

Chapter 8

NMC-RX Security

This chapter discusses creating and managing security for your element management system.

Topic	Page
Overview	105
Configuring User Authentication Settings	106
Creating User Profiles	108
Configuring Remote Login	110
Creating Group Security	115
Removing Devices	118
Summary	119

Overview

The NMC-RX application provides security features for users and groups. It does not currently provide security directly for elements (devices), but it does provide security *indirectly* to devices as members of groups.

The NMC-RX application allows an administrator to provide security for the network by:

- Determining how users will be authenticated; either locally or through a RADIUS server

- Assigning passwords and privilege levels to users

- Choosing a user's remote login method (Telnet or SSH)

- Creating access lists for groups



NOTE: The security features provided by the NMC-RX application are not available through the Juniper Networks command-line interface (CLI).

References

For additional information, see:

Chapter 6, Using Groups and Devices

Chapter 12, Using Device Utilities

Configuring User Authentication Settings

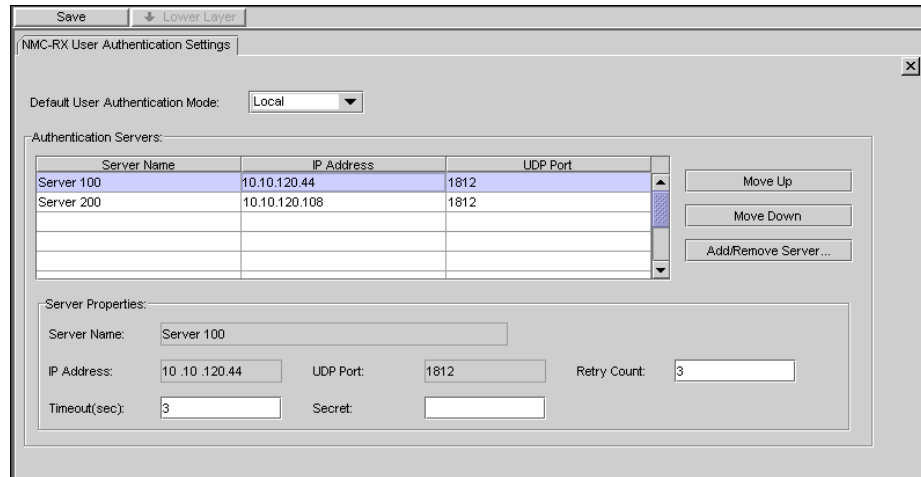
RADIUS authentication or local database authentication can be set as the default mode of user login authentication. A list of RADIUS servers can be specified to authenticate user logins; the order in which they are queried can also be set. RADIUS authentication can be set on a per user basis when creating a user profile (see *Creating User Profiles* on page 108 for more information).

Only users with admin rights can set user authentication settings.

To configure user authentication settings:

1. In either the Network or Device Workshop, from the Configuration menu, select User Authentication.

The NMC-RX User Authentication Settings tab appears in the work area.



2. Set user authentication settings parameters. See Table 24.

Table 24: User Authentication Settings Parameters

Parameter	Description
Default User Authentication Mode	Determines whether user logins will be authenticated locally or with a RADIUS server by default. Can be modified per user profile (see <i>Creating User Profiles</i> on page 108 later in this chapter).

Table 24: User Authentication Settings Parameters (continued)

Parameter	Description
RADIUS Authentication Servers	<p>List of RADIUS authentication servers available to authenticate NMC-RX user logins.</p> <p>List is sorted in the order that the servers are used when a user authentication takes place. When a server fails to respond with an acceptance, rejection, or challenge, the next server in the list is tried.</p> <p>To add or remove a server from the list, click the Add/Remove Server button (see the next section, <i>Related Dialog Box</i>).</p> <p>Select a server from the list and click the Move Up and Move Down buttons to change the order in which the servers are checked.</p>
Server Properties	
Server Name	Name of the selected RADIUS server; uneditable
IP Address	IP address of the selected RADIUS server; uneditable
UDP Port	UDP port of the selected RADIUS server; uneditable
Retry Count	Number of times to retry the selected RADIUS server; range 0-16; default 3
Timeout (sec)	Time to wait to receive a response from the selected RADIUS server; range 3-30; default 3
Secret	A string that is known by the server and the client used to obfuscate the packets that are exchanged between the server and client; range 0-32 characters; default is empty

