



## CHAPTER 5

# Configuring RBAC

---

This chapter describes how to configure user accounts and role-based access control (RBAC) on NX-OS devices.

This chapter includes the following sections:

- [Information About User Accounts and RBAC, page 5-1](#)
- [Licensing Requirements for User Accounts and RBAC, page 5-4](#)
- [Guidelines and Limitations, page 5-4](#)
- [Configuring User Accounts, page 5-5](#)
- [Configuring Roles, page 5-11](#)
- [Field Descriptions for RBAC, page 5-19](#)
- [Additional References, page 5-20](#)

## Information About User Accounts and RBAC

You can create and manage users accounts and assign roles that limit access to operations on the NX-OS device. RBAC allows you to define the rules for an assign role that restrict the authorization that the user has to access management operations.

This section includes the following topics:

- [About User Accounts, page 5-1](#)
- [Characteristics of Strong Passwords, page 5-2](#)
- [About User Roles, page 5-2](#)
- [About User Role Rules, page 5-3](#)
- [Virtualization Support, page 5-3](#)

## About User Accounts

You can configure up to a maximum of 256 user accounts. By default, the user account does not expire unless you explicitly configure it to expire. The expire option determines the date when the user account is disabled.

Users can have user accounts on multiple VDCs. These users can move between VDCs after an initial connection to a VDC.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***



**Tip**

The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nsd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.



**Note**

User passwords are not displayed in the configuration files.



**Caution**

The Cisco NX-OS software does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

## Characteristics of Strong Passwords

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21



**Note**

Clear text passwords cannot include the dollar sign (\$) special character.



**Tip**

If a password is trivial (such as a short, easy-to-decipher password), the NX-OS software will reject your password configuration if password-strength checking is enabled. Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive.

## About User Roles

User roles contain rules that define the operations allowed for the user who is assigned the role. Each user role can contain multiple rules and each user can have multiple roles. For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. You can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

The Cisco NX-OS software provides four default user roles:

- network-admin—Complete read-and-write access to the entire NX-OS device (only available in the default VDC)
- network-operator—Complete read access to the entire NX-OS device (only available in the default VDC)
- vdc-admin—Read-and-write access limited to a VDC
- vdc-operator—Read access limited to a VDC

**Note**

You cannot change the default user roles.

You can create custom roles within a VDC. By default, the user roles that you create do not allow access to any device operations. You must add rules to allow users to display or configure features.

The VDCs do not share user roles. Each VDC maintains an independent user role database. Within a VDC, roles are configured by rule and attribute assignment.

**Note**

If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the user also has RoleB, which has access to the configuration commands. In this case, the user has access to the configuration commands.

## About User Role Rules

The rule is the basic element of a role. A rule defines what operations the role allows the user to perform. You can apply rules for the following parameters:

- Command—A command or group of commands defined in a regular expression.
- Feature—Commands that apply to a function provided by the NX-OS software.
- Feature group—Default or user-defined group of features.

These parameters create a hierarchical relationship. The most basic control parameter is the command. The next control parameter is the feature, which represents all commands associated with the feature. The last control parameter is the feature group. The feature group combines related features and allows you to easily manage the rules. The NX-OS software also supports the predefined feature group L3 that you can use.

You can configure up to 256 rules for each role. The user-specified rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

## Virtualization Support

The users with the network-admin and network-operator roles can operate in all virtual device contexts (VDCs) when logged in from the default VDC. All other user roles are local to the VDC. Roles are not shared between VDCs. Each VDC maintains an independent user role database. For more information on VDCs, see the [Cisco DCNM Virtual Device Context Configuration Guide, Release 4.0](#).

