CHAPTER 4

Setting Up Cisco MNM Security

Revised: December 15, 2009, OL-18339-03

This chapter is designed for system administrators. It provides an overview of Cisco Media Gateway Controller (MGC) Node Manager (MNM) security capabilities and describes the following:

Note This chapter describes managing security as it applies to users of Cisco MNM; it does not cover the use of SSH or the Security Policy attribute in communicating with managed components. For information on installing SSH, see the *Cisco Media Gateway Controller Node Manager Installation Guide* at: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/prod_installation_guides_list.html. Information on using SSH-enabled functions is covered under the relevant functions in this guide. To define a component's security policy at deployment, see Chapter 5, "Deploying Your Network in Cisco MNM". To change the security policy of an existing component using the Accounts dialog box, see Chapter 8, "Other Network Management Tasks," "Viewing or Modifying Account and SNMP Information" section on page 8-6.

Overview of Cisco MNM Security

Cisco MNM provides user access control, which allows you as a system administrator to control the operations that different users can perform. Each user has a different login name and password and a specific set of privileges within the system.

A standard administrator user (admin) is available by default. The administrator user has access to all features at all times. Do not edit the administrator user except to change the password.

Cisco MNM requires every user to have a login ID and password. Users must specify their login ID and enter the correct password before they can start the application. An administrator account is provided to allow for creating, modifying, resetting, and deleting user accounts.

Within Cisco MNM, access to features can be restricted on the basis of the user's access level to a subset (or group) of these features. For example, administration of particular managed objects should be performed only by operators who are responsible for that particular site or for a region in which that site resides. However, these operators may also require visibility of objects outside their own area of control.

The basic building blocks used to control user access are described in the following sections.

User Groups

Cisco MNM user accounts can be collected by an administrator into groups. These user groups can be used to model user roles. A typical setup might involve a user group for system administrators, for network fault detail users, and for operators to manage a given site.

Cisco MNM applies access control based on user groups. The Cisco MNM administrator configures access control by assigning access specifications to the relevant user groups.

Feature Lists

All features are grouped together into feature lists. The benefit of feature lists is that it is easy to give access to a related set of features by simply choosing a feature list instead of having to assign features individually. A feature may appear in more than one feature list. Permissions are:

- R—Read only. Available to all users. Useful for new users finding their way around the system.
- RW—Read-Write. Normal level, allowing the user to make modifications, such as acknowledging and clearing events or deploying the network. Operators typically have Read-Write access to the features they need for day-to-day tasks.
- RWA—Administrator. Administration level, allowing the user Read-Write access to all features at all times. This is available to administrators only.

Table 4-1 describes feature lists available in Cisco MNM.

Table 4-1 Feature Lists in Cisco MNM

Feature List	Permissions[1]	Description
AccessManagement	RWA	Set up users, user groups, assign passwords, and define access parameters.
AutoDiscovery	RW	Launch the auto-discovery services.
Change Password	RWA	Change passwords.
Deployment	RW	Deploy sites, regions, and networks (generic object deployment).
EventGroupEditFeatureList	RW	Create and edit event groups.
EventGroupViewFeatureList	R	View existing event groups.
Events-View	R	Launch the event browser in read-only mode.
Events-Clear_Acknowledge	RW	Clear and acknowledge events.
GenericConfigApplication	RWA	Launch the object configuration utility.
Help	R	Launch online help.
Host-Dialplan-Properties	R	View properties of Cisco PGW 2200 Softswitch host dial plan components.
Host-Signaling-Performance	RW	View performance statistics for signaling components.
Host-Signaling-Properties	R	View properties of Cisco PGW 2200 Softswitch host signaling components.
Host-Trunking-Properties	R	View properties of Cisco PGW 2200 Softswitch host trunking components.

Table 4-1 Feature Lists in Cisco MNM (continued)

