Configuring Role-Based Access Control

This chapter includes the following sections:

• Role-Based Access Control, page 1
• User Accounts for Cisco VNMC, page 1
• User Roles, page 3
• Privileges, page 4
• User Locales, page 5
• Configuring User Roles, page 5
• Configuring User Locales, page 7
• Configuring Locally Authenticated User Accounts, page 10
• Monitoring User Sessions, page 13

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 SECSSH.

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.

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.
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.

<table>
<thead>
<tr>
<th>Privilege Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>System security and AAA</td>
</tr>
<tr>
<td>Admin</td>
<td>System administration</td>
</tr>
<tr>
<td>read-only</td>
<td>Read-only access</td>
</tr>
<tr>
<td></td>
<td>Read-only cannot be selected as a privilege; it is assigned to every user role</td>
</tr>
<tr>
<td>Resource Configuration</td>
<td>Compute firewall configuration</td>
</tr>
<tr>
<td>Policy Management</td>
<td>Compute firewall policy</td>
</tr>
<tr>
<td>Fault Management</td>
<td>Alarms and alarm policies</td>
</tr>
<tr>
<td>Operations</td>
<td>Logs, core file management, and <code>show tech-support</code> command</td>
</tr>
<tr>
<td>Tenant Management</td>
<td>Create, delete, and modify tenants and organization containers</td>
</tr>
</tbody>
</table>

Privileges and Role Assignments

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

<table>
<thead>
<tr>
<th>Default Role Name</th>
<th>Privilege Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>aaa</td>
</tr>
</tbody>
</table>
### 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, and access would be limited to the organizations specified in the locale. 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.

### Configuring User Roles

### Creating a User Role

**Procedure**

1. In the Navigation pane, click the Administration tab.
2. In the Navigation pane, click the Access Control subtab.
3. In the Navigation pane click Roles.
4. In the Work pane, click Create Role.
5. In the Create Role dialog box, complete the following fields:
### Editing a User Role

**Procedure**

1. In the *Navigation* pane, click the *Administration* tab.
2. In the *Navigation* pane, click the *Access Control* subtab.
3. In the *Navigation* pane, click the *Roles* node.
4. In the *Work* pane, select the *Role_name* you want to edit.
5. Click the *Edit* link.
6. In the *Edit* dialog box, check or uncheck the boxes for the privileges you want to add to the role.
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 the Roles node.
Step 4  In the Work pane, click the user role you want to delete.
Step 5  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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Administration tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Navigation pane, click the Access Control subtab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Navigation pane, click the Locales node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Work pane click the Create Locale link.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Create Locale dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

**Table 1: Properties Area**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name for the locale. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.</td>
</tr>
<tr>
<td>Description list</td>
<td>The description of the locale. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters</td>
</tr>
</tbody>
</table>
Editing a Locale

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, page 13.

Editing a Locale

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.</td>
</tr>
</tbody>
</table>

Step 6
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.
**Assigning an Organization to a Locale**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Administration tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Navigation pane, click the Access Control subtab.</td>
</tr>
<tr>
<td>3</td>
<td>In the Navigation pane, expand Locales ➤ Locale_name where you want to assign an organization.</td>
</tr>
<tr>
<td>4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>5</td>
<td>Click the Assign Organization link.</td>
</tr>
</tbody>
</table>
| 6    | In the Assign Organization dialog box, complete the following:  
|      | a) Expand root to view the organizations.  
|      | b) Check the appropriate check boxes. |
| 7    | Click OK. |

**Deleting an Organization from a Locale**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Navigation pane, click the Administration tab.</td>
</tr>
<tr>
<td>2</td>
<td>In the Navigation pane, click the Access Control subtab.</td>
</tr>
<tr>
<td>3</td>
<td>In the Navigation pane, expand Locales.</td>
</tr>
<tr>
<td>4</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>5</td>
<td>In the Assigned Organizations area, click the organization you want to delete.</td>
</tr>
<tr>
<td>6</td>
<td>Click the Delete Organization link.</td>
</tr>
<tr>
<td>7</td>
<td>In the Confirm dialog box, click Yes.</td>
</tr>
</tbody>
</table>
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 the Create Locally Authenticated Users link.
Step 5 In the Properties area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Login ID field     | The log in name.  
This name must be unique and meet the following guidelines and restrictions for Cisco VNMC user accounts:  
• The login ID can be between 1 and 32 characters, including the following:  
  ◦ Any alphabetic character  
  ◦ Any digit  
  ◦ _ (underscore)  
  ◦ - (dash)  
  ◦ @  
  • The user name for each user account cannot be all-numeric.  
  • The user name cannot start with a number.  
  After you save the user name, it cannot be changed. You must delete the user account and create a new one. You can create up to 48 user accounts for a single Cisco VNMC instance. |
| Description field  | A description of the user. |
| First Name field   | The first name of the user.  
This field can contain up to 32 characters. |
<p>| Last Name field    | The last name of the user. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email field</strong></td>
<td>The email address of the user.</td>
</tr>
<tr>
<td><strong>Phone field</strong></td>
<td>The telephone number of the user.</td>
</tr>
<tr>
<td><strong>Password field</strong></td>
<td>The password associated with this account.</td>
</tr>
</tbody>
</table>

For maximum security, each password must be strong. If the **Password Strength Check** checkbox is checked, the system rejects any password that does not meet the following requirements:

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

**Note**  The password strength check box 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.
Step 6  In the **Roles/Locales** tab area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Assigned Role** area | The area in which you manage roles. The **Assign Roles** area contains the following check boxes:  
  * aaa  
  * admin  
  * network  
  * operations  
  * read-only  
  When a check box is checked, the user is assigned that role. |
| **Assigned Locale** area | The area in which you manage locales. The **Assigned Locales** area contains the assigned locales check boxes. When a check box is checked, the user is assigned to that locale. |

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Key** | The SSH key.  
  **Note** When you choose the **Key** radio button, the **SSH Data** field is displayed in the area. |
| **Password** | The SSH password. |

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 In the Work pane, 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User column</td>
<td>The username that is involved in the session.</td>
</tr>
<tr>
<td>Host column</td>
<td>The IP address from which the user is logged in.</td>
</tr>
<tr>
<td>Login Time column</td>
<td>The date and time the session started.</td>
</tr>
<tr>
<td>UI column</td>
<td>The user interface used to create this user login session.</td>
</tr>
<tr>
<td></td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• web—GUI login</td>
</tr>
<tr>
<td></td>
<td>• shell—CLI login</td>
</tr>
<tr>
<td></td>
<td>• ep—endpoint</td>
</tr>
<tr>
<td></td>
<td>• none</td>
</tr>
<tr>
<td>Terminal Type column</td>
<td>The kind of terminal through which the user is logged in.</td>
</tr>
</tbody>
</table>