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Licensing Requirements for User Accounts and RBAC

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	User accounts and RBAC require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the <i>Cisco DCNM Licensing Guide, Release 4.0</i> .
NX-OS	User accounts and RBAC require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

## Guidelines and Limitations

User accounts and RBAC have the following configuration guidelines and limitations:

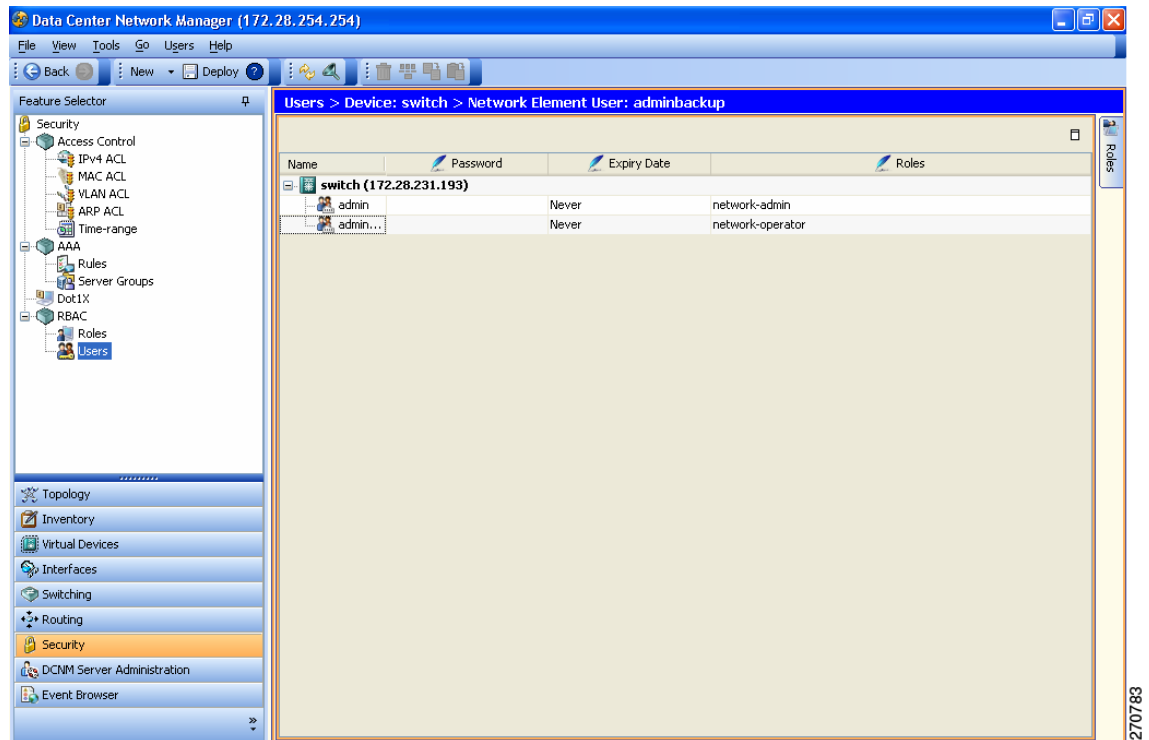
- You can create up to 64 user-defined roles in a VDC in addition to the four default user roles in the default VDC and the two default user roles in the nondefault VDCs.
- You can add up to 256 rules to a user role.
- You can add up to 64 user-defined feature groups to a VDC in addition to the default feature group, L3.
- You can configure up to 256 users in a VDC.
- You can assign a maximum of 64 user roles to a user account.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Configuring User Accounts

You can configure user accounts for the NX-OS device. [Figure 5-1](#) shows the Users pane.

**Figure 5-1** Users Pane



This section includes the following topics:

- [Creating a User Account, page 5-5](#)
- [Changing a User Account Password, page 5-8](#)
- [Changing a User Account Expiry Date, page 5-8](#)
- [Adding a User Account Role, page 5-9](#)
- [Deleting a User Account Role, page 5-9](#)
- [Deleting a User Account, page 5-10](#)

## Creating a User Account

You can create a maximum of 256 user accounts on an NX-OS device. User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).

The username is a case-sensitive, alphanumeric character string with a maximum length of 28 characters.

User accounts can have a maximum of 64 user roles.

User accounts are local to a VDC. However, users with the network-admin or network-operator role can log in to the default VDC and access other VDCs.

For more information on user roles, see the “Configuring Roles” section on page 5-11.



### Note

If you do not specify a password, the user might not be able to log in to the NX-OS device.

## DETAILED STEPS

To create a user account, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Users**.
- Step 2** From the Summary pane, double-click the device to display the users.
- Step 3** From the menu bar, choose **File > New > Add User**.

A new row appears in the list of users.

