CHAPTER 2

Managing User Accounts

This chapter describes how to configure user accounts and includes the following topics:

Information About User Accounts

Access to the Cisco Nexus 1000V is accomplished by setting up user accounts that define the specific actions permitted by each user. You can create up to 256 user accounts. Each user account includes the following criteria:

Role

A role is a collection of rules that define the specific actions that can be shared by a group of users. The following broadly defined roles, for example, can be assigned to user accounts. These roles are predefined in the Cisco Nexus 1000V and cannot be modified:

```
role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: network-operator
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
description: Predefined network operator role has access to all read
commands on the switch
------------------------------------------------------------------
Rule    Perm    Type        Scope               Entity
------------------------------------------------------------------
1       permit  read
```

You can create an additional 64 roles that define access for users.

Each user account must be assigned at least one role and can be assigned up to 64 roles.

You can create roles that, by default, permit access to the following commands only. You must add rules to allow users to configure features.

- **show**
- **exit**
- **end**
- **configure terminal**

Table 2-1 describes the components that make up a role.

Table 2-1 Role Components

Component	Description

Rule	One of the defined role criteria, such as a command that is permitted or denied. You can add up to 256 rules to each role.
	The following are the rules for the predefined roles:
	• **role: network-admin**
	`Rule Perm Type Scope Entity`
	`1 permit read-write`
	• **role: network-operator**
	`Rule Perm Type Scope Entity`
	`1 permit read-only`

Feature	An individual feature, such as syslog or TACACS+, whose access can be defined in a rule. To see a list of available features, use the **show role feature** command.
Feature Group	A grouping of features whose access can be defined in a rule. You can create up to 64 such groupings. To see a list of available feature groups, use the **show role feature-group** command.
Command	A single command, or group of commands collected in a regular expression, whose access can be defined in a rule. A role permitting access to a command takes precedence over a role that denies access to the command. For example, if a user is assigned a role that denies access to the configuration command, but is also assigned a role that permits access to this command, then access is permitted.

Send document comments to nexus1k-docfeedback@cisco.com.

User Name

A user name identifies an individual user by a unique character string, such as daveGreen. User names are case sensitive and can consist of up to 28 alphanumeric characters. A user name consisting of all numerals is not allowed. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Password

A password is a case-sensitive character string that enables access by a specific user and helps prevent unauthorized access. You can add a user without a password, but they may not be able to access the device. Passwords should be strong so that they cannot be easily guessed for unauthorized access. Table 2-2 lists the characteristics of strong passwords.

Table 2-2 Characteristics of strong passwords

Strong passwords have:	Strong passwords do not have:
• At least eight characters • Uppercase letters • Lowercase letters • Numbers • Special characters **Note** Clear text passwords cannot include the dollar sign ($) special character.	• Consecutive characters, such as “abcd” • Repeating characters, such as “aaabbb” • Dictionary words • Proper names

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Check of Password Strength

The device checks password strength automatically by default. When you add a user name and password, the strength of the password is evaluated. If it is a weak password, then the error message below displays to notify you.

```
n1000v# config t
n1000v(config)# username daveGreen password davey
password is weak
Password should contain characters from at least three of the classes:
 lower case letters,upper case letters, digits, and special characters
```

Password strength-checking can be disabled.

Send document comments to nexus1k-docfeedback@cisco.com.

Expiration Date

By default, a user account does not expire. You can, however, explicitly configure an expiration date on which the account will be disabled.

Guidelines and Limitations

User access has the following configuration guidelines and limitations:

- You can create up to 64 roles in addition to the two predefined user roles.
- You can create up to 256 rules in a user role.
- You can create up to 64 feature groups.
- You can add up to 256 users.
- You can assign a maximum of 64 user roles to a user account.
- If you have a user account that has the same name as a remote user account on an AAA server, the user roles for the local user account are applied to the remote user, not the user roles configured on the AAA server.

Configuring User Access

This section includes the following topics:

Enabling the Check of Password Strength

Use this procedure to enable the Cisco Nexus 1000V to check the strength of passwords to avoid creating weak passwords for user accounts.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following.

