

# NMC-RX Security

# 8

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

Topic	Page
Overview	8-1
Creating User Profiles	8-2
Configuring Remote Login	8-4
Creating Group Security	8-8
Removing Devices	8-12
Summary	8-12

## 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:

- 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 the following:

- *Chapter 6, Using Groups and Devices*
- *Using the Network Workshop in Chapter 3, Understanding the User Interface*
- *Chapter 12, Using Device Utilities*

## Creating User Profiles

---

Only an administrator can create a user profile. In addition to setting a username and password for each user, the NMC-RX application allows an administrator to assign a privilege level to each user.

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.

The screenshot shows the 'Create User Profile' dialog box. It features a title bar with a globe icon and the text 'Create User Profile'. The dialog is organized into several sections: 'User Name:', 'User Password:', and 'Re-enter Password:' each with a corresponding text input field. Below these is the 'User Preferences:' section, which includes a checkbox for 'Single Click Object View'. To the right of this is the 'User Privilege:' section, containing three radio button options: 'Read Only' (which is selected), 'Read/Write', and 'Admin'. Below the 'User Preferences' section is the 'SNMP Community Strings:' section, which contains three text input fields: 'Read Only:' with the value 'public', 'Read Write:' with the value 'private', and 'Admin:' with the value 'admin'. At the bottom of the dialog is the 'Remote Login:' section, which includes a dropdown menu for 'SSH User Name Source' set to 'NMC-RX User Name' and an empty text input field. 'OK' and 'Cancel' buttons are located at the bottom right of the dialog.

- 2 Set the parameters. See Table 8-1.

**Table 8-1** User profile parameters

Parameter	Description
User Name	Name can be 1–32 characters. Name must contain at least one alphabetic and one numeric character.
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.
User Preferences	
Single Click Object View	Select to enable. When enabled, a single click displays an object's current configuration in view mode. The default setting is disabled (cleared).
SNMP Community Strings:	<p>Values are set to the SNMPv2c industry standard defaults.</p> <ul style="list-style-type: none"> <li>• Read Only – public</li> <li>• Read/Write – private</li> <li>• Admin – admin</li> </ul> <p><b>Note:</b> For additional information on SNMP, see Chapter 3, <i>Configuring SNMP, ERX System Basics Configuration Guide</i>.</p>
User Privilege	Set the level by clicking the appropriate user privilege button. Your selection determines what actions a user can take in regard to a particular object.
Read Only	<ul style="list-style-type: none"> <li>• Can only view objects</li> <li>• Can configure own password</li> <li>• Default privilege level</li> </ul>
Read/Write	<ul style="list-style-type: none"> <li>• Can view, create, configure, and delete objects</li> <li>• Can take all context-specific actions (such as update, map, and statistics)</li> <li>• Cannot create, configure, or delete groups, devices, or users</li> </ul>
Admin	Can take all actions on all objects that the user has access to
Remote Login	To configure, see next section, <i>Configuring Remote Login</i> .

3 To save the settings, click OK.



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

## Configuring Remote Login

---

From the NMC-RX application, you can log into ERX systems 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 into ERX systems remotely.

Since there are a variety of SSH products and implementations, NMC-RX 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 ERX system. For information, see *Chapter 6, Passwords and Security, ERX System Basics Configuration Guide*.
- Determine your Telnet policy before you configure SSH on your ERX system. 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 ERX system. Refer to your RADIUS server documentation for information on choosing a host machine and installing the server hardware.
- You must configure the RADIUS client on your ERX system. To configure RADIUS through NMC-RX, see *Chapter 3, Configuring Virtual Routers*. For additional information about RADIUS, see the *ERX 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.

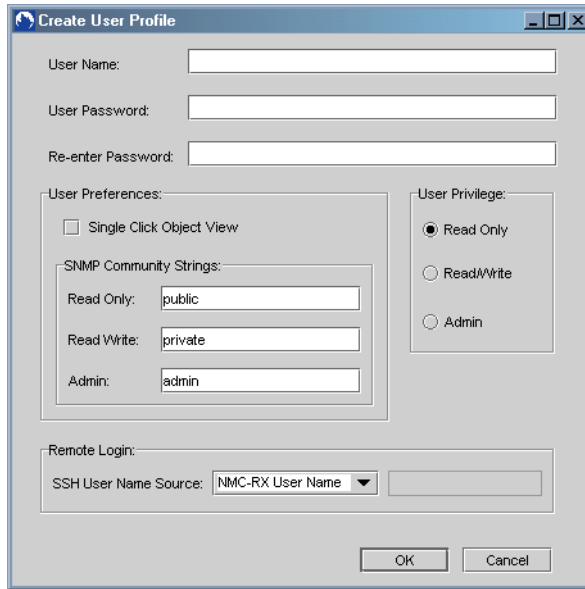
**Set SSH User Name Source**

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

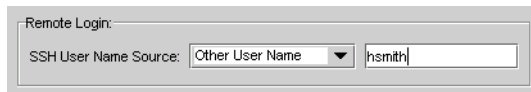
To set an SSH username source:

- 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 8-1.
- 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.

