Configuring User Accounts and RBAC

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

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, root, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Note User passwords are not displayed in the configuration files.

Caution Usernames must begin with an alphanumeric character in Cisco NX-OS Releases 6.x and earlier releases. Usernames can contain only these special characters: (+ = . _ \ -). The # and ! symbols are not supported. If the username contains characters that are not allowed, the specified user is unable to log in.

Note Usernames that begin with special characters (+ = . _ \ -) are not supported in Cisco NX-OS Releases 6.x and earlier releases.

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 All printable ASCII characters are supported in the password string if they are enclosed in quotation marks.

Note Beginning with Cisco NX-OS Release 7.1, the PSB 5.0 requirements in NXOS are supported. SEC-PWD-DEFMIN - Default minimum passphrase length must be non-zero and at least eight characters. The user interface may use the word PASSPHRASES as pass phrases or passphrases rather than as password.

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.

Related Topics

Enabling Password-Strength Checking, on page 7

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.

Note Some **show** commands may be hidden from network-operator and vdc-operator users. In addition, some non-**show** commands (such as **telnet**) may be available for these user roles.

You can create custom roles within a VDC. By default, the user accounts without administrator roles can access only the **show**, **exit**, **end**, and **configure terminal** commands. 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.

Note Only network-admin user can perform a Checkpoint or Rollback in the RBAC roles. Though other users have these commands as a permit rule in their role, the user access is denied when you try to execute these commands.

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.

The command, feature, and feature group 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.

User Role Configuration Distribution

Cisco Fabric Services (CFS) allows the Cisco NX-OS device to distribute the user role configuration to other Cisco NX-OS devices in the network. When you enable CFS distribution for a feature on your device, the device belongs to a CFS region containing other devices in the network that you have also enabled for CFS distribution for the feature. CFS distribution for the user role feature is disabled by default.

Note You must explicitly enable CFS for user roles on each device to which you want to distribute configuration changes.

After you enable CFS distribution for user roles on your Cisco NX-OS device, the first user role configuration command that you enter causes the Cisco NX-OS software to take the following actions:

- Creates a CFS session on your Cisco NX-OS device.

- Locks the user role configuration on all Cisco NX-OS devices in the CFS region with CFS enabled for the user role feature.
- Saves the user role configuration changes in a temporary buffer on the Cisco NX-OS device.

The changes stay in the temporary buffer on the Cisco NX-OS device until you explicitly commit them to be distributed to the devices in the CFS region. When you commit the changes, the Cisco NX-OS software takes the following actions:

- Applies the changes to the running configuration on your Cisco NX-OS device.
- Distributes the updated user role configuration to the other Cisco NX-OS devices in the CFS region.
- Unlocks the user role configuration in the devices in the CFS region.
- Terminates the CFS session.

For detailed information on CFS, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

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 and use the **switchto vdc** command to access other VDCs. All other user roles are local to the VDC. Roles are not shared between VDCs. Each VDC maintains an independent user role database.

The following guidelines and limitations apply to the **switchto vdc** command:

- Only users with the network-admin or network-operator role can use the **switchto vdc** command. No other users are permitted to use it.
- No user can grant permission to another role to use the **switchto vdc** command.
- After a network-admin uses the **switchto vdc** command, this user becomes a vdc-admin for the new VDC. Similarly, after a network-operator uses the **switchto vdc** command, this user becomes a vdc-operator for the new VDC. Any other roles associated with the user are not valid after the **switchto vdc** command is entered.
- After a network-admin or network-operator uses the switchto vdc command, this user cannot use this command to switch to another VDC. The only option is to use the **switchback** command to return to the original VDC.

Beginning with Cisco NX-OS Release 5.2, you can configure RBAC in the storage VDC. Note that RBAC in the storage VDC is RBAC for the Cisco Nexus 7000 Series switches, which is different from that for the Cisco MDS 9500 Series switches.

