



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:

- [About User Accounts and RBAC, on page 1](#)
- [Licensing Requirements for User Accounts and RBAC, on page 5](#)
- [Guidelines and Limitations for User Accounts and RBAC, on page 5](#)
- [Default Settings for User Accounts and RBAC, on page 5](#)
- [Enabling Password-Strength Checking, on page 6](#)
- [Configuring User Accounts, on page 7](#)
- [Configuring Roles, on page 9](#)
- [Verifying User Accounts and RBAC Configuration, on page 15](#)
- [Configuration Examples for User Accounts and RBAC, on page 15](#)
- [Additional References for User Accounts and RBAC, on page 17](#)

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 rules for assigned roles that restrict the authorization a 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.

These 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
- sys

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 or, starting with Cisco NX-OS Release 7.0(3)I2(2), an underscore (_). Usernames can contain only these special characters: (+ = . _ \ -). The #, @, and ! symbols are not supported. If you use any other characters, the specified user cannot log in.

Characteristics of Strong Passwords

This section explains strong passwords and their essential attributes for securing access to network devices such as NX-OS systems.

A strong password is a password type that

- is at least eight characters long,
- contains both uppercase and lowercase letters and numbers, and
- avoids dictionary words, personal information, consecutive or repeating characters.

Special characters, such as the dollar sign (\$) or percent sign (%), can be used in Cisco Nexus device passwords. All printable ASCII characters are allowed if enclosed in quotation marks.

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Additional reference information

- Clear text passwords cannot start with: quotation marks (" or '), vertical bars (|), or right angle brackets (>).
- Trivial passwords (such as short or easily decoded values) are rejected if password-strength checking is enabled.
- Passwords are case-sensitive.

Related Topics

[Enabling Password-Strength Checking](#), on page 6

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 a user who belongs to both role1 and role2 can access both configuration and debug operations. You can also limit access to specific virtual routing and forwarding instances (VRFs), VLANs, and interfaces.

The Cisco NX-OS software provides these user roles:

- network-admin—Complete read-and-write access to the entire Cisco NX-OS device
- network-operator or vdc-operator—Complete read access to the entire Cisco NX-OS device



-
- Note**
- The Cisco Nexus 9000 Series switches support a single VDC. Therefore, the vdc-admin has the same privileges and limitations as the network-admin.
 - The Cisco Nexus 9000 Series switches support a single VDC due to which the vdc-admin has the same privileges and limitations as the network-admin.
-



Note You cannot change the user roles.



Note Some **show** commands may be hidden from network-operator users. Some non- **show** commands, such as **telnet** , may be available for this user role.

By default, the user accounts without an administrator role can access only the **show** , **exit** , **end** , and **configure terminal** commands. You can add rules to allow users to configure features.



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 denies access to configuration commands, and RoleB, which allows access to configuration commands. In this case, the user has access to configuration 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 these parameters:

- Command—command or group of commands defined in a regular expression,
- Feature—command or group of commands defined in a regular expression,
- Feature group—default or user-defined group of features, and
- OID—an SNMP object identifier (OID).

The command, feature, and feature group parameters form a hierarchy. The command is the most basic control parameter. The feature parameter represents all commands associated with a feature. The feature group is the highest-level control parameter, combining related features for simplified rule management. The Cisco NX-OS software supports the predefined feature group L3 for your use.

SNMP OID is supported for RBAC. You can configure a read-only or read-and-write rule for an SNMP OID.

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.

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 nx-os image and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

Guidelines and Limitations for User Accounts and RBAC

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

- You can add up to 256 rules to a user role.
- You can add up to 64 user-defined feature groups in addition to the default feature group, L3.
- You can configure up to 256 users.
- 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 **configure terminal** command is always permitted and is not affected by any applied rules.
- The network-operator role cannot run the **show running-config** and **show startup-config** commands.
- The Cisco Nexus 9000 Series switches support a single VDC due to which the vdc-admin has the same privileges and limitations as the network-admin.



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	Network-operator, if the creating user has the network-admin role
Default user role	Network-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. This feature prevents the creation of 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

Step 1 Enter the global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Enable password-strength checking.

Example:

```
switch(config)# password strength-check
```

Password-strength checking is enabled by default. To disable it, use the **no** form of this command.

Step 3 Exit the global configuration mode.

Example:

```
switch(config)# exit
switch#
```

Step 4 (Optional) Display the password-strength check configuration.

