Managing Security

This chapter describes Cisco MGM security and how to manage users. This includes an overview of security domains and a description of the user security and NE security features available in Cisco MGM.

This chapter contains the following sections:

8.1 What Is Security Management?

Why create a security policy?

- To create a baseline of your current security posture
- To set the framework for security implementation
- To define allowed and disallowed behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

The following security domains govern Cisco MGM networks:

- Cisco MGM client—A Cisco MGM client must be created with one of the existing default user profiles or with a new custom user profile with appropriate access privileges. This new user profile should be created and assigned to a user.
- Cisco MGM OSS users—OSS-to-Cisco MGM sessions are configured by the Cisco MGM CORBA GateWay EMS-to-NMS interface architectural component. For more information about Cisco MGM CORBA GateWay, see Chapter 12, “Managing CORBA Interfaces.”

8.2 How Do I Customize the Login Advisory Message?

After logging into the Cisco MGM client, a login advisory message is shown. By default, the advisory message reads:

```
NOTICE: This is a private computer system. Unauthorized access or use may lead to
prosecution.
```

You can customize the default advisory message as follows:

Step 1 Log into the Cisco MGM server as the root user.

Step 2 Use a text editor to edit or create the advisory.txt file in the /opt/CiscoMGMServer/cfg directory. The new advisory message can contain up to 1,600 characters. The advisory.txt file does not exist by default.

Note The default directory /opt/CiscoMGMServer may have been changed during installation of the Cisco MGM server.

Step 3 Save the changes. All subsequent users who log into the Cisco MGM client will see the new advisory message.

Note You can also disable the advisory message altogether. See 8.3.4.13 Configuring Cisco MGM Security Parameters, page 8-28.

8.3 How Do I Manage User Security?

This section describes user security and management. This includes procedures on how to add a new user, modify a user's properties, delete a user, and end an active user session. It also includes procedures on how to add, modify, and delete custom profiles and how to perform NE user administration.

The following topics are covered:

8.3.1 Restricting User Access

The Administration > Cisco MGM Users menu launched from the Domain Explorer window manages user security. Cisco MGM administration allows restricted access logins to enable users to perform tasks based on detailed access privileges.

For each action, a user is given privileges to read to read/write. For definitions of the access privileges, see Table 8-1.

Table 8-1 Configuration Center Access Privileges

Access Privilege	Operation
Read	Enables the following read operations: • Reads the element attributes. • Reads the templates and loads the template parameters into the configuration internal frame.
Read/Write	Enables the following create operations: • Changes the attribute values in a create internal frame. • Commits changes on the switch. • Saves the attribute values into a new template. Enables the following modify operations: • Changes the attribute values in a details internal frame. • Commit changes on the switch. • Saves the attribute values into an existing template. • Selects and modifies the template with the new attribute values. Enables the **Delete** button in both the details and create internal frame only after the element is created. Also in the tabular view listing, when more than one element is selected and if you click **Delete**, an extra check verifies if the multiple delete permission is enabled, If not, you are blocked from attempting the operation and prompted to delete one element at a time. Specifies that the tabular view listing allows more than one element decision. The multiple delete operation means that the single delete operation is also enabled. The other delete permissions are also applicable.
No Access	User has no access permissions.

Table 8-2 lists the access privileges required to perform security-controlled operations within the Diagnostic Center application.

Table 8-2 Diagnostic Center Access Privileges

Access Privilege	Operation
Read	Enables get connections, test connections, connection trace, and trouble tickets attachment.
Read/Write	Enables up connections, and saves trouble tickets. Enables the following operations at different levels: • Node—Specifies node resync and checks manageability. • Line and path—Applies loopback and starts and modifies BERT[1]. • Port—Starts and modifies BERT and grooming functions. • Connections—Specifies loopback connections.
No Access	User has no access permissions.

1. BERT = Bit Error Rate Test

To perform security-controlled operations within Chassis View and Statistics Reporting Tool applications, Read is the only access privilege allowed. The Read access privilege enables all operations that are supported by the application.

8.3.2 Viewing the Audit Trail File

The Cisco MGM Audit Trail Viewer records activities across the four applications (Configuration Center, Chassis View, Statistics Reporting Tool, and Diagnostic Center) in a persistent file.

Note Audit trail logging is done per Cisco MGM workstation and each workstation performs an independent audit trail file. There is no communication or synchronization between workstations regarding an audit trail.

Using the Audit Trail Viewer, you can access audit trail files for specified days, and you can sort, filter, and search for specific log entries. All readand write activities are monitored and logged to a file. To open the Audit Trail Viewer, complete the following procedure:

Step 1 From the Cisco MGM Domain Explorer window, choose **Administration > MGX 8880/8850 MG > Audit Trail**.

Note If no NE is selected in the Domain Explorer, the Audit Trail option will be grayed out.

or

from the Configuration Center, Statistics Reporting Tool, Chassis View, or Diagnostic Center:

- Choose **Tools > Administration > Cisco MGM Audit Trail**
- Right-click on any object in the Hierarchy pane and choose **Administration > Cisco MGM Audit Trail**

Step 2 Enter the fields.

Note Table 8-3 describes fields in the Cisco MGM Audit Trail Viewer.

Step 3 Click **Submit** to submit the specified criteria for the log file.

Step 4 Click **Reset All** to reset all the fields to the default state.

Table 8-3 Field Descriptions for the Cisco MGM Audit Trail Viewer

Name	Description
Date	Specifies the days to view the audit trail for. Click in the **Date** field to populate the current date. If the Date field is not checked, all files in the directory are checked. The format is *MMDDYYYY*.
Time	Specifies the start and end times. The format is *HH:MM:SS*. If the Time field is not checked, time is not set as a filter.

Table 8-3 Field Descriptions for the Cisco MGM Audit Trail Viewer (continued)

Name	Description
Host Name	Specifies the host workstation name where the audit trail record is generated. If the Host Name field is not checked, all host names are displayed. This field corresponds to the Terminal column in the table. **Note** The exact hostname must be specified.
User Id	Specifies the user ID used to log into the Cisco MGM desktop. If the User Id field is not checked, all user IDs are used.
Application	Specifies the application name. If the Application field is not checked, all applications are used. You have the following application choices: • All • Chassis View • Configuration Center • Diagnostics Center • Statistics Reporting Tool
Event Type	Displays the type of user activity: • Write (Initial, Failed, Successful, Timeout, and Abort) • Read • Read and Write This field corresponds to the Status column in the table.
Max entries per page	Specifies the maximum entries displayed per page in the table. The maximum is 50.
Total	Displays the total entries found and the number of entries on the current page.
<<	Displays the previous page entries.
>>	Displays the next page entries.

