

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
- Guidelines and Limitations for User Accounts and RBAC, on page 4
- Default Settings for User Accounts and RBAC, on page 5
- Enabling Password-Strength Checking, on page 6
- Enabling Consecutive Characters Check in Passwords, on page 6
- Configuring User Accounts, on page 7
- Configuring Roles, on page 10
- About No Service Password-Recovery, on page 17
- Enabling No Service Password-Recovery, on page 18
- Verifying User Accounts and RBAC Configuration, on page 19
- Configuration Examples for User Accounts and RBAC, on page 20
- Additional References for User Accounts and RBAC, on page 21

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.

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.



Usernames must begin with an alphanumeric character and 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.

Characteristics of Strong Passwords

A strong password has the following characteristics:



Note

Special characters, such as the dollar sign (\$) or the percent sign (%), can be used in Cisco Nexus device passwords.

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

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21



Note Clear text passwords cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>). 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.



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

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 users who belong to both role1 and role2 can access 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 the following 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 do not support multiple VDCs; however, the vdc-operator role is available and has the same privileges and limitations as the network-operator role.

• 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. In addition, 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 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.

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.

OID

An SNMP object identifier (OID).

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.

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.

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 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.
- As per the AAA policy, if a role is associated as a last role with an user, then that role cannot be deleted until it is disassociated from that user.



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.

• Beginning with Cisco NX-OS Release 10.2(2)F, a new desynchronization CLI is introduced to provide you an option to disable the user synchronization between the SNMP and the security components. For more information, refer to the *Configuring SNMP* chapter in the *System Management Configuration Guide*.

For more information about the Cisco Nexus 9000 switches that support various features spanning from release 7.0(3)I7(1) to the current release, refer to Nexus Switch Platform Support Matrix.

- When the desynchronization CLI is enabled, remote users will not be synced to SNMP database.
- The security users created using DCNM (also called as Nexus Dashboard Fabric Controller from Release 12.0.1a) will not have a corresponding SNMPv3 profile when the desynchronization CLI is enabled. When the synchronization is disabled, the users created on the security component can log in to the switch, but the switches will not be discovered by the controller, as the controller uses the SNMP configuration created for the security user to discover the switch. Furthermore, the SNMP does not recognize the security users created due to the desynchronized state of the userDB, resulting in failure to discover the switch. Therefore, to have the switches discovered by the controller, the SNMP user must be explicitly created. It is not recommended to use the desynchronization CLI along with DCNM functionality. For more information, refer to the *Cisco Nexus 9000 NX-OS Security Configuration Guide*.
- Beginning with Cisco NX-OS Release 10.3(1)F, the type 8 and type 9 password hash is supported on Cisco Nexus 9000 Series switches.



```
Note
```

Type 8 and type 9 cannot be downgraded though type 5 supports downward compatibility.

• Beginning with Cisco NX-OS Release 10.3(1)F, the consecutive characters check in passwords is supported on Cisco Nexus 9000 Series switches.

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 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.

	Command or Action	Purpose	
Step 1	configure terminal	Enters global configuration mode.	
	Example:		
	<pre>switch# configure terminal switch(config)#</pre>		
Step 2	password strength-check	Enables password-strength checking. The default is enabled.	
	<pre>switch(config)# password strength-check</pre>	You can disable password-strength checking by using the no form of this command.	
Step 3	exit	Exits global configuration mode.	
	Example:		
	<pre>switch(config)# exit switch#</pre>		
Step 4	(Optional) show password strength-check	Displays the password-strength check	
	Example:	configuration.	
	switch# show password strength-check		
Step 5	(Optional) copy running-config startup-config	Copies the running configuration to the startup	
	Example:	configuration.	
	switch# copy running-config startup-config		

Procedure

Related Topics

Characteristics of Strong Passwords, on page 2

Enabling Consecutive Characters Check in Passwords

The password sequence keyboard length and alphabet length are imposed restrictions as they are vulnerable to attacks.

Following length limit of password string sequences are imposed on the password:

- Number of repeated characters based on configurable value (aaaa, bbbb, etc)
- Number of consecutive alphabetical/numeric sequence characters (abcd, 1234,..)
- Number of consecutive keyboard sequence characters (qwer, asdf..)

