

Chapter 9

Configuring Security Settings

This chapter describes how to create and manage security for your element management system.

This chapter contains the following sections:

- Overview on page 127
- Configuring User Authentication Settings on page 128
- Creating User Profiles with SNMPv2c of the NMC-RX Application on page 130
- Creating User Profiles with SNMPv3 of the NMC-RX Application on page 133
- Configuring Remote Login on page 137
- Creating Group Security on page 141
- Removing Devices on page 144
- Security Summary on page 145

Overview

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

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

- Determining how users are authenticated, either locally or through a RADIUS server
- Assigning passwords and privilege levels to users
- Choosing a remote login method (Telnet or SSH) for users
- Creating access lists for groups



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

References

For additional information, see *Chapter 7, Organizing Your Network with Groups and Devices*.

Configuring User Authentication Settings

Only users with security privileges can configure user authentication settings. You can set either RADIUS authentication or local database authentication as the default mode of user login authentication.

For RADIUS authentication, you specify a list of RADIUS servers to authenticate user logins and set the order in which they are queried. You configure RADIUS authentication on a per user basis when you create user profiles (see *Setting SSH Username Source* on page 138 for more information).

To configure user authentication settings:

1. From the Configuration menu in either the Network Workshop or the Device Workshop, select NMC-RX Application Settings, then click NMC-RX User Authentication.

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

Default User Authentication Mode: Local

Authentication Servers:

Server Name	IP Address	UDP Port

Server Properties:

Server Name:

IP Address: UDP Port: Retry Count:

Timeout(sec): Secret:

- Set the user authentication parameters (Table 30).

Table 30: User Authentication Parameters

Parameter	Description
Default User Authentication Mode	Method by which user logins are authenticated: either locally or with a RADIUS server by default.
RADIUS Authentication Servers	<p>List of RADIUS authentication servers that are 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 <i>Related Dialog Box</i> on page 130).</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; cannot edit
IP Address	IP address of the selected RADIUS server; cannot edit
UDP Port	UDP port of the selected RADIUS server; cannot edit
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	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

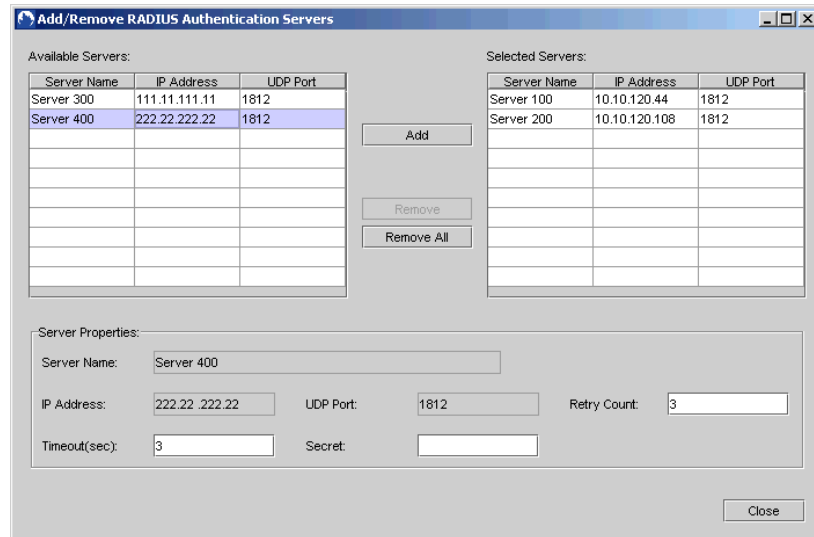
- Click the Save button.

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 you created or discovered that are not selected. You can select up to ten servers in the Selected Servers list (right) 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 you add a server, you can change the parameters for the selected server in the Server Properties group box (see Table 30 on page 129 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 with SNMPv2c of the NMC-RX Application

User profiles are created differently depending on which version of SNMP was chosen during the installation of the NMC-RX application. If you are using SNMPv2c of the NMC-RX application, use this section. If you are using SNMPv3 of the software, see *Creating User Profiles with SNMPv3 of the NMC-RX Application*.