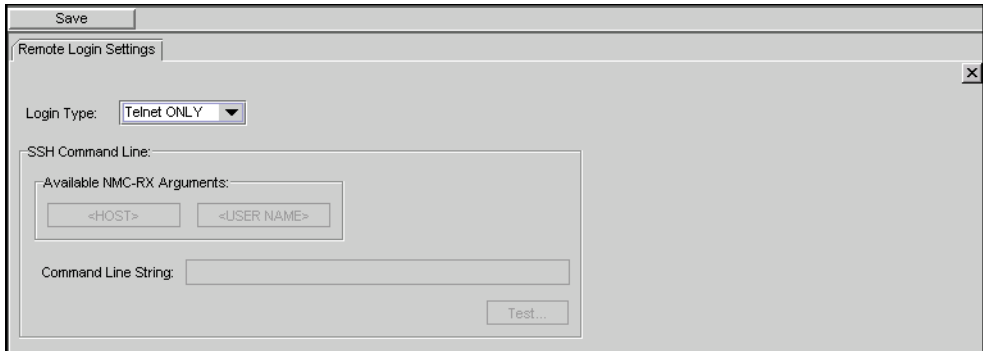
**Configure Remote Login Settings**

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.

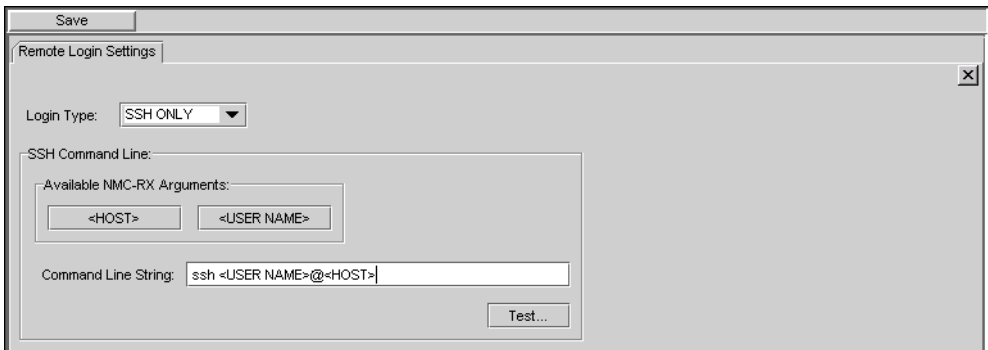
To configure the remote login settings:

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

The Remote Login Settings tab appears.



- 2 Set the parameters as shown in Table 8-2. For example:



**Table 8-2** Remote login settings parameters

Parameters	Description
Login Type	Determines the type of login specified through NMC-RX: <ul style="list-style-type: none"> <li>• Telnet ONLY – default. When selected, SSH is disabled.</li> <li>• SSH ONLY – when selected, the SSH Command Line parameters are enabled and must be specified.</li> </ul>

**Table 8-2** Remote login settings parameters

Parameters	Description
SSH Command Line	Specify the parameters in this section for SSH authentication.
Available NMC-RX Arguments	<ul style="list-style-type: none"> <li>• &lt;Host&gt; – specifies the IP address of the device to which you are connecting. When clicked, the &lt;HOST&gt; token is added to the Command Line String (see below).</li> <li>• &lt;USER NAME&gt; – 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 &lt;USER NAME&gt; token is added to the Command Line String (see below).</li> </ul>
Command Line String	<p>The command line string 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 &lt;USER NAME&gt;@&lt;HOST&gt;</pre> <ul style="list-style-type: none"> <li>• ssh2 – SSH executable</li> <li>• &lt;USER NAME&gt; – parameter syntax for username</li> <li>• &lt;HOST&gt; – parameter syntax for IP address</li> </ul>
Test	When clicked, the Remote Login action is started with the command line string that you specified.

3 Click Save.

**Test 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>
```

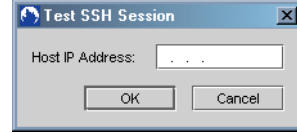
could translate to:

```
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.