Note For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for User Accounts and RBAC

The following table shows the licensing requirements for this feature:

Product	License Requirement
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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

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.
- You cannot delete the default admin and SNMP user accounts.
- You cannot remove the default user roles from the default admin user accounts.
- The network-operator and vdc-operator roles cannot run the **show running-config** and **show startup-config** commands.
- RBAC is not supported for traffic between F1 Series module ports and M1 Series module ports in the same VLAN.
- The following guidelines are applicable for the **rule** command:
  - When you use the **rule** *rule-id* **permit command** *command-string* command, the *command-string* argument should be complete or it should contain an asterisk (*) after the command name, for example, **show *** or **show running-config ***.
  - If you are adding more than one command in the command-string argument, the commands should be separated by a command separator (;) and a whitespace should be added.
  - When you are specifying interfaces, it is recommended to specify the entire media type keyword such as Ethernet or loopback. However, if you are using the short form of the media type keyword, it should be followed by an asterisk (*).

For example, **rule 22 permit command show run int Ethernet4/1**, **rule 22 permit command show run int loopback1**, or **rule 22 permit command show run int eth***.

Rules that do not follow this guideline are not accepted. For example, **rule 22 permit command show run int Eth1/4** and **rule 22 permit command show run int loop1**. For more information about using the **rule** command, see Creating User Roles and Rules, on page 11.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Default Settings for User Accounts and RBAC

This table lists the default settings for user accounts and RBAC parameters.

Table 1: Default User Accounts and RBAC Parameters

Parameters	Default
User account password	Undefined.
User account expiry date	None.
User account role in the default VDC	Network-operator if the creating user has the network-admin role, or vdc-operator if the creating user has the vdc-admin role.
User account role in the non-VDCs	Vdc-operator if the creating user has the vdc-admin role.
Default user roles in the default VDC	Network-operator.
Default user roles in the non-default VDCs	Vdc-operator.
Interface policy	All interfaces are accessible.
VLAN policy	All VLANs are accessible.
VRF policy	All VRFs are accessible.
Feature group	L3.

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.

SUMMARY STEPS

1. **configure terminal**
2. **password strength-check**
3. **exit**
4. (Optional) **show password strength-check**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

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

Related Topics

Characteristics of Strong Passwords, on page 2

Configuring User Accounts

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

You can enter the password in clear text format or encrypted format. The Cisco NX-OS password encrypts clear text passwords before saving them to the running configuration. Encrypted format passwords are saved to the running configuration without further encryption. SHA256 is the hashing algorithm used for password encryption. As a part of the encryption, a 5000 iteration of 64-bit SALT is added to the password.

User accounts can have a maximum of 64 user roles. The user can determine what commands are available by using the command-line interface (CLI) context sensitive help utility.

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

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show role**
3. **username** *user-id* [**password** [**0** | **5**] *password*] [**expire** *date*] [**role** *role-name*]
4. **exit**
5. (Optional) **show user-account**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	(Optional) **show role** **Example:** `switch(config)# show role`	Displays the user roles available. You can configure other user roles, if necessary.
Step 3	**username** *user-id* [**password** [**0** | **5**] *password*] [**expire** *date*] [**role** *role-name*] **Example:** `switch(config)# username NewUser password 4Ty18Rnt`	Configures a user account. The *user-id* argument is a case-sensitive, alphanumeric 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, hypen (-), period (.), underscore (_), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames.

	Command or Action	Purpose
		The default password is undefined. The **0** option indicates that the password is clear text, and the **5** option indicates that the password is encrypted. The default is **0** (clear text). **Note** If you do not specify a password, the user might not be able to log in to the Cisco NX-OS device. **Note** If you create a user account with the encrypted password option, the corresponding SNMP user will not be created. The **expire** *date* option format is YYYY-MM-DD. The default is no expiry date. User accounts can have a maximum of 64 user roles.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show user-account** **Example:** `switch# show user-account`	Displays the role configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Roles, on page 10
Creating User Roles and Rules, on page 11

Configuring Roles

This section describes how to configure user roles.

Enabling User Role Configuration Distribution

To distribute the user roles configuration to other Cisco NX-OS devices in the network, you must first enable CFS distribution for user roles.

