CHAPTER 3

Configuring Users and Common Role

The CLI and SNMP use common roles in all switches in the Cisco MDS 9000 Family. You can use the CLI to modify a role that was created using SNMP and vice versa.

Users, passwords, and roles for all CLI and SNMP users are the same. A user configured through the CLI can access the switch using SNMP (for example, DCNM for SAN (DCNM-SAN or Device Manager) and vice versa.

This chapter includes the following topics:

- Information About Role-Based Authorization, page 3-29
- Guidelines and Limitations, page 3-36
- Default Settings, page 3-36
- Configuring Users and Common Role, page 3-37
- Configuring SSH Services, page 3-46
- Verifying Users and Common Role Configuration, page 3-56
- Field Descriptions for Users and Common Role, page 3-62
- Feature History for Users and Common Role, page 3-62

Information About Role-Based Authorization

Switches in the Cisco MDS 9000 Family perform authentication based on roles. Role-based authorization limits access to switch operations by assigning users to roles. This kind of authentication restricts you to management operations based on the roles to which you have been added.

When you execute a command, perform command completion, or obtain context-sensitive help, the switch software allows the operation to progress if you have permission to access that command.

This section includes the following topics:

- About Roles, page 3-30
- Rules and Features for Each Role, page 3-30
- Rule Changes Between SAN-OS Release 3.3(1c) and NX-OS Release 4.2(1a) Affect Role Behavior, page 3-31
- About the VSAN Policy, page 3-31
- Role Distributions, page 3-32
- About Role Databases, page 3-32

- Locking the Fabric, page 3-32
- About Common Roles, page 3-32
- Mapping of CLI Operations to SNMP, page 3-33
- Creating Users Guidelines, page 3-34
- Characteristics of Strong Passwords, page 3-34
- About SSH, page 3-35
- Boot Mode SSH, page 3-35
- SSH Authentication Using Digital Certificates, page 3-35
- Passwordless File copy and SSH, page 3-36

About Roles

Each role can contain multiple users and each user can be part of multiple roles. For example, if role1 users are only allowed access to configuration commands, and role2 users are only allowed access to **debug** commands, then if Joe belongs to both role1 and role2, he can access configuration as well as **debug** commands.

Note If you belong to multiple roles, you can execute a union of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose you belong to a TechDocs group and you were denied access to configuration commands. However, you also belong to the engineering group and have access to configuration commands. In this case, you will have access to configuration commands.

Tip Any role, when created, does not allow access to the required commands immediately. The administrator must configure appropriate rules for each role to allow access to the required commands.

Rules and Features for Each Role

Up to 16 rules can be configured for each role. These rules reflect what CLI commands are allowed. The user-specified rule number determines the order in which the rules are applied. For example, rule 1 is applied before rule 2, which is applied before rule 3, and so on. A user not belonging to the network-admin role cannot perform commands related to roles.

For example, if user A is permitted to perform all **show** CLI commands, user A cannot view the output of the **show role** CLI command if user A does not belong to the network-admin role.

A **rule** specifies operations that can be performed by a specific role. Each rule consists of a rule number, a rule type (permit or deny), a CLI command type (for example, **config**, **clear**, **show**, **exec**, **debug**), and an optional feature name (for example, FSPF, zone, VSAN, fcping, or interface).

Note In this case, **exec** CLI commands refer to all commands in the EXEC mode that are not included in the **show**, **debug**, and **clear** CLI command categories.

Rule Changes Between SAN-OS Release 3.3(1c) and NX-OS Release 4.2(1a) Affect Role Behavior

The rules that can be configured for roles were modified between SAN-OS Release 3.3(1c) and NX-OS Release 4.2(1a). As a result, roles do not behave as expected following an upgrade from SAN-OS Release 3.3(1c) to NX-OS Release 4.2(1a). Manual configuration changes are required to restore the desired behavior.

Rule 4 and Rule 3: after the upgrade, **exec** and **feature** are removed. Change rule 4 and rule 3 as follows:

SAN-OS Release 3.3(1c) Rule	NX-OS Release 4.2(1a), Set the Rule to:
rule 4 permit exec feature debug	rule 4 permit debug
rule 3 permit exec feature clear	rule 3 permit clear

Rule 2: after the upgrade, **exec feature license** is obsolete.

SAN-OS Release 3.3(1c) Rule	NX-OS Release 4.2(1a) Rule
rule 2 permit exec feature debug	Not available in Release 4.2(1).

Rule 9, Rule 8, and Rule 7: after the upgrade, you need to have the feature enabled to configure it. In SAN-OS Release 3.3(1c), you could configure a feature without enabling it.

SAN-OS Release 3.3(1c) Rule	NX-OS Release 4.2(1a), to Preserve the Rule:
rule 9 deny config feature telnet	Not available in Release 4.2(1) and cannot be used.
rule 8 deny config feature tacacs-server	During the upgrade, enable the feature to preserve the rule; otherwise, the rule disappears.
rule 7 deny config feature tacacs+	During the upgrade, enable the feature to preserve the rule; otherwise, the rule disappears.

About the VSAN Policy

Configuring the VSAN policy requires the ENTERPRISE_PKG license (For more information, see *Cisco MDS 9000 Family NX-OS Licensing Guide*).

You can configure a role so that it only allows tasks to be performed for a selected set of VSANs. By default, the VSAN policy for any role is permit, which allows tasks to be performed for all VSANs. You can configure a role that only allows tasks to be performed for a selected set of VSANs. To selectively allow VSANs for a role, set the VSAN policy to deny, and then set the configuration to permit or the appropriate VSANs.

Note Users configured in roles where the VSAN policy is set to deny cannot modify the configuration for E ports. They can only modify the configuration for F or FL ports (depending on whether the configured rules allow such configuration to be made). This is to prevent such users from modifying configurations that may impact the core topology of the fabric.

Tip Roles can be used to create VSAN administrators. Depending on the configured rules, these VSAN administrators can configure MDS features (for example, zone, fcdomain, or VSAN properties) for their VSANs without affecting other VSANs. Also, if the role permits operations in multiple VSANs, then the VSAN administrators can change VSAN membership of F or FL ports among these VSANs.

Users belonging to roles in which the VSAN policy is set to deny are referred to as VSAN-restricted users.

Role Distributions

Role-based configurations use the Cisco Fabric Services (CFS) infrastructure to enable efficient database management, and to provide a single point of configuration for the entire fabric.