8.3.3 User Profiles

By default, Cisco MGM contains the following user profiles:

- NetworkAdmin—Typically, NOC supervisors who perform daily network surveillance, provisioning, and performance monitoring activities on any group or NE.
- Operator—Users who perform daily network surveillance and performance monitoring activities on specific NEs. Each operator can have only one active session. Operators cannot access administrative information.
- Provisioner—Users who perform daily network surveillance, provisioning, and performance monitoring activities on specific NEs. Each provisioner can have only one active session. Provisioners cannot access administrative information.
- SuperUser—Users who have access to all operations.
- SysAdmin—System administrators who manage Cisco MGM access.

The following sections describe how to view, add, modify, delete, and duplicate a user profile:

8.3.3.1 Viewing User Profiles

The Cisco MGM User Profiles table displays basic information about Cisco MGM user profiles. Use the menu options to manage user profiles.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Cisco MGM User Profiles** (or click the **Launch User Profiles Table** tool). Table 8-4 describes the fields in the Cisco MGM User Profiles table.

Table 8-4 Field Descriptions for the Cisco MGM User Profiles Table

Field	Description
User Profile Name	Name of the existing Cisco MGM user profiles.
NE Assignment	NE assignment for the selected user profile. NE assignments are: • Assign all NEs—SuperUser, NetAdmin • Assign NEs—Operator, Provisioner • Assign no NEs—SysAdmin When you create a new profile, only Assign NEs is available for the new profile, meaning that NEs or groups must always be assigned to the new profile.
Login Sessions	Number of permitted simultaneous logins assigned to the user profile: • 1—Only one user with a given profile can log into a specific Cisco MGM server at a time. • 2 to 10—The specified number of users (2 to 10) with a given profile can log into a specific Cisco MGM server simultaneously. • Unlimited—An unlimited number of users with a given profile can log into a specific Cisco MGM server simultaneously.
Description	Description of the user profile.

8.3.3.2 Adding a Custom User Profile

Cisco MGM allows SuperUsers and SysAdmins to generate custom user profiles with certain privileges. Custom user profiles are grouped into categories and each category has a set of operations (see Table 8-6). After the user profiles are generated, they can be assigned to new Cisco MGM users. This functionality, also known as network partitioning, allows you to control how much access particular users have to the network.

Use the Create New User Profile wizard to add Cisco MGM user profiles. Table 8-5 describes the fields in the wizard.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Cisco MGM User Profiles** (or click the **Launch User Profiles Table** tool).

Step 3 In the Cisco MGM User Profiles table, choose **Edit > Create** (or click the **Create a New User Profile** tool).

Step 4 In the Create New Cisco MGM User Profile wizard, specify the following:

- User profile name
- NE assignment (read only)
- Default user login sessions allowed
- Description

Step 5 Click **Next**.

Step 6 Select a user profile category from the Categories area. Operations for each category are displayed on the right side of the Categories area. See Table 8-6 for a complete list of Cisco MGM profile categories and operations.

Step 7 Specify user capabilities by setting permission or privileges for one or all operations. When setting privileges for each operation, select one of the following radio buttons:

- Read Only
- Read/Write
- No Access

When setting privileges for all operations, select one of the following buttons:

- Set All Read Only
- Set All Read/Write
- Set All No Access

Note The user profile operations displayed on the right side of the Create New Cisco MGM User Profile wizard depend on the category selected. You can select the root node to see all the operations for all categories.

Step 8 Click **Finish**.

Step 9 Click **Yes** in the message box. The message box will not be displayed if it is disabled in the User Preferences dialog box. See 8.3.4.11 Setting User Preferences, page 8-26 for more information.

Table 8-5 Field Descriptions for the Create New User Profile Wizard

Field	Description
User Profile Name	Enter the name of the new user profile. The profile name must contain between six and twenty alphanumeric characters (A-Z, a-z, 0-9). Alphabetic characters are case-sensitive. The profile name must be unique in Cisco MGM and cannot contain a space or any special characters.
NE Assignment	(Read only) The NE assignment for the new user profile. Values are: • Assign All NEs—SuperUser, NetworkAdmin • Assign NEs—Operator, Provisioner • Assign No NEs—SysAdmin When you create a new profile, only Assign NEs is available for the new profile, meaning that NEs or groups must always be assigned to the new profile.
Default User Login Sessions	Choose to allow single or multi-user sessions.
Description	Enter a description of the new user profile.
User Profile Privileges	Set user privileges for specific Cisco MGM categories. Select a category in the left panel to display that category's available operations. Select an operation from the Operations column; then, select a user privilege for the selected operation from the radio buttons in the Privileges column. • Set All Read Only—Specifies that the user can only view information related to all the operations with Read Only privilege listed under the specified category. All other operations will be set to No Access. • Set All Read/Write—Specifies that the user can view and perform any of the operations with Read/Write privilege listed under the specified category. All other operations will be set to Read Only. • Set All No Access—Specifies that the user is not allowed to perform any of the operations with No Access privilege listed under the specified category. All other operations will be set to Read Only. The Warning column lists the dependencies between various operations. After you click **Finish** to create the new user profile, a warning dialog box lists all of the warning messages. If you check the **Don't Display User Profile Creation Warning Messages** check box, the warning dialog box does not appear for subsequent user profile creations in the current client session. If you check the **Don't Display User Profile Creation Warning Messages** check box in the User Preferences dialog box, the warning dialog box is disabled as specified for the current user or as a template for new users.

