Configuring User Accounts and RBAC

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

Information About User Accounts and RBAC

You can create and manage users accounts and assign roles that limit access to operations on the Cisco 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.

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.

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, nscd, 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:

- Is 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.

If a password is trivial (such as a short, easy-to-decipher password), the Cisco 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.

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

- network-admin—Complete read-and-write access to the entire Cisco NX-OS device (only available in the default VDC)
- network-operator—Complete read access to the entire Cisco 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 accounts without administrator roles can only display feature information. You can add rules to allow users to configure features.
The VDCs on the same physical device 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	A command or group of commands defined in a regular expression.
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 Cisco 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 for RBAC

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 4.2*.

Licensing Requirements for User Accounts and RBAC

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco 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 Cisco DCNM licensing scheme, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.2*.
Cisco 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 Cisco NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*.

Guidelines and Limitations for User Accounts and RBAC

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.

Enabling Password-Strength Checking

You can enable password-strength checking which prevents you from creating weak passwords for user accounts.

Note When you enable password-strength checking, the Cisco NX-OS software does not check the strength of existing passwords.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**password strength-check** **Example:** `switch(config)# password strength-check`	Enables password-strength checking. The default is enabled. You can disable password-strength checking by using the **no** form of this command.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

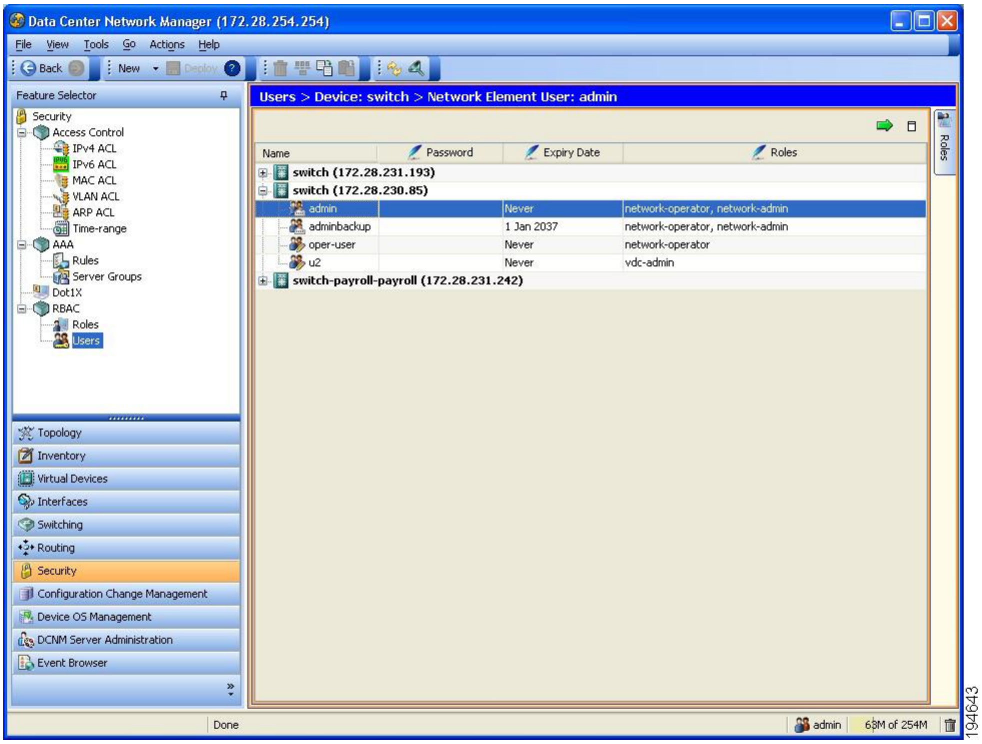
Step 4	**show password strength-check** **Example:** `switch# show password strength-check`	(Optional) Displays the password-strength check configuration.
Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring User Accounts

This section describes how to configure user accounts for the Cisco NX-OS device.

This figure shows the Users pane.

Figure 1: Users Pane



Name	Password	Expiry Date	Roles
switch (172.28.231.193)			
switch (172.28.230.85)			
admin		Never	network-operator, network-admin
adminbackup		1 Jan 2037	network-operator, network-admin
oper-user		Never	network-operator
u2		Never	vdc-admin
switch-payroll-payroll (172.28.231.242)			

Creating a User Account

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

- Username
- Password
- Expiry date
- User roles

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.

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

Procedure

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.

