# Security

Cisco MGM enforces security with user names and passwords, and manages user accounts individually and in groups. The use of access groups simplifies the process of assigning privileges to individual users because such groups enable you to define a set of privileges for each type of user.

## Cisco EMF User Accounts

Cisco EMF enforces security with the following types of accounts.

*Table 7-1 Cisco EMF Accounts*

| Access Level | Account Type | Number of Users | Access Type | Command Groups |
|---|---|---|---|---|
| 1 | Administrator | 1 | Read/Write | All categories |
| 2 | User defined | As many as needed | Read/Write | User can only invoke the categories of service defined by the access spec of its user group |

From Cisco EMF's Access application, an administrator can arrange Cisco EMF user accounts in groups. These groups can be used to model user roles; for example, administrators typically set up a user group for administrative users and system operators.

To add, change, or delete user accounts or groups, refer to the *Cisco Element Management Framework User Guide*.

## Changing Passwords

You can change your own password. System administrators can change any password.

To make administrative password changes, follow these steps:

**Step 1** Open the Access Manager window and select the name of the user whose password is to be changed.

**Step 2** From the Edit menu, select **Change Password**. For instance, to change the admin password, select **Change Admin Password**.

**Note** The **Change Admin Password** option is available only to system administrators.

The Change User Password window opens.

**Step 3** Enter the existing password in the Old Password field.

**Step 4** Enter a new password in the **New Password** field, and reenter the new password to verify your choice.

**Step 5** Click **OK**.

**Step 6** If an invalid password is entered or the new password is not verified correctly, an error message is displayed. Click **OK** to try again.

# Cisco MGM Community String and Security Configuration

When Cisco MGM communicates with Cisco MGX 8000 Series CVGs, security is enforced with community strings. SNMP communities group workstations and servers that can manage the Cisco MGX 8000 Series CVGs according to their access privileges. A read-only community string is required to perform an SNMP “get” function. A read-write community string is required to perform an SNMP “set” function (can also be used to perform a “get” function.)

For Cisco MGM to configure the gateways, both Cisco MGM and the gateways must agree on a community string. Community string configuration is a multistep process, starting with each gateway and ending with the Cisco MGM that manages them.

The following notes pertain to the configuring of community strings for Cisco MGM:

- You need to know the Cisco MGX 8000 Series CVG community strings when configuring Cisco MGM. The read community string you specified for auto discovery is the default read community for all of the managed objects on the Cisco MGX 8000 Series CVG and its children. The default read community for Cisco MGM is public.
- Always use the **SNMP and Security Configuration Dialog** option from the chassis or site level to modify the read/write community string.
- The connection between Cisco MGM and each Cisco MGX 8000 Series CVG has its own community string. You may use identical community strings for each gateway, or you may have different community string values for each managed gateway. The dialog box displays only the last value stored locally.

To configure community strings and security, follow these steps:

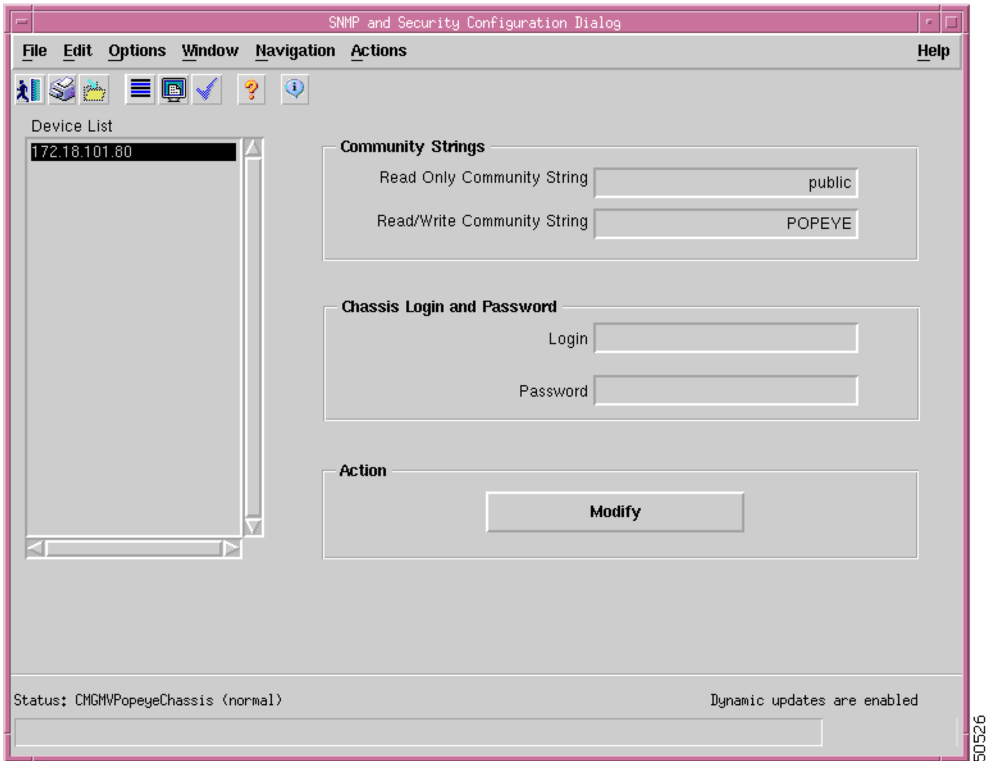
**Step 1** Log on to Cisco MGM.

**Step 2** On the Cisco EMF Launchpad, click **Viewer**. The Cisco EMF MapViewer opens.

**Step 3** Click the object tree, right-click on the desired site or object, and click **SNMP and Security Configuration Dialog**.

The SNMP and Security Configuration window opens. (See Figure 7-1.)

***Figure 7-1 SNMP and Security Configuration Dialog***



172.18.101.80

Community Strings

Read Only Community String: public

Read/Write Community String: POPEYE

Chassis Login and Password

Login:

Password:

Action

Status: CMGMVPopeyeChassis (normal)

Dynamic updates are enabled

**Note** For security reasons, the current chassis password is not displayed.

**Step 4** Select one or more IP addresses from the list, using the **Shift** key to select multiple addresses.

**Step 5** Modify the default read-only and read-write community strings in the corresponding fields as required.

**Note** The SNMP read–only community string parameter for PXM1 based chassis is always public on the device, therefore there is no need to change this value on the SNMP and Security Configuration window.

**Step 6** Enter the desired chassis login and password values to be used to telnet to the device to issue CLI commands and to transfer data (via FTP or TFTP.)

**Note** The TFTP function is used when a PXM1-based card is in the chassis while the FTP function is used when a PXM1E or PXM45-based card is in the chassis.

**Step 7** Click **Modify**.

A confirmation screen opens that reports successful and unsuccessful configuration attempts.

**Step 8** Click **Close**.

**Note** When subchassis synchronization is first invoked after auto-discovery, Cisco MGM uses the default read-write community string as specified in the UserData.ini file. If the device community string is different from the default read-write community string, objects under cards (lines and sessions) won't be found. In this case, configure the read-write community string of the device in Cisco MGM to match the actual read-write community string of the device, then perform a subchassis synchronization. For information about changing the default read-write community string, refer to the "Inventory Discovery" section on page 4-4.