



Configuring User Accounts and RBAC

This chapter contains the following sections:

- [Configuring User Accounts and RBAC, page 1](#)

Configuring User Accounts and RBAC

This section describes how to configure user accounts and role-based access control (RBAC) on the Cisco Nexus 5000 Series switch.

Information About User Accounts and RBAC

You can create and manage users accounts and assign roles that limit access to operations on the Cisco Nexus 5000 Series switch. 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



Tip

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



Note

User passwords are not displayed in the configuration files.



Caution

The Cisco Nexus 5000 Series switch does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Characteristics of Strong Passwords

A strong password has the following characteristics:

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

The following are examples of strong passwords:

- If2CoM18
- 2009AsdfLkj30
- Cb1955S21

**Note**

Clear text passwords can contain alphanumeric characters only. Special characters, such as the dollar sign (\$) or the percent sign (%), are not allowed.

**Tip**

If a password is trivial (such as a short, easy-to-decipher password), the Cisco Nexus 5000 Series switch will reject your password configuration. 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 VSANs, VLANs and interfaces.

The Cisco Nexus 5000 Series switch provides the following default user roles:

- network-admin (superuser)—Complete read and write access to the entire Cisco Nexus 5000 Series switch.
- network-operator—Complete read access to the Cisco Nexus 5000 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 5000 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.

Related Topics

- [Changing User Role Interface Policies, page 7](#)

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 5000 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.

To configure a user account, perform this task:

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	<code>switch(config)# show role</code>	(Optional) Displays the user roles available. You can configure other user roles, if necessary.
Step 2	<code>switch# configure terminal</code>	Enters configuration mode.
Step 3	<code>switch(config)# username user-id [password password] [expire date] [role role-name]</code>	Configures a user account. The <i>user-id</i> argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. The default password is undefined.

	Command or Action	Purpose
		Note If you do not specify a password, the user might not be able to log in to the Cisco Nexus 5000 Series switch. The expire <i>date</i> option format is YYYY-MM-DD. The default is no expiry date.
Step 4	switch# show user-account	(Optional) Displays the role configuration.
Step 5	switch# copy running-config startup-config	(Optional) 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 than 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.

	Command or Action	Purpose
Step 2	<code>switch(config)# role name <i>role-name</i></code>	Specifies a user role and enters role configuration mode. The <i>role-name</i> argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.
Step 3	<code>switch(config-role)# rule number {deny permit} command <i>command-string</i></code>	Configures a command rule. The <i>command-string</i> argument can contain spaces and regular expressions. For example, "interface ethernet *" includes all Ethernet interfaces. Repeat this command for as many rules as needed.
Step 4	<code>switch(config-role)# rule number {deny permit} {read read-write}</code>	Configures a read only or read and write rule for all operations.
Step 5	<code>switch(config-role)# rule number {deny permit} {read read-write} feature <i>feature-name</i></code>	Configures a read-only or read-and-write rule for a feature. Use the show role feature command to display a list of features. Repeat this command for as many rules as needed.
Step 6	<code>switch(config-role)# rule number {deny permit} {read read-write} feature-group <i>group-name</i></code>	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	<code>switch(config-role)# description <i>text</i></code>	(Optional) Configures the role description. You can include spaces in the description.
Step 8	<code>switch# show role</code>	(Optional) Displays the user role configuration.
Step 9	<code>switch# copy running-config startup-config</code>	(Optional) 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 <i>group-name</i>	Specifies a user role feature group and enters role feature group configuration mode. The <i>group-name</i> argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.
Step 3	switch# show role feature-group	(Optional) Displays the role feature group configuration.
Step 4	switch# copy running-config startup-config	(Optional) 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 <i>role-name</i>	Specifies a user role and enters role configuration mode.

	Command or Action	Purpose
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. Repeat this command for as many interfaces as needed. 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) Displays the role configuration.
Step 7	switch(config-role)# copy running-config startup-config	(Optional) 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.

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

Changing User Role VSAN Policies

You can change a user role VSAN policy to limit the VSANs that the user can access.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config-role)# **role name** *role-name*
3. switch(config-role)# **vsan policy deny**
4. switch(config-role-vsan)# **permit vsan** *vsan-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)# role name <i>role-name</i>	Specifies a user role and enters role configuration mode.
Step 3	switch(config-role)# vsan policy deny	Enters role VSAN policy configuration mode.
Step 4	switch(config-role-vsan)# permit vsan <i>vsan-list</i>	Specifies a range of VSANs that the role can access. Repeat this command for as many VSANs as needed.
Step 5	switch# show role	(Optional) Displays the role configuration.
Step 6	switch# copy running-config startup-config	(Optional) 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.
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.