- You are logged in to the CLI in EXEC mode.
- Checking password strength is enabled by default. This procedure can be used to enable it again should it become disabled.

Send document comments to nexus1k-docfeedback@cisco.com.

SUMMARY STEPS

1. **config t**
2. **password strength-check**
3. **show password strength-check**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Places you into the CLI Global Configuration mode.
Step 2	**password strength-check** **Example:** switch(config)# password strength-check	Enables password-strength checking. The default is enabled. You can disable the checking of password strength by using the **no** form of this command.
Step 3	**show password strength-check** **Example:** switch# show password strength-check Password strength check enabled switch(config)#	(Optional) Displays the configuration for checking password strength.
Step 4	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Disabling the Check of Password Strength

Use this procedure to disable the check of password strength.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following.

- You are logged in to the CLI in EXEC mode.
- Checking password strength is enabled by default. This procedure can be used to disable it.

SUMMARY STEPS

1. **config t**
2. **no password strength-check**
3. **show password strength-check**
4. **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Places you into the CLI Global Configuration mode.
Step 2	**no password strength-check** **Example:** switch(config)# no password strength-check switch(config)#	Disables password-strength checking. The default is enabled.
Step 3	**show password strength-check** **Example:** switch# show password strength-check Password strength check not enabled switch(config)#	(Optional) Displays the configuration for checking password strength.
Step 4	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a User Account

Use this procedure to create and configure a user account, defining access to the Cisco Nexus 1000V.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following.

- You are logged in to the CLI in EXEC mode.
- You can add up to 256 user accounts.
- Changes to user accounts do not take effect until the user logs in and creates a new session.
- Do not use the following words in user accounts. These words are reserved for other purposes.

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

- You can add a user password as either clear text or encrypted.
  - Clear text passwords are encrypted before they are saved to the running configuration.
  - Encrypted passwords are saved to the running configuration without further encryption.
- A user account can have up to 64 roles, but must have at least one role. For more information about roles, see the "Role" section on page 2-1.

Send document comments to nexus1k-docfeedback@cisco.com.

- If you do not specify a password, the user might not be able to log in.
- For information about using SSH public keys instead of passwords, see the "Configuring a User Account with a Public Key" section on page 6-5.

SUMMARY STEPS

1. **config t**
2. **show role**
3. **username** *user-name* **[password [0 | 5]***password***] [expire** *date***] [role** *role-name***]**
4. **show user-account** *user-name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Places you into the CLI Global Configuration mode.

Step 2	**show role** **Example:** `switch(config)# show role`	(Optional) Displays the available roles that can be assigned to users. You can create a new user role with the "Creating a Role" procedure on page 2-8)

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 3	**username** *name* [**password** [**0** | **5**] *password*] [expire date] [role *role-name*] **Example:** switch(config)# username NewUser password 4Ty18Rnt	Creates a user account. • **name**: A case-sensitive, alphanumeric character string of up to 28 characters in length. • **password**: The default password is undefined. – **0** = (the default) Specifies that the password you are entering is in clear text. The Cisco Nexus 1000V encrypts the clear text password before saving it in the running configuration. In the example shown, the password **4Ty18Rnt** is encrypted in your running configuration in password 5 format. – **5** = Specifies that the password you are entering is already in encrypted format. The Cisco Nexus 1000V does not encrypt the password before saving it in the running configuration. User passwords are not displayed in the configuration files. • **expire date**: YYYY-MM-DD. The default is no expiration date. • **role**: You must assign at least one role. You can assign up to 64 roles. The default role is **network-operator**.
Step 4	**show user-account** *username* **Example:** switch(config)# show user-account NewUser user:NewUser this user account has no expiry date roles:network-operator network-admin switch(config)#	Displays the new user account configuration.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a Role

Use this procedure to create a role defining a set of specific actions that are permitted or denied. This role will be assigned to users whose access requirements match the actions defined.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can configure up to 64 user roles.

Send document comments to nexus1k-docfeedback@cisco.com.

- You can configure up to up to 256 rules for each role.
- You can assign a single role to more that one user.
- The rule number specifies the order in which it is applied, in descending order. For example, if a role has three rules, rule 3 is applied first, rule 2 is applied next, and rule 1 is applied last.
- By default, the user roles that you create allow access only to the **show**, **exit**, **end**, and **configure terminal** commands. You must add rules to allow users to configure features.