Feature List	Permissions[1]	Description
Launchpad	R	Use the CEMF LaunchPad (start a CEMF session).
MGC-Node-Accounts	RWA	Change passwords, login IDs, and SNMP community strings.
MGC-Node-Admins	RWA	Use the Cisco MNM Administration Tool to start, stop, or reboot a device.
MGC-Node-Diagnostics	RW	Run diagnostic tools on Cisco PGW 2200 Softswitch node components.
MGC-Node-Filesystems	RW	View file system information on BAMS, HSI server, and Cisco PGW 2200 Softswitch host devices.
MGC-Node-Properties	R	View properties of Cisco PGW 2200 Softswitch node components.
MGC-Node-Provisioning	RWA	Deploy all Cisco PGW 2200 Softswitch node components (either manually or through a seed file).
MGC-Node-States	RW	Change the states of Cisco PGW 2200 Softswitch node components.
MGC-Node-Tools	RW	Launch Cisco PGW 2200 Softswitch node component tools.
MGC-Node-Transfer	RW	Configure performance.
MGC-Node-Trap-Forwarding	RWA	Configure trap forwarding destinations.
NotificationEditFeatureList	RW	Create and edit notification profiles.
NotificationViewFeatureList	R	View existing notification profiles.
ObjectGroups-Edit	RW	Create and edit object groups.
ObjectGroups-View	R	View existing object groups.
Performance Management	RW	Open the Performance Manager utility.
ThresholderEditFeatureList	RW	Define and edit thresholds.
ThresholderViewFeatureList	R	View existing thresholds.
Viewer-Edit	RW	Use the Map Viewer in read-write mode.
Viewer-View	R	Use the Map Viewer in read-only mode.

1. Use this column to determine which features are appropriate for various types of users. For more information, see the "Setting Up Security for Typical User Roles" section on page 4-10.

Note In Cisco MNM, features are preassigned to feature lists and cannot be modified.

Access Specifications

Access specifications define the features that can be invoked by a group of users and the objects upon which these features can be invoked.

Cisco MNM provides a number of access specifications. As a system administrator, you can create additional access specifications tailored to your needs.

Each access specification can include the following components:

- Feature lists—Lists the Cisco MNM features in the access specification. A feature list can appear in more than one access specification. Cisco MNM feature lists are shown in Table 4-1.
- User groups—Cisco MNM user accounts can be collected by an administrator into groups that correspond to user roles at your site. By associating user groups with access specifications, you can apply access control.
- A permission level—For example, read-only, read-write (view and modify information), and read-write-administrator (read and write all functions at all times).
- An optional object group—Where an object group is supplied, users have access to the features included in this access specification only for those objects contained within the group. Where no object group is supplied, the access specification provides the specified access to features for all objects. You might use this option to grant the administrative user group for a site read-write access to the objects on that site, while another access specification would be used for read-only access for non administrative users.

Table 4-2 lists access specifications predefined in Cisco MNM.

Table 4-2 Predefined Access Specifications in Cisco MNM

Access Specification	Permissions	Feature Lists Included
Full_User_Access_Control	RWA	AccessManagement
Generic_Config_Application	RWA	GenericConfigApplication
Deployment	RWA	Deployment
AutoDiscovery	RWA	AutoDiscovery
Full_Event_Browser_Access	RWA	EventsView
		EventsClear_Acknowledge
EventManagerAccessSpec	RWA	ThresholderEditFeatureList
		ThresholderViewFeatureList
		NotificationEditFeatureList
		NotificationViewFeatureList
		EventGroupEditFeatureList
		EventGroupViewFeatureList
MGCHostServices	R	HostSignalingProperties
		HostDialplanProperties
		HostTrunkingProperties
		HostSignalingPerformance
Launchpad	RWA	Launchpad
MGCNodeServices	RWA	MGCNodeProvisioning
		MGCNodeTrapForwarding
		MGCNodeStates
		MGCNodeAdmin

Table 4-2 Predefined Access Specifications in Cisco MNM (continued)

Access Specification	Permissions	Feature Lists Included
		MGCNodeAccounts
		MGCNodeFilesystems
		MGCNodeProperties
		MGCNodeTransfer
		MGCNodeDiagnostics
		MGCNodeTools
Full_Object_Group_Access	RWA	ObjectGroupsView
		ObjectGroupsEdit
Full_Viewer_Access	RWA	ViewerEdit
		ViewerView
PerformanceManager	RWA	PerformanceManager
All_Standard_Features	RWA	Launchpad
		ChangePassword
		AccessManagement
		GenericConfigApplication
		EventsView
		EventsClear_Acknowledge
		FilterEditor
		ObjectGroupsEdit
		ObjectGroupsView
		ViewerEdit
		ViewerView
		Help
		Deployment
		AutoDiscovery
		PerformanceManager
		ThresholderEditFeatureList
		ThresholderViewFeatureList
		NotificationEditFeatureList
		NotificationViewFeatureList
		EventGroupEditFeatureList
		EventGroupViewFeatureList

Setting Up Security

To set up security, define the following:

- User accounts—Assign login IDs and passwords to individuals and optionally place them in user groups.
- User groups—Assign access specifications to a named group and assign users to user groups.