This procedure describes how to configure the limits for password sequences.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	[no] userpassphrase sequence alphabet length Value	Configures the limit of sequence alphabet length. The range for sequence alphabet length is 2-10.
	switch(config)#userpassphrase sequence alphabet length 4	Example: userpassphrase sequence alphabet length 4
		username user password AbcDe19jd
		Password characters are sequential, hence cannot be accepted.
		The no option disables the alphabet sequence check.
Step 3	[no] userpassphrase sequence keyboard length Value	Configures the limit of sequence keyboard length. The range for sequence alphabet length
	Example:	
	<pre>switch(config)# userpassphrase sequence keyboard length 4</pre>	length 4
		username user password CvBnmwu204
		Password characters are sequential, hence cannot be accepted.
		The no option disables the keyboard sequence check.

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.

SHA256 is the default hashing algorithm used for password encryption. To generate a hash for type 8 and type 9 password, you must provide PBKDF2/SCRYPT option along with clear text 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.

	Command or Action	Purpose
Step 1	<pre>configure terminal Example: switch# configure terminal switch(config)#</pre>	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	<pre>username user-id [password [0 5 8 9] password [pbkdf2 scrypt]] [expire date] [role role-name] Example: switch(config)# username NewUser password 4Ty18Rnt</pre>	Configures a user account. The <i>user-id</i> 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, hyphen (-), period (.), underscore (_), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames. Usernames must begin with an alphanumeric character. The default password is undefined. • The 0 option indicates that the password is clear text • The 5 option indicates that the password is encrypted.

	Command or Action	Purpose	
		• The 8 is PBK • The 9 is Scry	option indicates that the password XDF2 hashed. option indicates that the password /pt hashed.
		The default	option is 0 (clear text).
		Note	The pbkdf2/scrypt keywords are optional and are note stored in running configurations.
		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.
		Note	When the desynchronization CLI is enabled, if you create a user account, the corresponding SNMP user will not be created.
		The expire YYYY-MN	<i>date</i> option format is <i>A</i> -DD. The default is no expiry date.
		User accoun roles.	nts can have a maximum of 64 user
Step 4	<pre>username user-id ssh-cert-dn dn-name {dsa rsa} 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</pre>	Specifies an name and E authenticati distinguishe and must fo examples. M are configu respectively	SSH X.509 certificate distinguished DSA or RSA algorithm to use for on for an existing user account. The ed name can be up to 512 characters blow the format shown in the Make sure the email address and state red as emailAddress and ST, y.
Step 5	exit Example: switch(config)# exit switch#	Exits globa	l configuration mode.

	Command or Action	Purpose
Step 6	(Optional) show user-account	Displays the role configuration.
	Example:	
	switch# show user-account	
Step 7	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	switch# copy running-config startup-config	

Related Topics

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

Configuring Roles

This section describes how to configure user roles.

Creating User Roles and Rules

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 through 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.

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

I

	Command or Action	Purpose
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	<pre>role name role-name Example: switch(config)# role name UserA switch(config-role)#</pre>	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	rule number {deny permit} command	Configures a command rule.
	Example: switch(config-role)# rule 1 deny command clear users	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	rule number {deny permit} {read read-write}	Configures a read-only or read-and-write rule for all operations.
	Example:	
	<pre>switch(config-role)# rule 2 deny read-write</pre>	
Step 5	rule number {deny permit} {read read-write} feature feature-name	Configures a read-only or read-and-write rule for a feature.
	Example:	Use the show role feature command to display
	<pre>switch(config-role)# rule 3 permit read feature router-bgp</pre>	Repeat this command for as many rules as needed.
Step 6	rule number {deny permit} {read read-write} feature-group group-name	Configures a read-only or read-and-write rule for a feature group.
	Example: switch(config-role)# rule 4 deny	Use the show role feature-group command to display a list of feature groups.
	read-write feature-group L3	Repeat this command for as many rules as needed.
Step 7	<pre>rule number {deny permit} {read read-write} oid snmp_oid_name</pre>	Configures a read-only or read-and-write rule for an SNMP object identifier (OID). You can
	<pre>Example: switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9</pre>	enter up to 32 elements for the OID. This 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

