



Setting Up CMNM Security

Introduction to CMNM Security

CMNM provides user access control, which allows a system administrator to control what different users are able to do. Each user has a different login name and password, with 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. The administrator user may not be edited other than to change the password.

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

Within CMNM, 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 belongs. 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

CMNM 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.

It is on the basis of these user groups that CMNM applies access control. The CMNM administrator configures access control by assigning access specifications to the relevant user groups.

Feature Lists

All features offered to a user 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. Any given feature may appear in more than one feature list.

The feature lists available in CMNM are described in Table 5-1.

Table 5-1 Feature Lists in CMNM

Feature List	Permissions ¹	Description
AccessManagement	RWA	Set up users, user groups, assign passwords, and define access params.
AutoDiscovery	RW	Launch the auto-discovery services
Change Password	RWA	Change passwords
Deployment	RW	Deploy sites, regions, and network (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	Allow user to 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)
MGC-Node-Accounts	RWA	Change the passwords, login IDs, and SNMP community strings
MGC-Node-Diagnostics	RW	Run diagnostic tools on Cisco MGC node components
MGC-Node-Filesystems	RW	View file system information on BAMS and Cisco MGC host devices
MGC-Node-Properties	R	View properties of Cisco MGC node components
MGC-Node-Provisioning	RW	Deploy all Cisco MGC node components (either manually or via 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	RWA	Performance configuration and image upload and download
MGC-Node-Trap-Forwarding	RWA	Configure trap forwarding destinations
MGX-Accounts	RWA	Change the passwords, IDs, and SNMP info for Cisco MGX 8260 components
MGX-Properties	R	View properties of Cisco MGX 8260 components
MGX-Provisioning	RW	Deploy Cisco MGX 8260 components
MGX-States	RW	Change the states of Cisco MGX 8260 components

Table 5-1 Feature Lists in CMNM

Feature List	Permissions ¹	Description
MGX-Tools	RW	Launch Cisco MGX 8260 component tools
MGX-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	Allow user to define and edit thresholds
ThresholderViewFeatureList	R	Allow user to 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 the permissions you want to assign to various types of users. For more information, see the “Creating Typical Types of Users” section on page 5-16.



Note

In CMNM, features are preassigned to feature lists and cannot be modified.

Access Specifications

Access specifications connect together the user groups, the features that can be invoked by a group, and the objects upon which these features can be invoked.

A number of access specifications are provided by default with the CMNM. More access specifications can be built at the discretion of the system administrator.

Each access specification may include the following components:

- Feature lists—Lists the CMNM features that the users in this group have access to. A feature list can appear in more than one access specification.
- User groups—CMNM user accounts can be collected by an administrator into groups. These user groups can be used to model user roles. It is on the basis of these user groups that CMNM applies access control.
- A permission level—For example, read-only, read-write, and so on.
- An optional object group—Where an object group is supplied, the users in the group have access to the features specified by 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. This object group could be used 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 nonadministrative users.

Setting Up Accounts

CMNM allows the administrator to associate privileges with user accounts. For example, regular users can be prevented from performing certain management functions, while more technically sophisticated users can be given full management privileges.

CMNM provides the following security features:

- User login IDs and alphanumeric passwords
- Per-user privileges and control of administrative functions
- Administrative control of accounts and password resets
- Attack alerts (the connection is closed after three unsuccessful login attempts)

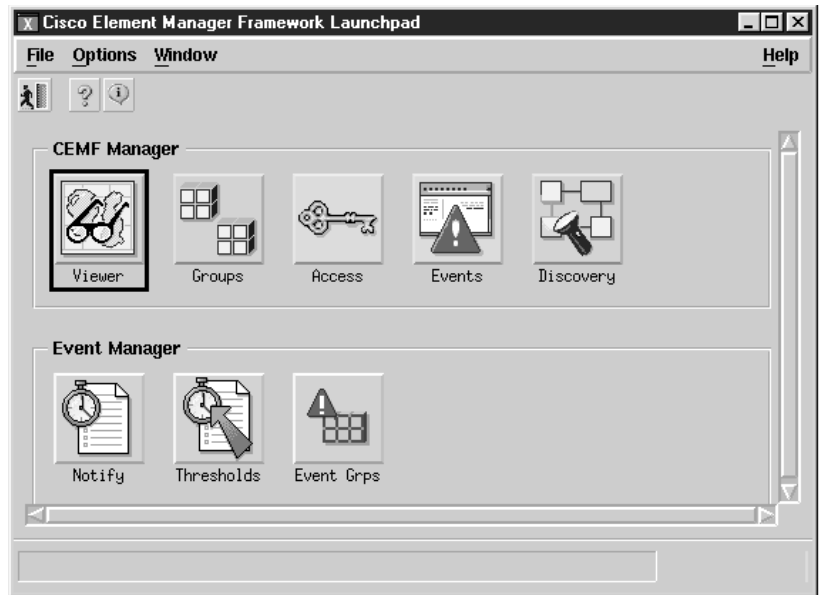
Setting Up New Accounts

You must set up new accounts for all users. You may also define user groups.

To create a new account for a user and assign a password:

-
- Step 1** Click the **Access** icon on the CEMF Launchpad, as shown in Figure 5-1.

Figure 5-1 CEMF Launchpad Screen



You see the Access Manager screen.