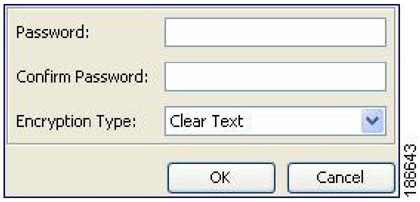
Step 3 From the menu bar, choose **Actions > Add User**.
A new row appears in the list of users.

Step 4 Enter the username.
The username is a case-sensitive character string with a maximum length of 28 characters. Valid characters are uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, hyphen (-), period (.), underscore (_), plus sign (+), and equal sign (=).

Step 5 Double-click the **Password** cell and click the down arrow to display the password dialog box.

This figure shows the password dialog box.

Figure 2: Password Dialog Box



Password:

Confirm Password:

Encryption Type: Clear Text

Step 6 From the password dialog box, enter the password in the Password and Confirm Password fields.

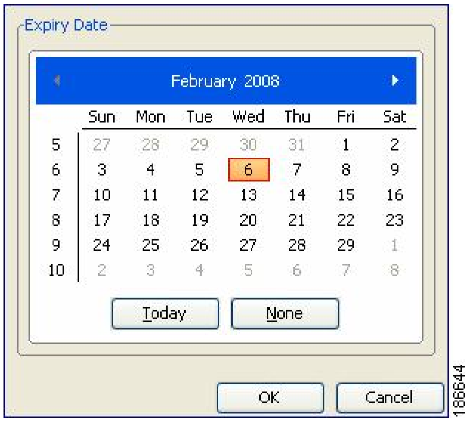
Step 7 From the Encryption Type menu list, choose **Clear Text** or **Strongly Encrypted**.

Step 8 Click **OK**.

Step 9 Double-click the **Expiry Date** cell and click the down arrow to display the Expiry Date dialog box.

This figure shows the Expiry Date dialog box.

Figure 3: Expiry Date Dialog Box



Expiry Date

February 2008

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
5	27	28	29	30	31	1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	29	1
10	2	3	4	5	6	7	8

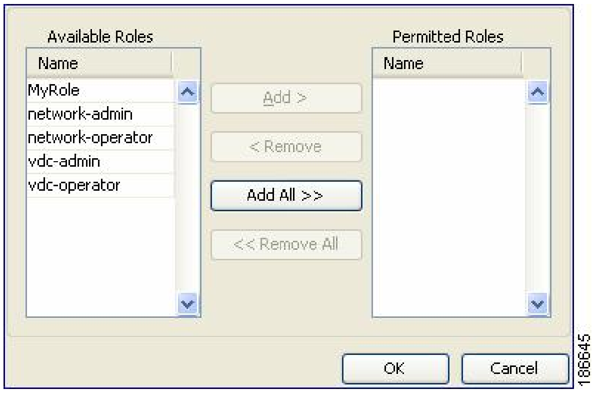
Step 10 Navigate to the desired expiry date and click **OK**.

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.

This figure shows the user role dialog box.

Figure 4: User Role Dialog Box



Name
MyRole
network-admin
network-operator
vdc-admin
vdc-operator

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.

Related Topics

- Configuring Roles, page 14
- Creating a User Account, page 6

Copying a User Account

You can copy the configuration of a user account from one Cisco NX-OS device to another Cisco NX-OS device.

Before You Begin

Create one or more user accounts.

Ensure that the roles assigned to the user account exist on the target device.

Procedure

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 on the user account that you want to copy.

Step 4 From the menu bar, choose **Actions > Copy**.

Step 5 Click the destination device.

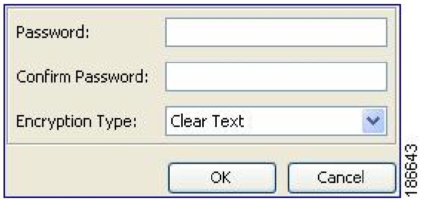
Step 6 From the menu bar, choose **Actions > Paste**.

The user account appears in the list of users for the device.

Step 7 Double-click the **Password** cell and click the down arrow to display the password dialog box.

This figure shows the password dialob box.

Figure 5: Password Dialog Box



Password:

Confirm Password:

Encryption Type: Clear Text

Step 8 From the password dialog box, enter the password in the Password and Confirm Password fields.

Step 9 From the Encryption Type menu list, choose **Clear Text** or **Strongly Encrypted**.

Step 10 Click **OK**.

Step 11 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Related Topics

- Creating a User Account, page 6
- Creating a User Role, page 14

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.

