Configuring Primary Authentication

This chapter includes the following sections:

Primary Authentication

Cisco VNMC supports two methods to authenticate user logins:

- Local to Cisco VNMC
- Remote through LDAP

Remote Authentication Providers

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

User Accounts in Remote Authentication Services

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

The temporary sessions for users who log in through remote authentication services can be viewed through the Cisco 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 Cisco VNMC and that the names of those roles and locales

match the names used in Cisco 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 Cisco VNMC, the LDAP attribute that holds the LDAP user roles and locales are preset. This property 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, Cisco 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 Cisco 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 Cisco VNMC. You can use an existing LDAP attribute that is mapped to the Cisco VNMC user roles and locales or 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)

Configure the properties for the LDAP provider connections in Cisco VNMC.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, select the **LDAP** node.

Step 4 In the **Work** pane, click the **Create LDAP Provider** link.

Step 5 In the **Create LDAP Provider** dialog box, complete the following fields :

Name	Description
Hostname/IP Address field	The 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.

Name	Description
	Note If you use a hostname rather than an IP address, you must configure a DNS server in the Cisco VNMC server.
Key field	The password for the LDAP database account specified in the **Root DN** field. The maximum is 32 characters.
Root DN field	The 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 field	The port through which Cisco VNMC communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	The check box to enable SSL.

Note Depending upon the object you select in the table, different options will appear in the area above the table.

Step 6 Click **OK**.

Step 7 In the **Work** pane, 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, page 5.

Editing an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, select the **LDAP** node.

Step 4 In the **Work** pane, click on an *LDAP Provider_name*.

Step 5 Click the **Edit** link.

Step 6 In the **Edit** dialog box modify the appropriate fields with the information about the LDAP service you want to use:

Name	Description
Name field	The hostname or IP address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database. If you use a hostname rather than an IP address, you must configure a DNS server in the Cisco VNMC This field is not editable.
Key field	The password for the LDAP database account specified in the **Root DN** field.
Root DN field	The distinguished name (DN) for the LDAP database account. This account has read and search permissions for all objects under the base DN. Password length maximum is 128 characters.
Port field	The port through which Cisco VNMC communicates with the LDAP database. The standard LDAP database port number is 389.
Enable SSL check box	The check box that you check to enable Secure Socket Layer (SSL).

Step 7 Click **OK**.

Step 8 In the **Work** pane, click **Save**.

Deleting an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click **LDAP**.
Step 4 In the **Work** pane, click the *LDAP provider_name* that you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.
Step 7 In the **Work** pane, click **Save**.

Selecting a Primary Authentication Service

Note If the default authentication is set to LDAP, and the LDAP servers are not operating or unreachable, the local admin user can login any time and make changes to the AAA system.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane click the **Authentication** node.
Step 4 In the **Work** pane, click the **Properties** tab.
Step 5 On the **Properties** tab, complete the following fields:

Name	Description
Default Authentication drop-down list	The default method by which a user is authenticated during remote login. This can be one of the following methods: • **ldap**—The user must be defined on the LDAP server specified for this Cisco VNMC instance. • **local**—The user must be defined locally in this Cisco VNMC instance. • **none**—A password is not required when the user logs in remotely.

Name	Description
Role Policy to Remote Users drop-down list	The action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information. This can be one of the following actions: • **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.

Step 6 Click **Save**.