Configuring Role-Based Access Control

This chapter includes the following sections:

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco VNMC

User accounts are used to access the system. Up to 48 local user accounts can be configured in each Cisco VNMC instance. Each user account must have a unique username.

A local user can be authenticated using a password or an SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each Cisco VNMC instance has a default user account, admin, which cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached the user account is disabled.

By default, user accounts do not expire.

Guidelines for Cisco VNMC Usernames

The username is also used as the login ID for Cisco VNMC. When you assign usernames to Cisco VNMC user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - . (period)
  - _ (underscore)
  - - (dash)
  - @
- The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.
- The unique username cannot start with a number.
- If an all-numeric username exists on an AAA server (LDAP) and is entered during login, Cisco VNMC cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

Note You can create up to 48 user accounts in a Cisco VNMC instance.

Guidelines for Cisco VNMC Passwords

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. If the **Password Strength Check** is enabled, then Cisco VNMC rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Note The **Password Strength Check** is enabled by default. You can disable it from the **Locally Authenticated Users** Pane.

Note If the Cisco VNMC instance is configured to use remote authentication with LDAP, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used just for authentication, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy and tenant related privileges.

All roles include read access to all configuration settings in the Cisco VNMC instance. The difference between the read-only role and other roles is that a user who is only assigned the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

The system contains the following default user roles:

aaa

User has read and write access to users, roles, and AAA configuration. Read access to the rest of the system.

admin

User has complete read-and-write access to the entire system and has all privileges. The default admin account is assigned this role by default, and it cannot be changed.

network

User creates organizations, security policies, and device profiles.

operations

User acknowledges faults and performs some basic operations such as logging configuration.

read-only

User has read-only access to system configuration and operational status with no privileges to perform any operations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

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

- the assigned role for a user
- the assigned locale for a user
- the privilege for a role that is assigned to a user
- the organization in a locale that is assigned to a user

Privileges

User Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and its description.

Privilege Name	Description
aaa	System security and AAA
admin	System administration

Privilege Name	Description
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role
res-config	Compute firewall configuration
policy	Compute firewall policy
fault	Alarms and alarm policies
operations	Logs, core file management, and **show tech-support** command
tenant	Create, delete, and modify tenants and organization containers

Privileges and Role Assignments

The following table lists the out-of-box default role name for each privilege.

Default Role Name	Privilege Name
aaa	aaa
admin	admin
read-only	read-only
network	policy, tenant, res-config
operations	fault, operations

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) to which the user is allowed access. In addition, the user has read-only access privileges outside their assigned locale and going up the organization tree. This enables the user to use these objects when creating policies. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations. Only the objects under organizations are controlled by locales. Access to other objects such as users, roles, and resources that are not present in the organization tree are not affected by locales.

Users with AAA Administrator privileges (AAA Administrator role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

Attention AAA privileges must be carefully assigned because it allows a user to manage users' privileges and role assignments.

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

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

- the assigned role for a user
- the assigned locale for a user
- the privilege for a role that is assigned to a user
- the organization in a locale that is assigned to a user

Configuring User Roles

Creating a User Role

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 **Roles**.

Step 4 In the **Work** pane, click **Create Role**.

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

Name	Description
Name field	A user-defined name for this user role.
Privileges list	A list of privileges defined in the system. Check the check box to assign that privilege to the selected user.

Step 6 Click **OK**.

Editing a User Role

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 **Roles**.
Step 4 In the **Work** pane, select the **Name** you want to edit
Step 5 In the **Work** pane, click the **Edit** link.
Step 6 In the **Edit** dialog box, check or uncheck the boxes for the privileges you want to add to the role.
Step 7 Click **OK**.

Deleting a User Role

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 **Roles**.
Step 4 In the **Work** pane, select the **Name** you want to delete.
Step 5 In the **Work** pane, click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring User Locales

Creating a Locale

Before You Begin

One or more organizations must exist before you create a locale.

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 **Locales** node.

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

Step 5 In the **Properties** area **Name** field, enter a unique name for the locale.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 6 Click the **Assign Organizations** link in the **Assigned Organizations** area, and do the following:

a) Expand the **root** node to view the organizations in the Cisco VNMC instance.

b) Click the check box next to one or more organizations that you want to assign to the locale.

Step 7 Click **OK**.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales Assigned to a Locally Authenticated User Account, on page 13.

Editing a Locale

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 **Locales** node.

Step 4 In the **Work** pane, expand the **Locales** node.

Step 5 Click the *Locales_name* you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Properties** area **Description** field, change the description as appropriate.

Step 8 Click the **Assign Organizations** link in the **Assigned Organizations** area, and do the following:

a) Expand the **root** node to view the organizations in the Cisco VNMC instance.

b) Check the appropriate check boxes.

Step 9 Click **OK**.

Deleting a Locale

Before You Begin

Caution If the locale you want to delete is assigned to any user/s, remove the locale from the user list of locales.

