Managing User Accounts

This chapter contains the following sections:

- Information About User Accounts, page 1
- Guidelines for Creating User Accounts, page 3
- Guidelines for Creating a Role, page 4
- Default Settings for User Access, page 4
- Configuring User Access, page 5
- Configuration Examples, page 12
- MIBs, page 13
- Feature History for User Accounts, page 13

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
- Username
- Password
- Expiration date

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
  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**

Username

A username identifies an individual user by a unique character string, such as daveGreen. Usernames are case sensitive and can consist of up to 28 alphanumeric characters. A username consisting of all numerals is not allowed. If an all-numeric username 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.

The following characters are not permitted in clear text passwords:

- dollar signs ($)
- spaces

The following special characters are not permitted at the beginning of the password:

- quotation marks (" or ')
- vertical bars (|)
- right angle brackets (>)

The following table lists the characteristics of strong passwords.

Table 1: Characteristics of Strong Passwords

Strong passwords have:	Strong passwords do not have:
At least eight characters	Consecutive characters, such as “abcd”
Uppercase letters	Repeating characters, such as “aaabbb”
Lowercase letters	Dictionary words
Numbers	Proper names
Special characters	

Some examples of strong passwords are as follows:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Check of Password Strength

The device checks password strength automatically by default. When you add a username and password, the strength of the password is evaluated. If it is a weak password, the following error message is displayed to notify you:

```
switch# config terminal
switch (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.

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 for Creating User Accounts

- 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	mtuser	rpcuser

bin	gopher	neews	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.
- 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 Configuring an OpenSSH Key.

Guidelines for Creating a Role

- You can configure up to 64 user roles.
- You can configure up to up to 256 rules for each role.
- You can assign a single role to more than 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.

Default Settings for User Access

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

Configuring User Access

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.

Checking password strength is enabled by default. This procedure can be used to enable it again should it become disabled.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	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	switch(config)# **show password strength-check**	(Optional) Displays the configuration for checking password strength.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# password strength-check
switch(config)# show password strength-check
Password strength check enabled
switch(config)# copy running-config startup-config
```

Disabling the Check of Password Strength

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no password strength-check**	Disables password-strength checking. The default is enabled.
Step 3	switch(config)# **show password strength-check**	(Optional) Displays the configuration for checking password strength.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# no password strength-check
switch(config)# show password strength-check
switch(config)# copy running-config startup-config
```

Creating a User Account

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **show role**	(Optional) Displays the available roles that can be assigned to users.
Step 3	switch(config)# **username** *name* [**password** [**0** | **5**] *password*] [**expire date**] [**role** *role-name*]	Creates a user account. The arguments and keywords are as follows: • 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.

	Command or Action	Purpose
		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	switch(config)# **show user-account** *username*	Displays the new user account configuration.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# show role
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# show user-account NewUser
user: NewUser
     this user account has no expiry date
     roles:network-operator network-admin
switch# copy running-config startup-config
```

Creating a Role

Before You Begin

- Before beginning this procedure, you must be logged in to the CLI in EXEC mode.
- You can configure up to 64 user roles.
- You can configure up to up to 256 rules for each role.
- You can assign a single role to more than 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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **role name** *role-name*	Names a user role and places you in role configuration mode for that role. The *role-name* is a case-sensitive, alphanumeric string of up to 16 characters.
Step 3	switch(config-role)# **description** *description-string*	(Optional) Configures the role description, which can include spaces.
Step 4	switch(config-role)# **rule** *number* {**deny**| **permit**} **command** *command-string* • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} Creates one rule to permit or deny all operations. • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* Creates a rule for feature access. Use the **show role feature** command to display a list of available features. • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* Creates a rule for feature group access. Use the **show role feature-group** command to display a list of feature groups. **Example:** This example configures a rule that denies access to the **clear users** command.	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 or denies access to all Ethernet interfaces.
Step 5	Repeat Step 4 to create all needed rules for the specified role.	
Step 6	switch(config-role)# **show role**	(Optional) Displays the user role configuration.
Step 7	switch(config-role)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# description Prohibits use of clear commands
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 eth-port-sec
switch(config-role)# rule 4 deny read-write feature-group eth-port-sec

switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule 3 permit read feature snmp
switch(config-role)# rule 2 permit read feature dot1x
switch(config-role)# rule 1 deny command clear *
```

Creating a Feature Group

Use this procedure to create and configure a feature group. You can create up to 64 custom feature groups.

Before You Begin

- Before beginning this procedure, you must be logged in to the CLI in EXEC mode.
- You can create up to 64 custom feature groups.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **role feature-group name** *group-name*	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	switch(config-role-featuregrp)# **show role feature**	Displays a list of available features for use in defining the feature group.
Step 4	switch(config-role-featuregrp)# **feature** *feature-name*	Adds a feature to the feature group. Repeat this step for all features to be added to the feature group.
Step 5	switch(config-role-featuregrp)# **show role feature-group**	(Optional) Displays the feature group configuration.
Step 6	switch(config-role-featuregrp)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

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

```
feature: aaa
feature: access-list
feature: cdp
feature: install
. . .
switch(config-role-featuregrp)# feature syslog
switch(config-role-featuregrp)# show role feature-group
feature group: GroupA
feature: syslog
feature: snmp
feature: ping
switch(config-role-featuregrp)# copy running-config startup-config
```

```
switch# configure terminal
switch(config)# role feature-group name Security-features
 switch(config-role-featuregrp)# feature radius
 switch(config-role-featuregrp)# feature tacacs
 switch(config-role-featuregrp)# feature dot1x
 switch(config-role-featuregrp)# feature aaa
 switch(config-role-featuregrp)# feature snmp
 switch(config-role-featuregrp)# feature acl
 switch(config-role-featuregrp)# feature access-list
```

Configuring Interface Access

By default, a role allows access to all interfaces. You modify a role you have already created by denying access to all interfaces, and then permitting access to selected interfaces.

Before You Begin

Before beginning this procedure you must have done the following:

- Logged in to the CLI in EXEC mode
- Created one or more user roles. In this procedure, you will be modifying a role you have already created.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **role name** *role-name*	Specifies a user role and enters role configuration mode for the named role.
Step 3	switch(config-role)# **interface policy deny**	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	switch(config-role-interface)# **permit interface***interface-list*	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.

	Command or Action	Purpose
Step 5	switch(config-role-interface)# **show role** *role-name*	(Optional) Displays the role configuration.
Step 6	switch(config-role-featuregrp)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# role name network-observer
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1-4
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
switch(config-role-featuregrp)# copy running-config startup-config
```

Configuring VLAN Access

By default, access is allowed to all VLANs. In this procedure you will modify a role you have already created by denying access to all VLANs, and then permitting access to selected VLANs.

Before You Begin

Before beginning this procedure, you must:

- Be logged in to the CLI in EXEC mode.
- Have already created one or more user roles. In this procedure, you will be modifying a role you have already created.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **role name** *role-name*	Specifies a user role and enters role configuration mode.
Step 3	switch(config-role)# **vlan policy deny**	Enters 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	switch(config-role-vlan)# **permit vlan** *vlan-range*	Specifies the VLANs that users assigned to this role can access.

	Command or Action	Purpose
		Specify a VLAN range by using a dash. For example, 1-9 or 20-30. Repeat this command to specify all VLANs that users assigned to this role are permitted to access.
Step 5	switch(config-role)# **show role** *role-name*	(Optional) Displays the role configuration. role-name is the name you have assigned to the role your created.
Step 6	switch(config-role)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# role name network-observer
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit interface ethernet 2/1-4
switch(config-role)# show role name network-observer
role: network-observer
  description: temp
  Vlan policy: permit (default)
  Interface policy: deny
  Permitted interfaces: Ethernet2/1-4
switch(config-role)# copy running-config startup-config
```

Configuration Examples

Configuration Example for Creating a Feature Group

```
switch# config terminal
switch(config-role)# role feature-group name security-features
switch(config-role)# feature radius
switch(config-role)# feature tacacs
switch(config-role)# feature dot1x
switch(config-role)# feature aaa
switch(config-role)# feature snmp
switch(config-role)# feature acl
switch(config-role)# feature access-list
```

Configuration Example for Creating a Role

```
switch# config terminal
switch(config)# role name UserA
switch(config-role)# rule 3 permit read feature snmp
switch(config-role)# rule 2 permit read feature dot1x
switch(config-role)# rule 1 deny command clear *
```

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 table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
User Accounts	5.2(1)SM1(5.1)	This feature was introduced.