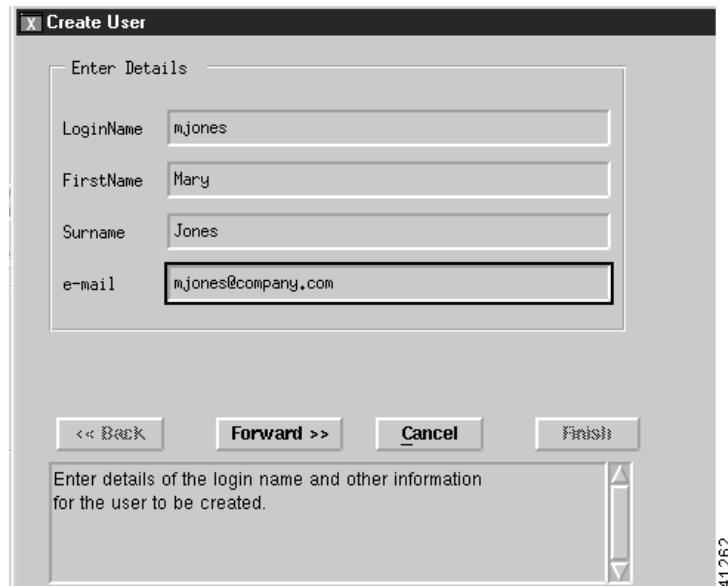
- Step 2** From the Access Manager screen, select **Edit**, **Create**, then **User** as shown in Figure 5-2.

Figure 5-2 Access Manager Screen—Edit->Create>User Option



You see the screen in Figure 5-3.

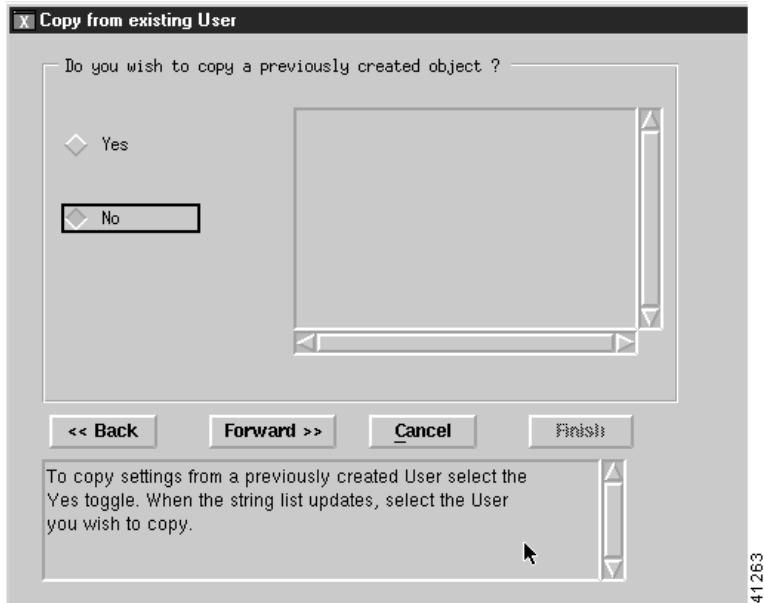
Figure 5-3 Create User Screen



Step 3 Enter the requested information and then click **Forward**.

You see the screen in Figure 5-4.

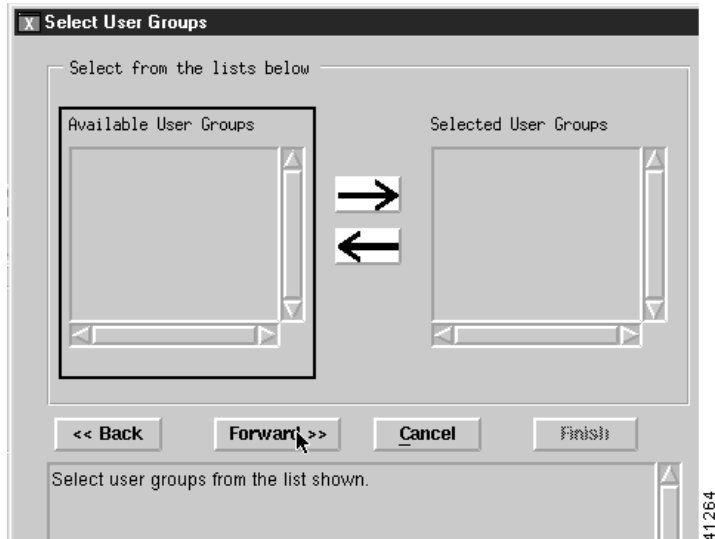
Figure 5-4 Copy from existing User Screen



Step 4 To use an existing user as a template for the user you are adding, click **Yes**, select the user you want to copy, then click **Forward**. If you do not want to copy an existing user or none exists, click **No** then click **Forward**.

You see the screen in Figure 5-5.

Figure 5-5 Select User Groups Screen



Step 5 Select a user group, click an arrow to move it to the Selected User Groups list, and click **Forward**. If no user groups are defined at this time, 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 User Groups” section on page 5-8.

You see the screen in Figure 5-6.

Figure 5-6 User Password Entry Screen

41265

- Step 6** 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**.

If you typed a valid password, you see the screen in Figure 5-7. If you typed an invalid password, you see Figure 5-6 again with an error message. Reenter a valid password.

Figure 5-7 Summary Details for User Screen

41267

- Step 7** To make changes, click **Back** and enter the corrected information. To add the user, click **Finish**. You see the screen in Figure 5-8 listing the defined users.

