



Setting Up Cisco MGC Node Manager Security

This chapter is intended for system administrators. It provides an overview of Cisco MNM security capabilities and describes:

- [Setting Up Security, page 4-5](#)
- [Modifying Security Settings, page 4-9](#)



Note

This chapter describes managing security as it applies to users of Cisco MGC Node Manager; it does not cover the use of SSH or the Security Policy attribute in communicating with managed components. For information on installing SSH, refer to the *Cisco MGC 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. You define a component's security policy at deployment (see [Chapter 5, "Deploying Your Network in Cisco MGC Node Manager"](#)). You can 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 MGC Node Manager Security

Cisco MGC Node Manager 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 MGC Node Manager 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 MGC Node Manager, 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 below.

User Groups

Feature Lists

- 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.

The feature lists available in Cisco MGC Node Manager are described in [Table 4-1](#).

Table 4-1 Feature Lists in Cisco MGC Node Manager

Feature List	Permissions ¹	Description
		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 MGC host dial plan components.
Host-Signaling-Performance	RW	View performance statistics for signaling components.
Host-Signaling-Properties	R	View properties of Cisco MGC host signaling components.
Host-Trunking-Properties	R	View properties of Cisco MGC host trunking components.
Launchpad	R	Use the CEMF LaunchPad (start a CEMF session)

Feature Lists in Cisco MGC Node Manager (continued)

		View file system information on BAMS, HSI server, and Cisco MGC host devices.
MGC-Node-Properties	R	View properties of Cisco MGC node components.
MGC-Node-Provisioning	RWA	Deploy all Cisco MGC node components (either manually or through a seed file).
MGC-Node-States	RW	Change the states of Cisco MGC node components.
MGC-Node-Tools	RW	Launch Cisco MGC 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 4-9.

**Note**

Access Specifications

•

User groups—Cisco MGC Node Manager 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.

Access specifications predefined in Cisco MNM are listed in [Table 4-2](#).

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
		MGCNodeAccounts
		MGCNodeFilesystems
		MGCNodeProperties
		MGCNodeTransfer
		MGCNodeDiagnostics

These tasks may be done in any order. They are interrelated—user groups have associated access specifications and users; access specifications are linked to user groups. Before beginning, think through the types of users who will be 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 4-9](#).

Setting Up New Accounts

Step 1 **Access**

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

The Create User window appears.

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 appears. If user groups have been defined and one or more users 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 appears.

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

The Select User Groups window appears.

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 appears.

Step 7 Enter a password for the user and confirm it. Passwords must contain 8 to 32 alphanumeric characters and at least one punctuation character such as `_`, `%`, `(`, or `^`. Click **Forward**.

The Summary Details for User window appears.




Note If you typed an invalid password, the User Password Entry window displays an error message. Enter a valid password.

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 closes. You return to the Launchpad.

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 appears.
- Step 2** Choose **Edit > Create > User Group**.
The Create User Group window appears.
- Step 3** Enter the name for the new group.
The Copy From Existing User Group window appears. If user groups have been defined and one or more users 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 click **Forward**.
If you want to base this user group on another, click **Yes**. The list of groups appears. Select the group you want to copy, and click **Forward**.
The Select Users window appears listing existing users.
- Step 5** Select each user you want in the new group, and 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 appears, 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 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**.
For details on access specifications, see the [“Creating a New Access Specification” section on page 4-7](#).
-  **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.
-
- The Summary Details for User Group window appears listing the user group name, members, and selected access specifications.
- 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 return to the Launchpad.
-

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 appears.

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, then click the **Modify > Access Specs** menu option to add or remove feature lists or users 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 appears. Select the one you want to copy, and click **Forward**. Skip to Step 10.

If you do not want to copy an existing access specification, click **No**, and click **Forward**. The Select Permission window appears. Go to Step 6.

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 appears listing user groups to which you can assign this specification.

Step 6 Select each user group to which 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 appears listing available feature lists. See [Table 4-1](#) for the list of available features.

Step 7 Select each feature you want to include in this 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 appears. 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, 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 appears, summarizing the new specification, including:

- The access specification name
- Permissions
- Feature lists included
- 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 return to the Launchpad.

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)	<p>Using the instructions in the “Creating a New Access Specification” section on page 4-7, create a new access specification with the features labeled with the permissions R and RW in Table 4-1, but not including:</p> <ul style="list-style-type: none"> • AutoDiscovery • ObjectGroups-Edit • ObjectGroups-View <p>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.</p> <p>Use the instructions in the “Setting Up New Accounts” section on page 4-6 to create a new account, create the user, and assign the user to the group you just created.</p>
Novice user or user who only needs to view information	<p>Using the instructions in the “Creating a New Access Specification” section on page 4-7, create a new access specification with the features labeled with the permission R in Table 4-1.</p> <p>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.</p> <p>Using the instructions in the “Setting Up New Accounts” section on page 4-6, create a new account, create the user, and assign the user to the group you just created.</p>

Modifying Security Settings

Using the Access Manager, you can:

- 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.