Only a security user can create a user profile. When you create a user profile, you can:

- Set the username and password.
- Select how the user login is authenticated (either locally or through a RADIUS authentication server; see *Configuring User Authentication Settings* on page 128).
- Assign a privilege level to the user.
- Configure SNMPv2c

User Privilege

Only users with the Security privilege enabled can modify the User Privilege settings. All user, however, can modify their own password.

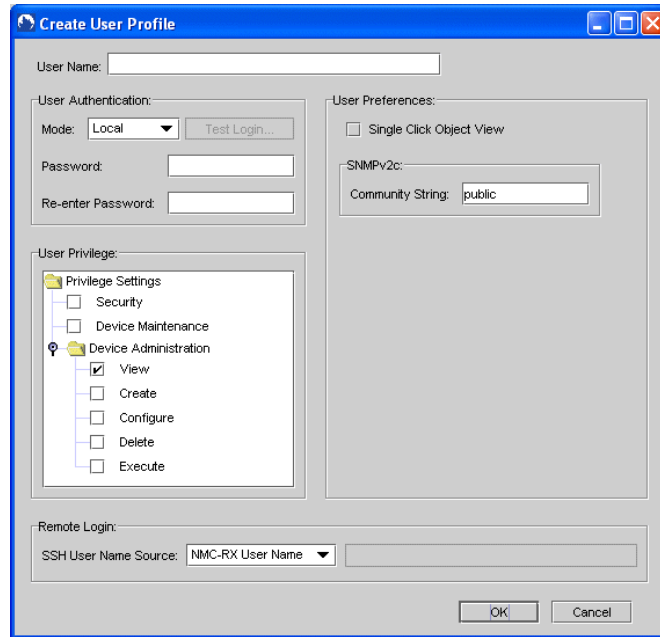
User privileges are divided into three categories:

- Security—Allows access to administer application-specific settings, such as inserting or removing members of groups, creating groups and new user profiles, and setting user authentication settings.
- Device Maintenance—Allows access to all device-specific settings or features.
- Device Administration—Allows access to device-specific settings and features. You can specify five areas for the device administration category: view, create, configure, delete, and execute.

To create a user profile:

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

The Create User Profile dialog box appears.



2. Set the user profile parameters (Table 31).

Table 31: User Profile Parameters (with SNMPv2c)

Parameter	Description
User Name	Name that identifies the user; range 1–32 characters; must contain at least one alphabetic and one numeric character
User Authentication	
Mode	(See <i>Configuring User Authentication Settings</i> earlier in this chapter for more information.) Determines the type of login: <ul style="list-style-type: none"> ■ Local—Authenticates the user login locally ■ RADIUS—Authenticates the user login through a RADIUS server
Test Login	When enabled (checked) and user authentication mode is set to RADIUS, the remote login action is tested.
Password	Password, which must be between 6 and 16 characters and contain at least one alphabetic and one numeric character. The password that the administrator assigns is the default password, and a user can change it.
Re-enter Password	Password that you typed in the User Password field
User Privilege	
Privilege Settings	Level that determines what actions a user can take in regard to a particular object. <ul style="list-style-type: none"> ■ 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. ■ Device Maintenance—Allows access to all device-specific settings or features

Table 31: User Profile Parameters (with SNMPv2c) (continued)