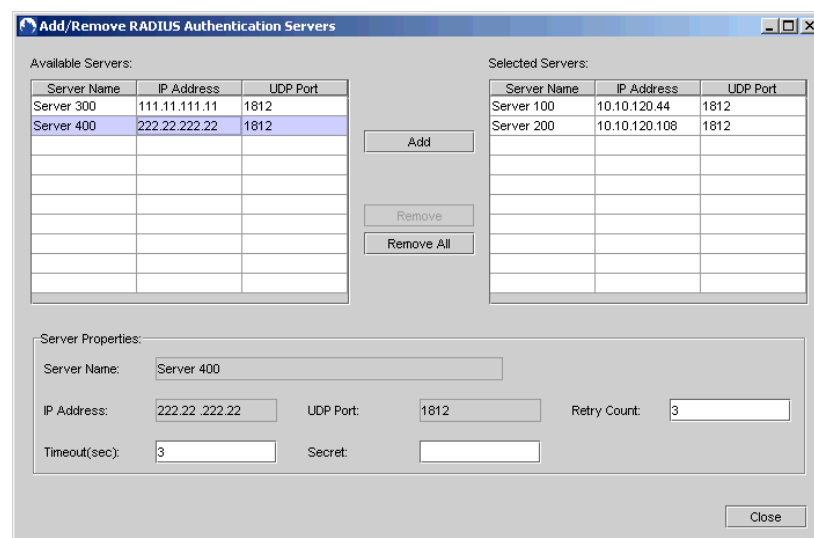
- Click the Save button.

The default user authentication settings are saved.

Related Dialog Box

Add/Remove RADIUS Authentication Servers

The Add/Remove RADIUS Authentication Servers dialog box appears when you click the Add/Remove Server button on the User Authentication Settings tab.



The Available Servers list (left) lists all authentication servers that have been created or discovered that have not yet been selected. The Selected Servers list (right) can have up to ten servers selected to authenticate user logins.

To add or remove servers:

1. Select a server from a list, and click either Add or Remove.

The server is added to or removed from the appropriate list.



NOTE: When adding a server, you can change parameters for the selected server in the Server Properties group box (see Table 24 for field descriptions).

2. Click Close.

The server(s) are added to or removed from the RADIUS Authentication Servers list on the NMC-RX User Authentication Settings tab.

Creating User Profiles

Only a security user can create a user profile. When creating a user profile, the security user can:

Set the username and password

Select how the user login will be authenticated (either locally or through a RADIUS authentication server; see the previous section)

Assign a privilege level to the user

Only users with the Security privilege enabled can modify the User Privilege settings. Privilege settings are enabled for an admin user and the settings can never be changed.

User privileges are divided into three categories:

Security—Allows access to administer application-specific settings, such as inserting/removing members of groups, creating groups and new users, and setting user authentication settings.

Backup—Allows you to save and restore running configurations on managed E-series routers.

Device Administration—Allows access to device-specific settings and features. You can specify five areas for the device administration category, which are: view, create, configure, delete, and execute.

To create a user profile:

1. In either the Network or Device Workshop, from the Configuration menu, select Create, and click User Profile.

The Create User Profile dialog box appears.

2. Set the user profile parameters. See Table 25.

Table 25: User Profile Parameters

Parameter	Description
User Name	Range 1–32 characters; must contain at least one alphabetic and one numeric character
User Authentication	
User Authentication Mode	(See <i>Configuring User Authentication Settings</i> earlier in this chapter for more information.) Determines the type of login: Local—Authenticates the user login locally RADIUS—Authenticates the user login through a RADIUS server
Test Login	Becomes active when RADIUS is selected as the user authentication mode. When clicked, the RADIUS login action is started. A RADIUS server must be configured for the test login to be successful.
User Password	Password must be between 6 and 16 characters. It must contain at least one alphabetic and one numeric character. The password assigned by the administrator is considered to be a default password that the user can change.
Re-enter Password	Password must be typed again exactly as typed in the User Password field.