Table 8-6 Cisco MGM Custom User Profiles

Category	Operations	Description	Privileges
Administration	Audit/Error Log	Launch the Audit Log and Error Log.	Read Only or No Access
	Control Panel	Launch the Control Panel and related tables.	Read/Write or No Access
	Logged In MGM Users	Launch the Logged In MGM Users Table.	Read Only, Read/Write, or No Access
	MGM User Profiles	Launch the Cisco MGM User Profiles Table and add, delete, or modify user profiles.	Read Only, Read/Write, or No Access
	MGM Users	Launch the MGM Users Table and add, delete, or modify users and user preferences.	Read Only, Read/Write, or No Access
	Save Map As Default	Save map customizations as default.	Read/Write or No Access
NE Administration	Add or Delete NE or Group	Add or delete NEs or groups from the domain.	Not assigned
	Audit Trail	Launch the Audit Trail Table.	Read Only, Read/Write, or No Access
	Edit Domain Node Properties	Edit properties on the property sheet associated with the root node in the Domain Explorer tree.	Read/Write or No Access
	Edit NE or Group Properties	Edit NE or group properties.	Read/Write or No Access
	SSH Secure Shell	Command line tool to gain secure shell access to MGX switches.	Read/Write, or No Access
	Supported NE Table	Launch the Supported NE Table.	Read Only, Read/Write, or No Access
	Telnet session	Command line tool to telnet to MGX switches.	Read/Write, or No Access
	Topology Modification	Drag, drop, cut, copy, and paste NEs in the Domain Explorer.	Not assigned
	User Preferences	Edit the user preferences.	Read/Write or No Access

Table 8-6 Cisco MGM Custom User Profiles (continued)

Category	Operations	Description	Privileges
NE CM[1]	Audit Logging in Chassis View	Activates or deactivates the Audit Trail in Chassis View.	Read Only, Read/Write, or No Access
	Audit Logging in Configuration Center	Activates or deactivates the Audit Trail in Configuration Center.	Read Only, Read/Write, or No Access
	Chassis View	Launches the Chassis View application.	Read Only, Read/Write, or No Access
	Configuration Center	Launches the Configuration Center application.	Read Only, Read/Write, or No Access
	Equipment Inventory	Launches the Equipment Inventory Table.	Read Only or No Access
NE FM[2]	Alarm Browser/Log	Launches the Alarm Browser, Alarm Log, or Event Export Manager, acknowledge alarms, and show alarm notes.	Read Only, Read/Write, or No Access
	Audit Logging In Diagnostics Center	Activates or deactivates the Audit Trail in the Diagnostics Center.	Read Only, Read/Write, or No Access
	Diagnostics Center	Launches the Diagnostic Center application.	Read Only, Read/Write, or No Access
	Show MGM EMS Alarms/Events	Show MGM-specific EMS alarms and events count in the Dashboard, show MGM specific EMS alarms in the Alarm Browser, and show MGM specific EMS alarms and events-related pop-ups.	Read/Write or No Access
NE Management	Audit Trail Table	Launches the Audit Trail table.	Read Only or No Access
	Job Monitor	Launch the Job Monitor Table and cancel job, cancel task, add user notes, or view user notes.	Read Only, Read/Write, or No Access
NE PM	Audit Logging in Statistics Reporting Tool	Activates or deactivates the Audit Trail in the Statistics Reporting Tool.	Read Only, Read/Write, or No Access
	Statistics Reporting Tool	Launches the Statistics Reporting Tool application.	Read Only, Read/Write, or No Access

1. NE Configuration Management
2. NE Fault Management

8.3.3.3 Modifying a User Profile

Use the Modify User Profile wizard to modify Cisco MGM user profiles. Table 8-5 describes the fields in the wizard.

Note Users created with a certain profile cannot be changed to another profile. To change profiles, the user must be deleted, then recreated with the new profile.

Modifying a profile will log out all users who are logged in with that profile.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Cisco MGM User Profiles** (or click the **Launch User Profiles Table** tool).

Step 3 In the table, click the user profile name to modify; then, choose **Edit > Modify** (or click the **Modify User Profile Properties** tool).

Step 4 In the Modify Cisco MGM User Profile wizard, modify the following:

- Default user login sessions allowed
- Description

Step 5 Click **Next**.

Step 6 Select a user profile category from the Categories area. Operations for each category are displayed on the right side of the Categories area. See Table 8-6 for a list of Cisco MGM profile categories and operations.

Step 7 Specify user capabilities by setting permission or privileges on one or all operations. When setting privileges for each operation, select one of the following radio buttons:

- Read Only
- Read/Write
- No Access

When setting privileges for all operations, select one of the following buttons:

- Set All Read Only
- Set All Read/Write
- Set All No Access

Note The user profile operations displayed on the right side of the Create New Cisco MGM User Profile wizard depend on the category selected. You can select the root node to see all the operations for all categories.

Step 8 Click **Finish**.

Step 9 Click **Yes** in the message box. The message box will not be displayed if it is disabled in the User Preferences dialog box. See 8.3.4.11 Setting User Preferences, page 8-26 for more information.

8.3.3.4 Deleting a User Profile

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Cisco MGM User Profiles** (or click the **Launch User Profiles Table** tool).

Step 3 In the Cisco MGM User Profiles table, select the profile you want to delete; then, choose **Edit > Delete** (or click the **Delete User Profile** tool).

Step 4 In the confirmation dialog box, click **OK**.

Note The default user profiles (SuperUser, SysAdmin, NetworkAdmin, Provisioner, and Operator) cannot be deleted. Custom user profiles cannot be deleted if they are assigned to any user. Delete the user with the custom user profile before deleting the user profile. See 8.3.4.5 Deleting a Cisco MGM User, page 8-23.

8.3.3.5 Duplicating a User Profile

Use the Create Duplicate Profile window to duplicate an existing Cisco MGM user profile.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Cisco MGM User Profiles** (or click the **Launch User Profiles Table** tool).

Step 3 In the Cisco MGM User Profiles table, select the profile you want to duplicate; then, choose **Edit > Duplicate** (or click the **Duplicate User Profile** tool).

Step 4 In the Create Duplicate Profile dialog box, enter the duplicate profile name. See Table 8-7 for name constraints.

Step 5 Click **OK**.

Table 8-7 Field Descriptions for the Create Duplicate Profile Window

Field	Description
Duplicate Profile Name	The name of the duplicate user profile must contain between six and twenty alphanumeric characters (A-Z, a-z, 0-9). Alphabetic characters are case-sensitive. The profile name must be unique in Cisco MGM and cannot contain a space or any special characters.

8.3.4 Performing User Administration

This section describes how to perform user administration, including:

8.3.4.1 Managing the Cisco MGM Default User Profiles

Table 8-8 lists the Cisco MGM default user profiles and the privileges associated with each profile.

Note The SuperUser profile has access to all operations, and is not specifically listed in a separate column.

The NetworkAdmin profile has access to all NEs and groups. The SysAdmin profile has access to no NEs or groups.

