Configuring Primary Authentication

This section includes the following topics:

Primary Authentication

Cisco VNMC supports two methods to authenticate user logins:

- Local to Cisco VNMC
- Remote through LDAP

The role and locale assignment for a local user can be changed on VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Remote Authentication Providers

If a system is configured for a supported remote authentication service, you must create a provider for that service to ensure that VNMC and the system configured with the service can communicate.

User Accounts in Remote Authentication Services

You can create user accounts in VNMC or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through the VNMC GUI.

User Roles and Locales in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles and locales those users require for working in VNMC and that the names of those roles and locales match the names used in VNMC. If an account does not have the required roles and locales, the user is granted only read-only privileges.

LDAP Attribute for User

In VNMC, the LDAP attribute that holds the LDAP user roles and locales is preset. This attribute is always a name-value pair. For example, by default CiscoAvPair specifies the role and locale information for the user, and if the filter is specified, the LDAP search is restricted to those values that match the defined filter. By default, the filter is sAMAccountName=$userid. The user can change these values to match the setting on the LDAP server. When a user logs in, VNMC checks for the value of the attribute when it queries the remote authentication service and validates the user. The value should be identical to the username.

An example of LDAP property settings is as follows:

- Timeout—30
- Retries—1
- Attribute—CiscoAvPair
- Filter—sAMAccountName=$userid
- Base DN—DC=cisco, DC=com (The specific location in the LDAP hierarchy where VNMC will start the query for the LDAP user.)

Creating an LDAP Provider

Before You Begin

Configure users with the attribute that holds the user role and locale information for VNMC. You can use an existing LDAP attribute that is mapped to the VNMC user roles and locales, or you can create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1. When you add the LDAP user to the LDAP server, specify the role and locale in the attribute (for example, shell:roles=network,aaa shell:locale=sanjose,dallas).

Procedure

Step 1 In the Administration tab, choose **Access Control > LDAP**.

Step 2 In the Work pane, click **Create LDAP Provider**.

Step 3 In the Create LDAP Provider dialog box, provide the following information:

Field	Description
Hostname/IP Address	Hostname or IP address of the LDAP provider. If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname instead of an IP address, you must configure a DNS server in the VNMC server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Root DN	Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 128 characters.
Port	Port through which VNMC communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL. If you enter 636 in the Port field, this option is not available.

Note Depending on the object you select in the table, different options appear above the table.

Step 4 Click **OK**, then click **Save**.

Following is an example of creating an LDAP provider:

- **Hostname/IP Address**—Provider-blr-sam-aaa-10.cisco.com
- **Key**—xxxxxx (The password of the LDAP database account specified in the **Root DN** field.)
- **Root DN**— CN=bob,DC=cisco,DC=com (The value of CN is the name of a user with query privileges. DC refers to the location in the LDAP directory where a user is created.)
- **Port**—389
- **Enable SSL**—check box

What to Do Next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, on page 5.

Editing an LDAP Provider

Procedure

Step 1 In the Administration tab, choose **Access Control > LDAP**.

Step 2 In the Work pane, select the required LDAP provider.

Step 3 Click **Edit**.

Step 4 In the Edit dialog box, modify the settings as required, using the following table as a guide:

Field	Description
Name	Hostname or IP address of the LDAP provider (read-only). If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname instead of an IP address, you must configure a DNS server in the VNMC server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Set	Whether or not the preshared key has been set and is properly configured (read-only). If the Set value is Yes, and the Key field is empty, it indicates that a key provided previously.
Root DN	Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 128 characters.
Port	Port through which VNMC communicates with the LDAP database. The default port number is 389.

Field	Description
Enable SSL	Check to enable SSL. If you enter 636 in the Port field, this option is not available.

Step 5 Click **OK**, then click **Save**.

Deleting an LDAP Provider

Procedure

Step 1 In the Administration tab, choose **Access Control > LDAP**.

Step 2 In the Work pane, select the LDAP provider that you want to delete, then click **Delete**.

Step 3 Confirm the deletion, then click **Save**.

Selecting a Primary Authentication Service

Note If the default authentication is set to LDAP, and the LDAP servers are not operating or are unreachable, the local admin user can log in at any time and make changes to the authentication, authorization, and accounting (AAA) system.

Procedure

Step 1 Choose **Administration > Access Control > Authentication**.

Step 2 In the Properties tab, specify the information as described in the following table, then click **OK**.

Field	Description
Default Authentication	Default method by which a user is authenticated during remote login: • LDAP—The user must be defined on the LDAP server specified for this VNMC instance. • Local—The user must be defined locally in this VNMC instance. • None—A password is not required when the user logs in remotely.

Field	Description
Role Policy to Remote Users	Action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information: • assign-default-role—The user is allowed to log in with a read-only user role. • no-login—The user is not allowed to log into the system, even if the user name and password are correct.