Procedure

Step 1 From the Feature Selector pane, choose **Security > RBAC > Users**.

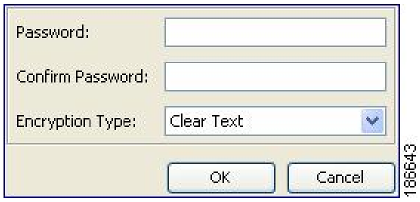
Step 2 From the Summary pane, double-click the device to display the users.

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.

This figure shows the password dialog box.

Figure 6: Password Dialog Box



Encryption Type: Clear Text

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.

Related Topics

- Creating a User Account, page 6

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.

Procedure

Step 1 From the Feature Selector pane, choose **Security > RBAC > Users**.

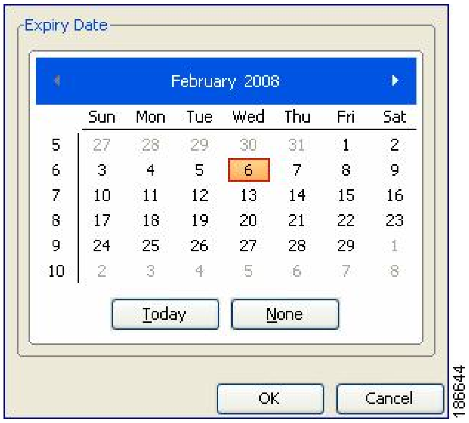
Step 2 From the Summary pane, double-click the device to display the users.

Step 3 Click the user account to change.

Step 4 Double-click the **Expiry Date** cell and click the down arrow to display the Expiry Date dialog box.

This figure shows the Expiry Date dialog box.

Figure 7: Expiry Date Dialog Box



	Sun	Mon	Tue	Wed	Thu	Fri	Sat
5	27	28	29	30	31	1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	29	1
10	2	3	4	5	6	7	8

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.

Procedure

Step 1 From the Feature Selector pane, choose **Security > RBAC > Users**.

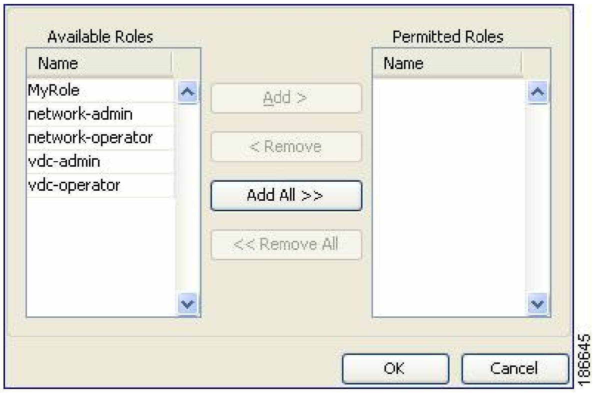
Step 2 From the Summary pane, double-click the device to display the users.

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.

This figure shows the user role dialog box.

Figure 8: User Role Dialog Box



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.

Related Topics

- Creating a User Account, page 6

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.

Add a role to the user account.

Procedure

Step 1 From the Feature Selector pane, choose **Security > RBAC > Users**.

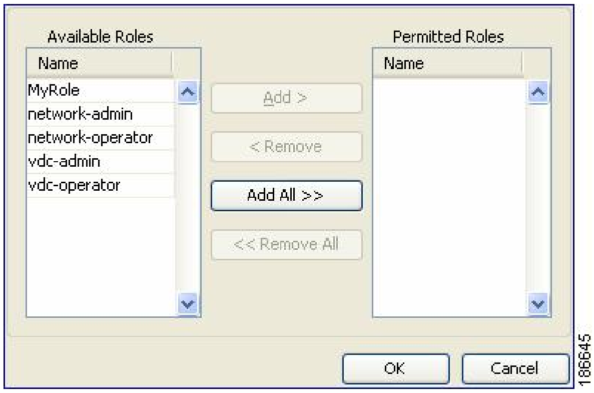
Step 2 From the Summary pane, double-click the device to display the users.

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.

This figure shows the user role dialog box.

Figure 9: User Role Dialog Box



Step 5 Delete one or more user roles by moving them to the Available Roles column and click **OK**.

Note A user account must have at least one user role.

Step 6 From the menu bar, choose **File** > **Deploy** to apply your changes to the device.

Related Topics

- Adding a User Account Role, page 11

Deleting a User Account

You can delete a user account.