- Step 4** Enter the username.

The maximum length of the username is 28 characters.



### Note

Do not include the “#” or “@” character in the username. These characters are reserved for special use.

- Step 5** Double-click the **Password** cell and click the down arrow to display the password dialog box (see [Figure 5-2](#)).

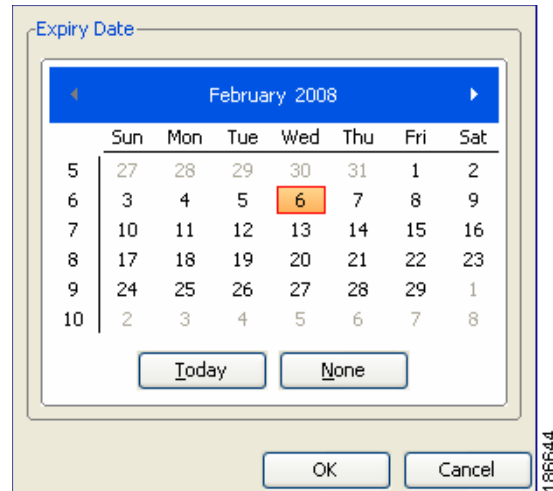
**Figure 5-2 Password Dialog Box**

The screenshot shows a dialog box with a light beige background. It has three rows of input fields. The first row is labeled 'Password:' and has an empty text box. The second row is labeled 'Confirm Password:' and has an empty text box. The third row is labeled 'Encryption Type:' and has a dropdown menu with 'Clear Text' selected. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'. A vertical number '186643' is visible on the right side of the dialog box.

- Step 6** From the password dialog box, enter the password in the Password and Confirm Password fields.
- Step 7** From the Encryption Type menu list, choose **Clear Text** or **Strongly Encrypted**.
- Step 8** Click **OK**.
- Step 9** Double-click the **Expiry Date** cell and click the down arrow to display the expiry date dialog box (see [Figure 5-3](#)).

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

**Figure 5-3 Expiry Date Dialog Box**

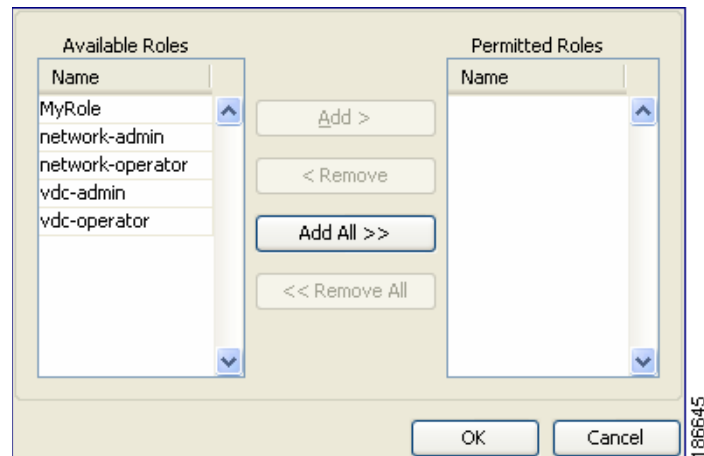


**Step 10** Navigate to the desired expiry date and click **OK**.

The default expiry date is Never.

**Step 11** Double-click the Roles cell and click the down arrow to display the user role dialog box (see [Figure 5-4](#)).

**Figure 5-4 User Role Dialog Box**



**Step 12** Choose one or more user roles by moving them to the Permitted column and click **OK**.

**Step 13** From the menu bar, choose **File > Deploy** to apply your changes to the device.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Changing a User Account Password

You can change the password for any user account if you have network-admin privileges in the default VDC or for VDC user accounts if you have vdc-admin privileges.



### Note

Changes to user account password do not take effect until the user logs in and creates a new session.

### BEFORE YOU BEGIN

Create one or more user accounts (see the [“Creating a User Account”](#) section on page 5-5).