Table 8-8 Cisco MGM Default User Profiles

Functional Area	Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Domain Explorer	File > New Group	Deny	Allow	Deny	Deny
	File > Add Network Element(s)	Deny	Allow	Deny	Deny
	File > Dashboard	Allow	Allow	Allow	Allow
	File > Network Map	Deny	Allow	Allow	Allow
	File > Domain NE table	Deny	Allow	Allow	Allow
	File > Notify Users	Allow	Allow	Allow	Allow
	File > Refresh Data	Allow	Allow	Allow	Allow
	File > Debug Options	Allow	Allow	Allow	Allow
	File > Lock Cisco MGM Client	Allow	Allow	Allow	Allow
	Edit > Cut	Deny	Allow	Deny	Deny
	Edit > Copy	Deny	Allow	Deny	Deny
	Edit > Paste	Deny	Allow	Deny	Deny
	Edit > Delete	Deny	Allow	Deny	Deny
	Edit > Delete All	Deny	Allow	Deny	Deny
	Edit > Undelete	Deny	Allow	Deny	Deny
	Edit > Expand	Deny	Allow	Allow	Allow
	Edit > Collapse	Deny	Allow	Allow	Allow
	Edit > Find	Deny	Allow	Allow	Allow
	Edit > Find Next	Deny	Allow	Allow	Allow
	Edit > User Preferences	Allow	Allow	Allow	Allow
	Edit > Change Password	Allow	Allow	Allow	Allow
	Fault > Alarm Browser	Allow	Allow	Allow	Allow
	Fault > Alarm Log	Allow	Allow	Allow	Allow

Table 8-8 Cisco MGM Default User Profiles (continued)

Functional Area	Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Domain Explorer (continued)	Fault > Event Export Manager	Allow	Allow	Allow	Allow
	Fault > Ping NE (*not applicable*)	Deny	Deny	Deny	Deny
	Fault > Test NE Connectivity (*not applicable*)	Deny	Deny	Deny	Deny
	Fault > Stop Continuous Beep	Deny	Allow	Allow	Allow
	Fault > MGX 8880/8850 MG > Diagnostic Center	Deny	Allow	Allow	Deny
	Performance > MGX 8880/8850 MG > Statistics Reporting Tool	Deny	Allow	Allow	Deny
	Configuration > MGX 8880/8850 MG > Equipment Inventory Table	Deny	Allow	Allow	Allow
	Configuration > MGX 8880/8850 MG > Chassis View	Deny	Allow	Allow	Deny
	Configuration > MGX 8880/8850 MG > Configuration Center	Deny	Allow	Allow	Deny
	Administration > Job Monitor	Deny	Allow	Allow	Deny
	Administration > Service Monitor	Allow	Deny	Deny	Deny
	Administration > Self Monitor	Allow	Deny	Deny	Deny
	Administration > Memory Backup	Deny	Deny	Deny	Deny
	Administration > Memory Restore	Deny	Deny	Deny	Deny
	Administration > Software Download	Deny	Deny	Deny	Deny
	Administration > Image Upload (*not applicable*)	Deny	Deny	Deny	Deny
	Administration > NE Software table (*not applicable*)	Deny	Deny	Deny	Deny
	Administration > Cisco MGM Users	Allow	Deny	Deny	Deny
	Administration > Control Panel	Allow	Deny	Deny	Deny
	Administration > Audit Log	Allow	Allow	Deny	Deny
	Administration > Error Log	Allow	Allow	Deny	Deny
	Administration > Supported NE table	Allow	Allow	Deny	Deny
	Administration > MGX 8880/8850 MG > Audit Trail	Deny	Allow	Deny	Deny

Table 8-8 Cisco MGM Default User Profiles (continued)

Functional Area	Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Network Map	File > Open	Deny	Allow	Allow	Allow
	File > Parent	Deny	Allow	Allow	Allow
	File > Save	Deny	Allow	Allow	Allow
	File > Save As Default	Deny	Allow	Deny	Deny
	File > Revert To Default	Deny	Allow	Allow	Allow
	File > Notify Users	Deny	Allow	Allow	Allow
	File > Refresh Data	Deny	Allow	Allow	Allow
	File > Debug Options	Deny	Allow	Allow	Allow
	Edit > Enable Drag	Deny	Allow	Allow	Allow
	Edit > Enable Offview	Deny	Allow	Allow	Allow
	Edit > Change Map Background	Deny	Allow	Allow	Allow
	Edit > Change Node Icon	Deny	Allow	Allow	Allow
	Edit > Zoom In	Deny	Allow	Allow	Allow
	Edit > Zoom Out	Deny	Allow	Allow	Allow
	Edit > Zoom Area	Deny	Allow	Allow	Allow
	Edit > Circular Layout	Deny	Allow	Allow	Allow
	Edit > Spring Layout	Deny	Allow	Allow	Allow
	Edit > Table Layout	Deny	Allow	Allow	Allow
	Edit > Declutter Layout	Deny	Allow	Allow	Allow
	Edit > User Preferences	Deny	Allow	Allow	Allow
	Edit > Change Password	Deny	Allow	Allow	Allow
Alarm Browser	Fault > Acknowledge Alarms	Allow	Allow	Allow	Allow
	Fault > Acknowledge All Alarms	Allow	Allow	Allow	Allow
	Fault > Clear Alarm(s)	Allow	Allow	Allow	Allow
	Fault > Show Alarm Note	Allow	Allow	Allow	Allow
	Fault > Hide Cleared Alarms	Allow	Allow	Allow	Allow
	Fault > Hide Acknowledged Alarms	Allow	Allow	Allow	Allow
	Fault > Reset All Alarms	Allow	Allow	Allow	Allow
Job Monitor	Edit > Cancel Task	—	Allow	—	—
	Edit > Cancel Job	—	Allow	—	—
	Edit > User Note	—	Allow	—	—
	Edit > NE Software table (*not applicable*)	—	Deny	—	—

Table 8-8 Cisco MGM Default User Profiles (continued)

Functional Area	Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Cisco MGM Users	Edit > Create	Allow	—	—	—
	Edit > Modify	Allow	—	—	—
	Edit > Delete	Allow	—	—	—
	Edit > Unlock	Allow	Deny	Deny	Deny
	Administration > Cisco MGM User Profiles	Allow	Deny	Deny	Deny
	Administration > Logged In Cisco MGM Users	Allow	Deny	Deny	Deny
Cisco MGM User Profiles	Edit > Create	Allow	Deny	Deny	Deny
	Edit > Modify	Allow	Deny	Deny	Deny
	Edit > Delete	Allow	Deny	Deny	Deny
	Edit > Duplicate	Allow	Deny	Deny	Deny
Logged In Cisco MGM Users table	Administration > Log Out User	Allow	Deny	Deny	Deny
Supported NE table	Edit > Add	Allow	Allow	—	—
	Edit > Delete	Allow	Allow	—	—

8.3.4.2 Viewing the Cisco MGM Users Table

The MGM Users table displays basic information about Cisco MGM users. The table menu options allow you to create new users, modify users, delete users, and unlock user accounts.