SUMMARY STEPS

1. **configure terminal**
2. **role distribute**
3. **exit**

4. (Optional) **show role session status**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**role distribute** **Example:** `switch(config)# role distribute`	Enables user role configuration distribution. The default is disabled.

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

Step 4	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role distribution status information.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating User Roles and Rules

You can configure up to 64 user roles in a VDC. Each user role can have up to 256 rules. You can assign a user role to more than one user account.

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.

Note Regardless of the read-write rule configured for a user role, some commands can be executed only through the predefined network-admin and vdc-admin roles. For more information on user roles, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Note Whenever a user role or privilege of a user account is changed, the changed role shall come into effect for subsequent logins only.

Before you begin

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **rule** *number* {**deny** | **permit**} **command** *command-string*
4. **rule** *number* {**deny** | **permit**} {**read** | **read-write**}
5. **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*
6. **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*
7. (Optional) **description** *text*
8. **exit**
9. (Optional) **show role**
10. (Optional) **show role** {**pending** | **pending-diff**}
11. (Optional) **role commit**
12. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**role name** *role-name*
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode. The *role-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.

Step 3	**rule** *number* {**deny**	**permit**} **command** *command-string* **Example:** `switch(config-role)# rule 1 deny command clear users`	Configures a command rule. The *command-string* argument can contain spaces and regular expressions. For example, interface ethernet includes all Ethernet interfaces. Repeat this command for as many rules as needed. For more information about guidelines for this command, see Guidelines and Limitations for User Accounts and RBAC, on page 6.
Step 4	**rule** *number* {**deny**	**permit**} {**read**	**read-write**} **Example:** `switch(config-role)# rule 2 deny read-write`	Configures a read-only or read-and-write rule for all operations.
Step 5	**rule** *number* {**deny**	**permit**} {**read**	**read-write**} **feature** *feature-name*	Configures a read-only or read-and-write rule for a feature.

	Command or Action	Purpose
	Example: `switch(config-role)# rule 3 permit read feature router-bgp`	Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
Step 6	**rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **Example:** `switch(config-role)# rule 4 deny read-write feature-group L3`	Configures a read-only or read-and-write rule for a feature group. Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.
Step 7	(Optional) **description** *text* **Example:** `switch(config-role)# description This role does not allow users to use clear commands`	Configures the role description. You can include spaces in the description.

Step 8	**exit**
	Example:
	`switch(config-role)# exit`
	`switch(config)#`
		Exits role configuration mode.

Step 9	(Optional) **show role** **Example:** `switch(config)# show role`	Displays the user role configuration.
Step 10	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 11	(Optional) **role commit** **Example:** `switch(config)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Committing the User Role Configuration to Distribution, on page 20

Creating Feature Groups

You can create custom feature groups to add to the default list of features provided by the Cisco NX-OS software. These groups contain one or more of the features. You can create up to 64 feature groups in a VDC.

Note You cannot change the default feature group L3.

Before you begin

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role feature-group name** *group-name*
3. **feature** *feature-name*
4. **exit**
5. (Optional) **show role feature-group**
6. (Optional) **show role** {**pending** | **pending-diff**}
7. (Optional) **role commit**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**role feature-group name** *group-name*
	Example:
	`switch(config)# role feature-group name GroupA`
	`switch(config-role-featuregrp)#`
		Specifies a user role feature group and enters role feature group configuration mode.
		The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.

Step 3	**feature** *feature-name* **Example:** `switch(config-role-featuregrp)# feature vdc`	Specifies a feature for the feature group. Repeat this command for as many features as needed. **Note** Use the **show role component** command to display a list of features.

Step 4	**exit**
	Example:
	`switch(config-role-featuregrp)# exit`
	`switch(config)#`
		Exits role feature group configuration mode.

Step 5	(Optional) **show role feature-group** **Example:** `switch(config)# show role feature-group`	Displays the role feature group configuration.

	Command or Action	Purpose
Step 6	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 7	(Optional) **role commit** **Example:** `switch(config)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Committing the User Role Configuration to Distribution, on page 20

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.