	Command or Action	Purpose
		Repeat this command for as many rules as needed.
Step 8	(Optional) description text	Configures the role description. You can
	Example:	include spaces in the description.
	<pre>switch(config-role)# description This role does not allow users to use clear commands</pre>	
Step 9	exit	Exits role configuration mode.
	Example:	
	<pre>switch(config-role)# exit switch(config)#</pre>	
Step 10	(Optional) show role	Displays the user role configuration.
	Example:	
	switch(config)# show role	
Step 11	(Optional) show role { pending pending-diff }	Displays the user role configuration pending for distribution.
	Example:	
	switch(config)# show role pending	
Step 12	(Optional) role commit	Applies the user role configuration changes in
	Example:	the temporary database to the running
	switch(config)# role commit	comparation.
Step 13	(Optional) copy running-config startup-config	Copies the running configuration to the startup configuration.
	Example:	
	<pre>switch(config)# copy running-config startup-config</pre>	

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.



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.

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	role feature-group name group-name	Specifies a user role feature group and enters role feature group configuration mode.
	<pre>switch(config)# role feature-group name GroupA switch(config-role-featuregrp)#</pre>	The <i>group-name</i> argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.
Step 3	feature feature-name	Specifies a feature for the feature group.
	<pre>Example: switch(config-role-featuregrp)# feature</pre>	Repeat this command for as many features as needed.
	radius	Note Use the show role component command to display a list of features.
Step 4	exit	Exits role feature group configuration mode.
	Example:	
	<pre>switch(config-role-featuregrp)# exit switch(config)#</pre>	
Step 5	(Optional) show role feature-group	Displays the role feature group configuration.
	Example:	
	<pre>switch(config)# show role feature-group</pre>	
Step 6	(Optional) show role {pending pending-diff}	Displays the user role configuration pending
	Example:	for distribution.
	<pre>switch(config)# show role pending</pre>	
Step 7	(Optional) role commit	Applies the user role configuration changes in
	Example:	the temporary database to the running
	<pre>switch(config)# role commit</pre>	
Step 8	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	<pre>switch(config)# copy running-config startup-config</pre>	

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.

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	role name role-name	Specifies a user role and enters role
	Example:	configuration mode.
	<pre>switch(config)# role name UserA switch(config-role)#</pre>	
Step 3	interface policy deny	Enters role interface policy configuration mode.
	Example:	
	<pre>switch(config-role)# interface policy</pre>	
	<pre>aeny switch(config-role-interface)#</pre>	
Step 4	permit interface interface-list	Specifies a list of interfaces that the role can
	Example:	access.
	<pre>switch(config-role-interface)# permit interface ethernet 2/1-4</pre>	Repeat this command for as many interfaces as needed.
Step 5	exit	Exits role interface policy configuration mode.
	Example:	
	<pre>switch(config-role-interface)# exit switch(config-role)#</pre>	
Step 6	(Optional) show role	Displays the role configuration.
	Example:	
	<pre>switch(config-role)# show role</pre>	
Step 7	(Optional) show role { pending pending-diff }	Displays the user role configuration pending
	Example:	for distribution.
	switch(config-role)# show role pending	

	Command or Action	Purpose
Step 8	(Optional) role commit	Applies the user role configuration changes in
	Example:	the temporary database to the running
	<pre>switch(config-role)# role commit</pre>	
Step 9 (Optional) copy running-config startup-config	Copies the running configuration to the startup	
	Example:	configuration.
	<pre>switch(config-role)# copy running-config startup-config</pre>	

Related Topics

Creating User Roles and Rules, on page 10

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.

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	role name role-name	Specifies a user role and enters role
	Example:	configuration mode.
	<pre>switch(config)# role name UserA switch(config-role)#</pre>	
Step 3	vlan policy deny	Enters role VLAN policy configuration mode.
	Example:	
	<pre>switch(config-role)# vlan policy deny switch(config-role-vlan)#</pre>	
Step 4	permit vlan vlan-list	Specifies a range of VLANs that the role can
	Example:	access.
	<pre>switch(config-role-vlan)# permit vlan 1-4</pre>	Repeat this command for as many VLANs as needed.
Step 5	exit	Exits role VLAN policy configuration mode.
	Example:	

	Command or Action	Purpose
	<pre>switch(config-role-vlan)# exit switch(config-role)#</pre>	
Step 6	(Optional) show role	Displays the role configuration.
	<pre>Example: switch(config)# show role</pre>	
Step 7	<pre>(Optional) show role {pending pending-diff} Example: switch(config-role) # show role pending</pre>	Displays the user role configuration pending for distribution.
Step 8	<pre>(Optional) role commit Example: switch(config-role)# role commit</pre>	Applies the user role configuration changes in the temporary database to the running configuration.
Step 9	<pre>(Optional) copy running-config startup-config Example: switch(config-role)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

Creating User Roles and Rules, on page 10

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.