Before You Begin

Create one or more user accounts.

Procedure

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.

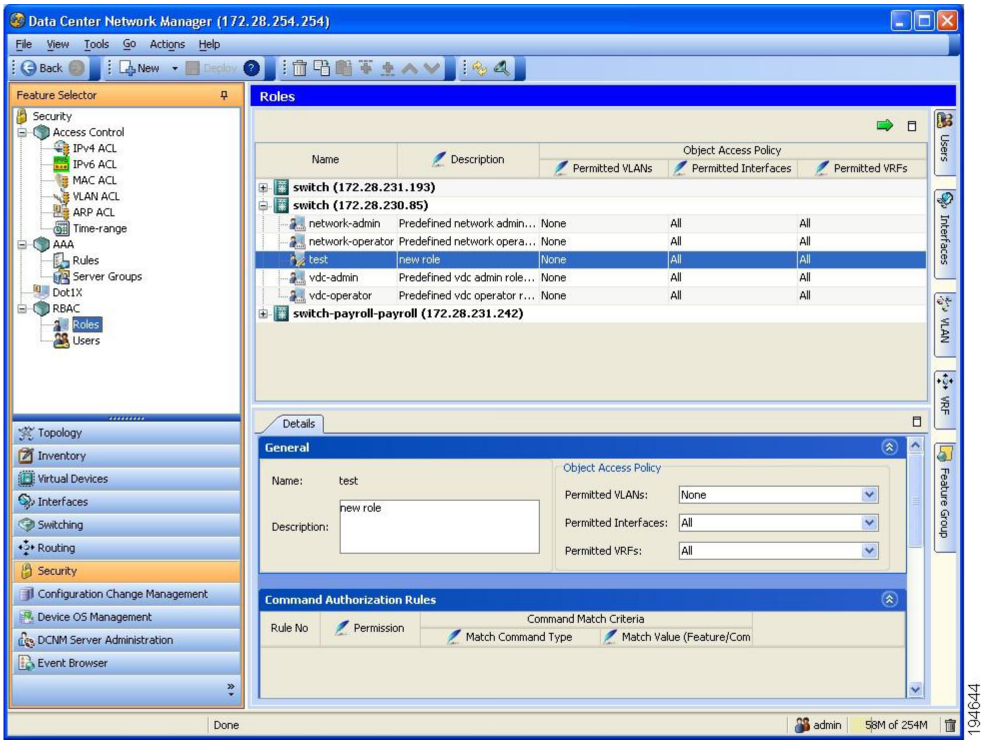
Step 5 From the menu bar, choose **File** > **Deploy** to apply your changes to the device.

Configuring Roles

This section describes how to configure user roles.

This figure shows the RBAC Roles content pane.

Figure 10: Roles Content Pane



Name	Description	Object Access Policy		
		Permitted VLANs	Permitted Interfaces	Permitted VRFs
switch (172.28.231.193)				
switch (172.28.230.85)				
network-admin	Predefined network admin...	None	All	All
network-operator	Predefined network opera...	None	All	All
test	new role	None	All	All
vdc-admin	Predefined vdc admin role...	None	All	All
vdc-operator	Predefined vdc operator r...	None	All	All
switch-payroll-payroll (172.28.231.242)				

General

Name: test

Description: new role

Object Access Policy

Permitted VLANs: None

Permitted Interfaces: All

Permitted VRFs: All

Command Authorization Rules

Rule No	Permission	Command Match Criteria	
		Match Command Type	Match Value (Feature/Com

Creating a User Role

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

Procedure

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 **Actions** > **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.

Copying a User Role

You can copy the configuration of a user role within a Cisco NX-OS device or from one Cisco NX-OS device to another Cisco NX-OS device.

Procedure

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 you that want to copy.

Step 4 From the menu bar, choose **Actions > Copy**.

Step 5 Click the destination device.

Step 6 From the menu bar, choose **Actions > Paste**.
The role appears in the list of roles for the device.

Step 7 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 Cisco 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.

Procedure

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**.

Step 5 From the menu bar, choose **Actions > Add Rule** or **Actions > Insert Rule Above** or **Actions > 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**.

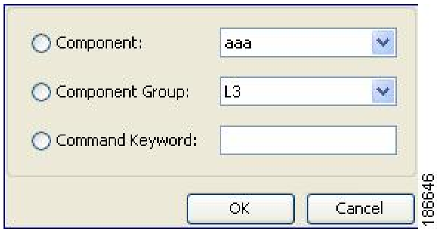
Step 7 Double-click the **Match Command Type** cell for the new rule and choose from the drop-down list.

