# Configuring User Accounts and RBAC

This chapter contains the following sections:



# Information About User Accounts and RBAC

Cisco Nexus Series switches use role-based access control (RBAC) to define the amount of access each user has when they log into the switch.

With RBAC, you define one or more user roles and then specify which management operations each user role is allowed to perform. When you create a user account for the switch, you associate that account with a user role, which then determines what the individual user is allowed to do on the switch.

## User Account Configuration Restrictions

The following words are reserved and cannot be used to configure users:

| | | | | |
|---|---|---|---|---|
| adm | bin | daemon | ftp | ftpuser |
| games | gdm | gopher | halt | lp |
| mail | mailnull | man | mtsuser | news |
| nobody | nscd | operator | rpc | rpcuser |
| shutdown | sync | sys | uucp | xfs |

**Caution** The Cisco Nexus 3000 Series switch does not support all numeric usernames, even if those usernames were created in TACACS+ or RADIUS. If an all numeric user name exists on an AAA server and is entered during login, the switch reject the login request.

# User Password Requirements

Cisco Nexus 3000 Series passwords are case sensitive can contain alphanumeric characters only. Special characters, such as the dollar sign ($) or the percent sign (%), are not allowed.

If a password is trivial (such as a short, easy-to-decipher password), the Cisco Nexus 3000 Series switch will reject the password. Be sure to configure a strong password for each user account. 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
- 2009AsdfLkj30
- Cb1955S21

**Note** For security reasons, user passwords are not displayed in the configuration files.

# 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 VSANs, VLANs, and interfaces.

The Cisco Nexus Series switch provides the following default user roles:

- network-admin (superuser)—Complete read and write access to the entire Cisco Nexus Series switch.

- network-operator—Complete read access to the Cisco Nexus Series switch.

**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 users also has RoleB, which has access to the configuration commands. In this case, the users has access to the configuration commands.

# About 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 Cisco Nexus 3000 Series switch.
  - Enter the **show role feature** command to display the feature names available for this parameter.
- Feature group—Default or user-defined group of features.
  - Enter the **show role feature-group** command to display the default feature groups available for this parameter.

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 of the rules.

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.

# About User Role Policies

You can define user role policies to limit the switch resources that the user can access. You can define user role policies to limit access to interfaces, VLANs, and VSANs.

User role policies are constrained by the rules defined for the role. For example, if you define an interface policy to permit access to specific interfaces, the user will not have access to the interfaces unless you configure a command rule for the role to permit the interface command.

If a command rule permits access to specific resources (interfaces, VLANs, or VSANs), the user is permitted to access these resources, even if they are not listed in the user role policies associated with that user.

# Guidelines and Limitations for User Accounts

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

- You can add up to 256 rules to a user role.
- You can assign a maximum of 64 user roles to a user account.

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

# Configuring User Accounts

You can create a maximum of 256 user accounts on a Cisco Nexus Series switch. User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

User accounts can have a maximum of 64 user roles.

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

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch(config)# **show role** | (Optional)<br>Displays the user roles available. You can configure other user roles, if necessary. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | switch# **configure terminal** | Enters configuration mode. |
| **Step 3** | switch(config)# **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*] | Configures a user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters.<br>The default password is undefined.<br>**Note** If you do not specify a password, the user might not be able to log in to the Cisco Nexus 3000 Series switch.<br>The expire *date* option format is YYYY-MM-DD. The default is no expiry date. |
| **Step 4** | switch# **show user-account** | (Optional)<br>Displays the role configuration. |
| **Step 5** | switch# **copy running-config startup-config** | (Optional)<br>Copies the running configuration to the startup configuration. |

The following example shows how to configure a user account:

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt

switch(config)# exit
switch# show user-account
```

# Configuring RBAC

## Creating User Roles and Rules

Each user role can have up to 256 rules. You can assign a user role to more that one user account.

The rule number 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.

## SUMMARY STEPS

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

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **role name** *role-name* | 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** | switch(config-role)# **rule** *number* {**deny** \| **permit**} **command** *command-string* | Configures a command rule.<br>The *command-string* argument can contain spaces and regular expressions. For example, "interface ethernet *" includes all Ethernet interfaces.<br>Repeat this command for as many rules as needed. |
| **Step 4** | switch(config-role)# **rule** *number* {**deny** \| **permit**} {**read** \| **read-write**} | Configures a read only or read and write rule for all operations. |
| **Step 5** | switch(config-role)# **rule** *number* {**deny** \| **permit**} {**read** \| **read-write**} **feature** *feature-name* | Configures a read-only or read-and-write rule for a feature.<br>Use the **show role feature** command to display a list of features.<br>Repeat this command for as many rules as needed. |
| **Step 6** | switch(config-role)# **rule** *number* {**deny** \| **permit**} {**read** \| **read-write**} **feature-group** *group-name* | Configures a read-only or read-and-write rule for a feature group.<br>Use the **show role feature-group** command to display a list of feature groups.<br>Repeat this command for as many rules as needed. |
| **Step 7** | switch(config-role)# **description** *text* | (Optional)<br>Configures the role description. You can include spaces in the description. |
| **Step 8** | switch# **show role** | (Optional)<br>Displays the user role configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | switch# **copy running-config startup-config** | (Optional)<br>Copies the running configuration to the startup configuration. |

The following example shows how to create user roles and specify rules:

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule deny command clear users
switch(config-role)# rule deny read-write
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# end
switch(config)# show role
```

# Creating Feature Groups

You can create feature groups.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role feature-group** *group-name*
3. (Optional) switch# **show role feature-group**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **role feature-group** *group-name* | Specifies a user role feature group and enters role feature group configuration mode.<br>The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters. |
| **Step 3** | switch# **show role feature-group** | (Optional)<br>Displays the role feature group configuration. |
| **Step 4** | switch# **copy running-config startup-config** | (Optional)<br>Copies the running configuration to the startup configuration. |

# Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role name** *role-name*
3. switch(config-role)# **interface policy deny**
4. switch(config-role-interface)# **permit interface** *interface-list*
5. switch(config-role-interface)# **exit**
6. (Optional) switch(config-role)# **show role**
7. (Optional) switch(config-role)# **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **role name** *role-name* | Specifies a user role and enters role configuration mode. |
| **Step 3** | switch(config-role)# **interface policy deny** | Enters role interface policy configuration mode. |
| **Step 4** | switch(config-role-interface)# **permit interface** *interface-list* | Specifies a list of interfaces that the role can access.<br>Repeat this command for as many interfaces as needed.<br>For this command, you can specify Ethernet interfaces, Fibre Channel interfaces, and virtual Fibre Channel interfaces. |
| **Step 5** | switch(config-role-interface)# **exit** | Exits role interface policy configuration mode. |
| **Step 6** | switch(config-role)# **show role** | (Optional)<br>Displays the role configuration. |
| **Step 7** | switch(config-role)# **copy running-config startup-config** | (Optional)<br>Copies the running configuration to the startup configuration. |

The following example shows how to change a user role interface policy to limit the interfaces that the user can access:

```
switch# configure terminal
switch(config)# role name UserB
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface fc 3/1
switch(config-role-interface)# permit interface vfc 30/1
```

You can specify a list of interfaces that the role can access. You can specify it for as many interfaces as needed.

# Changing User Role VLAN Policies

You can change a user role VLAN policy to limit the VLANs that the user can access.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **role name** *role-name*
3. switch(config-role)# **vlan policy deny**
4. switch(config-role-vlan)# **permit vlan** *vlan-list*
5. (Optional) switch# **show role**
6. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **role name** *role-name* | Specifies a user role and enters role configuration mode. |
| **Step 3** | switch(config-role)# **vlan policy deny** | Enters role VLAN policy configuration mode. |
| **Step 4** | switch(config-role-vlan)# **permit vlan** *vlan-list* | Specifies a range of VLANs that the role can access.<br>Repeat this command for as many VLANs as needed. |
| **Step 5** | switch# **show role** | (Optional)<br>Displays the role configuration. |
| **Step 6** | switch# **copy running-config startup-config** | (Optional)<br>Copies the running configuration to the startup configuration. |

# Verifying User Accounts and RBAC Configuration

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

| Command | Purpose |
|---|---|
| switch# **show role** | Displays the user role configuration |
| switch# **show role feature** | Displays the feature list. |
| switch# **show role feature-group** | Displays the feature group configuration. |
| switch# **show startup-config security** | Displays the user account configuration in the startup configuration. |

| Command | Purpose |
|---|---|
| switch# **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. |
| switch# **show user-account** | Displays user account information. |

# Default User Account and RBAC Settings

The following 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. |
| Interface policy | All interfaces are accessible. |
| VLAN policy | All VLANs are accessible. |
| VFC policy | All VFCs are accessible. |
| VETH policy | All VETHs are accessible. |