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
Step 2	role name role-name	Specifies a user role and enters role configuration mode.
	Example:	
	<pre>switch(config)# role name UserA switch(config-role)#</pre>	

I

-	1		
	Command or Action	Purpose	
Step 3	vrf policy deny	Enters role VRF policy configuration mode.	
	Example:		
	<pre>switch(config-role)# vrf policy deny switch(config-role-vrf)#</pre>		
Step 4	permit vrf vrf-name	Specifies the VRF that the role can access.	
	<pre>Example: switch(config-role-vrf)# permit vrf vrf1</pre>	Repeat this command for as many VRFs as needed.	
Step 5	exit	Exits role VRF policy configuration mode.	
	Example:		
	<pre>switch(config-role-vrf)# exit switch(config-role)#</pre>		
Step 6	(Optional) show role	Displays the role configuration.	
	Example:		
	<pre>switch(config-role)# show role</pre>		
Step 7	(Optional) show role {pending pending-diff}	Displays the user role configuration pending	
	Example:	for distribution.	
	<pre>switch(config-role)# show role pending</pre>		
Step 8	(Optional) role commit	Applies the user role configuration changes in	
	Example:	the temporary database to the running	
	<pre>switch(config-role)# role commit</pre>	configuration.	
Step 9	(Optional) copy running-config startup-config	Copies the running configuration to the startup	
	Example:	configuration.	
	<pre>switch(config-role)# copy running-config startup-config</pre>		

Related Topics

Creating User Roles and Rules, on page 10

About No Service Password-Recovery

The No Service Password-Recovery feature enables anyone with console access, the ability to access the router and its network. The No Service Password-Recovery feature prevents the password recovery with standard procedure as described in the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide.

Enabling No Service Password-Recovery

If the no service password-recovery feature is enabled, then none except the administrator with network privileges will be able to modify the administrator password.

Before you begin

If you plan to enter the no service password-recovery command, Cisco recommends that you save a copy of the system configuration file in a location away from the device.

Command or Action	Purpose
configure terminal	Enters global configuration mode.
Example:	
switch# configure terminal switch(config)#	
no service password-recovery	Disables the password recovery mechanism.
Example:	
<pre>switch(config)# no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [####################################</pre>	
(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.
switch# copy running-config startup-config	
Reload	
Example:	
<pre>switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %\$ VDC-1 %\$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface CISCO SWITCH Ver 8.34</pre>	
	Command or Action configure terminal Example: switch# configure terminal switch (config) # no service password-recovery Example: switch (config) # no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch (config) # copy run start [####################################

	Command or Action	Purpose
	CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, switch(boot)# config t Enter configuration commands, one per line. End with CNTL/2.	
	<pre>switch(boot)(config)# admin-password Abcd!123\$ ERROR: service password-recovery disabled. Cannot change password! switch(boot)(config)#</pre>	
Step 5	exit	Exits global configuration mode.
	Example:	
	switch(config)# exit switch#	
Step 6	(Optional) show user-account	Displays the role configuration.
	Example: switch# show user-account	
Step 7	(Optional) copy running-config startup-config	Copies the running configuration to the startup
	Example:	configuration.
	switch# copy running-config startup-config	

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.
show cli syntax roles network-operator	Displays the syntax of the commands that the network-operator role can use.
show role	Displays the user role configuration.
show role feature	Displays the feature list.

Command	Purpose
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.

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)
 _____
                                   Entity
 Rule Perm Type
                    Scope
 _____
 2
     deny read oid
permit read featur
                                   1.3.6.1.2.1.1.9
      permit read
                     feature
 1
                                    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
                                    Entitv
 _____
     permit read-write oid
deny read oid
permit read feature
                                   1.3.6.1.2.1.1.5
 3
                                   1.3.6.1.2.1.1.9
 2
 1
                                   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	Cisco NX-OS Licensing Guide
VRF configuration	Cisco Nexus 9000 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
MIBs related to user accounts and RBAC	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/ Nexus9000MIBSupportList.html