To view the MGM Users table, choose **Administration > Cisco MGM Users** in the Domain Explorer window. Table 8-9 describes the fields in the table.

Table 8-9 Field Descriptions for the MGM Users Table

Field	Description
Username	Username of the selected MGM user.
User Privilege	User privilege level (SuperUser, SysAdmin, NetworkAdmin, Provisioner, Operator, or a custom profile).
User Domain	Name of the management domain where the username belongs.
Password Set Time (*time zone*)	Last time the password was set.
Locked State	Whether the user's account is locked or unlocked. If the user repeatedly attempts unsuccessfully to log into the Cisco MGM client (the default maximum is 5 attempts), the user's account is locked automatically. You can set the maximum number of login attempts a user is allowed before being locked out in the **Control Panel > Security Properties** pane.
Last Login Time (*time zone*)	Last time the user logged in.
Failed Attempts	Number of times the user tried to log in, but failed.
Login State	Administrative state (Enabled or Disabled) of the user.

Table 8-9 Field Descriptions for the MGM Users Table (continued)

Field	Description
Description	Description of the user.
Password Change	Current state (Enabled or Disabled) of the password change option.
Multiple Login	Whether this user is allowed to perform multiple logins simultaneously.

8.3.4.3 Creating a Cisco MGM User

Use the Create New MGM User wizard to add new Cisco MGM users to the domain. Table 8-10 describes the fields in the wizard.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the MGM Users table, choose **Edit > Create** (or click the **Create a New User** tool).

Step 3 In the Create New MGM User wizard, enter the following information:

- Username
- User password (and confirm password)
- User privilege
- Domain name
- Login state
- Password change
- Description
- Use Global Settings check box
- Enable check box
- Period
- User login sessions

Step 4 Click **Next**. When you finish adding a new SuperUser, NetworkAdmin, or SysAdmin, click **Finish**.

Step 5 When adding a new Provisioner, Operator, or custom user profile, select the groups and NEs that the Provisioner or Operator will monitor. Selected groups and NEs appear in the Assigned Objects list. (SuperUsers and NetworkAdmins monitor the entire management domain, so there is no need to select groups or NEs when adding one of these users. SysAdmin users do not access any of the NEs.)

a. To assign groups, click the **Groups** radio button. In the Available Objects list, select the groups that will be assigned to the new user and click **Add**.

b. To assign NEs, click the **Network Elements** radio button. In the Available Objects list, select the NEs that will be assigned to the new user and click **Add**.

Note When individual NEs are assigned, these NEs will appear directly under the top level domain for the user in the Domain Explorer. It is possible that a given NE may have already been assigned as part of a group assignment to the user. In such a case, the same NE will appear directly under the top level domain and also within the assigned group. This behavior is consistent with the Domain Explorer's ability to represent the same group or NE within multiple locations of the hierarchy.

c. To remove groups or NEs from the Assigned Objects list, select the group or NE from the Assigned Objects list and click **Remove**.

d. Click **Next** (or **Finish**).

Step 6 Click **Finish**.

The new user is listed in the MGM Users table.

Table 8-10 Field Descriptions for the Create New MGM User Wizard

Screen	Field	Description
User Properties	Username	Name that the user will use to access the system. The Cisco MGM username must contain between six and twelve alphanumeric characters (A-Z, a-z, 0-9). Alphabetic characters are case-sensitive. The username must be unique in Cisco MGM and cannot contain a space or a special character. **Note** After the username is set, it cannot be changed without deleting the user.
	User Password	Login password that the user will use to access the system. The password complexity is configurable in the Control Panel > Security Properties pane. By default, the user password must: • Contain at least six characters, but not more than 12 characters. • Contain at least two alphabetic characters (A-Z, a-z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase. • Contain at least one numeric character (0-9). • Contain at least one special character (+ # % , . ; & !). • Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu. • Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters. **Note** By default, the minimum time between password changes is 20 days. The new password must differ from the previous password by 3 characters, and the new password is compared against the previous 5 passwords.
	Confirm Password	Retype the password to confirm it.
	User Privilege	User privilege level. **Note** After the user privilege is set, it cannot be changed without deleting the user.

Table 8-10 Field Descriptions for the Create New MGM User Wizard (continued)

Screen	Field	Description
User Properties (continued)	Domain Name	Domain name. When the user logs into the system, he or she sees all of the devices contained within this domain.
	Login State	Permit (enable) or prevent (disable) the user from logging into the system.
	Password Change	Permit (enable) or prevent (disable) the user from changing his or her password.
	Description	Description of the new user.
	Use Global Settings/ Enable check boxes	Lockout—Cisco MGM automatically locks the current session after the period in the Period field. Click **Use Global Settings** to use the settings from the Security window. If you do not select Use Global Settings, click **Enable** to activate lockout for the selected user. Enter a lockout length in the Period field.
		Logout—Cisco MGM automatically logs the user out of the Cisco MGM session after the period in the Period field. Click **Use Global Settings** to use the settings from the Security window. If you do not select Use Global Settings, click **Enable** to activate logout for the selected user. Enter a logout length in the Period field.
	User Login Sessions	Select whether to allow single or multiple user logins.
Assign Objects to User (*for Provisioner and Operator users only*)	Select Object Type	Assign groups or NEs to the new user. **Note** The Discovered NEs and Deleted NEs groups cannot be assigned to a Provisioner, Operator, or custom user profile.
	Select Objects	Select from the list of available objects that can be assigned to the new user. By clicking the **Add** and **Remove** buttons, you can move objects back and forth between the Available Objects list and the Assigned Objects list.

8.3.4.4 Modifying a Cisco MGM User's Properties

Use the Modify MGM User Properties wizard to modify the properties of an existing Cisco MGM user. Table 8-11 describes the fields in the wizard.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, select the user whose properties will be modified.

Step 3 Choose **Edit > Modify** (or click the **Modify User Properties** tool). The Modify MGM User Properties wizard opens.