The following configurations are distributed:

- Role names and descriptions
- List of rules for the roles
- VSAN policy and the list of permitted VSANs

About Role Databases

Role-based configurations use two databases to accept and implement configurations.

- Configuration database—The running database currently enforced by the fabric.
- Pending database—Your subsequent configuration changes are stored in the pending database. If you modify the configuration, you need to commit or discard the pending database changes to the configuration database. The fabric remains locked during this period. Changes to the pending database are not reflected in the configuration database until you commit the changes.

Locking the Fabric

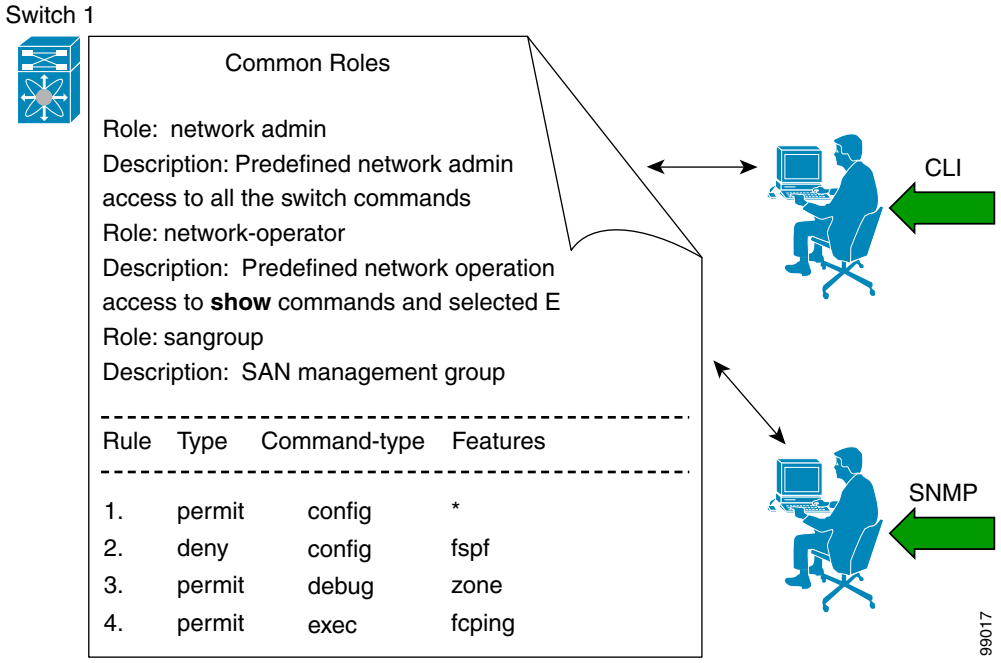
The first action that modifies the database creates the pending database and locks the feature in the entire fabric. Once you lock the fabric, the following situations apply:

- No other user can make any configuration changes to this feature.
- A copy of the configuration database becomes the pending database along with the first change.

About Common Roles

The CLI and SNMP in all switches in the Cisco MDS 9000 Family use common roles. You can use SNMP to modify a role that was created using the CLI and vice versa (see Figure 3-1).

Figure 3-1 Common Roles



Each role in SNMP is the same as a role created or modified through the CLI (see the "Information About Role-Based Authorization" section on page 3-29).

Each role can be restricted to one or more VSANs as required.

You can create new roles or modify existing roles using SNMP or the CLI.

- SNMP—Use the CISCO-COMMON-ROLES-MIB to configure or modify roles. Refer to the *Cisco MDS 9000 Family MIB Quick Reference*.
- CLI—Use the **role name** command.

Mapping of CLI Operations to SNMP

SNMP has only three possible operations: GET, SET, and NOTIFY. The CLI has five possible operations: DEBUG, SHOW, CONFIG, CLEAR, and EXEC.

Note NOTIFY does not have any restrictions like the syslog messages in the CLI.

Table 3-1 explains how the CLI operations are mapped to the SNMP operations.

Table 3-1 CLI Operation to SNMP Operation Mapping

CLI Operation	SNMP Operation
DEBUG	Ignored
SHOW	GET
CONFIG	SET

Table 3-1 CLI Operation to SNMP Operation Mapping (continued)

CLI Operation	SNMP Operation
CLEAR	SET
EXEC	SET

Creating Users Guidelines

The passphrase specified in the **snmp-server user** option and the password specified **username** option are synchronized.

By default, the user account does not expire unless you explicitly configure it to expire. The **expire** option determines the date on which the user account is disabled. The date is specified in the YYYY-MM-DD format.

When creating users, note the following guidelines:

- You can configure up to a maximum of 256 users on a switch.
- The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.
- User passwords are not displayed in the switch configuration file.
- If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case-sensitive. “admin” is no longer the default password for any Cisco MDS 9000 Family switch. You must explicitly configure a strong password.
- To issue commands with the **internal** keyword for troubleshooting purposes, you must have an account that is a member of the network-admin group.

Caution Cisco MDS NX-OS supports user names that are created with alphanumeric characters or specific special characters (+ [plus], = [equal], _ [underscore], - [hyphen], \ [backslash], and . [period]) whether created remotely (using TACACS+ or RADIUS) or locally. Local user names cannot be created with any special characters (apart from those specified). If a non-supported special character user name exists on an AAA server, and is entered during login, then the user is denied access.

Characteristics of Strong Passwords

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both upper- and lower-case characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

About SSH

SSH provides secure communications to the Cisco NX-OS CLI. You can use SSH keys for the following SSH options:

- SSH2 using RSA
- SSH2 using DSA

Boot Mode SSH

Due to the increasing emphasis on security and security-related issues, the **ssh** command in this release runs in the Boot mode. SSH is a preferred and more secure method of data exchange over the network because it communicates over the secure channel, and the data is encrypted before sending on the channel.

Example 3-1 shows how to use the **ssh** command to conncet to a remote server from any switch.

Example 3-1 Connecting a Remote Server from Any Switch

```
switch# ssh admin @ hostname
```

SSH Authentication Using Digital Certificates

SSH authentication on the Cisco MDS 9000 Family switches provide X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that vouches for the origin and integrity of a message. It contains encryption keys for secured communications and is “signed” by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through query or notification. Verification of certificates is successful if the certificates are from any of the trusted CAs.