SUMMARY STEPS

1. **config t**
2. **role name** *role-name*
3. (Optional) **description** *string*
4. **rule** ***number*** **{deny | permit} command** *command-string*

   rule *number* {**deny** | **permit**} {**read** | **read-write**}

   rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*

   rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*
5. **Repeat 4 to create all needed rules for this role.**
6. **show role**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Places you into the CLI Global Configuration mode.
Step 2	**role name** *role-name* **Example:** switch(config)# role name UserA switch(config-role)#	Names a user role and places you in Role Configuration mode for that role. The name is a case-sensitive, alphanumeric string of up to 16 characters.
Step 3	**description** *description-string* **Example:** switch(config-role)# description Prohibits use of clear commands	(Optional) Configures the role description, which can include spaces.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 4	**rule** *number* {**deny** | **permit**} **command** *command-string* **Example:** `switch(config-role)# rule 1 deny command clear users`	Creates a rule to permit or deny a specific command. The command you specify can contain spaces and regular expressions. For example, "interface ethernet *" permits/denies access to all Ethernet interfaces. This example rule denies access to the **clear users** command.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **Example:** `switch(config-role)# rule 2 deny read-write`	Creates a blanket rule to permit or deny all operations. This example rule permits read-only access for any operation.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* **Example:** `switch(config-role)# rule 3 permit read feature eth-port-sec`	Creates a rule for feature access. Use the **show role feature** command to display a list of available features. This example rule permits users read-only access to the Ethernet port security feature.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **Example:** `switch(config-role)# rule 4 deny read-write feature-group eth-port-sec`	Creates a rule for feature group access. Use the **show role feature-group** command to display a list of feature groups. This example configures a rule denying access to a feature group.
Step 5	Repeat Step 4 to create all needed rules for the specified role.	
Step 6	**show role** **Example:** `switch(config)# show role`	(Optional) Displays the user role configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a Feature Group

Use this procedure to create and configure a feature group.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can create up to 64 custom feature groups.

Send document comments to nexus1k-docfeedback@cisco.com.

SUMMARY STEPS

1. **config t**
2. **role feature-group name** *group-name*
3. **show role feature**
4. **feature** *feature-name*
5. **Repeat 4 for all features to be added to the feature group.**
6. **show role feature-group**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Places you into the CLI Global Configuration mode.
Step 2	**role feature-group name** *group-name* **Example:** switch(config)# role feature-group name GroupA switch(config-role-featuregrp)#	Places you into the Role Feature Group Configuration mode for the named group. • **group-name**: A case-sensitive, alphanumeric string of up to 32 characters in length.
Step 3	**show role feature** **Example:** switch(config-role-featuregrp)# **show role feature** feature: aaa feature: access-list feature: cdp feature: install . . . switch(config-role-featuregrp)#	Displays a list of available features for use in defining the feature group.
Step 4	**feature** *feature-name* **Example:** switch(config-role-featuregrp)# feature syslog switch(config-role-featuregrp)#	Adds a feature to the feature group.
Step 5	Repeat Step 6 for all features to be added to the feature group.	

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose

Step 6	**show role feature-group**
	
	Example:
	`switch(config-role-featuregrp)# show role feature-group`
	`feature group: GroupA`
	`feature: syslog`
	`feature: snmp`
	`feature: ping`
	`switch(config-role-featuregrp)#`
		(Optional) Displays the feature group configuration.

Step 7	**copy running-config startup-config** **Example:** `switch(config-role-featuregrp)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring Interface Access

Use this procedure to configure interface access for a specific role.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already created one or more user roles using the "Creating a Role" procedure on page 2-8. In this procedure, you will be modifying a role you have already created.
- By default, a role allows access to all interfaces. In this procedure you will, first, deny access to all interfaces and then permit access to selected interfaces.