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **interface policy deny**
4. **permit interface** *interface-list*
5. **exit**
6. (Optional) **show role**
7. (Optional) **show role** {**pending** \| **pending-diff**}
8. (Optional) **role commit**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**role name** *role-name*
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**interface policy deny**
	Example:
	`switch(config-role)# interface policy deny`
	`switch(config-role-interface)#`
		Enters role interface policy configuration mode.

Step 4	**permit interface** *interface-list* **Example:** `switch(config-role-interface)# permit interface ethernet 2/1-4`	Specifies a list of interfaces that the role can access. Repeat this command for as many interfaces as needed.

Step 5	**exit**
	Example:
	`switch(config-role-interface)# exit`
	`switch(config-role)#`
		Exits role interface policy configuration mode.

Step 6	(Optional) **show role** **Example:** `switch(config-role)# show role`	Displays the role configuration.
Step 7	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config-role)# show role pending`	Displays the user role configuration pending for distribution.
Step 8	(Optional) **role commit** **Example:** `switch(config-role)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating User Roles and Rules, on page 11
Committing the User Role Configuration to Distribution, on page 20

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.

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **vlan policy deny**
4. **permit vlan** *vlan-list*
5. **exit**
6. (Optional) **show role**
7. (Optional) **show role** {**pending** | **pending-diff**}
8. (Optional) **role commit**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**role name** *role-name*
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**vlan policy deny**
	Example:
	`switch(config-role)# vlan policy deny`
	`switch(config-role-vlan)#`
		Enters role VLAN policy configuration mode.

Step 4	**permit vlan** *vlan-list* **Example:** `switch(config-role-vlan)# permit vlan 1-4`	Specifies a range of VLANs that the role can access. Repeat this command for as many VLANs as needed.
Step 5	**exit** **Example:**	Exits role VLAN policy configuration mode.

	Command or Action	Purpose
	`switch(config-role-vlan)# exit` `switch(config-role)#`	
Step 6	(Optional) **show role** **Example:** `switch(config)# show role`	Displays the role configuration.
Step 7	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config-role)# show role pending`	Displays the user role configuration pending for distribution.
Step 8	(Optional) **role commit** **Example:** `switch(config-role)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating User Roles and Rules, on page 11
Committing the User Role Configuration to Distribution, on page 20

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.

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **vrf policy deny**
4. **permit vrf** *vrf-name*
5. **exit**
6. (Optional) **show role**
7. (Optional) **show role** {**pending** | **pending-diff**}
8. (Optional) **role commit**

9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**role name** *role-name*
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**vrf policy deny**
	Example:
	`switch(config-role)# vrf policy deny`
	`switch(config-role-vrf)#`
		Enters role VRF policy configuration mode.

Step 4	**permit vrf** *vrf-name* **Example:** `switch(config-role-vrf)# permit vrf vrf1`	Specifies the VRF that the role can access. Repeat this command for as many VRFs as needed.

Step 5	**exit**
	Example:
	`switch(config-role-vrf)# exit`
	`switch(config-role)#`
		Exits role VRF policy configuration mode.

Step 6	(Optional) **show role** **Example:** `switch(config-role)# show role`	Displays the role configuration.
Step 7	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config-role)# show role pending`	Displays the user role configuration pending for distribution.
Step 8	(Optional) **role commit** **Example:** `switch(config-role)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating User Roles and Rules, on page 11
Committing the User Role Configuration to Distribution, on page 20

Committing the User Role Configuration to Distribution

You can apply the user role global and/or server configuration stored in the temporary buffer to the running configuration across all switches in the fabric (including the originating switch).

Before you begin

You have enabled user role configuration distribution on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show role** {**pending** | **pending-diff**}
3. (Optional) **role commit**
4. **exit**
5. (Optional) **show role session status**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	(Optional) **show role** {**pending**	**pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 3	(Optional) **role commit** **Example:** `switch(config)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.

	Command or Action	Purpose
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Applies the running configuration to the startup configuration on all Cisco NX-OS devices in the network that have CFS enabled.