### DETAILED STEPS

To change user account passwords, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Users**.
- Step 2** From the Summary pane, double-click the device to display the users.
- Step 3** Click the user account to change.
- Step 4** Double-click the **Password** cell and click the down arrow to display the password dialog box (see [Figure 5-2](#)).
- Step 5** From the password dialog box, enter the password in the Password and Confirm Password fields.
- Step 6** From the Encryption Type menu list, choose **Clear Text** or **Strongly Encrypted** and click **OK**.
- Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Changing a User Account Expiry Date

You can change the expiry date for any user account if you have network-admin privileges in the default VDC or you can change the expiry date for a VDC user account if you have vdc-admin privileges.



### Note

Changes to the user account expiry date do not take effect until the user logs in and creates a new session.

### BEFORE YOU BEGIN

Create one or more user accounts (see the [“Creating a User Account”](#) section on page 5-5).

### DETAILED STEPS

To change a user account expiry date, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Users**.
- Step 2** From the Summary pane, double-click the device to display the users.
- Step 3** Click the user account to change.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- Step 4** Double-click the **Expiry Date** cell and click the down arrow to display the expiry date dialog box (see [Figure 5-3](#)).
- Step 5** Navigate to the desired expiry date and click **OK**.  
The default expiry date is Never.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Adding a User Account Role

You can add roles to a user account if you have network-admin privileges in the default VDC or you can add roles for VDC user accounts if you have vdc-admin privileges.

**Note**

Changes to user account roles do not take effect until the user logs in and creates a new session.

---

### BEFORE YOU BEGIN

Create one or more user accounts (see the [“Creating a User Account”](#) section on page 5-5).

### DETAILED STEPS

To add a user account role, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Users**.
- Step 2** From the Summary pane, double-click the device to display the users.
- Step 3** Click the user account to change.
- Step 4** Double-click the **Roles** cell and click the down arrow to display the user roles dialog box (see [Figure 5-4](#)).
- Step 5** Choose one or more user roles by moving them to the Permitted Roles column and click **OK**.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Deleting a User Account Role

You can delete the roles from a user account if you have network-admin privileges in the default VDC or for VDC user accounts if you have vdc-admin privileges.

**Note**

Changes to a user account role do not take effect until the user logs in and creates a new session.

---

### BEFORE YOU BEGIN

Create one or more user accounts (see the [“Creating a User Account”](#) section on page 5-5).  
Add a role to the user account (see the [“Adding a User Account Role”](#) section on page 5-9).

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## DETAILED STEPS

To delete a user account role, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Users**.
  - Step 2** From the Summary pane, double-click the device to display the users.
  - Step 3** Click the user account to change.
  - Step 4** Double-click the Roles cell and click the down arrow to display the user roles dialog box (see [Figure 5-4](#)).
  - Step 5** Delete one or more user roles by moving them to the Available Roles column and click **OK**.
  - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Deleting a User Account

You can delete a user account.

### BEFORE YOU BEGIN

Create one or more user accounts (see the [“Creating a User Account”](#) section on page 5-5).

## DETAILED STEPS

To delete a user account, follow these steps:

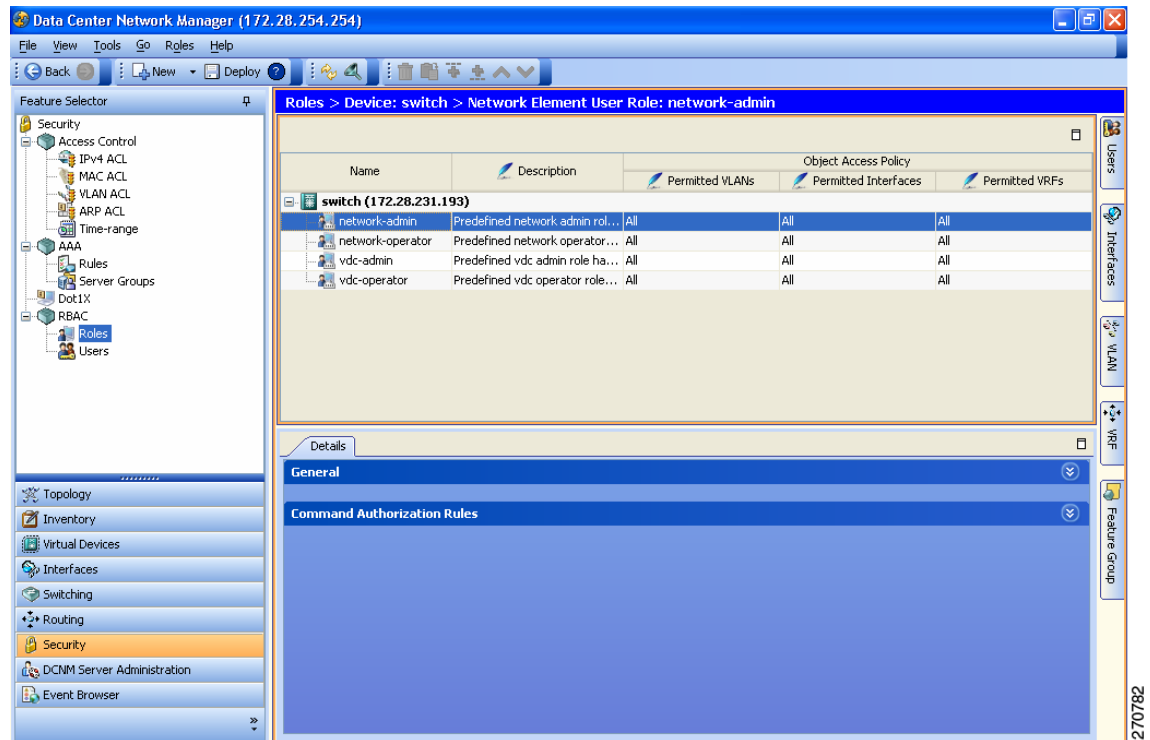
- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Users**.
  - Step 2** From the Summary pane, double-click the device to display the users.
  - Step 3** Click the user account to delete.
  - Step 4** From the top menu bar, choose **Users > Delete User** and click **Yes** in the confirmation dialog.  
The user account name disappears from the user account list.
  - Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Configuring Roles

Figure 5-5 shows the RBAC Roles content pane.

**Figure 5-5 Roles Content Pane**



This section includes the following topics:

- [Creating User Roles, page 5-12](#)
- [Adding a Rule to a User Role, page 5-12](#)
- [Changing a Rule in a User Role, page 5-13](#)
- [Rearranging a Rule in a User Role, page 5-14](#)
- [Deleting a Rule from a User Role, page 5-15](#)
- [Changing User Role Interface Policies, page 5-15](#)
- [Changing User Role VLAN Policies, page 5-16](#)
- [Changing User Role VRF Policies, page 5-18](#)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Creating User Roles

You can configure up to 64 user roles in a VDC. You can assign a user role to more than one user account.

### DETAILED STEPS

To create user roles, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
  - Step 2** From the Summary pane, double-click the device to display the roles.
  - Step 3** From the menu bar, choose **File > New > Add Role**.  
A new row appears in the list of roles.
  - Step 4** In the **Name** cell, enter the role name.  
The maximum length of the role name is 16 characters.
  - Step 5** (Optional) In the Description cell, enter the role description.
  - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Adding a Rule to a User Role

You can use rules to define the actions that users can perform on the NX-OS device. Each user role can have up to 256 rules.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

### BEFORE YOU BEGIN

Create one or more user roles (see the [“Creating User Roles” section on page 5-12](#)).

### DETAILED STEPS

To add a rule to a user role, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
  - Step 2** From the Summary pane, double-click the device to display the user roles.  
The Details tab appears in the Details pane.
  - Step 3** Click the user role to which to add a rule.




---

**Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.

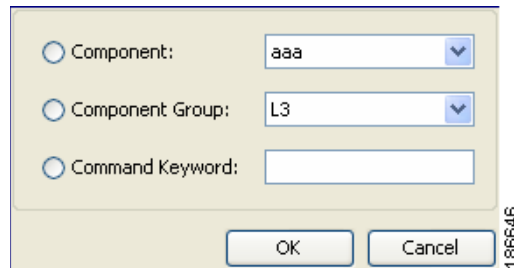
---

- Step 4** From the Details tab, click **Command Authorization Rules**.

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).