You can add new access specifications to define new groupings of features tailored to specific user roles in your system.

These tasks may be done in any order. They are interrelated—user groups have associated access specifications and users, and access specifications are linked to user groups. Before beginning, think through the types of users working with your system and the kinds of tasks they need to perform. Use this to plan user groups and access specifications on paper before you create user accounts, user groups, and access specifications. For examples, see the "Setting Up Security for Typical User Roles" section on page 4-10.

Setting Up New Accounts

You must set up new accounts for all users. Use the following procedure to create a new account for a user and assign a password:

Step 1 Click the **Access** icon on the Cisco EMF LaunchPad.

The Access Manager window opens.

Step 2 Choose **Edit > Create > User**.

The Create User window opens.

Step 3 Enter the login information for the new user. The login name must contain 5 to 32 characters; only alphanumeric characters and underscores are valid, and the first character must be a letter. Click **Forward**.

The Copy From Existing User window opens. If user groups have been defined and one or more user is already assigned to a group, "Copy from existing user" copies the user group assignment of the selected user.

Step 4 If you do not want to copy the assignment of an existing user or none exists, click **No**, and then click **Forward**.

To automatically place this user in the same user group as another user, click **Yes**. The list of users displays.

Step 5 Select the user whose assignment you want to copy, and click **Forward**.

The Select User Groups window opens.

Step 6 Select a user group, click the right arrow to move the group to the Selected User Groups list, and click **Forward**.

If no user groups are defined, click **Forward**. You may define a user group later and assign the user to it at any time. For more information on user groups, see the "Creating a User Group" section on page 4-7.

The User Password Entry window opens.

Step 7 Enter a password for the user and confirm it.

The Summary Details for User window opens.

Note Passwords must contain 8 to 32 alphanumeric characters and at least one punctuation character such as _, %, (, or ^. Click **Forward**.

Step 8 If you are satisfied with the user definition, click **Finish**. If not, click **Back** to make modifications.

When you click **Finish**, the user is added and the Access Manager window closes. You are returned to the Launchpad window.

Creating a User Group

Use the following procedure to define an access privilege user group to which you can assign users:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2 Choose **Edit > Create > User Group**.

The Create User Group window opens.

Step 3 Enter the name for the new group.

The Copy From Existing User Group window opens. If user groups have been defined and one or more user is already assigned to a group, "Copy from existing user group" copies the access specifications and user membership of the selected group. Use this to base a group on an existing group, and then click the **Modify > User Groups** menu option to add or remove access specifications or users.

Step 4 If you do not want to copy an existing user or none exists, click **No**, and then click **Forward**.

If you want to base this user group on another, click **Yes**. The list of groups displays. Select the group you want to copy, and then click **Forward**.

The Select Users window opens listing existing users.

Step 5 Select each user you want in the new group, and then click the right arrow to move the user to the Selected Users list. Press Ctrl-click to select multiple users. When you are finished, click **Forward**.

The Select Access Specifications window opens, listing available access specifications. See Table 4-2 for the list of predefined Cisco MNM access specifications.

Step 6 Select each desired access specification, and then click the right arrow to move the specification to the Selected Access Specs list. Press Ctrl-click to select multiple specifications. When you are finished, click **Forward**.

The Summary Details for User Group window opens listing the user group name, members, and selected access specifications.

For details on access specifications, see the "Creating a New Access Specification" section on page 4-8.

Note Giving a user group Full User Access Control allows each user in the user group to add or delete other users to or from the group and to change specifications for all other users.

Step 7 If you are satisfied with the user group definition, click **Finish**. If not, click **Back** to make modifications.

When you click **Finish**, the user group is added and the Access Manager closes. You are returned to the Launchpad window.

Creating a New Access Specification

Use the following procedure to create a new access specification:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2 Choose **Edit > Create > Access Spec**.

The Create Access Specification window appears.

Step 3 Enter the name for the new specification.

The Copy From Existing Access Spec window appears. “Copy from existing access spec” copies the access specification and its user group assignments, if any. Use this to base a specification on an existing specification, and then click the **Modify > Access Specs** menu option to add or remove feature lists or user groups. See Table 4-2 for a list of predefined access specifications.

Step 4 If you want to base this specification on another, click **Yes**. The list of specifications displays. Select the one you want to copy, and then click **Forward**. Skip to Step 9.

If you do not want to copy an existing access specification, click **No,** and click **Forward**. The Select Permission window opens. Continue to Step 5.