Step 4 Modify the following information, as needed; then, click **Next**:

- Username
- User password (and confirm password)
- User privilege
- Domain name
- Login state
- Password change
- Description
- Use Global Settings check box

- Enable check box
- Period
- User login sessions

Step 5 (Optional) For Provisioner, Operator, and custom user profiles, modify the list of assigned objects by adding groups or NEs to the Assigned Objects list or removing groups or NEs from the list. Click **Next**.

Step 6 Click **Finish**. The user whose properties were modified is listed in the MGM Users table.

Table 8-11 Field Descriptions for the Modify MGM User Properties Wizard

Screen	Field	Description
Cisco Media Gateway Manager User Properties	Username	(Read-only) Active username for accessing the system. The Cisco MGM username must contain between six and twelve alphanumeric characters (A-Z, a-z, 0-9). Alphabetic characters are case-sensitive. The username must be unique in Cisco MGM and cannot contain a space or a special character. **Note** Once the username is set, it cannot be changed without deleting the user.
	User Password	Login password used to access the system. The password complexity is configurable in the Control Panel > Security Properties pane. By default, the user password must: • Contain at least six characters, but not more than 12 characters. • Contain at least two alphabetic characters (A-Z, a-z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase. • Contain at least one numeric character (0-9). • Contain at least one special character (+ # % , . ; & !). • Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu. • Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters. **Note** By default, the minimum time between password changes is 20 days. The new password must differ from the previous password by 3 characters, and the new password is compared against the previous 5 passwords.

Table 8-11 Field Descriptions for the Modify MGM User Properties Wizard (continued)

Screen	Field	Description
Cisco Media Gateway Manager User Properties (continued)	Confirm Password	Retype the password to confirm it.
	User Privilege	(Read-only) User's privilege level. **Note** The user privilege level cannot be modified without deleting the user.
	Domain Name	Domain name. When the user logs into the system, he or she sees all the devices contained within this domain.
	Login State	Permit (enable) or prevent (disable) the user from logging into the system.
	Password Change	Permit (enable) or prevent (disable) the user from changing his or her password.
	Description	User description.
	Autodisable Account	Number of days of non-use that will prompt the account to be automatically disabled. The range is 0 to 365 days in 1-day increments. The default is 0 days, meaning the account will not be disabled automatically as a result of non-use.
	Use Global Settings/ Enable check boxes	Lockout—Cisco MGM automatically locks the current session after the number of minutes in the Period field. Click **Use Global Settings** to use the settings from the Security window. If you do not select Use Global Settings, click **Enable** to activate lockout for the selected user. Enter a lockout length in the Period field.
		Logout—Cisco MGM automatically logs the user out of the Cisco MGM session after the number of minutes in the Period field. Click **Use Global Settings** to use the settings from the Security window. If you do not select Use Global Settings, click **Enable** to activate logout for the selected user. Enter a logout length in the Period field.
	User Login Sessions	Whether to allow single or multiple user login.
Assign Objects to User (*for Provisioner and Operator users only*)	Select Object Type	Assign specific groups and NEs to operator and provisioner users.
	Select Objects	Modify the objects that are assigned to operators and provisioners. Click **Add** and **Remove** to move objects back and forth between the Available Objects list and the Assigned Objects list.

8.3.4.5 Deleting a Cisco MGM User

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, select the user to be deleted.

Note A user cannot be deleted from the database until that user logs out. However, an active user session can be ended. See 8.3.4.7 Ending an Active Cisco MGM User Session, page 8-23.

Step 3 Choose **Edit > Delete** (or click the **Delete User** tool).

Step 4 Click **OK** to remove the user from the database.

8.3.4.6 Viewing Logged In Cisco MGM Users

The Logged In Cisco MGM Users table allows you to view the users who are currently logged into the Cisco MGM application.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Logged In Cisco MGM Users**. Table 8-12 describes the fields in the table.

Table 8-12 Field Descriptions for the Logged In Cisco MGM Users Table

Field	Description
Username	Name of the user who is currently logged in.
Logged in At	Date and time when the user logged in.
IP Address	User's IP address.
Session ID	Unique session ID number that the Cisco MGM server assigns to each Cisco MGM user during login.

8.3.4.7 Ending an Active Cisco MGM User Session

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, choose **Administration > Logged In Cisco MGM Users**.

Step 3 In the Logged In Cisco MGM Users table, select the user whose session will be ended and choose **Administration > Log Out User** (or click the **Log Out User** tool).

Step 4 Click **Yes** at the following prompt:

```
This operation will log out the selected Cisco MGM user. It will take approximately
a minute and this Cisco MGM client will be unusable until then. Do you wish to continue?
```

Wait while the Cisco MGM server logs out the selected Cisco MGM client. The Cisco MGM GUI is frozen for approximately 1 minute until the request is complete.

8.3.4.8 Using the Cisco MGM Locked Window

You can use the Cisco MGM Locked window to lock the current Cisco MGM session:

From the Domain Explorer window, choose:

File > Lock Cisco MGM Client

or

File > Lock Cisco MGM Users

Once the session is locked, the Domain Explorer disappears, and the Cisco MGM Locked window prompts you to enter your password to unlock the Cisco MGM session. You can attempt login up to the configured maximum login attempts to unlock the session. If the threshold is exceeded, Cisco MGM will terminate. Table 8-13 describes the field in the Cisco MGM Locked window.

Table 8-13 Field Descriptions for the Cisco MGM Locked Window

Field	Description
Password	Enter your password; then, click **Unlock** to unlock the Cisco MGM session.

8.3.4.9 Unlocking a User Account

By default, Cisco MGM allows users a maximum of five login attempts; the user account is locked after the fifth unsuccessful login attempt. The lockout duration is configurable and can be from 0 to 600 seconds or infinite.

Step 1 In the Domain Explorer window, choose **Administration > Cisco MGM Users**.

Step 2 In the Cisco MGM Users table, select the locked user.

Step 3 Choose **Edit > Unlock** (**or** click the **Unlock User** tool).

8.3.4.10 Changing Your User Password

Cisco MGM users can use the Change Password dialog box to change their Cisco MGM passwords at any time. The password change applies to the Cisco MGM user who is currently logged in. There is an enforced password change request when the default user logs in for the first time. If the user does not change the password, the Cisco MGM session is canceled.

Note The password complexity is configurable in the Control Panel > Security Properties pane.

Table 8-14 describes the fields in the Change Password dialog box.

Step 1 In the Domain Explorer window, choose **Edit > Change Password**.