- Step 5** From the menu bar, choose **Roles > Add Rule** or **Roles > Insert Rule Above** or **Roles > Insert Rule Below**.
- A new rule appears in the Details pane.
- Step 6** Double-click the **Permission** cell for the new rule and choose **Permit** or **Deny**.
- Step 7** Double-click the **Match Command Type** cell for the new rule and choose from the drop-down list.
- Step 8** Double-click the **Match Value (Component/Command)** cell for the new rule.
- Step 9** Click the down arrow to display the match value dialog box (see [Figure 5-6](#)).

**Figure 5-6 Match Value Dialog Box**



The screenshot shows a dialog box titled "Match Value Dialog Box". It contains three radio button options: "Component:", "Component Group:", and "Command Keyword:". The "Component:" option is selected, and its corresponding dropdown menu shows "aaa". The "Component Group:" option is also selected, and its dropdown menu shows "L3". The "Command Keyword:" option is not selected, and its text box is empty. At the bottom of the dialog box are "OK" and "Cancel" buttons. A vertical text label "186646" is visible on the right side of the dialog box.

- Step 10** From the dialog box, specify the match value for the rule and click **OK**.
- Step 11** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Changing a Rule in a User Role

You can change the command authorization criteria for a rule in a user role.

### BEFORE YOU BEGIN

Add one or more rules to a user role (see the [“Adding a Rule to a User Role”](#) section on page 5-12).

### DETAILED STEPS

To change a rule to a user role, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
- Step 2** From the Summary pane, double-click the device to display the user roles.
- The Details tab appears in the Details pane.
- Step 3** Click the user role to change.



**Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.

- Step 4** From the Details tab, click **Command Authorization Rules**.
- Step 5** Click the rule to rearrange.

## ***Send document comments to nexus7k-docfeedback@cisco.com.***

- Step 6** Double-click the **Match Command Type** cell for the rule and choose from the drop-down list.
  - Step 7** Double-click the **Match Value (Component/Command)** cell for the rule.
  - Step 8** Click the down arrow to display the match value dialog box (see [Figure 5-6 on page 5-13](#)).
  - Step 9** From the dialog box, specify the match value for the rule and click **OK**.
  - Step 10** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Rearranging a Rule in a User Role

You can rearrange a rule in a user role.


### BEFORE YOU BEGIN

Add one or more rules to a user role (see the “[Adding a Rule to a User Role](#)” section on page 5-12).

### DETAILED STEPS

To rearrange a rule to a user role, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
  - Step 2** From the Summary pane, double-click the device to display the user roles.  
The Details tab appears in the Details pane.
  - Step 3** Click the user role to change.
 



**Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.
  - Step 4** From the Details tab, click **Command Authorization Rules**.
  - Step 5** Click the rule to rearrange.
  - Step 6** From the menu bar, choose **Roles > Move Up** or **Roles > Move Down**.
  - Step 7** Double-click the **Match Value (Component/Command)** cell for the rule.
  - Step 8** Click the down arrow to display the match value dialog box (see [Figure 5-6 on page 5-13](#)).
  - Step 9** From the dialog box, specify the match value for the rule and click **OK**.
  - Step 10** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Deleting a Rule from a User Role


You can delete rules from a user role. Each role must have at least one rule.

### BEFORE YOU BEGIN

Add one or more rules to a user role (see the [“Adding a Rule to a User Role”](#) section on page 5-12).

### DETAILED STEPS

To delete a rule from a user role, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
- Step 2** From the Summary pane, double-click the device to display the user roles.  
The Details tab appears in the Details pane.
- Step 3** Click the user role from which to delete the rule.
-  **Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.
- 
- Step 4** From the Details tab, click **Command Authorization Rules**.
- Step 5** Click the rule that you want to delete.
- Step 6** From the menu bar, choose **Roles > Delete Rule** and click **Yes** in the confirmation dialog box.  
The rule disappears from the Details pane.
- Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access. By default, a user role allows access to all interfaces in the VDC.

### BEFORE YOU BEGIN

Create one or more user roles (see the [“Creating User Roles”](#) section on page 5-12).

### DETAILED STEPS

To change user role interface policies, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
- Step 2** From the Summary pane, double-click the device to display the roles.
- Step 3** Click the role to change.  
The Details tab appears in the Details pane.