Step 5 Select the permission for the new specification:

Read Only (basic level)—Information can be viewed only.

Read-Write (normal level)—Information can be viewed or modified.

Read-Write-Admin (administration level)—Read-Write access to all features at all times. This is available to administrators only.

Click **Forward**.

The Select User Groups window opens listing user groups to which you can assign this specification.

Step 6 Select each user group you want to assign the new specification, and click the right arrow to move it to the Selected User Groups list. Press Ctrl-click to select multiple groups. When you are finished, click **Forward**.

The Select Feature Lists window opens displaying the available feature lists. See Table 4-1.

Step 7 Select each feature you want to include in the specification, and click the right arrow to move the group to the Selected Features list. Press Ctrl-click to select multiple features. When you are finished, click **Forward**.

The Select Object Groups window opens. Each access specification can have one associated object group to limit this specification to a particular type of object.

Step 8 Select the object group, if any, that you want to associate with this access specification, and click **Finish**.

Note If you do not select a group, the specification is not restricted to a specific object group.

Step 9 The Summary Details for Access Specifications window opens, summarizing the new specification, including:

- The access specification name
- Permissions
- Feature lists included

- The object group associated with the specification
- User groups to which the specification is assigned

If you are satisfied with the new access specification, click **Finish**. If not, click **Back** to make modifications.

When you click **Finish**, the access specification is added to the specification list and the Access Manager closes. You are returned to the Launchpad window.

Setting Up Security for Typical User Roles

Table 4-3 summarizes how to set up security for typical user roles.

Table 4-3 Security for Typical Roles

For This Role	Perform These Steps
Administrator	Use the instructions in the "Setting Up New Accounts" section on page 4-6 to create a new user by copying the existing administrator template. The administrator should have all the features labeled with the permissions R, RW, and RWA in Table 4-1.
Normal user (read permission and ability to deploy and launch tools, but not to use configuration management)	Using the instructions in the "Creating a New Access Specification" section on page 4-8, create a new access specification with the features labeled with the permissions R and RW in Table 4-1, but not including: • AutoDiscovery • ObjectGroups-Edit • ObjectGroups-View Use the instructions in the "Creating a User Group" section on page 4-7 to create a new user group with the access specification you just created. Use the instructions in the "Setting Up New Accounts" section on page 4-6 to create a new account and user, and assign the user to the group you just created.
Novice user or user who only needs to view information	Using the instructions in the "Creating a New Access Specification" section on page 4-8, create a new access specification with the features labeled with the permission R in Table 4-1. Using the instructions in the "Creating a User Group" section on page 4-7, create a new user group with the access specification you just created. Using the instructions in the "Setting Up New Accounts" section on page 4-6, create a new account and user, and assign the user to the group you just created.

Modifying Security Settings

You can do the following using the Access Manager:

- Modify a user account to change the user login, name, or user group membership.
- Modify a user group or access specification:
  - To complete the definition of a new user group or access specification created by copying an existing one.
  - To change properties of an existing group or specification.

- Delete users, user groups, and access specifications.
- Change the administrative password.
- Change user passwords.

Details are provided in the following sections.

Modifying a User Account

Use the following procedure to modify a user login, name, or user group membership:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad.

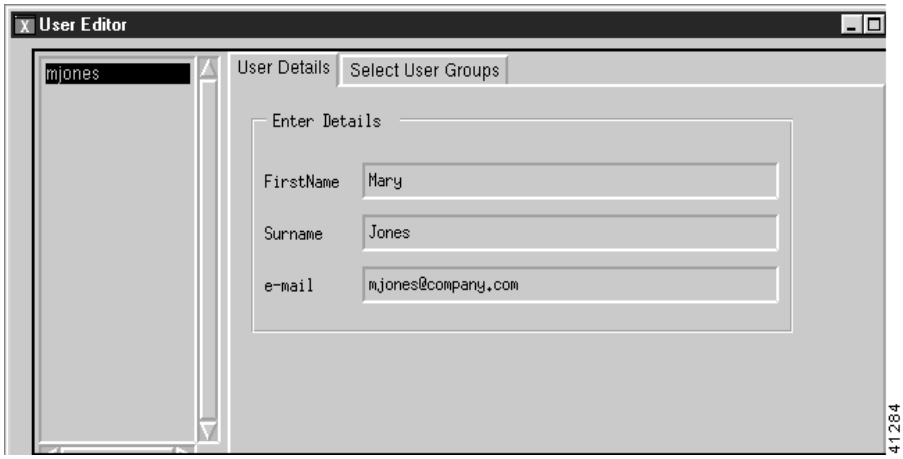
The Access Manager window opens.