Table 25: User Profile Parameters (continued)

Parameter	Description
User Privilege	
Privilege Settings	<p>Sets the level to determine what actions a user can take in regard to a particular object.</p> <p>Security—Allows a user to administer application settings. For example, a user is limited to creating groups and devices, and cannot access the Device Workshop or perform device configuration.</p> <p>Backup—Allows a user to save or restore E-series configurations. For example, a user can restore or save a running configuration.</p>
Device Administration	<p>Sets the level to determine what actions a user can take in regard to a particular object.</p> <p>View—Allows a user to view a device's configuration.</p> <p>Create—Allows a user to create configurations on a device.</p> <p>Configure—Allows a user to configure a device's configuration.</p> <p>Delete—Allows a user to delete device configurations.</p> <p>Execute—Allows a user to execute certain device actions. For example, user is allowed to run ping on a device or log in remotely to a device.</p>
User Preferences	
Single Click Object View	Displays an object's current configuration in view mode with a single click; default: disabled (cleared)
SNMP Community Strings:	<p>Values are set to the SNMPv2c industry standard defaults.</p> <p>Read Only—public</p> <p>Read/Write—private</p> <p>Admin—admin</p> <p>NOTE: For additional information about SNMP, see <i>E-series System Basics Configuration Guide, Chapter 3, Configuring SNMP</i>.</p>
Remote Login	To configure, see the next section, <i>Configuring Remote Login</i> .



NOTE: You cannot delete the Admin user profile (admin), but you can modify the password (nmc-rxadmin) delivered with the NMC-RX application.

- To save the settings, click OK.

Configuring Remote Login

From the NMC-RX application, you can log in to E-series routers remotely through Telnet or Secure Shell Server (SSH). The selection of either Telnet or SSH is an NMC-RX application-wide setting and is accessible only to admin-level users. Although the NMC-RX application automatically defaults to Telnet, SSH is considered a more secure alternative to Telnet for logging in to E-series routers remotely.

Because there are a variety of SSH products and implementations, the NMC-RX application provides administrators with the flexibility to specify the desired command line and options for their SSH implementation. Administrators can specify the relationship between an individual NMC-RX user and an SSH session.

If you select SSH as your remote login choice, you must:

Configure SSH on your E-series router. For information, see *JUNOS System Basics Configuration Guide, Chapter 6, Passwords and Security*.

Determine your Telnet policy before you configure SSH on your E-series router. Effective use of SSH implies that you should severely limit Telnet access to the system.

Obtain and install a commercial SSH client on the same machine on which you are running the NMC-RX application.

Install and configure a RADIUS server on a host machine before you configure SSH on your E-series router. Refer to your RADIUS server documentation for information about choosing a host machine and installing the server hardware.

Configure the RADIUS client on your E-series router. To configure RADIUS through NMC-RX, see *Configuring RADIUS Servers* in *NMC-RX User Guide, Vol. 2, Chapter 3, Configuring Virtual Routers*. For additional information about RADIUS, see the *JUNOS Broadband Access Configuration Guide*.

This section provides procedures for three tasks associated with configuring remote login:

Set the SSH username source in the Create User Profile dialog box.

Set the remote login settings.

Test the remote login action that you specify.

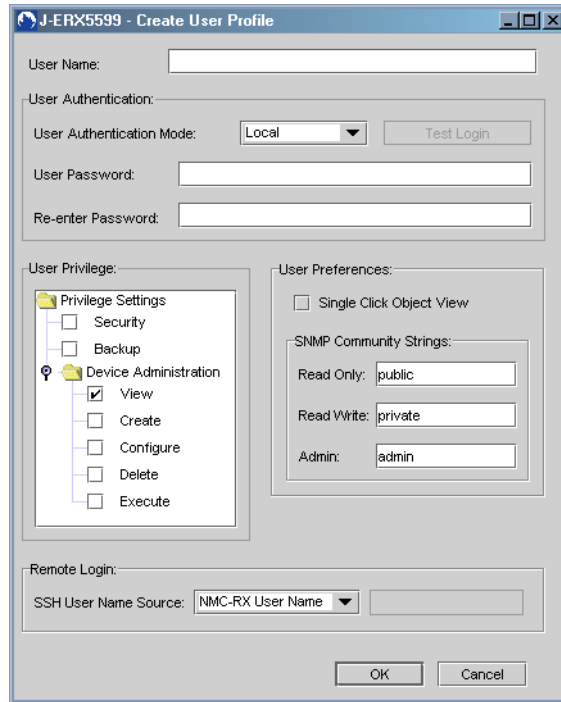
Setting SSH Username Source

When SSH is the remote login type, admin-level users must set this field to assign every user a username source for remote logins.

To set an SSH username source:

1. In either the Network or Device Workshop, from the Configuration menu, choose Create, and click User Profiles.

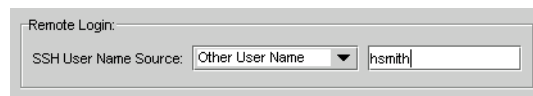
The Create User Profile dialog box appears.