Related Topics

User Role Configuration Distribution, on page 4

Discarding the User Role Distribution Session

You can discard the temporary database of user role changes and end the CFS distribution session.

Before you begin

You have enabled user role configuration distribution on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show role** {**pending** | **pending-diff**}
3. **role abort**
4. **exit**
5. (Optional) **show role session status**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	(Optional) **show role** {**pending**	**pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 3	**role abort** **Example:** `switch(config)# role abort`	Discards the user role configuration in the temporary storage and ends the session.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command or Action	Purpose
Step 5	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.

Related Topics

Committing the User Role Configuration to Distribution, on page 20
User Role Configuration Distribution, on page 4

Clearing the User Role Distribution Session

You can clear the ongoing Cisco Fabric Services distribution session (if any) and unlock the fabric for the user role feature.

You have enabled user role configuration distribution on the Cisco NX-OS device.

SUMMARY STEPS

1. **clear role session**
2. (Optional) **show role session status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear role session** **Example:** `switch# clear role session`	Clears the session and unlocks the fabric.
Step 2	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.

Related Topics

Committing the User Role Configuration to Distribution, on page 20
User Role Configuration Distribution, on page 4

Verifying User Accounts and RBAC Configuration

To display user account and RBAC configuration information, perform one of the following tasks:

Command	Purpose
show cli syntax roles network-admin	Displays the syntax of the commands that the network-admin role can use but the vdc-admin role cannot.

Command	Purpose
show cli syntax roles network-operator	Displays the syntax of the commands that the network-operator role can use but the vdc-operator role cannot.
show role	Displays the user role configuration.
show role feature	Displays the feature list.
show role feature-group	Displays the feature group configuration.
show startup-config security	Displays the user account configuration in the startup configuration.
show running-config security [**all**]	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.
show user-account	Displays user account information.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for User Accounts and RBAC

The following example shows how to configure a user role:

```
role name User-role-A
  rule 3 permit read-write feature l2nac
  rule 2 permit read-write feature dot1x
  rule 1 deny command clear *
```

The following example shows how to create a user role that can configure an interface to enable and show HSRP and show GLBP:

```
role name iftest
   rule 1 permit command config t; interface *; hsrp *
   rule 2 permit read-write feature hsrp
   rule 3 permit read feature glbp
```

In the above example, rule 1 allows you to configure HSRP on an interface, rule 2 allows you to configure the **config hsrp** commands and enable the exec-level **show** and **debug** commands for HSRP, and rule 3 allows you to enable the exec-level **show** and **debug glbp** commands.

The following example shows how to configure a user role that can configure only a specific interface:

```
role name Int_Eth2-3_only
  rule 1 permit command configure terminal; interface *
  interface policy deny
    permit interface Ethernet2/3
```

The following example shows how to configure a user role feature group:

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature l2nac
  feature acl
  feature access-list
```

The following example shows how to configure a user account:

```
username user1 password A1s2D4f5 role User-role-A
```

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 NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

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

Related Documents for User Accounts and RBAC

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards for User Accounts and RBAC

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 for User Accounts and RBAC

MIBs	MIBs Link
• CISCO-COMMON-MGMT-MIB	To locate and download MIBs, go to the following URL: 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 2: Feature History for User Accounts and RBAC

Feature Name	Releases	Feature Information
RBAC	6.0(1)	Added support for F2 Series modules.
User accounts and RBAC	6.0(1)	Added the ability to configure a read-only or read-and-write rule for an SNMP OID.
User accounts and RBAC	5.2(1)	No change from Release 5.1.
User accounts and RBAC	5.2(1)	Added support for the Cisco Nexus 3000 Series Switches.
User roles	5.1(1)	Added the ability to display the syntax of the commands that the network-admin and network-operator roles can use.

Feature Name	Releases	Feature Information
User accounts and RBAC	5.1(1)	No change from Release 5.0.
User accounts and RBAC	5.0(2)	Added the ability to support the at symbol (@) in remote usernames.
User accounts and RBAC	5.0(2)	No change from Release 4.2.
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 (.).