</th>
<th>Left Operand</th>
<th>Operator</th>
<th>Right Operand</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN ID</td>
<td>VLAN ID</td>
<td>belongs to</td>
<td>2,5,7,100-128,556-520</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 7-27  Example Add LDAP Mapping Rule (Attribute)

Example of adding an LDAP mapping rule with an attribute condition.
Map Users to Roles Using Attributes or VLAN IDs

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. 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.
Map Users to Roles Using Attributes or VLAN IDs

**Edit**—Click the Edit icon 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 icon next to the Mapping Rule entry for an auth server to delete that individual mapping rule. Click the delete icon 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 7-30  CiscoVPN—Standard Attribute Names**

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>Standard</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Auth</td>
</tr>
<tr>
<td>Data Type</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 7-31  RADIUS—Standard Attribute Names**

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>Standard</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Auth</td>
</tr>
<tr>
<td>Data Type</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 7-32  RADIUS—Cisco Attribute Names**

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>Cisco</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>avpair</td>
</tr>
<tr>
<td>Data Type</td>
<td></td>
</tr>
</tbody>
</table>
The Auth Test tab is allows you to test Kerberos, RADIUS, Windows NT, LDAP, and AD SSO authentication providers you configured against actual user credentials, and lists the role assigned to the user. Error messages are provided to assist in debugging authentication sources, particularly LDAP and RADIUS servers.

To use the Auth Test function to test AD SSO authentication in Cisco NAC Appliance, you must perform the following set-up steps, as described in the “Configuring Active Directory Single Sign-On (AD SSO)” chapter of the Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x), before testing AD SSO server authentication:


2. Create an AD SSO authentication provider and associate the AD SSO authentication provider with the LDAP Lookup Server using the LDAP Lookup Server field, as described in the “Add Active Directory SSO Auth Server” section of the Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x).

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:

**Step 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** tab.

**Step 2**  
Type the username and password (if required) for the user, and the appropriate VLAN ID value if needed.

**Step 3**  
Click **Submit**. The test results appear at the bottom of the page.

![Figure 7-35 Auth Test](image)

**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.
RADIUS Accounting

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

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

---

**Table 7-1  Example “Authentication Failed” Results**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message: Invalid User Credential</td>
<td>Correct user name, incorrect password</td>
</tr>
<tr>
<td>Message: Unable to find the full DN for user &lt;User Name&gt;</td>
<td>Correct password, incorrect user name (LDAP provider)</td>
</tr>
<tr>
<td>Message: Client Receive Exception: Packet Receive Failed (Receive timed out)</td>
<td>Correct password, incorrect user name (RADIUS provider)</td>
</tr>
<tr>
<td>Message: Invalid Admin(Search) Credential</td>
<td>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)</td>
</tr>
<tr>
<td>Message: Naming Error (x.x.x.x: x)</td>
<td>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)</td>
</tr>
</tbody>
</table>

---

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


**Step 2**  Select **Enable RADIUS Accounting** to enable the Clean Access Manager to send accounting information to the named RADIUS accounting server.

**Step 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.

**Note**  If your CAM is deployed as a member of an HA failover pair, be sure you specify the service IP address for the HA pair to ensure the RADIUS accounting server receives the proper RADIUS accounting packets from the CAM. Regardless of whether the HA-Primary or HA-Standby CAM sends the accounting packets it will show up in the accounting packets as the pair. You must also configure the RADIUS accounting server to accept accounting packets from both the HA-Primary and HA-Secondary CAM eth0 IP addresses to ensure that the RADIUS server accepts the packets regardless of which CAM in the HA pair sends them. This is done in Cisco Secure ACS under AAA Clients.

- **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.
Step 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.
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 7-39, Figure 7-40, and Figure 7-41 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 7-39, Figure 7-40, and Figure 7-41 show examples of Login, Logout, and Shared events, respectively.
Chapter 7  User Management: Configuring Authentication Servers

Figure 7-39  Login Events

Figure 7-40  Logout Events

Figure 7-41  Shared Events