2. Set the parameters described in the previous section. See Table 26.
3. Set the SSH User Name Source field by selecting either:

NMC-RX User Name—Select if you always want to use the NMC-RX username as the SSH username source. This is the default.

Other User Name—Select if you want to use a username other than the NMC-RX username as the SSH username source. When selected, the text box to the right of the field becomes editable. The username can be 1–128 characters.



Type the username in the text box.

4. To create the user profile and save the remote login settings, click OK.

Configuring Remote Login Settings

Remote Login Settings can be configured only by an admin-level user. If you do not have admin level privileges, this menu item is disabled.

To configure the remote login settings:

1. In either the Network or Device Workshop, from the Configuration menu, select Remote Login Settings.

The Remote Login Settings tab appears.

The screenshot shows the 'Remote Login Settings' dialog box. At the top left is a 'Save' button. The dialog title is 'Remote Login Settings'. Below the title bar, there is a 'Login Type:' dropdown menu currently set to 'Telnet ONLY'. Underneath, there is a section for 'SSH Command Line:' which is currently disabled. This section contains a sub-section for 'Available NMC-RX Arguments:' with two buttons labeled '<HOST>' and '<USER NAME>'. Below this is a 'Command Line String:' text input field, which is currently empty. A 'Test...' button is located at the bottom right of the dialog.

2. Set the parameters as shown in Table 26. For example:

The screenshot shows the 'Remote Login Settings' dialog box with the 'Login Type:' dropdown menu set to 'SSH ONLY'. The 'SSH Command Line:' section is now enabled. The 'Available NMC-RX Arguments:' buttons are still present. The 'Command Line String:' text input field is now populated with the text 'ssh <USER NAME>@<HOST>'. The 'Test...' button remains at the bottom right.

Table 26: Remote Login Settings Parameters

Parameters	Description
Login Type	Determines the type of login specified through the NMC-RX application: Telnet ONLY—Default. When selected, SSH is disabled. SSH ONLY—When selected, the SSH command line parameters are enabled and must be specified.
SSH Command Line	Specifies the parameters in this section for SSH authentication.

Table 26: Remote Login Settings Parameters (continued)

Parameters	Description
Available NMC-RX Arguments	<p>< Host> —Specifies the IP address of the device to which you are connecting. When clicked, the < HOST> token is added to the command line string (see below).</p> <p>< USER NAME> —Specifies the username, which is the SSH username set in the NMC-RX user profile. Either the NMC-RX username or another username specified by the administrator can be used. When clicked, the < USER NAME> token is added to the command line string (see below).</p>
Command Line String	<p>Specifies what will be executed when the remote login action is started. The string contains arguments necessary for SSH authentication. Syntax example:</p> <pre>ssh2 <USER NAME>@<HOST></pre> <p>ssh2—SSH executable</p> <p>< USER NAME> —Parameter syntax for username</p> <p>< HOST> —Parameter syntax for IP address</p>
Test	<p>When clicked, the remote login action is started with the command line string that you specified.</p>

3. Click Save.

Testing Remote Login Action

When remote login is started, the arguments that you have specified in the Command Line String field are translated to the specified username and IP address. For example,

```
ssh2 <USER NAME>@<HOST>
```

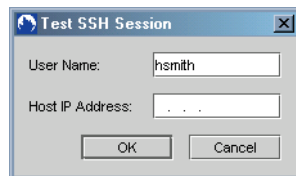
could translate to:

```
ssh2 hsmith@10.5.129.39
```

To test the remote login action that you specified in the Command Line String field:

1. Click Test.

An SSH Test Session dialog box appears. One of these dialogs appears when a *username* and *host* argument is specified or when only a *host* argument is specified.



- (Optional) Specify a username.



NOTE: The username that appears in the text box is the SSH username that is specified in the user profile.

- Enter the host IP address.
- Click OK.

The SSH application remotely logs in to the E-series router's command-line interface (CLI).

```
ssh2 hsmith@10.6.129.39
Authentication successful.
Telnet password: *****
Logged in on vty 1 via SSH.
Copyright (c) 1999-2002 Juniper Networks, Inc. All rights reserved.
NMS-7-2>
```



NOTE: Once you have configured SSH, you can log in remotely to the E-series router via the Tools menu. Select Device Utilities and Remote Login. The SSH Sessions dialog box appears. Enter the host IP address, and click OK. The E-series router's CLI appears. For more information, see *NMC-RX User Guide, Vol. 2, Chapter 12, Using Device Utilities*.