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 **Locales** node.
Step 4 In the **Work** pane **Locales** pane, expand the **Locales** node.
Step 5 Click the *Locales_name* you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Assigning an Organization to a Locale

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 **Locales** node.
Step 4 In the **Work** pane, expand the **Locales** node.
Step 5 Click the *Locales_name* where you want to assign an organization.
Step 6 Click the **Assign Organization** link to open the **Assign Organization** dialog box and do the following:
a) Expand the **root** node to view the organizations in the Cisco VNMC instance.
b) Check the appropriate check boxes.
Step 7 Click **OK**.
Step 8 In the *Organization_name* pane, click **Save**.

Deleting an Organization from a Locale

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 **Locales** node.
Step 4 In the **Work** pane, expand the **Locales** node.
Step 5 Click the *Locales_name* where you want to delete an organization.
Step 6 Click the **Edit Locale** link to open the **Edit Locale** dialog box.
Step 7 In the **Assigned Organizations** area, select the organization you want to delete.
Step 8 Click the **Delete Organization** link.
Step 9 In the **Confirm** dialog box, click **Yes**.

Configuring Locally Authenticated User Accounts

Creating a User Account

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 **Locally Authenticated Users** node.
Step 4 In the **Work** pane, click and open the **Create Locally Authenticated Users** dialog box.
Step 5 In the **Properties** area, complete the following fields with the required information about the user:

Name	Description
Login ID field	The account name that is used when logging into this account. This account must be unique and meet the guidelines and restrictions for Cisco VNMC user accounts. • The login ID can contain between 1 and 32 characters, including the following: ◦ Any alphabetic character ◦ Any digit ◦ _ (underscore) ◦ - (dash) ◦ @ • The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username. • The unique username cannot start with a number. After you save the user, the name cannot be changed. You must delete the user account and create a new one. **Note** You can create up to 48 user accounts in a Cisco VNMC instance.
Description field	The user-defined description of the locally authenticated user.
First Name field	The first name of the user. This field can contain up to 32 characters.
Last Name field	The last name of the user. This field can contain up to 32 characters.
Email field	The email address of the user.
Phone field	The telephone number of the user.

Name	Description
Password field	The password associated with this account. To prevent users from choosing insecure passwords, each password must be strong. If the **Password Strength Check** checkbox is checked on the Locally Authenticated Users pane, Cisco VNMC rejects any password that does not meet the following requirements: • Must contain a minimum of 8 characters • Must contain at least three of the following: ◦ Lower case letters ◦ Upper case letters ◦ Digits ◦ Special characters • Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. • Must not be identical to the username or the reverse of the username. • Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. • Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). • Should not be blank for local user and admin accounts. **Note** The password strength checkbox on the Locally Authenticated Users pane can be checked off, so that the password is not restricted to be strong. It must, however, contain a minimum of 8 characters. The password field is not a required field and a user can be created without providing a password.
Confirm Password field	The password a second time for confirmation purposes.
Password Expires check box	If checked, this password expires and must be changed on the selected date.

Step 6 In the **Roles/Locales** tab area, complete the following fields:

Name	Description
Assigned Role(s) list	A list of the user roles defined in the system. If the associated check box is checked, the user has been assigned that user role.
Assigned Locale(s) list	A list of locales defined in the system, if any. If the associated check box is checked, the user has been assigned to that locale.

Step 7 In the **SSH** tab area, complete the following fields:

Name	Description
Type field	This can be: • **Password**—the user must enter a password when they log in • **Key**—SSH encryption is used when this user logs in
SSH Data field	If **Type** is set to **Key**, this field contains the associated SSH key.

Step 8 Click **OK**.

Changing the Locales Assigned to a Locally Authenticated User Account

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, expand the **Locally Authenticated Users** node.
Step 4 Click the *User_name* you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Click the **Roles/Locales** tab.
Step 7 In the **Assigned Locale(s)** area, do the following:

- To assign a new locale to the user account, check the appropriate check boxes.

- To remove a locale from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Changing the Roles Assigned to a Locally Authenticated User Account

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, expand the **Locally Authenticated Users** node.
Step 4 Click the *User_name* you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Click the **Roles/Locales** tab.
Step 7 In the **Assigned Role(s)** area, do the following:

- To assign a new role to the user account, check the appropriate check boxes.
- To remove a role from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Monitoring User Sessions

You can monitor a Cisco VNMC session for both locally authenticated users and remotely authenticated users.

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 and expand one of the following nodes:

- **Locally Authenticated Users**
- **Remotely Authenticated Users**

Step 4 Select a *User_name* to monitor.
Step 5 In the **Work** pane, click the **Sessions** tab to view the user session.

Name	Description
User column	The username that is involved in the session.
Host column	The IP address from which the user is logged in.
Login Time column	The date and time the session started.
UI column	The user interface used to create this user login session. This can be: • **web**—GUI login • **shell**—CLI login • **ep**—end point • **none**
Terminal Type column	The kind of terminal through which the user is logged in.