Figure 5-8 Access Manager Screen—List of Users



Creating User Groups

To divide users into groups by creating user groups:

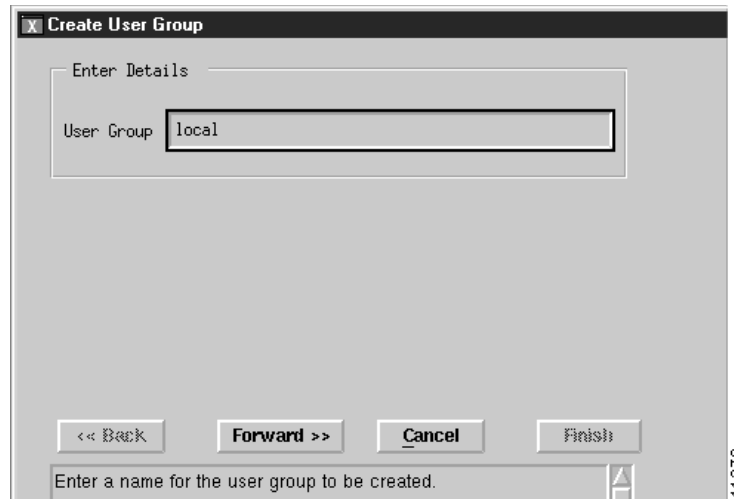
- Step 1** From the Access Manager screen, select **Edit**, **Create**, then **User Group** as shown in Figure 5-9.

Figure 5-9 Access Manager Screen—Edit->Create->User Group Option



You see the screen in Figure 5-10.

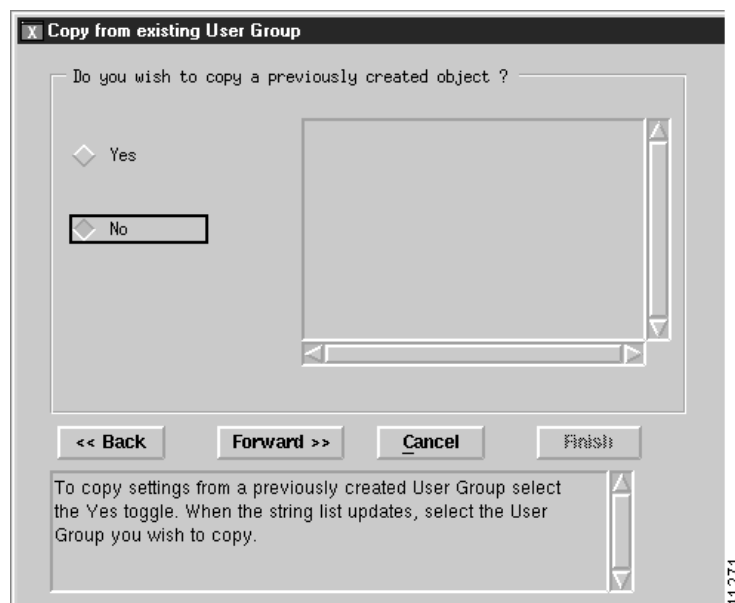
Figure 5-10 Create User Group Screen



Step 2 Type the name of a user group in the field and click **Forward**.

Step 3 You see the screen in Figure 5-11.

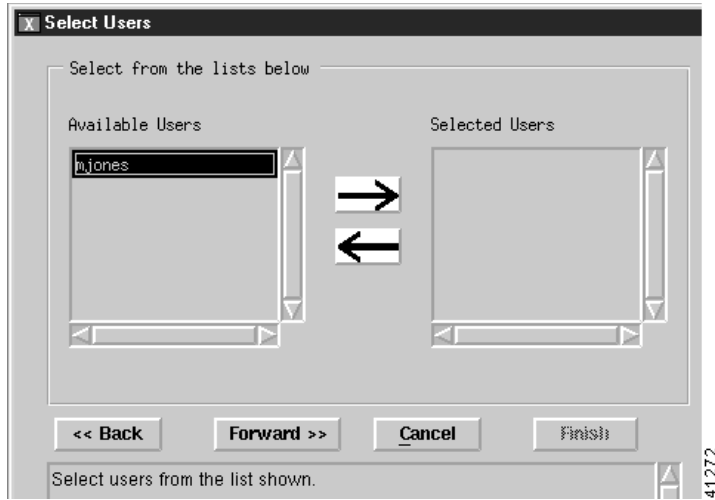
Figure 5-11 Copy from existing User Group Screen



Step 4 If you:

- Want to use an existing user group as a template for the user group you are adding, click **Yes**, select the user group you want to copy, then click **Forward**. You see the screen in Figure 5-14.
- Do not want to copy an existing user group or none exists, click **No**, then click **Forward**. You see the screen in Figure 5-12.

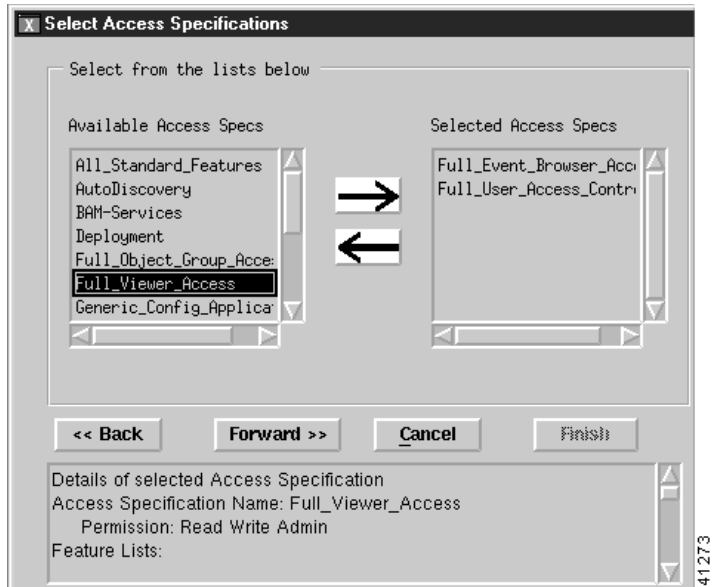
Figure 5-12 Select Users Screen



Step 5 Select each user you want in the new group and click the arrow to move each to the Selected Users list. When you are finished, click **Forward**.

You see the screen in Figure 5-13.

Figure 5-13 Select Access Specifications Screen



Step 6 Select each access specification you want for the new group and click the arrow to move each to the Selected Access Specs list. When you are finished, click **Forward**.