You can configure your switch for either SSH authentication using an X.509 certificate or SSH authentication using a Public Key Certificate, but not both. If either of them is configured and the authentication fails, you will be prompted for a password.

For more information on CAs and digital certificates, see Chapter 6, “Configuring Certificate Authorities and Digital Certificates.”

Passwordless File copy and SSH

Secure Shell (SSH) public key authentication can be used to achieve password-free logins. SCP and SFTP uses SSH in the background, which enables these copy protocols to be used for a password-free copy with public key authentication. The NX-OS version only supports the SCP and STFP client functionality.

You can create an RSA and DSA identity that can be used for authentication with SSH. The identity consists of two parts: public and private keys. The public and the private keys are generated by the switch or can be generated externally and imported to the switch. For import purposes, the keys should be in OPENSSH format.

To use the key on a host machine hosting an SSH server, you must transfer the public key file to the machine and add the contents of it to the authorized_keys file in your SSH directory (for example, $HOME/.ssh) on the server. For the import and export of private keys, the key is protected by encryption. You are asked to enter the passphrase for the keys. If you enter a passphrase, the private key is protected by encryption. If you leave the password field blank, the key will not be encrypted.

If you need to copy the keys to another switch, you will have to export the keys out of the switch to a host machine, and then import the keys to other switches from that machine.

The key files are persistent across reload.

Guidelines and Limitations

Fabric merge does not modify the role database on a switch. If two fabrics merge, and the fabrics have different role databases, the software generates an alert message.

See the "Merge Guidelines for RADIUS and TACACS+ Configurations" section on page 4-81 for detailed concepts.

- Verify that the role database is identical on all switches in the entire fabric.
- Be sure to edit the role database on any switch to the desired database and then commit it. This synchronizes the role databases on all the switches in the fabric.

Default Settings

Table 3-2 lists the default settings for all switch security features in any switch.

Table 3-2 Default Switch Security Settings

Parameters	Default
Roles in Cisco MDS Switches	Network operator (network-operator)
AAA configuration services	Local
Authentication port	1812
Accounting port	1813
Preshared key communication	Clear text
RADIUS server time out	1 (one) second
RADIUS server retries	Once

Table 3-2 Default Switch Security Settings (continued)

Parameters	Default
TACACS+	Disabled
TACACS+ servers	None configured
TACACS+ server timeout	5 seconds
AAA server distribution	Disabled
VSAN policy for roles	Permit
User account	No expiry (unless configured)
Password	None
Password-strength	Enabled
Accounting log size	250 KB
SSH service	Enabled
Telnet service	Disabled

Configuring Users and Common Role

This section includes the following topics:

- Configuring Roles and Profiles, page 3-38
- Deleting Common Roles, page 3-38
- Modifying Profiles, page 3-39
- Modifying Rules, page 3-39
- Modifying the VSAN Policy, page 3-40
- Committing Role-Based Configuration Changes, page 3-41
- Discarding Role-Based Configuration Changes, page 3-41
- Enabling Role-Based Configuration Distribution, page 3-42
- Clearing Sessions, page 3-42
- Checking Password Strength, page 3-43
- Configuring Users, page 3-43
- Logging Out Users, page 3-45
- Deleting a User, page 3-46

Configuring Roles and Profiles

Detailed Steps

To create an additional role or to modify the profile for an existing role, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# role name techdocs` `switch(config-role)#`	Places you in the mode for the specified role (techdocs). **Note** The role submode prompt indicates that you are now in the role submode. This submode is now specific to the techdocs group.
	`switch(config)# no role name techdocs`	Deletes the role called techdocs.
Step 3	`switch(config-role)# description Entire Tech Docs group`	Assigns a description to the new role. The description is limited to one line and can contain spaces.
	`switch(config-role)# no description`	Resets the description for the Tech Docs group.

Note Only users belonging to the network-admin role can create roles.

To create an additional role or to modify the profile for an existing role using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Roles** tab in the Information pane.

Step 3 Click **Create Row** to create a role in DCNM-SAN.

Step 4 Select the switches on which to configure a role.

Step 5 Enter the name of the role in the Name field.

Step 6 Enter the description of the role in the Description field.

Step 7 (Optional) Check the **Enable** check box to enable the VSAN scope and enter the list of VSANs in the Scope field to which you want to restrict this role.

Step 8 Click **Create** to create the role.

Note Device Manager automatically creates six roles that are required for Device Manager to display a view of a switch. These roles are **system**, **snmp**, **module**, **interface**, **hardware**, and **environment**.

Deleting Common Roles

Detailed Steps

To delete a common role using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Roles** tab in the Information pane.

Step 3 Click the role you want to delete.

Step 4 Click **Delete Row** to delete the common role.

Step 5 Click **Yes** to confirm the deletion or **No** to cancel it.

Modifying Profiles

Detailed Steps

To modify the profile for an existing role, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# role name sangroup` `switch(config-role)#`	Places you in role configuration submode for the existing role sangroup.

Step 3	`switch(config-role)# rule 1 permit config`
	`switch(config-role)# rule 2 deny config feature fspf`
	`switch(config-role)# rule 3 permit debug feature zone`
	`switch(config-role)# rule 4 permit exec feature fcping`
		Allows users belonging to the sangroup role to perform all configuration commands except **fspf config** commands. They can also perform **zone debug** commands and the **fcping** EXEC mode command.

Step 4	`switch(config-role)# no rule 4`	Deletes rule 4, which no longer permits the sangroup to perform the **fcping** command.

In Step 3, rule 1 is applied first, thus permitting sangroup users access to all **config** commands. Rule 2 is applied next, denying FSPF configuration to sangroup users. As a result, sangroup users can perform all other **config** commands, except **fspf** configuration commands.

Modifying Rules

Detailed Steps

To modify the rules for an existing role using Device Manager, follow these steps:

Step 1 Choose **Security** > **Roles**.

Step 2 Click the role for which you want to edit the rules.

Step 3 Click **Rules** to view the rules for the role.

You see the Edit Role Rules dialog box.

Step 4 Edit the rules you want to enable or disable for the common role.

Step 5 Click **Apply** to apply the new rules.

Rule 1 is applied first, which permits, for example, sangroup users access to all **config** CLI commands. Rule 2 is applied next, denying FSPF configuration to sangroup users. As a result, sangroup users can perform all other **config** CLI commands, except the **fspf** CLI configuration commands.