SUMMARY STEPS

1. **config t**
2. **role name** *role-name*
3. **interface policy deny**
4. **permit interface** *interface-list*
5. **show role**
6. **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Places you into the CLI Global Configuration mode.
Step 2	**role name** *role-name* **Example:** switch(config)# role name network-observer switch(config-role)#	Specifies a user role and enters Role Configuration mode for the named role.
Step 3	**interface policy deny** **Example:** switch(config-role)# interface policy deny switch(config-role-interface)#	Enters the Interface Configuration mode, and denies all interface access for the role. Access to any interface must now be explicitly defined for this role using the **permit interface** command.
Step 4	**permit interface** *interface-list* **Example:** switch(config-role-interface)# permit interface ethernet 2/1-4	Specifies the interface(s) that users assigned to this role can access. Repeat this command to specify all interface lists that users assigned to this role are permitted to access.
Step 5	**show role** *role-name* **Example:** switch(config-role-interface)# show role name network-observer role: network-observer description: temp Vlan policy: permit (default) Interface policy: deny Permitted interfaces: Ethernet2/1-4	(Optional) Displays the role configuration.
Step 6	**copy running-config startup-config** **Example:** switch(config-role-featuregrp)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring VLAN Access

Use this procedure to define the VLAN access for a role.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already created one or more user roles using the "Creating a Role" procedure on page 2-8. In this procedure, you will be modifying a role you have already created.

Send document comments to nexus1k-docfeedback@cisco.com.

- By default, access is allowed to all VLANs. In this procedure you will, first, deny access to all VLANs and then permit access to selected VLANs.

SUMMARY STEPS

1. **config t**
2. **role name** ***role-name***
3. **vlan policy deny**
4. **permit vlan** ***vlan-range***
5. **exit**
6. **show role**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Places you into the CLI Global Configuration mode.

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

Step 3	**vlan policy deny**
	
	Example:
	`switch(config-role)# vlan policy deny`
	`switch(config-role-vlan)#`
		Enters the VLAN Configuration mode, and denies all VLAN access for the role.
		
		Access to any VLAN must now be explicitly defined for this role using the **permit vlan** command.

Step 4	**permit vlan** *vlan-list* **Example:** `switch(config-role-vlan)# permit vlan 1-4`	Specifies the VLAN(s) that users assigned to this role can access. Repeat this command to specify all VLANs that users assigned to this role are permitted to access.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose

Step 5	**show role** *role-name*
	
	Example:
	`switch(config-role)# show role network-observer`
	
	`role: network-observer`
	`  description: temp`
	`  Vlan policy: deny`
	`  Permitted vlans: vlan 1-4`
	`  Interface policy: deny`
	`  Permitted interfaces: Ethernet2/1-4`
		(Optional) Displays the role configuration.

Step 6	**copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the User Access Configuration

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

Command	Purpose
show role	Displays the available user roles and their rules.
show role feature	Displays a list of available features.
show role feature-group	Displays a list of available feature groups.
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.

Example Configuration

The following example shows how to configure a role:

```
role name UserA
  rule 3 permit read feature snmp
  rule 2 permit read feature dot1x
  rule 1 deny command clear *
```

The following example shows how to configure a feature group:

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

Send document comments to nexus1k-docfeedback@cisco.com.

Default Settings

Table 2-3 lists the default settings for user access.

Table 2-3 User Access Defaults

Parameters	Default
User account password	Undefined
User account expiration date.	None
User account role	Network-operator
Interface policy	All interfaces are accessible.
VLAN policy	All VLANs are accessible.

Additional References

For additional information related to implementing RBAC, see the following sections:

- Related Documents, page 2-16
- Standards, page 2-16
- MIBs, page 2-17

Related Documents

Related Topic	Document Title
User access commands	Cisco Nexus 1000V Command Reference, Release 4.0
Managing users on the switch	Cisco Nexus 1000V Getting Started Guide, Release 4.0

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.	—

Send document comments to nexus1k-docfeedback@cisco.com.

MIBs

MIBs	MIBs Link
• CISCO-COMMON-MGMT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for User Accounts

This section provides the user accounts release history.

Feature Name	Releases	Feature Information
User Accounts	4.0	This feature was introduced.

Send document comments to nexus1k-docfeedback@cisco.com.