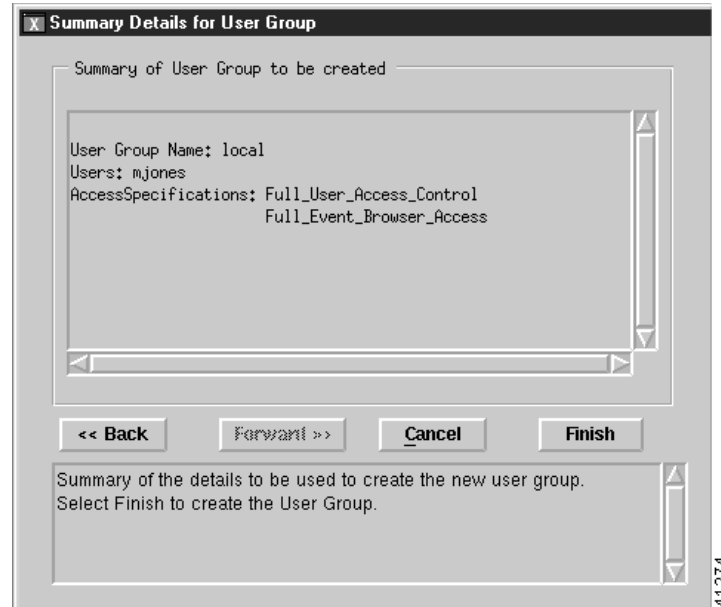

Caution

Giving a user group full access allows each user in the user group to add or delete other users and to change specifications for all other users.

For more information about access specifications, see the “Creating New Access Specifications” section on page 5-11.

You see the screen in Figure 5-14.

Figure 5-14 Summary Details for User Group Screen



- Step 7** To make changes, click **Back** and enter the corrected information. To add the user group, click **Finish**.

Creating New Access Specifications

To create new access specifications:

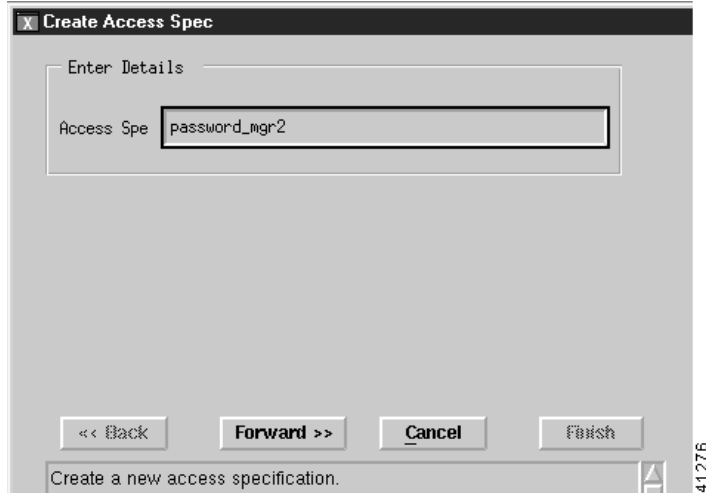
- Step 1** From the Access Manager screen, select **Edit**, **Create**, then **Access Spec**, as shown in Figure 5-15.

Figure 5-15 Access Manager Screen—Edit->Create->Access Spec Option



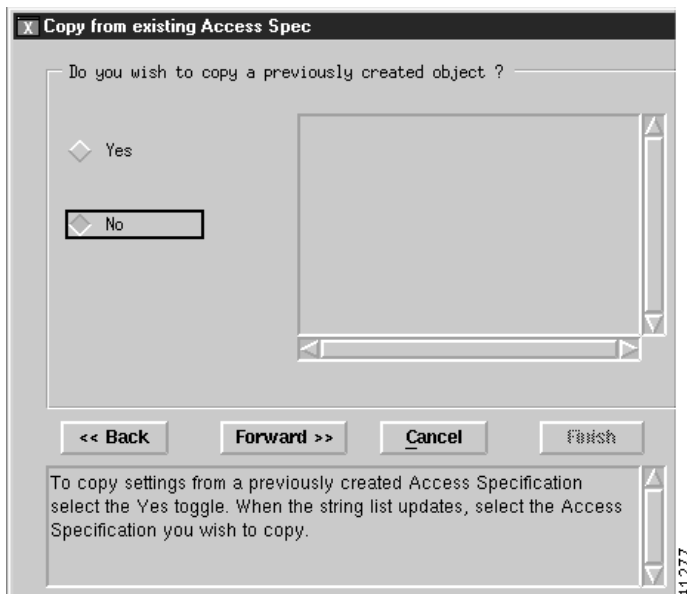
You see the screen in Figure 5-16.

Figure 5-16 Create Access Spec Screen



- Step 2** Type the name of a new access specification and click **Forward**. You see the screen in Figure 5-17.