Note The order of rule placement is important. If you had swapped these two rules and issued the **deny config feature fspf** rule first and issued the **permit config** rule next, you would be allowing all sangroup users to perform all configuration commands because the second rule globally overrode the first rule.

Modifying the VSAN Policy

Detailed Steps

To modify the VSAN policy for an existing role, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# role name sangroup` `switch(config-role)#`	Places you in role configuration submode for the sangroup role.
Step 3	`switch(config)# vsan policy deny` `switch(config-role-vsan)`	Changes the VSAN policy of this role to **deny** and places you in a submode where VSANs can be selectively permitted.
	`switch(config-role)# no vsan policy deny`	Deletes the configured VSAN role policy and reverts to the factory default (**permit**).
Step 4	`switch(config-role-vsan)# permit vsan 10-30`	Permits this role to perform the allowed commands for VSANs 10 through 30.
	`switch(config-role-vsan)# no permit vsan 15-20`	Removes the permission for this role to perform commands for VSANs 15 to 20. So, the role is now permitted to perform commands for VSAN 10 to 14, and 21 to 30.

To modify the VSAN policy for an existing role using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Roles** tab in the Information pane.

Step 3 Check the **Scope Enable** check box if you want to enable the VSAN scope and restrict this role to a subset of VSANs.

Step 4 Enter the list of VSANs in the Scope VSAN Id List field that you want to restrict this role to.

Step 5 Click **Apply Changes** to save these changes.

Committing Role-Based Configuration Changes

If you commit the changes made to the pending database, the configuration is committed to all the switches in the fabric. On a successful commit, the configuration change is applied throughout the fabric and the lock is released. The configuration database now contains the committed changes and the pending database is now cleared.

Detailed Steps

To commit role-based configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# role commit vsan 3`	Commits the role-based configuration changes.

To commit role-based configuration changes using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** in the Physical Attributes pane.

Step 2 Click the **Roles CFS** tab in the Information pane.

Step 3 Set the Global drop-down menu to **enable** to enable CFS.

Step 4 Click the **Apply Changes** icon to save this change.

Step 5 Set the Config Action drop-down menu to **commit** to commit the roles using CFS.

Step 6 Click the **Apply Changes** icon to save this change.

Discarding Role-Based Configuration Changes

If you discard (abort) the changes made to the pending database, the configuration database remains unaffected and the lock is released.

Detailed Steps

To discard role-based configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# role abort`	Discards the role-based configuration changes and clears the pending configuration database.

To discard role-based configuration changes using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** in the Physical Attributes pane.

Step 2 Click the **Roles CFS** tab in the Information pane.

Step 3 Set the Config Action drop-down menu to **abort** to discard any uncommitted changes.

Step 4 Click the **Apply Changes** icon to save this change.

Enabling Role-Based Configuration Distribution

Detailed Steps

To enable role-based configuration distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# role distribute`	Enables role-based configuration distribution.
	`switch(config)# no role distribute`	Disables role-based configuration distribution (default).

To enable role-based configuration distribution using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** in the Physical Attributes pane.

Step 2 Click the **Roles CFS** tab in the Information pane.

Step 3 Set the Global drop-down menu to **enable** to enable CFS distribution.

Step 4 Click the **Apply Changes** icon to save this change.

Clearing Sessions

Detailed Steps

To forcibly clear the existing role session in the fabric, issue the **clear role session** command from any switch that is part of the initiated session.

```
switch# clear role session
```

To forcibly clear the existing role session in the fabric using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** in the Physical Attributes pane.

Step 2 Click the **Roles CFS** tab in the Information pane.

Step 3 Set the Config Action drop-down menu to **clear** to clear the pending database.

Step 4 Click the **Apply Changes** icon to save this change.

Caution Any changes in the pending database are lost when you clear a session.

Checking Password Strength

You can check the strength of the configured password.

When you enable password checking, the NX-OS software allows you to create strong passwords only.

Detailed Steps

To enable password strength checking, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# password strength-check`	Enables (default) password checking.
Step 3	`switch(config)# no password strength-check`	Disables password checking.

Configuring Users

Before configuring users, make sure that you have configured roles to associate with the users that you are creating.

Note As of Cisco SAN-OS Release 3.1(2b), DCNM-SAN automatically checks whether encryption is enabled, which allows you to create users.

Detailed Steps

To configure a new user or to modify the profile of an existing user, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# username usam password abcd123AAA expire 2003-05-31`	Creates or updates the user account (usam) along with a password (abcd123AAA) that is set to expire on 2003-05-31. The password is limited to 64 characters. **Note** User account names must contain non-numeric characters.
	`switch(config)# username msam password 0 abcd12AAA role network-operator`	Creates or updates the user account (msam) along with a password (abcd12AAA) specified in clear text (indicated by 0). The password is limited to 64 characters. **Note** User account names must contain non-numeric characters.
	`switch(config)# username user1 password 5 !@*asdsfsdfjh!@df`	Specifies an encrypted (specified by 5) password (!@*asdsfsdfjh!@df) for the user account (user1).

	Command	Purpose
Step 3	`switch(config)# username usam role network-admin`	Adds the specified user (usam) to the network-admin role.
	`switch(config)# no username usam role vsan-admin`	Deletes the specified user (usam) from the vsan-admin role.
Step 4	`switch(config)# username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSI YZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8d veqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=`	Specifies the SSH key for an existing user account (admin).
	`switch(config)# no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSI YZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8d veqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=`	Deletes the SSH key for the user account (admin).
Step 5	`switch(config)# username usam ssh-cert-dn usam-dn dsa`	Specifies an SSH X.509 certificate distinguished name and DSA algorithm to use for authentication for an existing user account (usam).
	`switch(config)# username user1 ssh-cert-dn user1-dn rsa`	Specifies an SSH X.509 certificate distinguished name and RSA algorithm to use for authentication for an existing user account (user1).
	`switch(config)# no username admin ssh-cert-dn admin-dn dsa`	Removes the SSH X.509 certificate distinguished name for the user account (admin).