Step 2 To change the Cisco MGM password:

a. In the Cisco MGM Password area, enter the current Cisco MGM password in the Old Password field.

b. Enter the new password in the New Password field. For Cisco MGM password constraints, see Table 8-14.

c. Confirm the new password.

d. Click **OK**.

Table 8-14 Field Descriptions for the Change Password Dialog Box

Field	Subfield	Description
Cisco MGM Password	Old Password	Enter the old Cisco MGM user password.
	New Password	Enter the new login password. The password complexity is configurable in the Control Panel > Security Properties pane. By default, the new password must: • Contain at least six characters, but not more than 12 characters. • Contain at least two alphabetic characters (A-Z, a-z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase. • Contain at least one numeric character (0-9). • Contain at least one special character (+ # % , . ; & !). • Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu. • Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters. **Note** By default, the minimum time between password changes is 20 days. The new password must differ from the previous password by 3 characters, and the new password is compared against the previous 5 passwords.
	Confirm Password	Retype the password to confirm it.

Note Do not change the Cisco MGM passwords at the same time in the Change Password dialog box.

It is possible to set up the user account such that the change password function is disabled. See the description of the Password Change field in 8.3.4.3 Creating a Cisco MGM User, page 8-18.

8.3.4.11 Setting User Preferences

Use the User Preferences dialog box to configure the Cisco MGM user interface.

Step 1 In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens. Table 8-15 describes the fields in the dialog box.

Step 2 After specifying the settings, check the **Save current settings** check box to preserve the current settings even after logging out. Users with the appropriate privileges can check the **Save as the default user template** check box to save the current settings as the default for new users who are added in the future. Current users who have not altered their default settings adopt the new default settings when they log out.

Step 3 Click **OK** to save the settings. After you save the selections, all subsequent views use the saved preferences.

Table 8-15 Field Descriptions for the User Preferences Dialog Box

Tab	Field	Description
Event Notification	Show Notification Dialog For	Select whether an alert popup displays when a specific alarm or event occurs on NEs in your management domain or on the EMS. You can specify the alarm severity that will generate an alert popup, and whether to include cleared alarms. **Note** Selections that apply to NEs are allowed only if you have NEs assigned to you. Selections that apply to the EMS are allowed only if you have the appropriate user privilege.
	Play Audible Notification For	Select whether an audible alert sounds when a specific alarm or event occurs on an NE or on the Cisco MGM application. You can specify the alarm severity that will generate an audible alert, and whether to include cleared alarms. Check the **Continuous Alarm for Dashboard Notifications** check box to enable continuous audible notification whenever a new update occurs in the Dashboard window. Uncheck this check box to disable continuous audible notifications. **Note** Selections that apply to NEs are allowed only if you have NEs assigned to you. Selections that apply to the EMS are allowed only if you have the appropriate user privilege.

Table 8-15 Field Descriptions for the User Preferences Dialog Box (continued)

Tab	Field	Description
Miscellaneous	Time Zone for Date/Time Display	Change the time zone selection. You can select one of the following: • Local—Displays time information adjusted for the time zone that is configured on the PC or workstation where the Cisco MGM client is running. • GMT—Displays time information (for example, alarm time stamps) according to the GMT time zone. • User Defined—Specify a fixed offset from GMT. The offset range is –12 to +13 hours from GMT, in one-hour increments. For offsets other than zero, specify a display string of four characters maximum (to indicate the time zone, for example).
	Display Log/15-min PM Data	Change the time period used to display time-sensitive data in 15-minute increments. **Note** This field is visible only if you have read permission for the Performance Monitor operation.
	Display 1 Day PM Data	Change the time period used to display time-sensitive data in 24-hour increments. **Note** This field is visible only if you have read permission for the Performance Monitor operation.
	Don't Display User Profile Creation Warning Messages	Enable or disable the warning dialog box that pops up when you click Finish after creating or modifying a user profile. The warnings are still visible in the User Profile table.
Map Preferences	Open Network Map in New Window	Within network map views, this setting specifies whether to open subsequent frames in the same window, or open a new window for subsequent map views.
	Show Off View Icons	This option is available in the GUI, but is not used by Cisco MGM.
FM Preferences	Color Entire Row in Table View	Set the Alarm Browser or Alarm Log to full background color for the entire selected row. The color corresponds to the alarm status and severity.

8.3.4.12 Enabling or Disabling the Continuous Audible Alarm

You can enable or disable the continuous audible alarm, which can be enabled to sound when a specific alarm or event of a specific severity occurs on an NE or on the system.

Step 1 In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens.

Step 2 In the **Event Notification tab > Play Audible Notification For** area, check the **Continuous Alarm For Dashboard Notifications** check box.

Step 3 Click **OK**.

Step 4 To disable the continuous audible alarm, choose **Fault > Stop Continuous Beep** in the Domain Explorer window.

8.3.4.13 Configuring Cisco MGM Security Parameters

Use the Security Properties pane to configure Cisco MGM security parameters and password complexity rules. You can also specify usernames and passwords.

Note Passwords that are already in the system are not affected by modification(s) to the password complexity rules. The password complexity rules are checked when:

- A privileged user adds a new user to the system
- A privileged user modifies an existing user's password
- A user changes his or her own existing password

Step 1 In the Domain Explorer window, choose **Administration > Control Panel**.

Step 2 Click **Security Properties** and set the parameters described in Table 8-16.

Step 3 Click **Save**.