Figure 5-17 Copy from existing Access Spec Screen



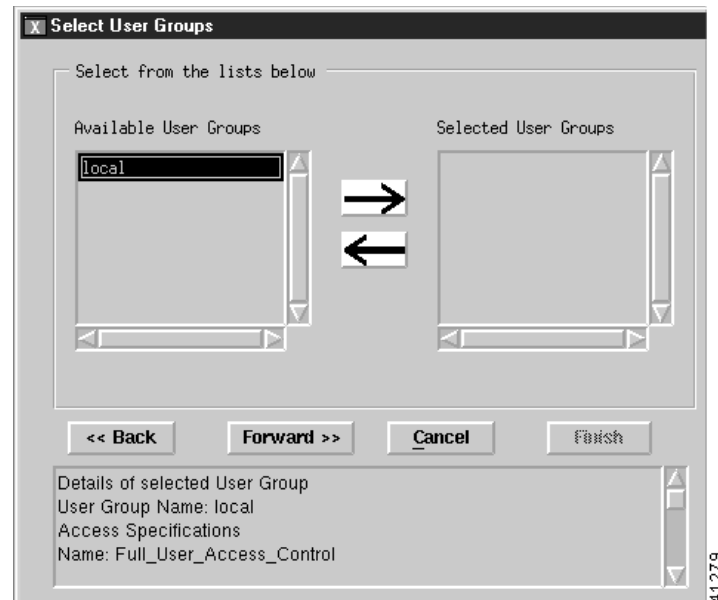
- Step 3** If you:
- Want to use an existing access specification as a template for the access specification you are adding, click **Yes**, select the access specification you want to copy, then click **Forward**. You see the screen in Figure 5-22.
 - Do not want to copy an existing access specification or none exists, click **No**, then click **Forward**. You see the screen in Figure 5-18.

Figure 5-18 Select Permission Screen



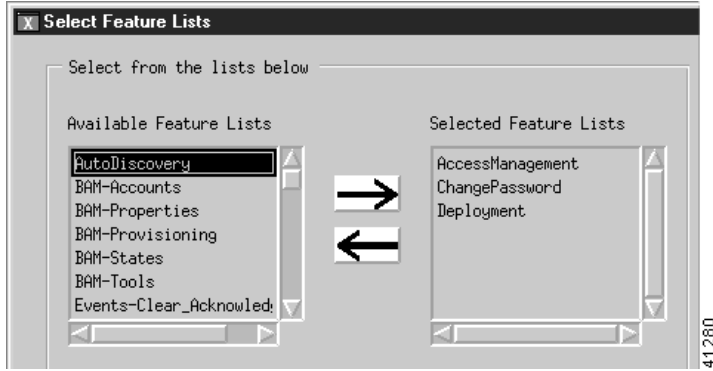
- Step 4** Select the permission level desired and click **Forward**.
You see the screen in Figure 5-19.

Figure 5-19 Select User Groups Screen



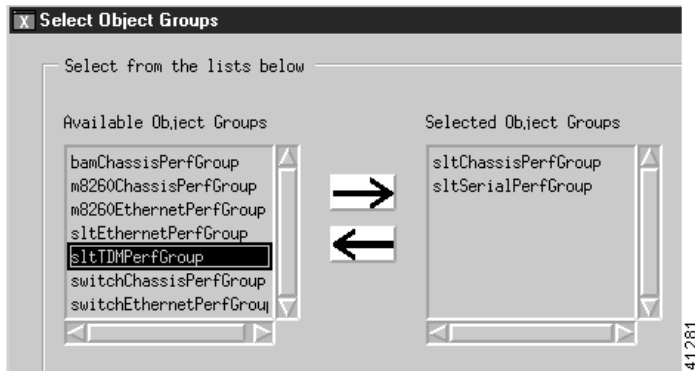
- Step 5** Select a user group from the available user groups list and click the right arrow to move it to the Selected User Groups list. Click **Forward**.
You see the screen in Figure 5-20.

Figure 5-20 Select Feature Lists Screen



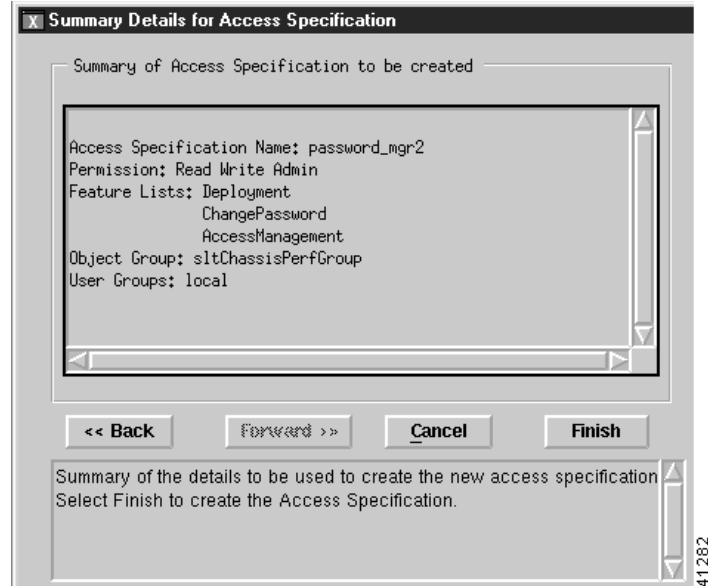
- Step 6** Select each feature you want for the new access specification and click the right arrow to move each to the Selected Feature Lists. When you are finished, click **Forward**.
 You see the screen in Figure 5-21.

Figure 5-21 Select Object Groups Screen



- Step 7** Select each object group you want for the new access specification and click the right arrow to move each to the Selected Object Groups list. When you are finished, click **Forward**.
 You see the screen in Figure 5-22.

Figure 5-22 Summary Details for Access Specification Screen



- Step 8** To make changes, click **Back** and enter the corrected information. To add the access specification, click **Finish**.
-

Creating Typical Types of Users

Table 5-2 summarizes how you would create three typical users.