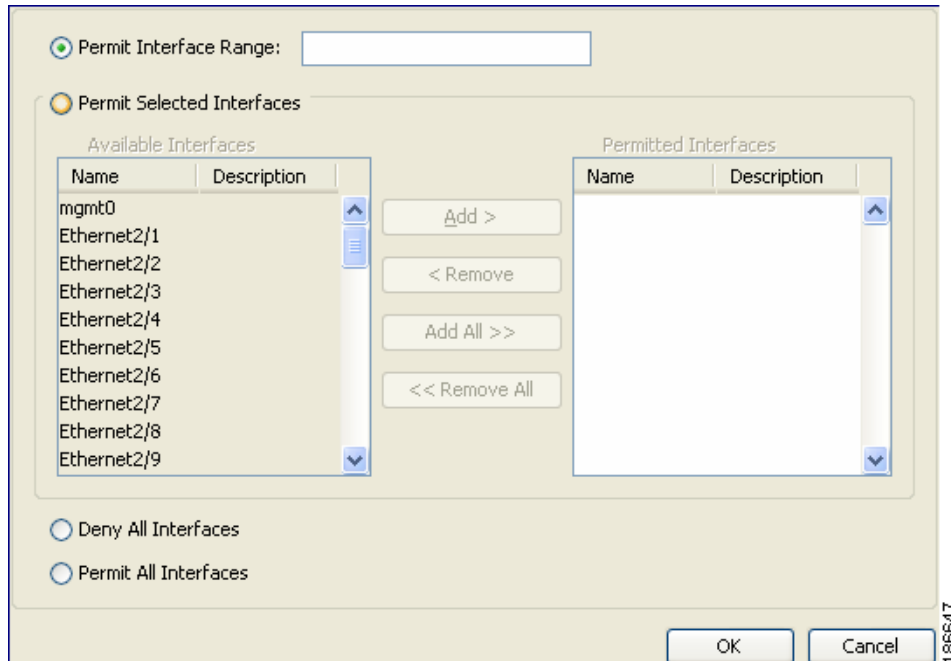
**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**



**Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.

- Step 4** From the Details pane, click **General**.
- Step 5** From the Permitted Interfaces field, click the down arrow to display the permitted interfaces dialog box (see [Figure 5-7](#)).

**Figure 5-7 Permitted Interfaces Dialog Box**



- Step 6** From the dialog box, you can enter the range of interfaces to permit, specify selected interfaces to permit, deny all interfaces, or permit all interfaces.
- Step 7** Click **OK**.
- Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Changing User Role VLAN Policies

You can change a user role VLAN policy to limit the VLANs that the user can access. By default, a user role allows access to all VLANs in the VDC.

### BEFORE YOU BEGIN

Create one or more user roles (see the [“Creating User Roles”](#) section on page 5-12).

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## DETAILED STEPS

To change user role VLAN policies, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
- Step 2** From the Summary pane, double-click the device to display the roles.
- Step 3** Click the role to change.

The Details tab appears in the Details pane.



**Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.

- Step 4** From the Details pane, click **General**.
- Step 5** From the Permitted VLANs field, click the down arrow to display the permitted VLANs dialog box (see [Figure 5-8](#)).

**Figure 5-8 Permitted VLANs Dialog Box**

- Step 6** From the dialog box, you can enter the range of VLANs to permit, specify selected VLANs to permit, deny all VLANs, or permit all VLANs.
- Step 7** Click **OK**.
- Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Changing User Role VRF Policies

You can change a user role VRF policy to limit the VRFs that the user can access. By default, a user role allows access to all VRFs in the VDC.

### BEFORE YOU BEGIN

Create one or more user roles (see the “Creating User Roles” section on page 5-12).

### DETAILED STEPS

To change user role VRF policies, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > RBAC > Roles**.
  - Step 2** From the Summary pane, double-click the device to display the roles.
  - Step 3** Click the role to change.

The Details tab appears in the Details pane.