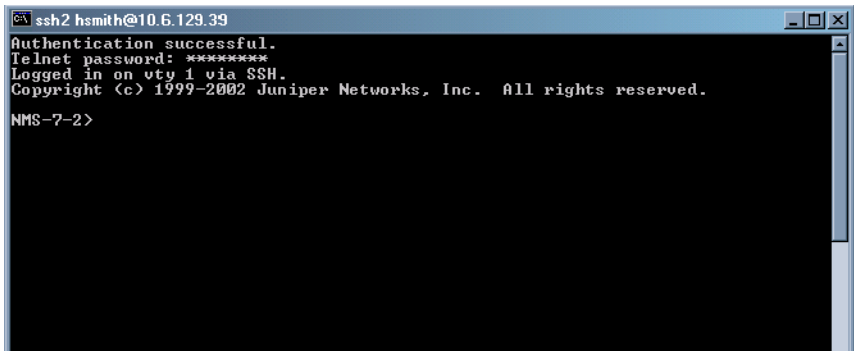
- 2 (Optional) Specify a username.



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

- 3 Enter the host IP address.
- 4 Click OK.

The SSH application remotely logs in to the ERX system's command line interface (CLI).



**Note:** Once you have configured SSH, you can log in remotely to the ERX system 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 ERX system's CLI appears. For more information, see 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.

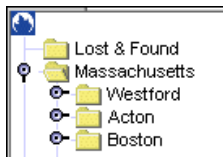
The NMC-RX application does not support security at the device level. To establish security for a particular device, the admin user can create the device as a member of a group and apply a security setting and, if needed, a security filter to the group.



**Note:** Group security cannot be enforced at the CLI, because the ERX device itself does not have a group concept.

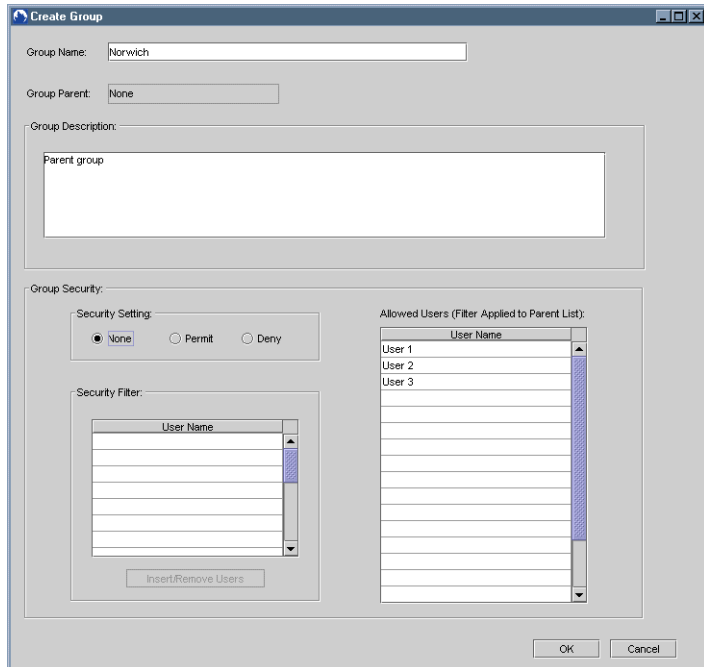
To create a group:

- 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 8-3.

**Table 8-3** Group parameters

Parameter	Description
Group Name	Identifies the group. Name may not exceed 32 alphanumeric characters and may include spaces.
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 8-4.

**Table 8-4** 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.

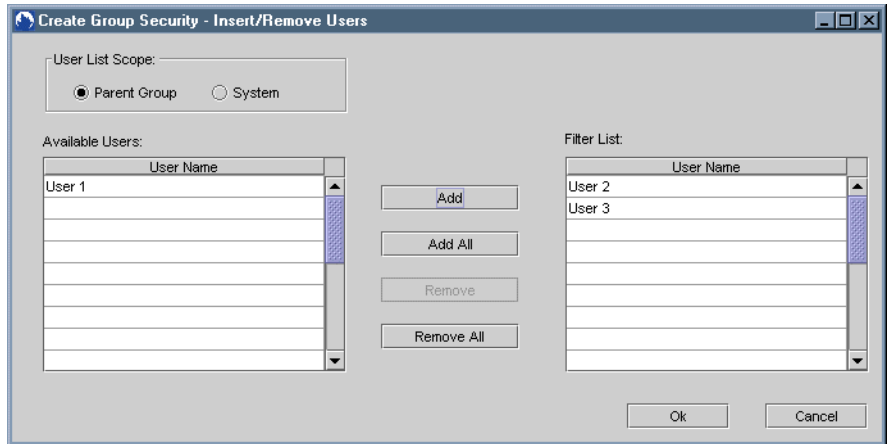
If the group is a top-level group and you select None, the Allowed Users list contains all the users configured for the NMC-RX application. If the group is the child of a parent group and you select None, the Allowed Users list will contain all of the users that have access to the parent group.

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. Since 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.
- 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, since 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, since 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, since 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.

### *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, since 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, since 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, since 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.