Table 5-2 Creating Typical Users

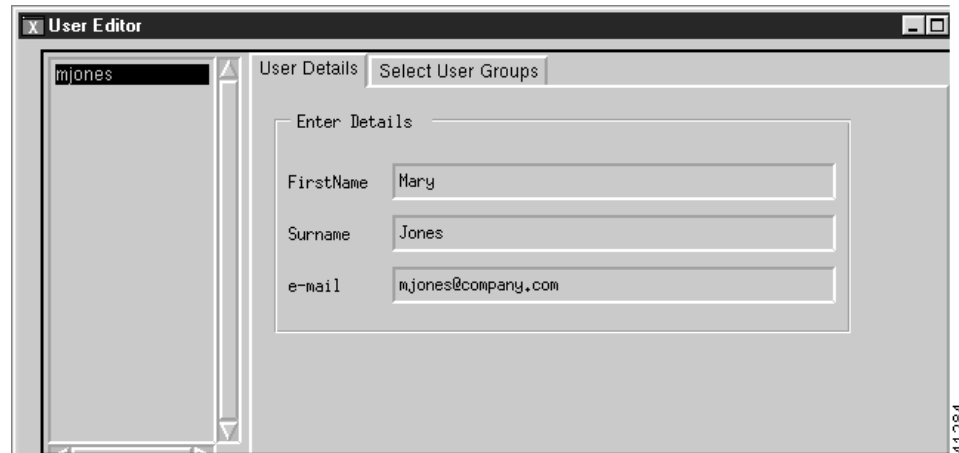
To Create This Type of Account:	Perform These Steps:
Administrator	Using the instructions in the “Setting Up New Accounts” section on page 5-4, create a new account and create the user by copying the existing administrator template. The administrator should have all the features labeled with the permissions R, RW, and RWA in Table 5-1.
Operator with read permission that can deploy and launch tools	<p>Using the instructions in the “Creating New Access Specifications” section on page 5-11, create a new access specification with the features labeled with the permissions R and RW in Table 5-1.</p> <p>Using the instructions in the “Creating User Groups” section on page 5-8, create a new user group with the access specification you just created.</p> <p>Then using the instructions in the “Setting Up New Accounts” section on page 5-4, create a new account, create the user, and assign the user to the group you just created.</p>
Operator with read-only permission	<p>Using the instructions in the “Creating New Access Specifications” section on page 5-11, create a new access specification with the features labeled with the permission R in Table 5-1.</p> <p>Using the instructions in the “Creating User Groups” section on page 5-8, create a new user group with the access specification you just created.</p> <p>Then using the instructions in the “Setting Up New Accounts” section on page 5-4, create a new account, create the user, and assign the user to the group you just created.</p>

Modifying Users

To modify a user:

-
- Step 1** From the Access Manager screen, select **Edit, Modify**, then **User**.
You see the screen in Figure 5-23.

Figure 5-23 User Editor Screen



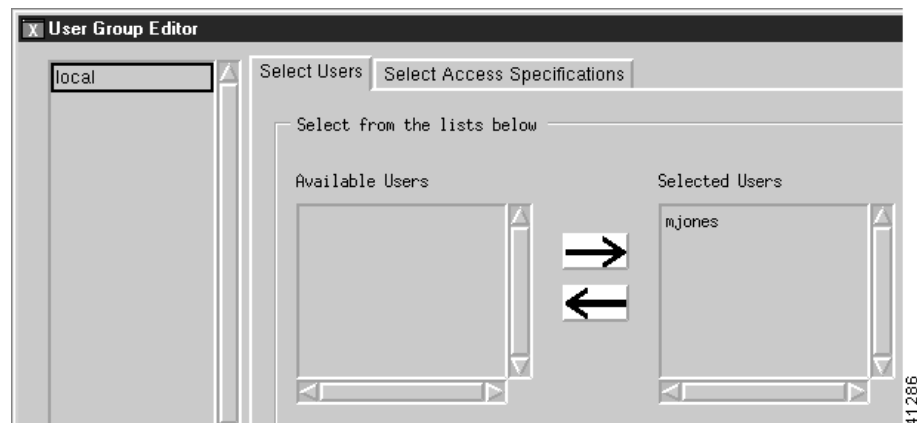
- Step 2** Select a user from the list and change any information in the fields. To change the user groups that the user belongs to, click the **Select User Groups** tab and make any changes.
- Step 3** Click **Apply**. To cancel changes, click **Revert**.

Modifying User Groups

To modify a user group:

- Step 1** From the Access Manager screen, select **Edit, Modify**, then **User Group**.
You see the screen in Figure 5-24.

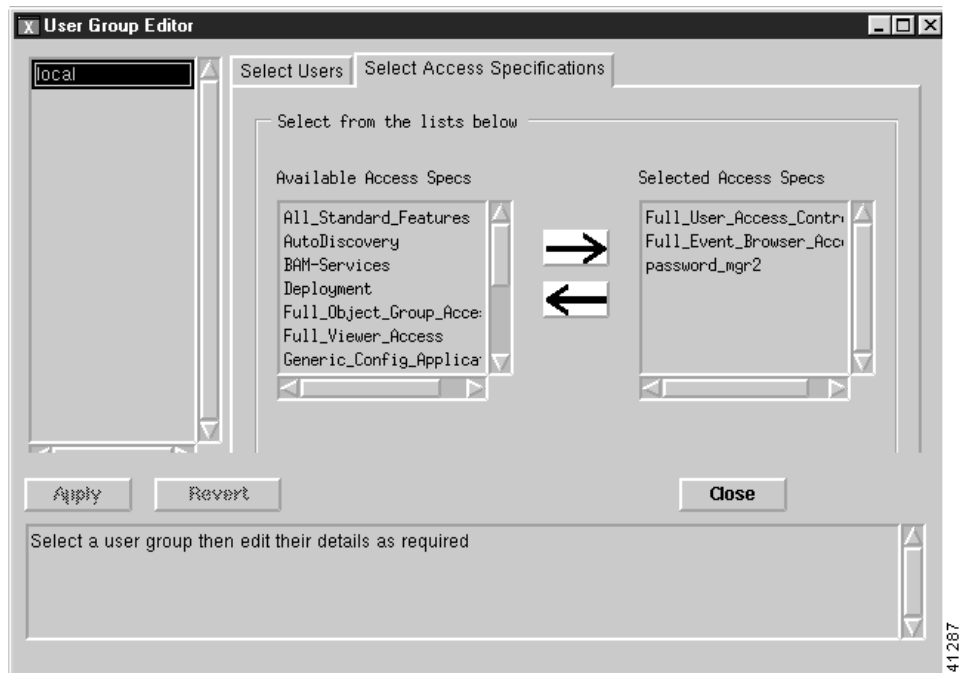
Figure 5-24 User Group Editor Screen—Select Users Tab



- Step 2** Select a user group from the list of available user groups. Select users and click the arrows to add or remove users from the group.
- Step 3** To modify access specifications for the user group, click the **Select Access Specifications** tab.

