CHAPTER 5

Managing Administrator Access

The Cisco Fabric Manager lets you control management access to Cisco MDS 9000 Family switches, whether you are using the command-line interface (CLI) or SNMP. The Cisco Fabric Manager uses SNMP to communicate remotely with switches. This chapter describes how to set up SNMP users and roles, and how to assign different administrative privileges to different roles.

This chapter also describes how to set up a RADIUS server to provide authentication services to CLI users. To remotely access switches using the CLI, you use Telnet or SSH. For information about managing remote CLI access or configuring a local database for authenticating CLI users, refer to the *Cisco 9000 Family Configuration Guide*.

This chapter includes the following sections:

Managing SNMP Users and Roles

This section describes how to configure or view SNMPv3 users and roles, which allow you to control remote administrative access to Cisco MDS 9000 Family switches. It includes the following topics:

Viewing SNMP Users, Roles, and Communities

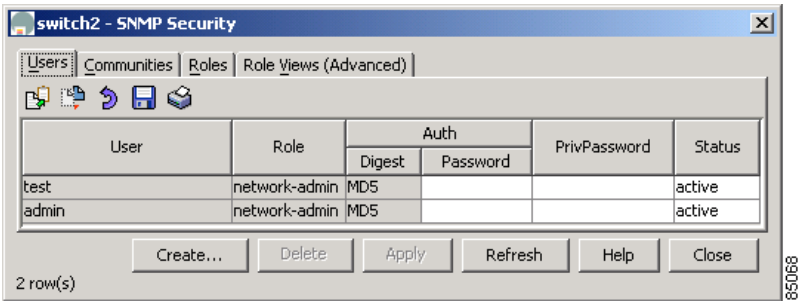
SNMP v3 provides a security model for controlling management access to managed devices in the form of a set of users and roles. Users are assigned to specific roles, and specific administrative privileges are assigned to each role. User names are authenticated through passwords, which are stored and transmitted in encrypted form. In addition, SNMPv3 includes the Privacy option, which encrypts all management traffic exchanged between switches.

SNMP v1 and v2 provide a very limited authentication scheme in the form of read and write community strings. Community strings are like user names, without passwords, and are stored and sent over the SNMP network in clear text (unencrypted) form. For this reason, SNMPv3 should be used wherever network security is a concern.

Send documentation comments to

To view information about SNMP users, roles, and communities from Fabric Manager, choose **Security > SNMP > Users** on the menu tree. To view this information from the Device Manager, choose **SNMP** from the Security menu. Figure 5-1 shows the SNMP dialog box from the Device Manager.

Figure 5-1 Security > SNMP Dialog Box, Device Manager



Both dialog boxes show the display-only information described in Table 5-1.

Table 5-1 Security > SNMP—Display-only Attributes

Display-Only Information	Description
Switch	Displays the switch ID. This attribute is only displayed from the Fabric Manager.
User	Displays the name of the user with system access.
Role	Displays the name of the role or group to which this user belongs. For example, nwadminGroup indicates that the user belongs to the network administration group.
Auth: Digest	Displays the encryption (Hash) algorithm used to encrypt passwords.

Table 5-2 describes the configurable attributes for SNMP security.

Table 5-2 Security > SNMP—Display-only Attributes

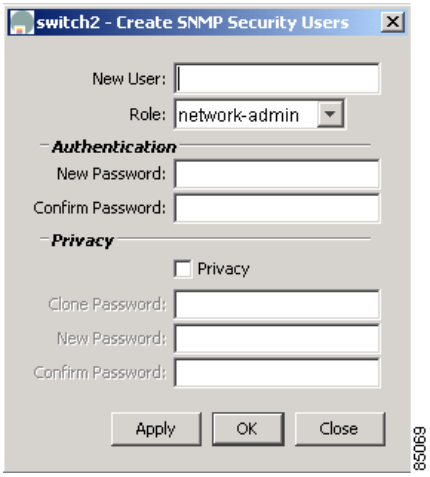
Display-Only Information	Description
Auth: Password	Specifies the password used for authenticating the user.
PrivPassword	Specifies the password used for encrypting management traffic.
Status	Determines the status of the user's access. Valid values are: • active—The user has valid system access. • NotInService—The user does not have valid system access. • notReady—The user account is not ready.

To add a user or community string, follows these steps:

Step 1 Click **Create** on the Device Manager dialog box, or click the **Create Row** button on the Fabric Manager toolbar.

From Device Manager, you see the dialog box shown in Figure 5-2.