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.

This figure shows the match value dialog box.

Figure 11: Match Value Dialog Box



○ Component: aaa

○ Component Group: L3

○ Command Keyword:

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.

Related Topics

- Creating a User Role, page 14

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.

Procedure

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.

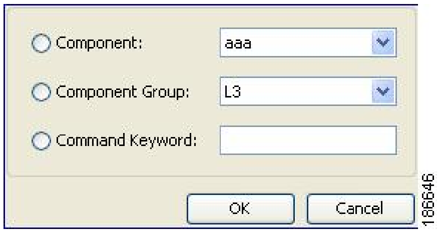
Step 6 Double-click the **Match Command Type** cell for the rule and choose from the drop-down list.

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.

This figure shows the match value dialog box.

Figure 12: Match Value Dialog Box



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.

Related Topics

- Adding a Rule to a User Role, page 15

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.

Procedure

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.

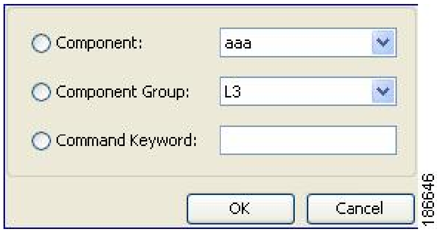
Step 6 From the menu bar, choose **Actions > Move Up** or **Actions > Move Down**.

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.

This figure shows the match value dialog box.

Figure 13: Match Value Dialog Box



○ Component: aaa

○ Component Group: L3

○ Command Keyword:

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.

Related Topics

- Adding a Rule to a User Role, page 15

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.

Procedure

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 **Actions > 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 a User Role Interface Policy

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.

Procedure

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.

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

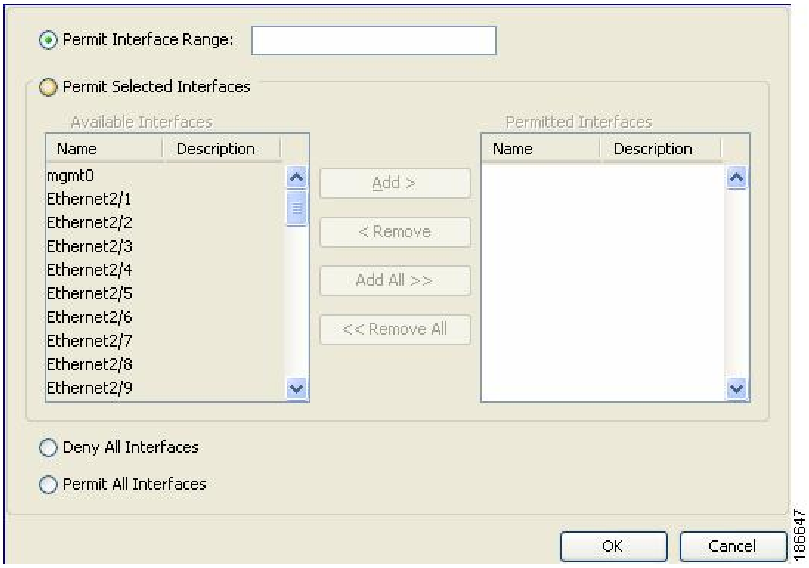
The Details tab appears in the Details pane.

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.

This figure shows the permitted interfaces dialog box.

Figure 14: Permitted Interfaces Dialog Box



● Permit Interface Range:

○ Permit Selected Interfaces

Available Interfaces

Name	Description
mgmt0	
Ethernet2/1	
Ethernet2/2	
Ethernet2/3	
Ethernet2/4	
Ethernet2/5	
Ethernet2/6	
Ethernet2/7	
Ethernet2/8	
Ethernet2/9	

Permitted Interfaces

Name	Description

○ Deny All Interfaces

○ Permit All Interfaces

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.

Related Topics

- Configuring Roles, page 14

Changing a User Role VLAN Policy

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.

Procedure

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.