To configure a new user or to modify the profile of an existing user using DCNM-SAN, follow these steps:

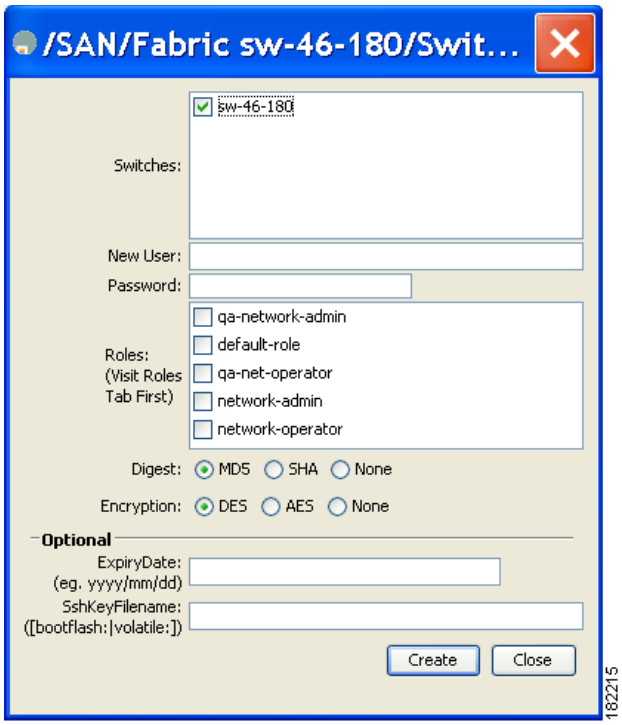
Step 1 Expand **Switches > Security** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Users** tab in the Information pane to see a list of users.

Step 3 Click the **Create Row** icon.

You see the Users - Create dialog box as shown in Figure 3-2.

Figure 3-2 Users - Create Dialog Box



Step 4 (Optional) Alter the Switches check boxes to specify one or more switches.

Step 5 Enter the user name in the New User field.

Step 6 Enter the password for the user.

Step 7 Check the roles that you want to associate with this user.

See the "Rules and Features for Each Role" section on page 3-30.

Step 8 Select the appropriate option for the type of authentication protocol used. The default value is MD5.

Step 9 Select the appropriate option for the type of privacy protocol used. The default value is DES.

Step 10 (Optional) Enter the expiry date for this user.

Step 11 (Optional) Enter the SSH Key filename.

Step 12 Click **Create** to create the entry.

Logging Out Users

Detailed Steps

To log out another user on the switch, use the **clear user** command.

In the following example, the user named vsam is logged out from the switch:

```
switch# clear user vsam
```

Use the **show users** command to view a list of the logged in users (see Example 3-2).