Figure 5-2 Create User, Device Manager



The dialog box from Fabric Manager also provides a check box to specify one or more switches.

Step 2 Enter the user name in the New User field.

Step 3 Select the role from the drop-down list.

Step 4 Enter the password for the user twice in the New Password and Confirm Password fields.

Step 5 Click the **Privacy** check box and complete the password fields to enable encryption of management traffic,

Enter the Authentication password in the Clone Password field to use the same password. Enter a new password twice in the New Password and Confirm Password fields.

Step 6 Click **Apply** to create the new entry or click **OK** to create the entry and close the dialog box.

Configuring SNMP Communities

If you are running SNMPv3, you must define users (or security names), assign them to roles (or groups), and assign system access based on those roles. If you are running SNMPv1 or SNMPv2c, you must define communities, which are equivalent to SNMPv3 users or security names. SNMPv3 allows you to define user access to the object level. SNMPv1 and SNMPv2c do not allow you to define system access at the object level.

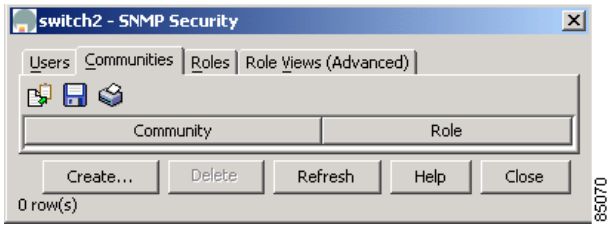
Table 5-3 shows the mapping of users (SNMPv3) and communities (SNMPv1 and SNMPv2c).

Table 5-3 SNMP Mappings

SNMPv3	SNMPv1, SNMPv2c
user or security name	community
role	role

To configure users and communities from the Device Manager, choose **SNMP** from the Security menu. and click the **Communities** tab. To configure users and communities from the Fabric Manager, choose **Security** > **SNMP** > **Communities** from the menu tree. Figure 5-3 shows the SNMP dialog box with the Communities tab selected from the Device Manager.

Figure 5-3 Security > SNMP > Communities Dialog Box, Device Manager



Both dialog boxes show the display-only information described in Table 5-4.

Table 5-4 Security > SNMP > Communities—Display-Only Attributes

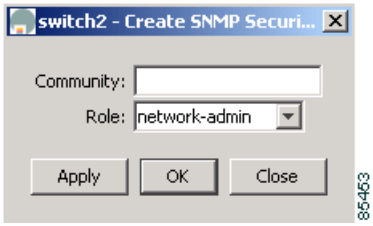
Display-Only Information	Description
Switch	Displays the switch ID. This attribute is only displayed from the Fabric Manager.
Community	Specifies the SNMPv1/SNMPv2c community name, which is equivalent to an SNMPv3 user.
Role	Specifies the name of the group to which the community or user belongs.

To add a community string, follow these steps:

Step 1 Click **Create** on the Device Manager dialog box or click the **Create Row** button on the Fabric Manager toolbar.

From Device Manager, the system displays the dialog box shown in Figure 5-4.

Figure 5-4 Create Community, Device Manager



The dialog box from Fabric Manager also provides a check box to specify one or more switches.

Step 2 Enter the community string in the Community field.

Step 3 Select the user role from the pull-down selection list.

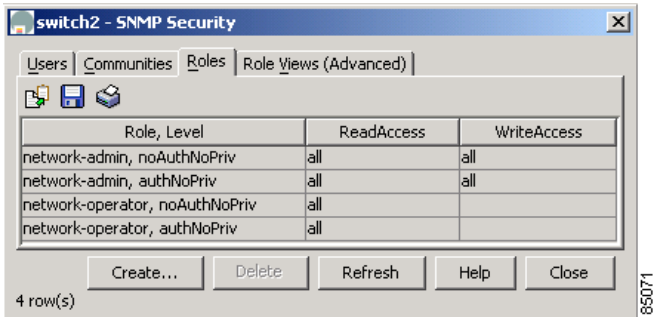
Step 4 Click **Create**.

Configuring User Roles

User roles let you define a set of administrative permissions to a role and then assign this role to different users.

To configure users roles, choose **SNMP** from the Device Manager Security menu, and click the **Roles** tab. See Figure 5-5.

Figure 5-5 Security > SNMP > Roles Dialog Box, Device Manager



This dialog box shows the display-only information described in Table 5-5.