Example:

```
switch# show password strength-check
```

Step 5 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch# copy running-config startup-config
```

Related Topics

[Characteristics of Strong Passwords](#), on page 3

Configuring User Accounts

You can create a maximum of 256 user accounts on a Cisco NX-OS device. User accounts have these 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. Beginning with Cisco NX-OS Release 7.0(3)I2(1), the SHA256 hashing method, which is stronger than MD5 hashing, is used to encrypt user passwords. 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 available commands by using the 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.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 (Optional) Display the available user roles.

Example:

```
switch(config)# show role
```

You can configure other user roles, if necessary.

Step 3 Configure a user account.

Example:

```
switch(config)# username NewUser password 4Tyl8Rnt
```

The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters for both local and remote users .

Valid characters include uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, a hyphen (-), a period (.), an underscore (_), a plus sign (+), and an equal sign (=). The at symbol (@) is supported in usernames.

Usernames must begin with an underscore (_) (supported starting with Cisco NX-OS Release 7.0(3)I2(2)) or an alphanumeric character.

The default password is undefined. The **0** option indicates that the password is clear text, and the **5** option indicates that the password is SHA-256 hashed . By default, the password type 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 Specify if an SSH X.509 certificate distinguished name and DSA or RSA algorithm must be used to authenticate an existing user account.

Example:

```
switch(config)# username NewUser ssh-cert-dn "/CN = NewUser, OU = Cisco Demo, O = Cisco, C = US" rsa
```

Example:

```
switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa
```

The distinguished name can be up to 512 characters and must use the format shown in the examples. Make sure the email address and state are configured as "emailAddress" and "ST", respectively.

Step 5 Exit the global configuration mode.

Example:

```
switch(config)# exit
switch#
```

Step 6 (Optional) Display the role configuration.

Example:

```
switch# show user-account
```

Step 7 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch# copy running-config startup-config
```

Related Topics

[Configuring Roles](#), on page 9

[Configure User Roles and Rules](#), on page 9

Configuring Roles

This section describes how to configure user roles.

Configure User Roles and Rules

- Use this procedure to create user roles and rules in NX-OS.

You can configure up to 64 user roles. 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.

When processing an RBACL for a match, a partial match does not stop the evaluation process. Evaluation continues through each rule until an exact match is found. If no exact match is found, the most precise rule in the list will be chosen for the result. Also, if a permit and deny rule exists for the same match logic, the higher numbered rule (evaluated first) will be chosen for the result.



Note Regardless of the read-write rule configured for a user role, some commands can be executed only by using the predefined network-admin role.

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.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Specify a user role and enters role configuration mode.

Example:

```
switch(config)# role name UserA
switch(config-role)#
```

The *role-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.

Step 3 Configure from these available options.

- Configure a command rule.
- Configure a read-only or read-and-write rule for all operations.
- Configure a read-only or read-and-write rule for a feature.
- Configure a read-only or read-and-write rule for a feature group.
- Configure a read-only or read-and-write rule for an SNMP object identifier (OID).

Example:

```
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 2 deny read-write
switch(config-role)# rule 3 permit read feature router-bgp
switch(config-role)# rule 4 deny read-write feature-group L3
switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9
```

The *command-string* argument can contain spaces and regular expressions. For example, interface ethernet includes all Ethernet interfaces.

Use the **show role feature** command to display a list of features.

Use the **show role feature-group** command to display a list of feature groups.

You can enter up to 32 elements for the OID. The **rule <num> deny read-write oid** command can be used to allow SNMP-based performance monitoring tools to poll devices but restrict their access to system-intensive branches such as the IP routing table, MAC address tables, specific MIBs, and so on.

Note

The deepest OID can be at the scalar level or at the table root level.

Repeat the commands for each rule you need to configure.

Step 4 (Optional) Configure the role description. You can include spaces in the description.

Example:

```
switch(config-role)# description This role does not allow users to use clear commands
```

Step 5 Exit the role configuration mode.

Example:

```
switch(config-role)# exit
switch(config)#
```

Step 6 (Optional) Display the user role configuration.

Example:

```
switch(config)# show role
```

Step 7 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch(config)# copy running-config startup-config
```

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.



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.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Specify a user role feature group and enters role feature group configuration mode.

Example:

```
switch(config)# role feature-group name GroupA
switch(config-role-featuregrp)#
```

The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.

Step 3 Specify a feature for the feature group.

Example:

```
switch(config-role-featuregrp)# feature radius
```

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 the role feature group configuration mode.

Example:

```
switch(config-role-featuregrp)# exit
switch(config)#
```

Step 5 (Optional) Display the role feature group configuration.

Example:

```
switch(config)# show role feature-group
```

Step 6 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch(config)# copy running-config startup-config
```

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.