Example 3-2 Displays All Logged in Users

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (user.example.com)
admin    pts/10       Jan 13 03:05 (dhcp-10-10-1-1.example.com)
admin    pts/11       Jan 13 01:53 (dhcp-10-10-2-2.example.com)
```

Deleting a User

Detailed Steps

To delete a user using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Users** tab in the Information pane to see a list of users.

Step 3 Click the name of the user you want to delete.

Step 4 Click **Delete Row** to delete the selected user.

Step 5 Click **Apply Changes** to save this change.

Configuring SSH Services

A secure SSH connection with an RSA key is available as a default on all Cisco MDS 9000 Family switches. If you require a secure SSH connection with a DSA key, you need to disable the default SSH connection, Generate a DSA key and then enable the SSH connection (see the "Generating the SSH Server Key Pair" section on page 3-47).

Use the **ssh key** command to generate a server key.

Caution If you are logging in to a switch through SSH and you have issued the **aaa authentication login default none** command, you must enter one or more key strokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

This section includes the following topics:

- Generating the SSH Server Key Pair, page 3-47
- Specifying the SSH Key, page 3-48
- Overwriting a Generated Key Pair, page 3-49
- Enabling SSH or Telnet Service, page 3-50
- Generating SSH User Key Pairs, page 3-51
- Changing Administrator Password Using DCNM-SAN, page 3-53
- Recovering the Administrator Password, page 3-54

Generating the SSH Server Key Pair

Ensure that you have an SSH server key pair with the appropriate version before enabling the SSH service. Generate the SSH server key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 2048.

The SSH service accepts two types of key pairs for use by SSH version 2.

- The **dsa** option generates the DSA key pair for the SSH version 2 protocol.
- The **rsa** option generates the RSA keypair for the SSH version 2 protocol.

Caution If you delete all of the SSH keys, you cannot start a new SSH session.

Detailed Steps

To generate the SSH server key pair, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# ssh key dsa 1024`
	`generating dsa key.....`
	`generated dsa key`
		Generates the DSA server key pair.

	`switch(config)# ssh key rsa 1024`
	`generating rsa key.....`
	`generated rsa key`
		Generates the RSA server key pair.

	`switch(config)# no ssh key rsa 1024` `cleared RSA keys`	Clears the RSA server key pair configuration.

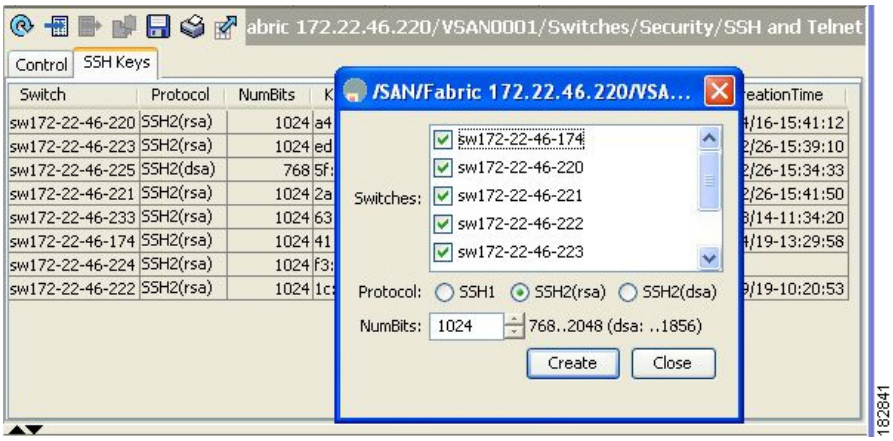
To generate the SSH key pair using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **SSH and Telnet**.

Step 2 Click the **Create Row** icon.

You see the SSH and Telnet Key - Create dialog box (see Figure 3-3).

Figure 3-3 SSH and Telnet - Create Dialog Box



Step 3 Check the switches you want to assign to this SSH key pair.

Step 4 Choose the key pair option type from the listed Protocols. The listed protocols are SSH1, SSH2(rsa), and SSH2(dsa).

Step 5 Set the number of bits that will be used to generate the key pairs in the NumBits drop-down menu.

Step 6 Click **Create** to generate these keys.

Note 1856 DSA NumberKeys are not supported by switches that running Cisco MDS NX-OS software version 4.1(1) and later.

Specifying the SSH Key

You can specify an SSH key to log in using the SSH client without being prompted for a password. You can specify the SSH key in three different formats:

- Open SSH format
- IETF SECSH format
- Public Key Certificate in PEM format

Detailed Steps

To specify or delete the SSH key in OpenSSH format for a specified user, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.

	Command	Purpose
Step 2	`switch(config)# username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ 0EOdJ3l5RONWcwSgAuTUSrLk3a9hdYkzY94fhHmNGQGCjVg+8cbO xyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2UsoreC U6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=`	Specifies the SSH key for the user account (admin).
	`switch(config)# no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ 0EOdJ3l5RONWcwSgAuTUSrLk3a9hdYkzY94fhHmNGQGCjVg+8cbO xyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2UsoreC U6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=`	Deletes the SSH key for the user account (admin).

To specify or delete the SSH key in IETF SECSH format for a specified user, follow these steps:

	Command	Purpose
Step 1	`switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub`	Downloads the file containing the SSH key in IETF SECSH format.
Step 2	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 3	`switch(config)# username admin sshkey file bootflash:secsh_file.pub`	Specifies the SSH key for the user account (admin).
	`switch(config)# no username admin sshkey file bootflash:secsh_file.pub`	Deletes the SSH key for the user account (admin).

To specify or delete the SSH key in PEM-formatted Public Key Certificate form for a specified user, follow these steps:

	Command	Purpose
Step 1	`switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem`	Downloads the file containing the SSH key in PEM-formatted Public Key Certificate form.
Step 2	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 3	`switch(config)# username admin sshkey file bootflash:cert.pem`	Specifies the SSH key for the user account (usam).
	`switch(config)# no username admin sshkey file bootflash:cert.pem`	Deletes the SSH key for the user account (usam).

Overwriting a Generated Key Pair

If the SSH key pair option is already generated for the required version, you can force the switch to overwrite the previously generated key pair.

Detailed Steps

To overwrite the previously generated key pair, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# ssh key dsa 768`
	`ssh key dsa 512`
	`dsa keys already present, use force option to overwrite them`
	`switch(config)# ssh key dsa 512 force`
	`deleting old dsa key.....`
	`generating dsa key.....`
	`generated dsa key`
		Tries to set the server key pair. If a required server key pair is already configured, use the **force** option to overwrite that server key pair.
		Deletes the old DSA key and sets the server key pair using the new bit specification.

To overwrite the previously generated key pair using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **SSH and Telnet**.

You see the configuration in the Information pane.

Step 2 Highlight the key that you want to overwrite and click **Delete Row**.

Step 3 Click the **Apply Changes** icon to save these changes.

Step 4 Click the **Create Row** icon.

You see the SSH and Telnet Key - Create dialog box.

Step 5 Check the switches you want to assign this SSH key pair.

Step 6 Choose the key pair option type from the Protocols radio buttons.

Step 7 Set the number of bits that will be used to generate the key pairs in the NumBits drop-down menu.

Step 8 Click **Create** to generate these keys.

Enabling SSH or Telnet Service

By default, the SSH service is enabled with the RSA key.

Detailed Steps

To enable or disable the SSH or Telnet service, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# feature ssh` `updated`	Enables the use of the SSH service.
	`switch(config)# no feature ssh` `updated`	Disables (default) the use of the SSH service.
	`switch(config)# feature telnet` `updated`	Enables the use of the Telnet service.
	`switch(config)# no feature telnet` `updated`	Disables (default) the use of the Telnet service.

Note If you are logging in to a switch through SSH and you have issued the **aaa authentication login default none CLI** command, you must enter one or more key strokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

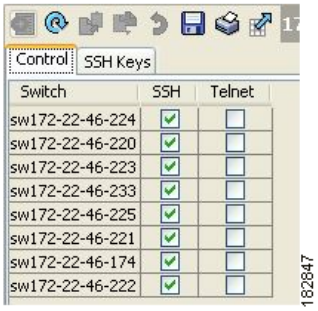
DCNM-SAN enables SSH automatically when you configure it.

To enable or disable SSH using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **SSH and Telnet**.

Step 2 Select the **Control** tab and check an **SSH** check box or **Telnet** check box for each switch (see Figure 3-4).

Figure 3-4 Control Tab under SSH and Telnet



Step 3 Click the **Apply Changes** icon to save this change.

Generating SSH User Key Pairs

Detailed Steps

To import and export the key pair, the following CLIs are provided. The CLI command to generate the ssh user key pairs on the switch is defined as follows:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

Step 2	`switch(config)# username admin keypair generate rsa`
	`generating rsa key(1024 bits).....`
	`generated rsa key`
		Generates public and private RSA keys for the account (admin). It then stores the key files in the home directory of the specified user. Use the force option to overwrite that server keypair.
		Note This example is for RSA keys. Replace rsa with dsa for DSA keys.

	`switch(config)# no username admin keypair generate rsa`	Deletes the public and private RSA keys for the account (admin).

	Command	Purpose
Step 3	**switch# show username admin keypair** ************************************ rsa Keys generated: Thu Jul 9 11:10:29 2009 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD 0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0= bitcount:262144 fingerprint: 8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d ************************************ could not retrieve dsa key information ************************************	Shows the public key for the account (admin).
Step 4	**switch(config)# username admin keypair export bootflash:key_rsa rsa** Enter Passphrase: switch(config)# dir 951 Jul 09 11:13:59 2009 key_rsa 221 Jul 09 11:14:00 2009 key_rsa.pub	Exports the keypair from the user's (admin's) home directory to the bootflash memory. The key pair (both public and private keys) will be exported to the specified location. The user will be prompted to enter a Passphrase which will encrypt the private key. The private key will be exported as the file name specified in the uri and the public key will be exported with the same file name followed by a ".pub" extension. The user can now copy this key pair to any switch, and also copy the public file to the home directory of the SCP server.

	Command	Purpose
Step 5	**switch(config)# username admin keypair import bootflash:key_rsa rsa** Enter Passphrase: switch(config)# show username admin keypair ********** rsa Keys generated: Thu Jul 9 11:10:29 2009 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD 0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0= bitcount:262144 fingerprint: 8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d ********** could not retrieve dsa key information **********	Imports the keypair to the home directory of the switch. The uri given here must be the uri of the private key and the public should be present on the same location with extension ".pub". The user will be prompted for the passphrase, and the same passphrase must be entered as was used to encrypt the key. Once the private keys are copied to the switches which need to do passwordless copy to a server, and that server has the public key copied to its authorized_keys file in home directory, the user will be able to do passwordless file copy and ssh to the server from the switches. **Note** To copy the public key to the authorized_keys file on the server, user can also copy the key from the show command mentioned above.
Step 6	server# **cat key_rsa.pub >> $HOME/.ssh/authorized_keys**	Appends the public key stored in key_rsa.pub to the authorized_keys file on the SCP server. The passwordless ssh/scp is then enabled from the switch to this server using the standard ssh and scp commands.

Changing Administrator Password Using DCNM-SAN

Detailed Steps

To change the administrator password in DCNM-SAN, follow these steps:

Step 1 Click the **Open** tab in the control panel.

Step 2 Choose the password field to change the password for an already existing user for the fabric.

Step 3 Click **Open** to open the fabric.

Note New password will be saved after the fabric is open. The user name and password fields are editable in the Fabric tab only after you unmanage the fabric.

Recovering the Administrator Password

You can recover the administrator password using one of two methods:

- From the CLI with a user name that has network-admin privileges.
- Power cycling the switch.

Note To recover an administrator's password, refer to the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.

The following topics included in this section:

- Using the CLI with Network-Admin Privileges, page 3-54
- Power Cycling the Switch, page 3-54

Using the CLI with Network-Admin Privileges

Detailed Steps

If you are logged in to, or can log into, switch with a user name that has network-admin privileges and then recover the administrator password, follow these steps:

Step 1 Use the **show user-accounts** command to verify that your user name has network-admin privileges.

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin

user:dbgusr
        this user account has no expiry date
        roles:network-admin network-operator
```