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

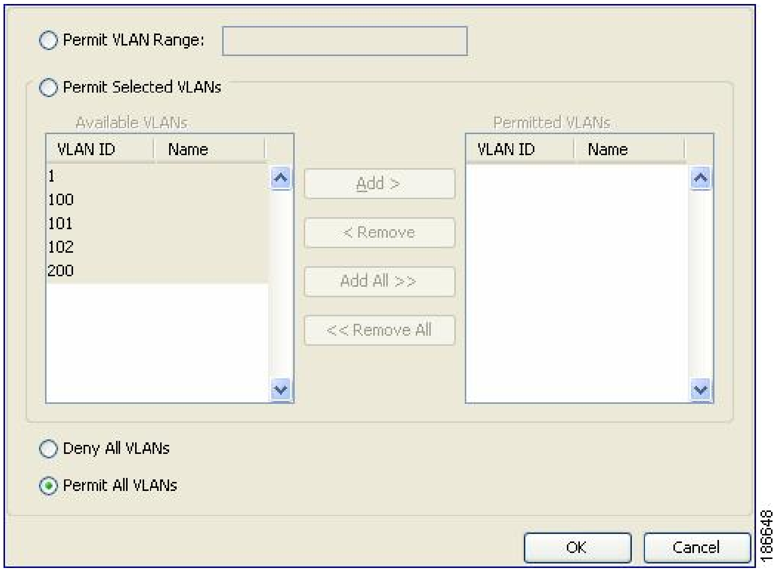
The Details tab appears in the Details pane.

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.

This figure shows the permitted VLANs dialog box.

Figure 15: Permitted VLANs Dialog Box



○ Permit VLAN Range:

○ Permit Selected VLANs

Available VLANs

VLAN ID	Name
1	
100	
101	
102	
200	

Permitted VLANs

VLAN ID	Name

○ Deny All VLANs

● Permit All VLANs

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.

Related Topics

- Configuring Roles, page 14

Changing a User Role VRF Policy

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.

Procedure

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.

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

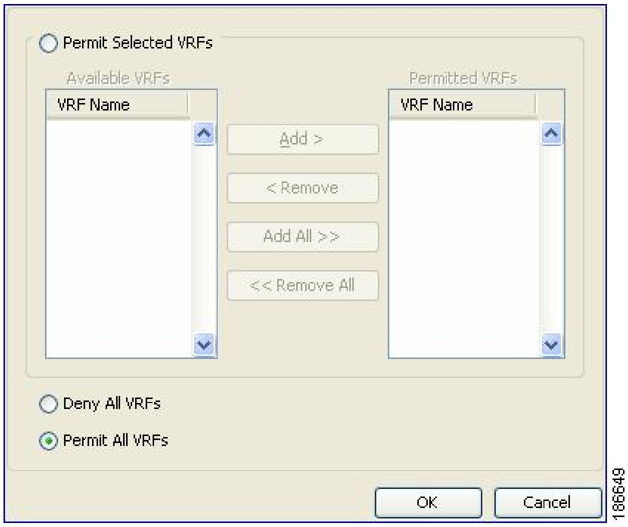
The Details tab appears in the Details pane.

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.

This figure shows the permitted VRFs dialog box.

Figure 16: Permitted VRFs Dialog Box



○ Permit Selected VRFs

○ Deny All VRFs

● Permit All VRFs

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.

Step 7 Click **OK**.

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

Related Topics

- Configuring Roles, page 14

Field Descriptions for RBAC

This section describes the fields for RBAC.

Security: RBAC: Roles: Summary Pane

Table 1: Security: RBAC: Roles: Summary Pane

Element	Description
Name	Role name

Element	Description
Description	Role description
Object Access Policy	
Permitted VLANs	Permitted VLANs
Permitted Interfaces	Permitted interfaces
Permitted VRFs	Permitted VRFs

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

Table 2: Security: RBAC: Roles: device: role: Details Tab

Element	Description
Name	Role name
Description	Role description
Object Access Policy	
Permitted VLANs	Permitted VLANs
Permitted Interfaces	Permitted interfaces
Permitted VRFs	Permitted VRFs

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

Table 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 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 User Accounts and RBAC

This section includes additional information related to implementing user accounts and RBAC.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*
Cisco DCNM Licensing	*Cisco DCNM Fundamentals Configuration Guide, Release 4.2*
VRF configuration	

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
- CISCO-COMMON-MGMT-MIB	To locate and download MIBs, go to the following URL:

MIBs	MIBs Link
	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for User Accounts and RBAC

This table lists the release history for this feature.

Table 5: Feature History for User Accounts and RBAC

Feature Name	Releases	Feature Information	
Usernames	4.2(1)	Valid characters in username are limited to lowercase a through z, uppercase A through Z, the numbers 0 through 9, plus sign (+), hyphen (-), equal sigh (=), underscore (_) and period (.).	