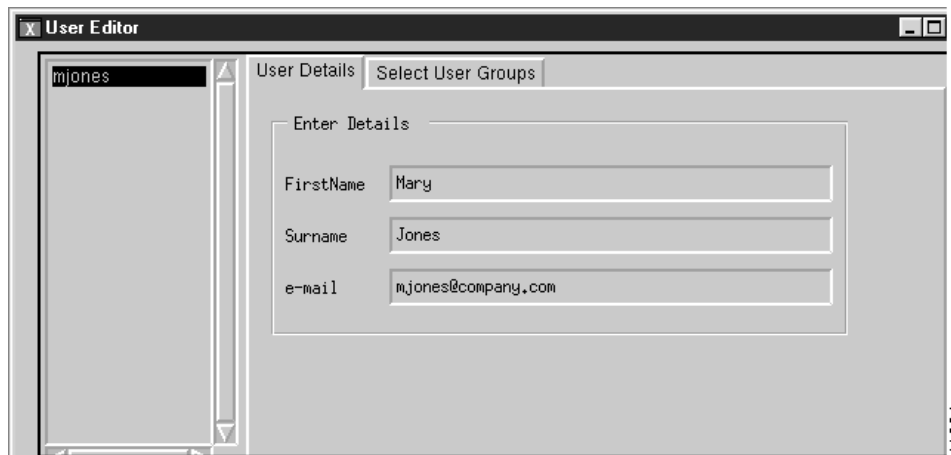
The Access Manager window appears.

Step 2 Do one of the following:

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

The User Editor window appears. On the left, the window includes a list of users. On the right, 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**.

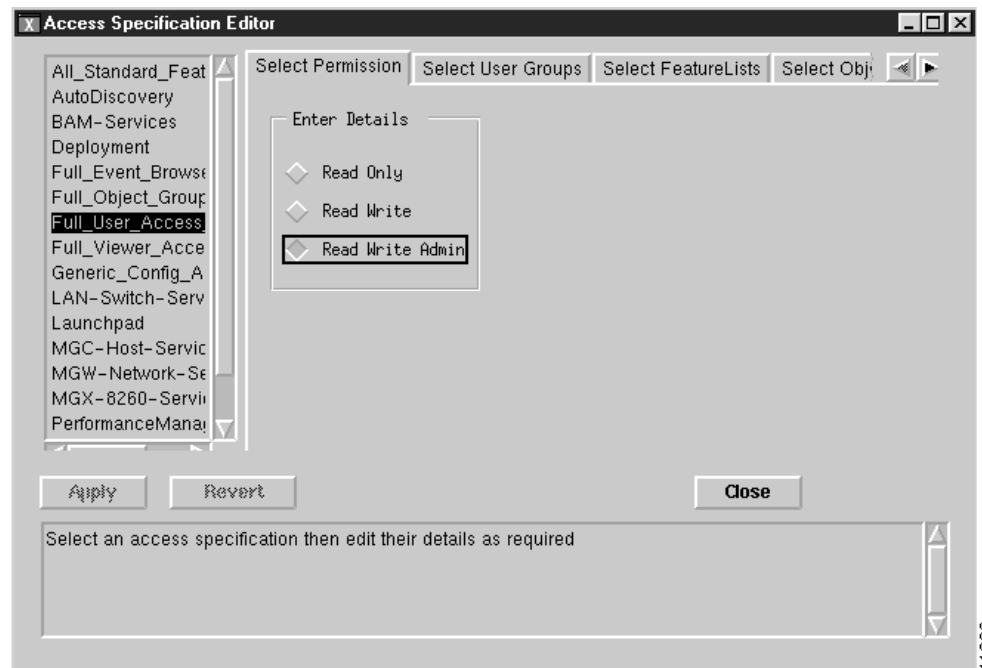
Step 6 When you are done, click **Close**. You return to the Access Manager.

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 appears.
- Step 2** Do one of the following:
- Choose **Edit > Modify > User Group** or **Access Spec**.
 - From the dropdown list, select **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 appears. On the left, it includes a list of existing objects, user groups, or access specifications. On the right, it 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** Select 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 return to the Access Manager.

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 appears.
- Step 2** In the dropdown list, select 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 appears.
- 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 appears.
- Step 2** Choose **Edit > Change Password**.
- Step 3** Change the password, and click **OK**.
-