Step 2 If your user name has network-admin privileges, issue the **username** command to assign a new administrator password.

```
switch# config t
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

Step 3 Save the software configuration.

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

Power Cycling the Switch

If you cannot start a session on the switch that has network-admin privileges, you must recover the administrator password by power cycling the switch.

Caution This procedure disrupts all traffic on the switch. All connections to the switch will be lost for 2 to 3 minutes.

Note You cannot recover the administrator password from a Telnet or SSH session. You must have access to the local console connection.

Detailed Steps

To recover a administrator password by power cycling the switch, follow these steps:

Step 1 For Cisco MDS 9500 Series switches with two supervisor modules, remove the supervisor module in slot 6 from the chassis.

Note On the Cisco MDS 9500 Series, the password recovery procedure must be performed on the active supervisor module. Removing the supervisor module in slot 6 ensures that a switchover will not occur during the password recovery procedure.

Step 2 Power cycle the switch.

Step 3 Press the **Ctrl-]** key sequence when the switch begins its Cisco NX-OS software boot sequence to enter the `switch(boot)#` prompt mode.

```
Ctrl-]
switch(boot)#
```

Step 4 Change to configuration mode.

```
switch(boot)# config terminal
```

Step 5 Issue the admin-password command to reset the administrator password. This will disable remote authentication for login through console, if enabled. This is done to ensure that admin is able to login through console with new password after password recovery. Telnet/SSH authentication will not be affected by this.

```
switch(boot-config)# admin-password <new password>
WARNING! Remote Authentication for login through console will be disabled#
```

For information on strong passwords, see the "Checking Password Strength" section on page 3-43.

Step 6 Exit to the EXEC mode.

```
switch(boot-config)# admin-password <new password>
```

Step 7 Issue the **load** command to load the Cisco NX-OS software.

```
switch(boot)# load bootflash:m9500-sf1ek9-mz.2.1.1a.bin
```

Caution If you boot a system image that is older than the image you used to store the configuration and do not use the **install all** command to boot the system, the switch erases the binary configuration and uses the ASCII configuration. When this occurs, you must use the **init system** command to recover your password.

Step 8 Log in to the switch using the new administrator password.

```
switch login: admin
Password: <new password>
```

Step 9 Reset the new password to ensure that is it is also the SNMP password for DCNM-SAN.

```
switch# config t
```

```
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

Step 10 Save the software configuration.

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

Step 11 Insert the previously removed supervisor module into slot 6 in the chassis.

Verifying Users and Common Role Configuration

To display Monitoring Users and Common Role configuration information, perform one of the following tasks:

Command	Purpose
show role	Displays information for all roles.
show role status	Displays the Role Status Information.
show role pending	Displays Information on the Pending Roles Database.
show role pending-diff	Displays the Differences Between the Two Databases.
show role name my_role	Displays CLI Operation to SNMP Operation Mapping.
show user-account user1	Displays Information for a Specified User.
show user-account	Displays Information for All Users.
show ssh server	Displays SSH Protocol Status.
show ssh key	Displays Server Key-Pair Details.

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference*.

This section includes the following topics:

- Displaying Role-Based Information, page 3-56
- Displaying Role-Based Information, page 3-57
- Displaying Roles When Distribution is Enabled, page 3-58
- Displaying User Account Information, page 3-60
- Displaying SSH Protocol Status, page 3-61

Displaying Role-Based Information

The rules are displayed by rule number and are based on each role. All roles are displayed if the role name is not specified.

To view rules for a role using Device Manager, follow these steps:

Step 1 Click **Security > Roles.**

You see the Roles dialog box.

Step 2 Select a role name and click **Rules**.

You see the Rules dialog box.

Step 3 Click **Summary** to get a summarized view of the rules configured for this role.

Displaying Role-Based Information

Use the **show role** command to display rules configured on the switch. The rules are displayed by rule number and are based on each role. All roles are displayed if the role name is not specified. See Example 3-3.

Example 3-3 Displays Information for All Roles

```
switch# show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands

Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands

Role: TechDocs
  vsan policy: permit (default)

Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping
```

Displaying Roles When Distribution is Enabled

Use the **show role** command to display the configuration database.

Use the **show role status** command to display whether distribution is enabled for role configuration, the current fabric status (locked or unlocked), and the last operation performed. See Example 3-4.

Example 3-4 Displays the Role Status Information

```
switch# show role status
Distribution: Enabled
Session State: Locked

Last operation (initiated from this switch): Distribution enable
Last operation status: Success
```

Use the **show role pending** command to display the pending role database.