You see the screen in Figure 5-25.

Figure 5-25 User Group Editor Screen—Select Access Specifications Tab



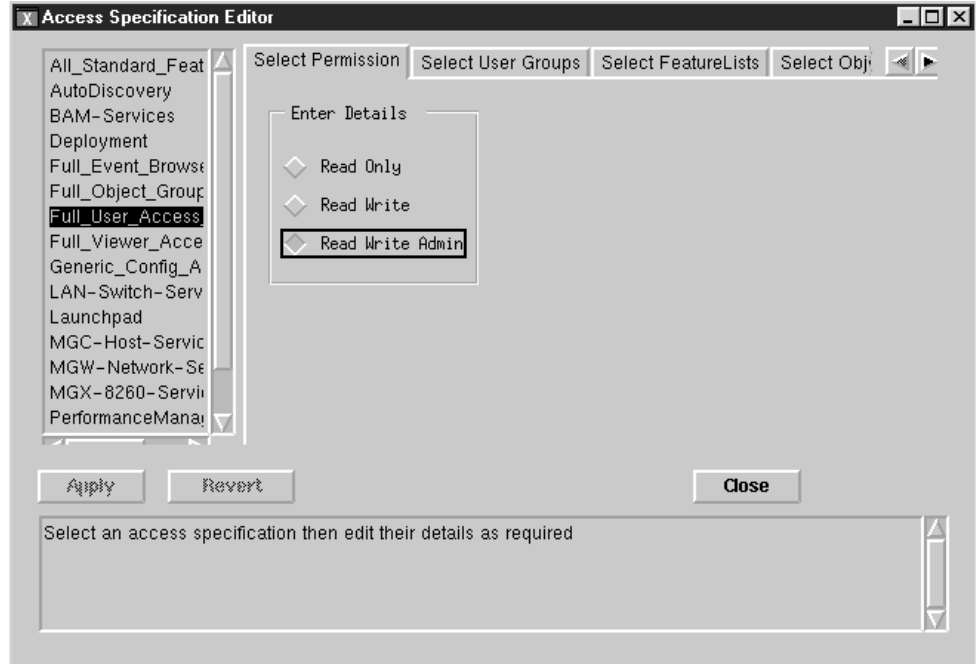
- Step 4 Select access specifications and click the arrows to add or remove access specifications from the group.
- Step 5 Click **Apply**. To cancel changes, click **Revert**.

Modifying Access Specifications

To modify an access specification:

- Step 1 From the Access Manager screen, select **Edit, Modify**, then **Access Spec**.
- Step 2 You see the screen in Figure 5-26.

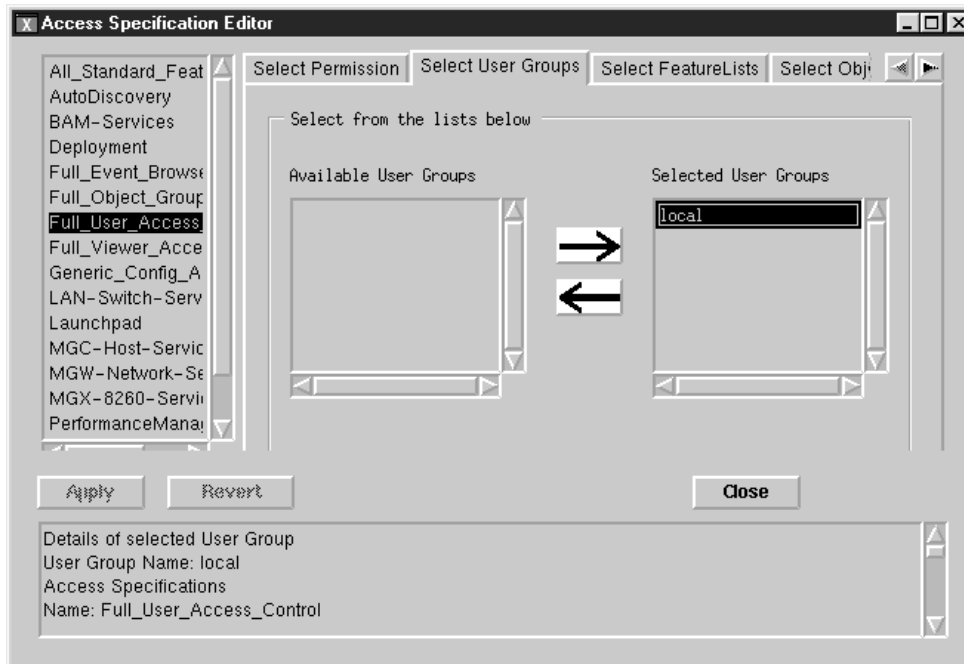
Figure 5-26 Access Specification Editor Screen—Select Permission Tab



41290

- Step 3 Edit the permission if necessary.
- Step 4 Click the **Select User Groups** tab.
- Step 5 You see the screen in Figure 5-27.