Table 5-5 Security > SNMP > Roles—Display-Only Attributes

Display-Only Information	Description
Role	Specifies the name of the group to which the community or user belongs.
Level	Specifies access level for the selected view. Check the radio button for the appropriate level: • authNoPriv—Authenticated with no privacy (encryption) • authPriv—Authenticated with privacy (encryption)

Table 5-5 Security > SNMP > Roles—Display-Only Attributes (continued)

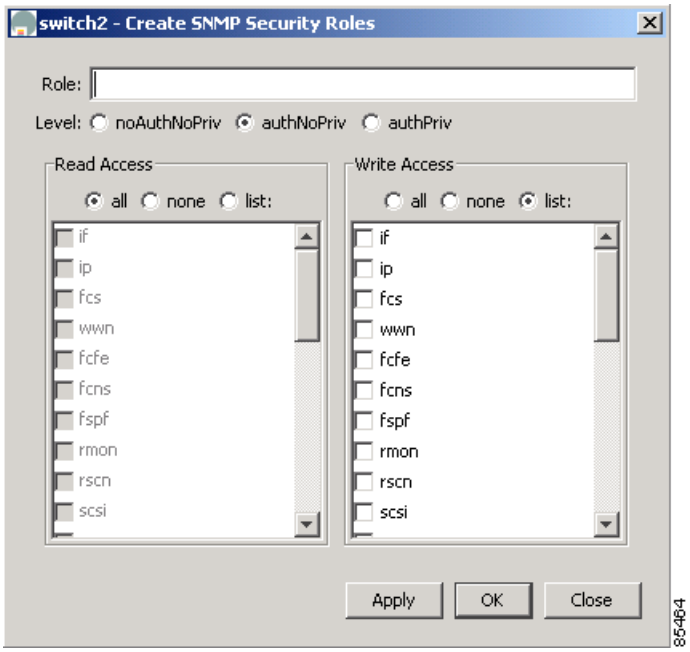
Display-Only Information	Description
ReadAccess	Specifies read-only access for the selected view. Check the appropriate radio button to select views for access: • all—Grants read-only access to all views. • none—Denies read-only access to all views. • list—Grants read-only access to selected views. Check the check boxes to select views for which read access is to be granted.
WriteAccess	Specifies write access for the selected view. Check the appropriate radio button to select views: • all—Grants read-only access to all views. • none—Denies read-only access to all views. • list—Grants read-only access to selected views. Check the check boxes to select views for which write access is to be granted.

To create a new role, follow these steps:

Step 1 Click **Create**.

The system displays the dialog box shown in Figure 5-6.

Figure 5-6 Create Role, Device Manager



Step 2 Enter an identifier for the role in the Role field.

Step 3 Select one of the following security levels:

- authNoPrv—Authentication without encryption
- AuthPriv—Authentication with encryption

Step 4 For Read access, click the **All** radio button to enable full read access or click **List** and click each check box in the list to enable read access to specific information.

Step 5 For Write access, click the **All** radio button to enable full read access or click **List** and click each check box in the list to enable read access to specific information.

Step 6 Click **Apply** to create the new role or click **OK** to create the role and close the window.

Role Views (Advanced)

To see role views from the Device Manager, choose **SNMP** from the Security menu, and click the **Role Views (Advanced)** tab.

The dialog box shows the display-only information described in Table 5-6.

Table 5-6 Security > SNMP > Role Views—Display-Only Attributes

Display-Only Information	Description
Switch	Displays the switch ID. This attribute is only displayed from the Fabric Manager.
ViewName, Subtree	Displays the text and numeric names of the subtree of accessible views.
Type	Displays the type. Valid values are: • included—The view is accessible. • excluded—The view is not accessible.
Mask	Displays the bit mask of the subtree.

Configuring RADIUS Security for CLI Access

This section describes how to configure RADIUS servers for managing administrative access to the CLI. It includes the following topics:

Configuring RADIUS Authentication

To configure RADIUS authentication from the Fabric Manager, choose **Radius** > **General** from the menu tree. To configure RADIUS authentication from the Device Manager, choose **Radius** (CLI) from the Security menu. Figure 5-7 shows the dialog box with the General tab selected from the Device Manager.

Figure 5-7 Security > Radius Dialog Box, Device Manager

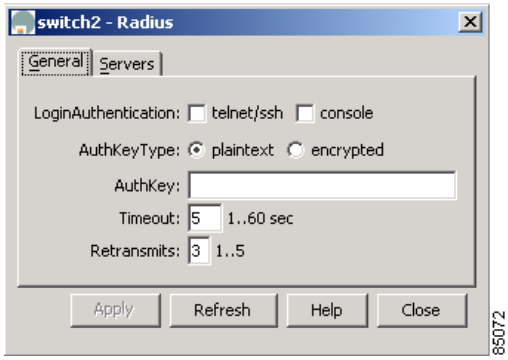


Table 5-7 describes the configurable attributes for RADIUS authentication.