Step 2 Do one of the following:

- Choose **Edit > Modify > User**.
- If the user list is not selected, choose **Users** from the drop-down list. Double-click the user account you want to modify.

The User Editor window opens. In the left, the window includes a list of users. In the right pane, it includes the tabs User Details and Select User Groups. The description pane at the bottom of the window provides details on the current selection.

Figure 4-1 User Editor Window



Step 3 Select a user from the list.

Step 4 Make the desired modifications.

Step 5 Click **Apply**. To cancel the changes, click **Revert**.

Step 6 When you are done, click **Close**. You are returned to the Launchpad window.

Modifying User Groups or Access Specifications

Use the following procedure to modify a user group or access specification:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad.

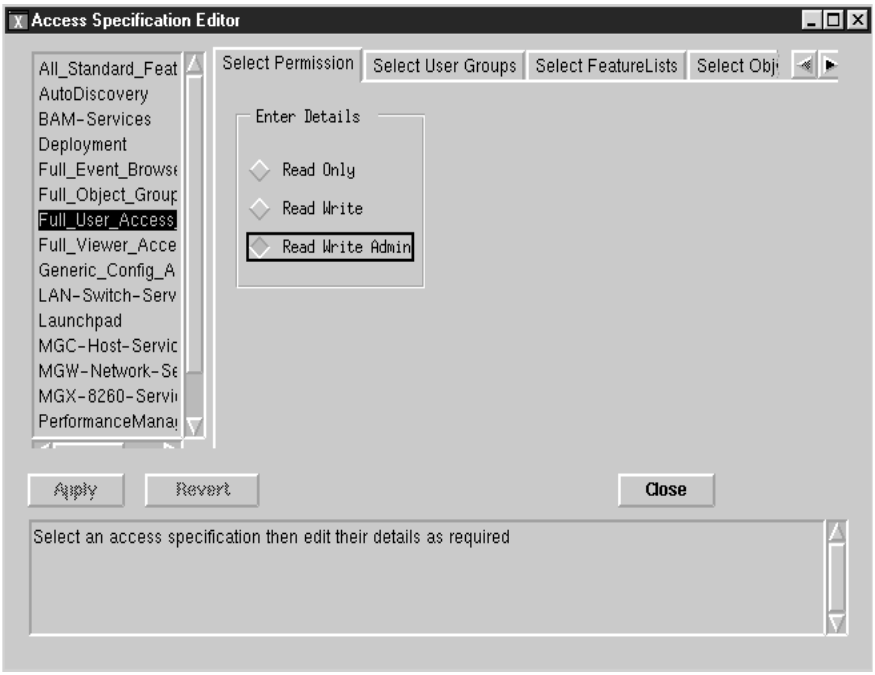
The Access Manager window opens.

Step 2 Do one of the following:

- Choose **Edit > Modify > User Group** or **Access Spec**.
- From the drop-down list, choose **User Groups** or **Access Specifications** to display a list of groups or specifications. Double-click the object you want to modify.

Step 3 The Editor window opens. The left pane includes a list of existing objects, user groups, or access specifications. The right pane includes a tab for each of the windows you used when you created the group or specification. The description pane at the bottom of the window provides details on the current selection. Figure 4-2 shows an example.

Figure 4-2 Access Specification Editor Window



Step 4 Click the object you want to modify.

Step 5 Make the desired modifications.

Step 6 Click **Apply**. To cancel the changes, click **Revert**.

Step 7 When you are done, click **Close**. You are returned to the Launchpad window.

Deleting a User, User Group, or Access Specification

Use the following procedure to delete a user, user group, or access specification:

Step 1 Click the **Access** icon on the Cisco EMF LaunchPad.

The Access Manager window opens.

Step 2 In the drop-down list, choose the users, groups, or specifications you want to delete. Use Ctrl-click for multiple selections.

Step 3 Choose **Edit > Delete**. You are prompted for confirmation.

Step 4 Click **Yes**.

The selections are deleted from the list.

Changing the Administrative Password

Use the following procedure to change the administrative password:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2 Choose **Edit > Change Admin Password**.

Step 3 Change the password, and click **OK**.

Changing a User's Password

Use the following procedure to change a user's password:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad.

The Access Manager window opens.

Step 2 Choose **Edit > Change Password**.

Step 3 Change the password, and click **OK**.