Example 3-5 displays the output of the **show role pending** command by following this procedure:

1. Create the role called `myrole` using the **role name myrole** command.
2. Enter the **rule 1 permit config feature fspf** command.
3. Enter the **show role pending** command to see the output.

Example 3-5 Displays Information on the Pending Roles Database

```
switch# show role pending
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands

Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands

Role: TechDocs
  vsan policy: permit (default)

Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping

Role: myrole
```

```
  vsan policy: permit (default)
  ----------------------------------------------
  Rule     Type     Command-type       Feature
  ----------------------------------------------
    1.    permit     config                 fspf
```

Use the **show role pending-diff** command to display the differences between the pending and configuration role database. See Example 3-6.

Example 3-6 Displays the Differences Between the Two Databases

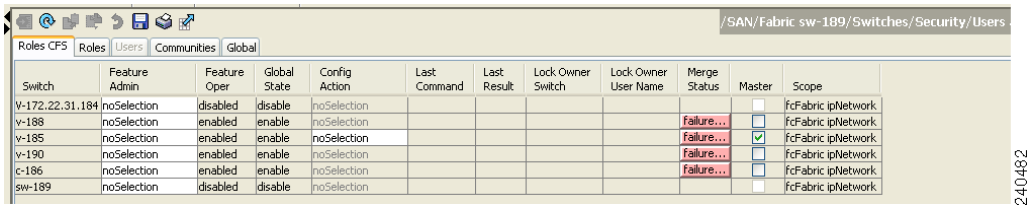
```
switch# show role pending-diff
    +Role: myrole
    +  vsan policy: permit (default)
    +  ----------------------------------------------
    +  Rule     Type     Command-type       Feature
    +  ----------------------------------------------
    +    1.    permit     config                 fspf
```

To view the roles using DCNM-SAN, follow these steps:

Step 1 Expand **Switches > Security** and then select **Users and Roles** in the Physical Attributes pane.

Step 2 Click the **Users** tab in the Information pane (see Figure 3-5).

Figure 3-5 Roles CFS Tab



Step 3 Set the Config View As drop-down value to **pending** to view the pending database or set the Config View as drop-down menu to **running** to view the running database.

Step 4 Click **Apply Changes** to save this change.

Example 3-7 shows the privileges and rules mapping CLI operations to SNMP operations for a role named my_role.

Example 3-7 Displays CLI Operation to SNMP Operation Mapping

```
switch# show role name my_role
Role:my_role
  vsan policy:permit (default)
  ----------------------------------------------
  Rule     Type     Command-type       Feature
  ----------------------------------------------
    1.    permit      clear                   *
    2.      deny      clear                 ntp
    3.    permit     config                   *
    4.      deny     config                 ntp
    5.    permit      debug                   *
    6.      deny      debug                 ntp
```

```
7.   permit      show                  *
8.     deny      show                ntp
9.   permit      exec                  *
```

Note Although CONFIG is denied for NTP in rule 4, rule 9 allows the SET to NTP MIB objects because EXEC also maps to the SNMP SET operation

Displaying User Account Information

Use the **show user-account** command to display configured information about user accounts. See Examples 3-8 to 3-9.

Example 3-8 Displays Information for a Specified User

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

Example 3-9 Displays Information for All Users

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

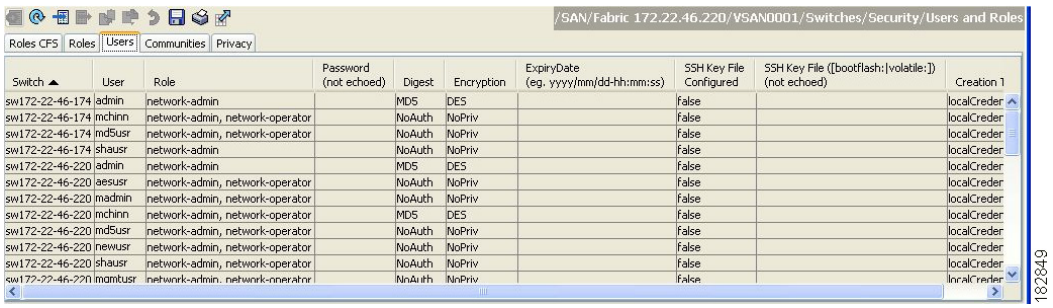
To display information about configured user accounts using DCNM-SAN, follow these steps:

Step 1 Expand **Security** and then select **Users and Roles** in the Physical Attributes pane.

Step 2 Click the **Users** tab.

You see the list of SNMP users shown in Figure 3-6 in the Information pane.

Figure 3-6 Users Listed Under the Users Tab



Displaying SSH Protocol Status

Use the **show ssh server** command to display the status of the SSH protocol (enabled or disabled) and the versions that are enabled for that switch (see Example 3-10).

Example 3-10 Displays SSH Protocol Status

```
switch# show ssh server
ssh is enabled
version 1 enabled
version 2 enabled
```

Use the **show ssh key** command to display the server key-pair details for the specified key or for all keys, (see Example 3-11).

Example 3-11 Displays Server Key-Pair Details

```
switch# show ssh key
rsa1 Keys generated:Sun Jan 13 07:16:26 1980
1024 35
fingerprint:
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07
could not retrieve rsa key information
dsa Keys generated:Sun Jan 13 07:40:08 1980
ssh-dss
AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaWcMMYsEgxc9ada1NElp
8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAOi/Cti84qFb3kTqXlS9mEhdQUo0lH
cH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsAAABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9F
NipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/QwI4q68/eaw=
fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

Note If you are logging in to a switch through SSH and you have issued the **aaa authentication login default none CLI** command, you must enter one or more key strokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

Field Descriptions for Users and Common Role

Common Roles

Note Common roles is not available in displayFCoE mode (use security roles).

Field	Description
Description	Description of the common role.
Enable	This specifies whether the common role has a VSAN restriction or not.
List	List of VSANs user is restricted to.

Feature History for Users and Common Role

Table 3-3 lists the release history for this feature. Only features that were introduced or modified in 5.x or a later release appear in the table.

Remove the second sentence, above, if it does not apply to the table.

Table 3-3 Feature History for FIPS

Feature Name	Releases	Feature Information
Changes to SSH	5.0(1a)	Boot Mode SSH, Passwordfree File copy, and SSH.
Role Distributions	5.0(1a)	Enabling role-based configuration distribution.
Creating Users Guidelines	5.0(1a)	Caution has been changed.