Creating Group Security

Only a user with admin privileges can create groups and provide them with network group security. Users having read/write and read-only privileges can perform functions only in groups to which an admin user has given them access. All groups an admin user creates participate in this network group security feature.

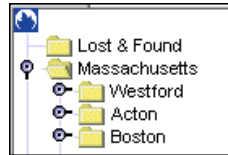
The NMC-RX application does not support security at the device level. To establish security for a particular device, the admin user can create the device as a member of a group and apply a security setting and, if needed, a security filter to the group.



NOTE: Group security cannot be enforced at the CLI, because the E-series router itself does not have a group concept.

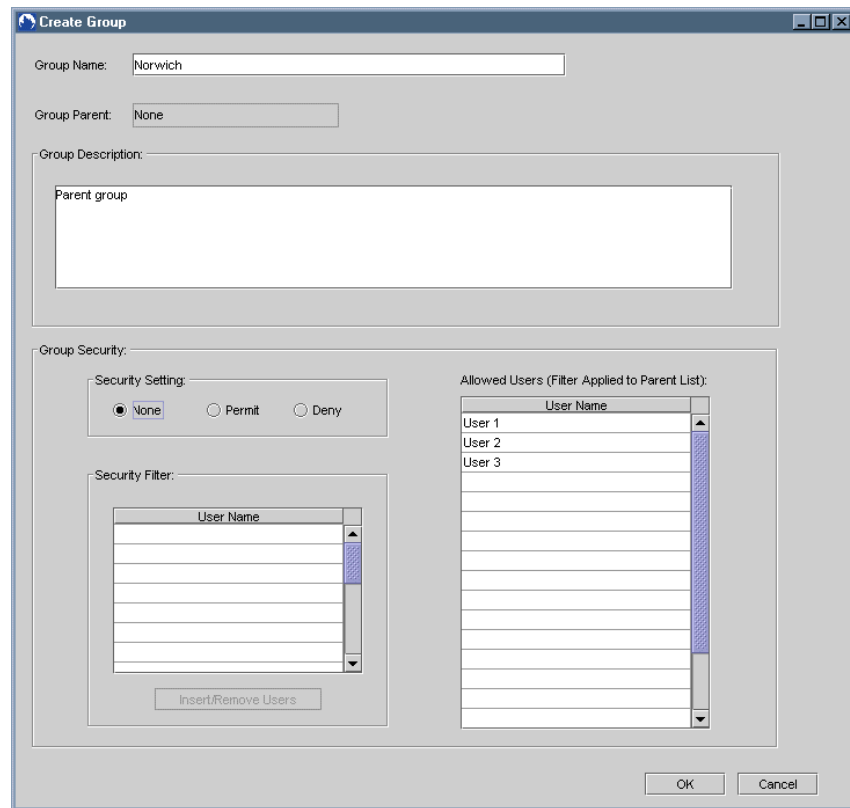
To create a group:

1. From the Network Workshop, click the Juniper Networks icon in the upper-left corner of the context area.



2. Right-click, select Create, and click Group.

The Create Group dialog box appears.



3. Set the Create Group parameters. See Table 27.

Table 27: Group Parameters

Parameter	Description
Group Name	Identifies the group. Name may not exceed 32 alphanumeric characters and may include spaces.

Table 27: Group Parameters (continued)

Parameter	Description
Group Parent	Identifies the name of the new group's parent. If the new group does not have a parent, the Group Parent text box reads None. This means the group is at the top level.
Group Description	Stores descriptive or contextual information of up to 255 alphanumeric characters. The resulting description is displayed whenever its associated group is accessed. A description can easily be changed or deleted at any time.

4. Select a Security Setting option. See Table 28.

Table 28: Security Settings

Setting	Description
None	Also known as public access. This is the default. If the group is a subgroup, no filter is applied to the group's level. The group is visible to any user who is in the group's parent's group access list or is available systemwide.
Permit	Also known as private access. This group is visible to users in the group's filter list, provided they are also in the group's parent's access list, which is the intersection of the parent group access list and this group's filter list.
Deny	This group is visible to anyone in the group's parent's access list except those users to whom the group's own filter denies access.