Table 8-16 Field Descriptions for the Security Properties Pane

Tab	Field	Description
Cisco MGM Security	Password Aging	Number of days before the password expires. The user is prompted to change the password after the specified number of days. The range is 0 to 999 days; the default is 30 days. A value of 0 disables this feature.
	Max Retries	Maximum number of login attempts a user is allowed before being denied access. The range is 0 to 10 retries; the default is 5 retries. A value of 0 disables this feature. **Note** When the number of login attempts is exceeded for a given user, Cisco MGM generates an alarm. Alarm information includes the username and IP address of the client workstation where the final login attempt was made.
	Infinite	Enable or disable infinite user lockout. If checked, Cisco MGM does not automatically re-enable the account, but always requires the intervention of a user with the appropriate user profile to re-enable.
	Login Disable Period	Number of seconds a user's login is disabled after the maximum login retries value is exceeded. The range is 0 to 600 seconds; the default is 30 seconds. A value of 0 disables this feature and the Max Retries feature. For example, if the maximum number of retries is 5 and the login disable period is 30 seconds, the user account will be disabled for 30 seconds after the fifth failed login attempt. **Note** If you check the Infinite check box, the Login Disable Period field is grayed out. The user will not be allowed to log in until that user's login state is re-enabled from the Cisco MGM Users table.
	Enable Cisco MGM Security Advisory Message	If checked, the advisory message that appears on login is enabled. Uncheck to disable the login advisory message.
	Lockout Enable	If checked, Cisco MGM automatically locks the current session after the period in the Lockout Period field. **Note** If both Lockout Enable and Logout Enable are checked, logout only occurs after the lockout period.
	Lockout Period	Number of minutes a user's Cisco MGM session is inactive before Cisco MGM automatically locks the user out. The range is 0 to 120 minutes in 1-minute increments; the default is 30 minutes. A value of 0 disables this feature.
	Logout Enable	If checked, Cisco MGM automatically logs the user out of the Cisco MGM session after the period in the Logout Period field.
	Logout Period	Number of minutes a user's Cisco MGM session is inactive before Cisco MGM automatically logs the user out. The range is 0 to 1440 minutes in 1-minute increments. A value of 0 disables this feature.

8.3.4.14 Sending Messages to Other Users

Use the Notify Users dialog box to type and send a message to all Cisco MGM users, or to all Cisco MGM users with the same user privileges. For example, you might want to use the Notify Users dialog box to alert all Cisco MGM users before shutting down the Cisco MGM server.

Table 8-17 describes the fields in the dialog box.

Step 1 In the Domain Explorer window, choose **File > Notify Users**. The Notify Users dialog box opens.

Step 2 In the Message Targets area, select the recipients of the message.

Step 3 Type the message in the Message area.

Step 4 To send the message to the specified recipients, click **Send**. To cancel the message and close the dialog box, click **Cancel**. To launch the online help for the Notify Users dialog box, click **Help**.

Table 8-17 Field Descriptions for the Notify Users Dialog Box

Field	Description
Message Targets	Select recipients for your message. This list includes the default SuperUser, SysAdmin, NetworkAdmin, Provisioner, and Operator profiles, as well any custom user profile that has been generated. You can select custom and multiple profiles by using the Shift and Control keys while clicking the profile, or click the **All Cisco MGM Users** radio button to send your message to all users, regardless of user type.
Message	Type your message. The maximum length is 512 characters. If you enter a message that is longer than 512 characters, only the first 512 characters are sent.

8.3.4.15 Viewing User Notification Messages

The User Notification dialog box pops up on your screen when another user sends a message to a certain user profile or to all Cisco MGM users, and you belong to one of those groups. Table 8-18 describes the fields in the dialog box.

Table 8-18 Field Descriptions for the User Notification Dialog Box

Field	Subfield	Description
Message Received	From	Username of the user who sent you the message.
	Time	Date and time when you received the message.
Message	—	Text of the message. The maximum message length is 512 characters.

8.4 How Do I Manage the Audit Log?

The Audit Log table contains information about significant events (user-initiated changes and activities) that occurred on the Cisco MGM server during a specified time period. By default, the Audit Log displays information about significant events that occurred during the last four hours. You can change the default time period in the User Preferences dialog box. Each record has a time stamp, record type, and message string.

There are two types of audit log available in Cisco MGM:

- Audit logs for the Diagnostic Center, Configuration Center, Statistics Reporting Tool and Chassis View. These audit logs are accessed directly from the log directory on the server at /opt/svplus/log.
- Audit logs for the other applications in Cisco MGM. Choose **Administration > Audit Log** to view these Audit logs.

Audit Log data can be filtered, see section 8.4.2 Filtering Audit Log Data, page 8-32.

The Audit Log records the following runtime-affecting operations for monitoring purposes:

- Cisco MGM client logins, logouts, and security violations (including successful/unsuccessful client user logins and forced logouts)
- NE or group location changes in the Domain Explorer tree
- Domain Explorer group operations (add, delete, or modify a group)
- Changes in the Domain Explorer properties of an NE
- NE Service, PM Service, and Cisco MGM GateWay Service start or stop operations
- Cisco MGM user administration (add, delete, or modify user profile)
- Changes in:
  - UI properties
  - Security settings
  - High availability settings
  - Recovery settings
  - Database configuration
  - Error log configuration
  - NE autobackup parameters
  - NE service parameters
- Job or task cancellation in the Job Monitor table
- Manual memory backup
- Memory restore
- Software download
- OSS profile changes (CORBA)
- Cisco MGM GateWay/CORBA client logins/logouts

The following topics are covered:

8.4.1 Viewing the Audit Log

To view the Audit Log, choose **Administration > Audit Log** in the Domain Explorer window. Table 8-19 describes the fields in the Audit Log.

Table 8-19 Field Descriptions for the Audit Log

Field	Description
Source ID	Source of the event. Events performed by the Cisco MGM server show *Cisco MGM* as the source ID.
Username	Name of the user performing the logged event. Events performed by the Cisco MGM server are logged under the username *Internal*.
Service	Name of the service that generated the audit log entry.
Cisco MGM Time Stamp (*time zone*)	Date and time when the event occurred on the Cisco MGM server.
Category	Name of the category in which the event occurred. Events belong to one of the following categories: Cisco MGM server administration, Cisco MGM server connectivity, Cisco MGM server security, Cisco MGM server topology, Cisco MGM server network, or NE provisioning.
Message	Description of the significant event that occurred.

8.4.2 Filtering Audit Log Data

Use the Audit Log Filter dialog box to filter data according to criteria that you select and to display the results in the Audit Log table. To access the Audit Log Filter dialog box, in the Cisco MGM Audit Log window, choose **File > Filter**. Table 8-20 describes the fields in the filter dialog box.

Table 8-20 Field Descriptions for the Audit Log Filter Dialog Box

Tab	Description
Time Stamp (*time zone*)	Filter audit log data for a specified time period, ranging from the past hour to the past 6 months. You can click the **User Specified** radio button to specify an exact filter starting and ending time by month, day, year, and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. If you want to filter audit log data and the time period is not important, click **No Time Specified**.
Source ID	Move NEs back and forth between the list of available NEs and selected NEs and then run the filter.
Category	Filter audit log data by task.
Username	Move users back and forth between the list of available users and selected users and then run the filter. Events performed by the Cisco MGM server are logged under the username *Internal*.
Service	Move services back and forth between the list of available services and selected services and then run the filter.