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.

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.

Procedures for managing SNMP users and roles, which allow you to control remote administrative access to Cisco MDS 9000 Family switches, include:

- Viewing SNMP Users, Roles, and Communities, page 5-2
- Adding a User or Community String, page 5-2
- Configuring SNMP Communities, page 5-3
- Configuring User Roles, page 5-4
- Configuring Common Roles, page 5-4

You can also 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*.

Procedures for setting up a RADIUS server include:

- Configuring RADIUS Authentication, page 5-6
- Configuring RADIUS Servers, page 5-6

Viewing SNMP Users, Roles, and Communities

To view information about SNMP users, roles, and communities from Fabric Manager, choose **Security > SNMP** from the menu tree and click the **Users** tab. The list of SNMP users, roles, and communities is displayed in the Information pane.

To view this information from the Device Manager, choose **SNMP** from the Security menu. The SNMP dialog box is displayed.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Adding a User or Community String

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.

The Create Community string dialog box is displayed.

The dialog box from Fabric Manager also provides check boxes 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 **Create** to create the new entry or click **Close** to create the entry and close the dialog box.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

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 5-1 shows the mapping of users (SNMPv3) and communities (SNMPv1 and SNMPv2c).

Table 5-1 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. The SNMP dialog box with the Communities tab selected is displayed.

To configure users and communities from the Fabric Manager, choose **Security > SNMP** from the menu tree and click the **Communities** tab. The SNMP Communities information is displayed in the Fabric Manager Information pane.

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.

The Create Community string dialog box is displayed.

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**.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring User Roles

User roles let you define a set of administrative permissions for 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.

To create a new role, follow these steps:

Step 1 Click **Create**.

The system displays the Create Roles dialog box.

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.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring Common Roles

Common Roles allow you to use a set of rules to set the scope of VSAN security. To configure Common Roles from the Device Manager, select Common Roles from the Security menu. You can then access the Rules dialog box to configure the set of rules. To configure Common Roles from Fabric Manager, select **Security > SNMP** and click the **Roles** tab in the Information pane. Fabric Manager uses a default rules set for roles; therefore, no Rules dialog box is displayed.

The list below shows the Common Roles tasks you can perform with Device Manager or Fabric Manager.

- Creating Common Roles, page 5-4
- Editing Common Role Rules (DM Only), page 5-5
- Deleting Common Roles, page 5-6

Creating Common Roles

To create a common role, perform the following steps.

Step 1 From the Device Manager, choose **Common Roles** from the **Security** menu. The Common Roles dialog box is displayed.

From Fabric Manager, select **Security > SNMP** from the menu tree, and click the **Roles** tab in the information pane.

Step 2 Click the **Create** button.

The Create Common Roles dialog box is displayed.

Step 3 From Fabric Manager, select the switches for which you want to configure the Common Role. If you are using Device Manager, skip to Step 4.

Step 4 Enter the name of the Common Role in the Name field.

Step 5 Enter the description of the Common Role in the Description field.

Step 6 From Fabric Manager, check (or uncheck) the **Has Config and Exec Permission** checkbox. If you are using Device Manager, skip to Step 7.

If you check the checkbox, your role will have read, write, and create permission. If you do not check the checkbox, your role will have read-only permission.

Step 7 Click **Enable** to enable the VSAN scope.

Step 8 Enter the scope in the Scope field.

Step 9 From Device Manager, click the **Rules** button to view the rules for the role, and select the rules you want to enable. Then click **Close** to close the Rules dialog. If you are using Fabric Manager, skip to Step 10.

The Rules dialog may take a few minutes to display.

Step 10 Click **Create** to create the common role, or click **Close** to close the Common Role dialog without creating the common role.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Editing Common Role Rules (DM Only)

To edit the rules for a common role, perform the following steps.

Step 1 From the Device Manager, choose **Common Roles** from the **Security** menu.

The Common Roles dialog box is displayed.

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

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

The Rules dialog may take a few minutes to display.

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

Step 5 Click **Apply** to apply the new rules and close the Rules dialog, or click **Close** to close the Rules dialog without applying the rules.

Step 6 Click **Apply** to create the common role, or click **Close** to close the Common Role dialog without creating the common role.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Deleting Common Roles

To delete a common role, perform the following steps.

Step 1 From the Device Manager, choose **Common Roles** from the **Security** menu. The Common Roles dialog box is displayed.

From Fabric Manager, select **Security > SNMP** from the menu tree, and click the **Roles** tab in the information pane.

Step 2 Click once to select the common role you want to delete.

Step 3 Click the **Delete** button to delete the common role.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring RADIUS Authentication

To configure RADIUS authentication from the Fabric Manager, choose **Security > Radius** from the menu tree.

To configure RADIUS authentication from the Device Manager, choose **Radius** (CLI) from the Security menu.

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.

Configuring RADIUS Servers

To configure RADIUS servers, perform the following steps:

Step 1 From the Device Manager, choose **Radius** from the **Security** menu and click the **Servers** tab. The Radius dialog box with the Servers tab selected is displayed.

To configure RADIUS servers from the Fabric Manager, choose **Security> Radius** from the menu tree and click the **Servers** tab. The Radius information is displayed in the Information pane.

Step 2 To add a Radius server, click **Create** on the Device Manager dialog box, or click the **Create Row** button on the Fabric Manager toolbar.

The Create Radius Server dialog box is displayed. In Fabric Manager, you can specify the switches to which the configuration applies

Step 3 Complete the fields, and click **OK.**

Note You can access the field descriptions for the windows or dialog boxes in this procedure in the Reference section of the Fabric Manager or Device Manager help systems.