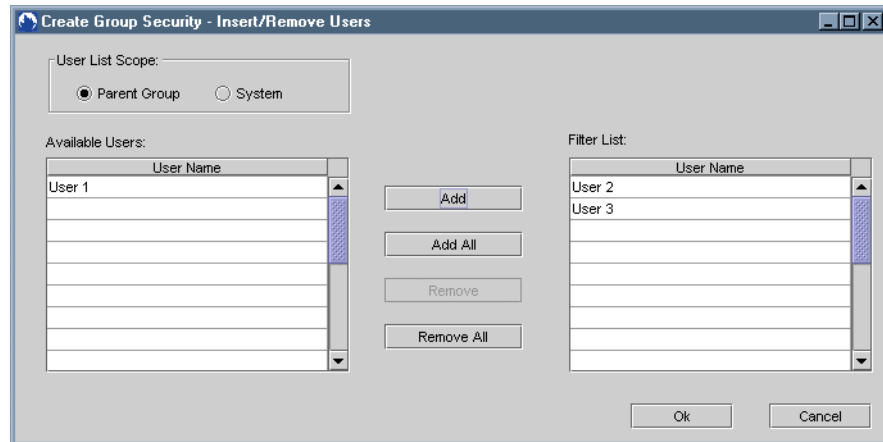
NOTE: A group's access list is derived from filtering the access lists from the top level of the navigational tree down to the given group.

If the group is a top-level group and you select None, the Allowed Users list contains all the users configured for the NMC-RX application. If the group is the child of a parent group and you select None, the Allowed Users list will contain all of the users that have access to the parent group.

If you select None, the Insert/Remove Users button is disabled. If you select either Permit or Deny, the Insert/Remove Users button is enabled, allowing you to create a filter list of users who are permitted or denied access to the group.

5. Click the Insert/Remove Users button.

The Create Group Security - Insert/Remove Users dialog box appears. In this dialog box, you can display a list of users for either the parent group or the entire system. From this list, you can create a filtered list of users with access to the group (or subgroup) that you are creating.



To create a filter list for the group, individually select the users in the Available Users list, and click the Add button to add them to the Filter List.

To add the entire list of available users to the Filter List, click the Add All button.

To remove users from the Filter List individually or collectively, either select a user in the Filter List and click Remove, or click Remove All.

6. Click OK to save the settings.

The dialog box closes, and the Create Group dialog box appears. The filter list of users is displayed in the security filter list.

7. Click OK to save the new group.

The new group's name and folder icon appear in the list in the Network Workshop's context area.



NOTE: If you set security to Deny access but have not listed at least one user in the Security Filter list, an error message appears.

Removing Devices

Only an admin user who has access to all of the group's parent groups will be able to delete the group or device. An admin user who does not have such access will be offered the option to unmap the group or device. Unmapping removes a device from a group, but does not delete it from the NMC-RX database.

To delete a device:

1. In the Network Workshop, select the device you want to delete.
2. Right-click, and click Delete.

The Confirm Delete dialog box appears.

3. Click OK.

If you do not have the necessary access, the Delete Not Allowed dialog box appears. Because you cannot delete the device, this dialog box offers you the option of removing the device from its group.

4. Click OK.

The device is removed from the group and no longer appears as a member of the group, but it is not deleted from the NMC-RX database.

Summary

This section summarizes NMC-RX security relative to users, groups, devices, and the NMC-RX application itself.

Admin Users

Admin users can:

- Create user profiles, groups, and devices.

- Modify user and group security.

- Set the default user login authentication setting.

- Change a user's privilege level.

- Delete a group or device only if they have access to all of the group's or device's parent groups.

- Insert and remove group members.

- Change their own password.



NOTE: The *Golden admin* (the admin provided with the NMC-RX application) user has access to everything even though this user is not specifically listed in the access list.

Read/Write Users

Read/write users can:

- Configure a device.

- Change their own password.



NOTE: Only the groups that a user has access to are visible to that user throughout the NMC-RX application.

Read-Only Users

Read-only users can:

- View objects at the system level.

- Configure their own password.

Groups

A group's security depends on the navigational path to the particular group from the top-level group. When you navigate through a hierarchy of groups:

- If the child group security setting is None, then, because the user has access to the parent, the child group is also accessible to the user.

- If the child group security setting is Permit, the child group is displayed if the user is in the child group's filter list, because this is a list of users permitted access.

- If the child group security setting is Deny, the child group is displayed if the user is not in the child group's filter list, because this is a list of users denied access.

Devices

You can view a list of devices by clicking the All Elements tab in the Network Workshop. Those elements that the particular user is allowed to see appear in the list.

NMC-RX Application

The NMC-RX application does not support direct security for a device; it secures a device via the security of the group to which the device belongs.

All users with admin privileges can configure a group to which they have access. If another user with admin privileges has access to a group that you created, that user can configure that group, changing its name, its members, and its security settings.