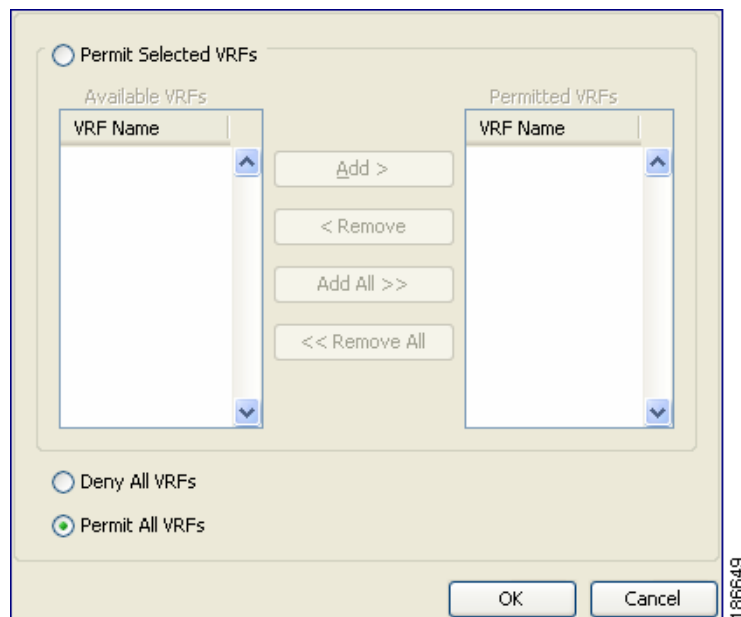


**Note** You cannot modify the default roles network-admin, network-operator, vdc-admin, and vdc-operator.

---

- Step 4** From the Details pane, click **General**.
- Step 5** From the Permitted VRFs field, click the down arrow to display the permitted VRFs dialog box (see [Figure 5-9](#)).

**Figure 5-9 Permitted VRFs Dialog Box**



- Step 6** From the dialog box, you can enter the range of VRFs to permit, specify selected VRFs to permit, deny all VRFs, or permit all VRFs.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Step 7** Click **OK**.

**Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Field Descriptions for RBAC

This section includes the following topics:

- [Security: RBAC: Roles: Summary Pane, page 5-19](#)
- [Security: RBAC: Roles: device: role: Details Tab: General Area, page 5-19](#)
- [Security: RBAC: Roles: device: role: Details Tab: Command Authorization Rules Area, page 5-20](#)
- [Security: RBAC: Users: Summary Pane, page 5-20](#)

### Security: RBAC: Roles: Summary Pane

**Table 5-1** *Security: RBAC: Roles: Summary Pane*

Element	Description
Name	Role name
Description	Role description
<b>Object Access Policy</b>	
Permitted VLANs	Permitted VLANs
Permitted Interfaces	Permitted interfaces
Permitted VRFs	Permitted VRFs

### Security: RBAC: Roles: device: role: Details Tab: General Area

**Table 5-2** *Security: RBAC: Roles: device: role: Details Tab*

Element	Description
Name	Role name
Description	Role description
<b>Object Access Policy</b>	
Permitted VLANs	Permitted VLANs
Permitted Interfaces	Permitted interfaces
Permitted VRFs	Permitted VRFs

**[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)**

## Security: RBAC: Roles: device: role: Details Tab: Command Authorization Rules Area

**Table 5-3** Security: RBAC: Roles: device: role: Details Tab

Element	Description
Rule No	Rule sequence number
Permission	Rule permission
Match Command Type	Match command type
Match Value (Component/Command)	Match value

## Security: RBAC: Users: Summary Pane

**Table 5-4** Security: RBAC: Users: Summary Pane

Element	Description
Name	User account name.
Password	User account password. The default password is none.
Expiry Date	User account expiry date. The default is never.
Roles	User account roles. The default is network-operator for user accounts created in the default VDC by a user with the network-admin role. For all other accounts, the default is vdc-operator.

## Additional References

For additional information related to implementing RBAC, see the following sections:

- [Related Documents, page 5-20](#)
- [Standards, page 5-21](#)
- [MIBs, page 5-21](#)

## Related Documents

Related Topic	Document Title
NX-OS Licensing	<a href="#">Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</a>
DCNM Licensing	<a href="#">Cisco DCNM Licensing Guide, Release 4.0</a>
VRF configuration	<a href="#">Cisco DCNM Unicast Routing Configuration Guide, Release 4.0</a>

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"><li>CISCO-COMMON-MGMT-MIB</li></ul>	To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***