Table 5-7 Security > Radius

Configurable Attribute	Description
Switch	Displays the switch ID. This is a display-only attribute, in Fabric Manager only.
LoginAuthentication	Enables RADIUS login authentication for either Telnet or console sessions.
AuthKeyType	Specifies the authentication key type. Check the radio button to select either a plain text or an encrypted authentication key type.
AuthKey	Specifies the authentication key to be used to encrypt packets that are passing between the RADIUS server and the client. This key must match the key configured on the server.

Table 5-7 Security > Radius (continued)

Configurable Attribute	Description
Timeout	Specifies the time (in seconds) between retransmissions to the RADIUS server. Valid values are 1 to 1000 seconds.
Retransmits	Specifies the number of times the authentication request should be tried before giving up on the RADIUS server. Valid values are 1 to100 retransmits.

Configuring RADIUS Servers

To configure RADIUS servers from the Device Manager, choose **Radius** from the **Security** menu and click the **Servers** tab. To configure RADIUS servers from the Fabric Manager, choose **Radius** > **Servers** from the menu tree. Figure 5-8 shows the dialog box with the Servers tab selected from the Device Manager.

Figure 5-8 Security > Radius > Servers Dialog Box, Device Manager

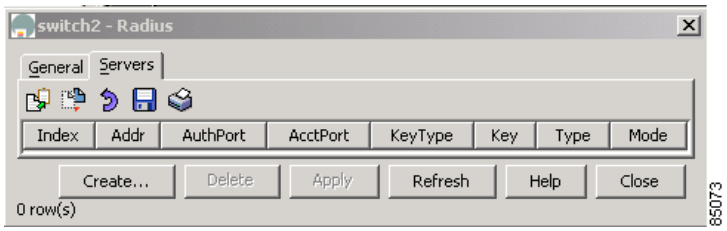


Table 5-8 describes the configurable attributes for RADIUS servers.

Table 5-8 Security > Radius > Servers—Configurable Attributes

Configurable Attribute	Description
Switch	Displays the switch ID. This is a display-only attribute, in Fabric Manager only.
Index	Specifies the RADIUS server's index or ID.
IpAddress	Specifies the RADIUS server's IP address.
AuthPort	Specifies the destination UDP port number to which RADIUS authentication messages should be sent. Valid values are 0 to 65535. If set to 0, this RADIUS server is not used for authentication.
AcctPort	Specifies the destination UDP port number to which RADIUS accounting messages should be sent. Valid values are 0 to 65535.
KeyType	Specifies the authentication key type. Check the radio button to select either a plain text or an encrypted authentication key type.

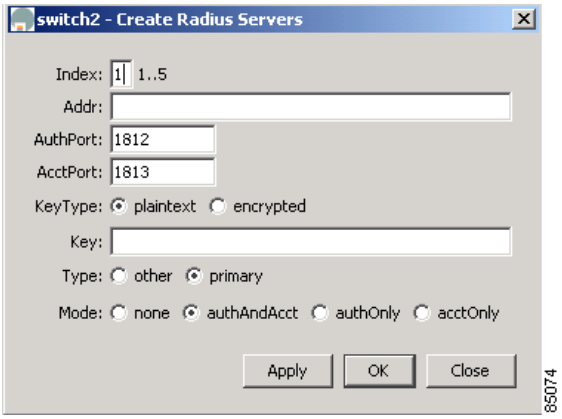
Table 5-8 Security > Radius > Servers—Configurable Attributes (continued)

Configurable Attribute	Description
Key	Specifies the authentication key to be used to encrypt packets that are passing between the RADIUS server and the client. This key must match the key configured on the server.
Type	Specifies the RADIUS server type. Click the radio button to specify either primary or other.
Mode	Specifies the RADIUS server mode. Click the radio button to select: • authAndAcct—Selects both authentication and accounting mode. • authOnly—Selects authentication mode only. • acctOnly—Selects accounting mode only. • none—Specifies no mode.

To add a Radius server, click **Create** on the Device Manager dialog box, or click the **Create Row** button on the Fabric Manager toolbar.

From Device Manager, you see the dialog box shown in Figure 5-9.

Figure 5-9 Create Radius Server, Device Manager



The dialog box from Fabric Manager lets you specify the switches to which the configuration applies

See Table 5-8 for information about each field, complete the fields, and click **OK**.