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.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Specify a user role and enters role configuration mode.

Example:

```
switch(config)# role name UserA
switch(config-role)#
```

Step 3 Enter the role interface policy configuration mode.

Example:

```
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

Step 4 Specify a list of interfaces that the role can access.

Example:

```
switch(config-role-interface)# permit interface ethernet 2/1-4
```

Repeat this command for as many interfaces as needed.

Step 5 Exit the role interface policy configuration mode.

Example:

```
switch(config-role-interface)# exit
switch(config-role)#
```

Step 6 (Optional) Display the role configuration.

Example:

```
switch(config-role)# show role
```

Step 7 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch(config-role)# copy running-config startup-config
```

Related Topics

[Configure User Roles and Rules](#), on page 9

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.

Before you begin

Create one or more user roles.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Specify a user role and enters role configuration mode.

Example:

```
switch(config)# role name UserA
switch(config-role)#
```

Step 3 Enter role VLAN policy configuration mode.

Example:

```
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

Step 4 Specify a range of VLANs that the role can access.

Example:

```
switch(config-role-vlan)# permit vlan 1-4
```

Repeat this command for as many VLANs as needed.

Step 5 Exit the role VLAN policy configuration mode.

Example:

```
switch(config-role-vlan)# exit
switch(config-role)#
```

Step 6 (Optional) Display the role configuration.

Example:

```
switch(config)# show role
```

Step 7 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch(config-role)# copy running-config startup-config
```

Related Topics

[Configure User Roles and Rules](#), on page 9

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.

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	role name <i>role-name</i> 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 <i>vrf-name</i> 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:	Displays the role configuration.

	Command or Action	Purpose
	<code>switch(config-role)# show role</code>	
Step 7	(Optional) copy running-config startup-config Example: <code>switch(config-role)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Related Topics

[Configure User Roles and Rules](#), on page 9

Verifying User Accounts and RBAC Configuration

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

Command	Purpose
<code>show cli syntax roles network-admin</code>	Displays the syntax of the commands that the network-admin role can use.
<code>show cli syntax roles network-operator</code>	Displays the syntax of the commands that the network-operator role can use.
<code>show role</code>	Displays the user role configuration.
<code>show role feature</code>	Displays the feature list.
<code>show role feature-group</code>	Displays the feature group configuration.
<code>show startup-config security</code>	Displays the user account configuration in the startup configuration.
<code>show running-config security [all]</code>	Displays the user account configuration in the running configuration. The all keyword displays the default values for the user accounts.
<code>show user-account</code>	Displays user account information.

Configuration Examples for User Accounts and RBAC

The following example shows how to configure a user role:

```

role name User-role-A
  rule 2 permit read-write feature bgp
  rule 1 deny command clear *

```

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

```

role name iftest
  rule 1 permit command config t; interface *; bgp *
  rule 2 permit read-write feature bgp
  rule 3 permit read feature eigrp

```

In the above example, rule 1 allows you to configure BGP on an interface, rule 2 allows you to configure the **config bgp** command and enable the exec-level **show** and **debug** commands for BGP, and rule 3 allows you to enable the exec-level **show** and **debug eigrp** 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 aaa
  feature acl
  feature access-list

```

The following example shows how to configure a user account:

```

username user1 password A1s2D4f5 role User-role-A

```

The following example shows how to add an OID rule to restrict access to part of the OID subtree:

```

role name User1
  rule 1 permit read feature snmp
  rule 2 deny read oid 1.3.6.1.2.1.1.9
show role name User1

```

```

Role: User1
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)

```

Rule	Perm	Type	Scope	Entity
2	deny	read	oid	1.3.6.1.2.1.1.9
1	permit	read	feature	snmp

The following example shows how to give write permission to a specified OID subtree:

```

role name User1
rule 3 permit read-write oid 1.3.6.1.2.1.1.5
show role name User1

```

```

Role: User1
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)

```

```

-----
Rule      Perm      Type      Scope      Entity
-----
3         permit   read-write  oid        1.3.6.1.2.1.1.5
2         deny     read       oid        1.3.6.1.2.1.1.9
1         permit   read       feature    snmp

```

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	<i>Cisco NX-OS Licensing Guide</i>
VRF configuration	<i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i>

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
MIBs related to user accounts and RBAC	To locate and download supported MIBs, go to the following URL: https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