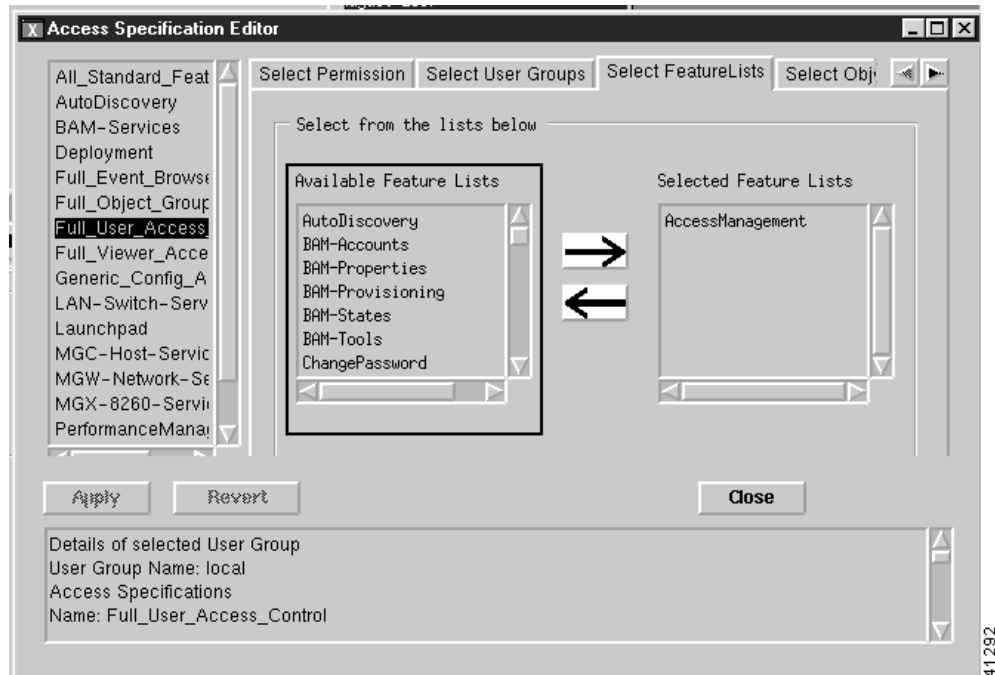
Figure 5-27 Access Specification Editor Screen—Select User Groups Tab



41291

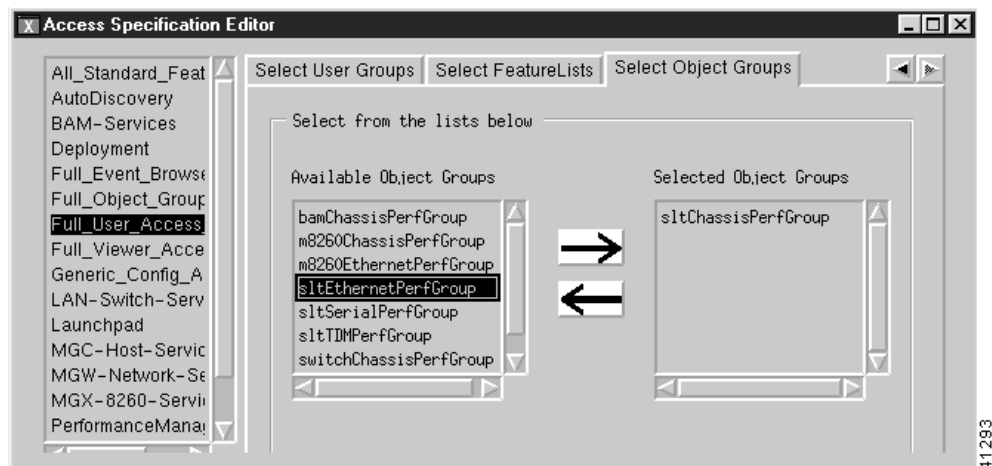
- Step 6** Select user groups and click the arrows to add or remove users groups from the access specification.
- Step 7** Click the **Select Feature Lists** tab.
- You see the screen in Figure 5-28.

Figure 5-28 Access Specification Editor Screen—Select Feature Lists Tab



- Step 8** Select features and click the arrows to add or remove features from the access specification.
- Step 9** Click the **Select Object Groups** tab.
- Step 10** You see the screen in Figure 5-29.

Figure 5-29 Access Specification Editor Screen—Select Object Groups Tab



- Step 11** Select object groups and click the arrows to add or remove object groups from the access specification.

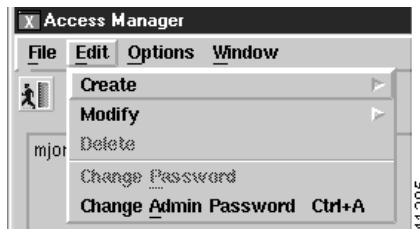
Step 12 When you are finished, click **Apply**. To discard changes, click **Revert**. Click **Close**.

Changing the Administrative Password

To change the administrative password:

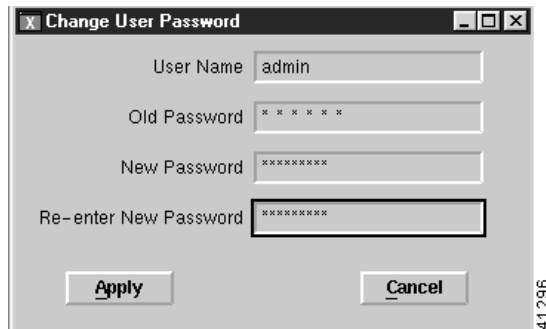
Step 1 From the Access Manager screen, select **Edit**, then **Change Admin Password**, as shown in Figure 5-30.

Figure 5-30 Access Manager Screen—Edit>Change Admin Password Option



You see the screen in Figure 5-31.

Figure 5-31 Change User Password Screen



Step 2 Change the password and click **Apply**.