Parameter	Description
Device Administration	<p>Level that determines what actions a user can take in regard to a particular object.</p> <ul style="list-style-type: none"> ■ View—Allows a user to view the configuration of a device. ■ Create—Allows a user to create configurations on a device. ■ Configure—Allows a user to configure a device. ■ Delete—Allows a user to delete the configurations of a device. ■ Execute—Allows a user to execute certain device actions. For example, the user is allowed to run ping on a device or log in remotely to a device.
Remote Login	
SSH User Name Source	<ul style="list-style-type: none"> ■ 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 is active and you can edit the text. <p>Type the user name in the text box. The username can be from 1 to 128 characters.</p>
User Preferences	
Single Click Object View	Indicator that specifies whether or not you can view the current configuration of an object with a single click. When checked, single-click view mode is enabled; default: disabled (cleared)
SNMPv2c	
Community String:	<p>Used to authenticate messages sent to the device. Default: public</p> <p>NOTE: For additional information about SNMP, see <i>JUNOS System Basics Configuration Guide, Chapter 4, Configuring SNMP</i>.</p>



NOTE: You cannot delete the Admin user profile (admin), but you can modify the default password (nmc-rxadmin).

3. To save the settings, click OK.

Creating User Profiles with SNMPv3 of the NMC-RX Application

User profiles are created differently depending on which version of SNMP was chosen during the installation of the NMC-RX application. If you are using SNMPv3 of the NMC-RX application, use this section. If you are using SNMPv2c of the software, see *Creating User Profiles with SNMPv2c of the NMC-RX Application* on page 130.

Only users with the Security privilege can create a user profile. When you create a user profile, you 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 user privilege level
- Configure SNMPv3 settings

User Privilege

Only users with the Security privilege enabled can modify the User Privilege settings. Privilege settings are enabled for an admin user and 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.
- Device Maintenance—Allows access to all device-specific settings or features; default.
- Device Administration—Allows access to device-specific settings and features. You can specify five areas for the device administration category: view, create, configure, delete, and execute.

SNMPv3

A router can provide authentication and privacy for users via SNMPv3. Each user is associated with a group. A group is a set of users with the same access privileges to the router (see Table 32). For each NMC-RX user, you can configure only one SNMP user.

Three predefined groups are available:

- Public—No authentication and no privacy. Users are not configured for authentication or privacy.
- Private—Authentication only. Users need to be authenticated by the SNMP agent, but the data is not encrypted.
- Admin—Authentication and privacy. Users are configured for authentication and privacy.



NOTE: Before the NMC-RX application can begin to communicate with the router, SNMPv3 parameters must be set on the router by using the CLI. Use the NMC-RX application's remote login feature to access the CLI.

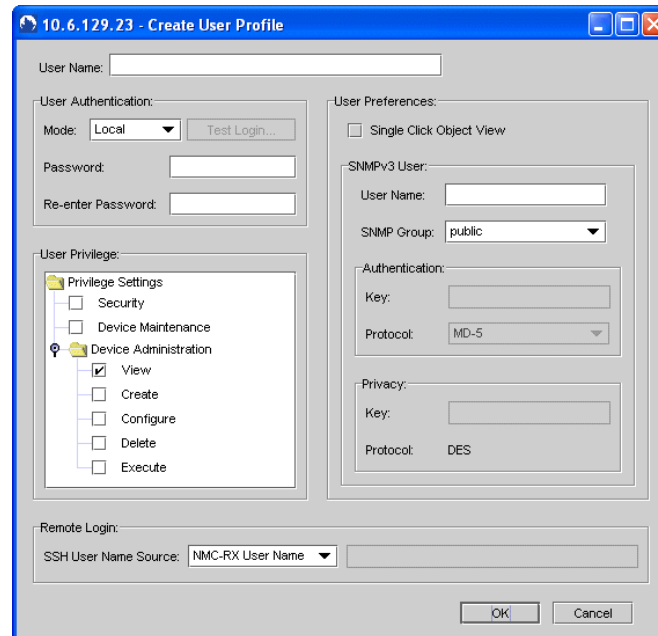
Because each virtual router has its own security model, SNMP users must be added to each virtual router on the E-series router. Only then can the virtual router be managed via SNMPv3. For example, when a virtual router is created through the NMC-RX application, it can be configured only after the SNMP users have been added to the virtual router via the CLI.

For more information about SNMP, see *JUNOS System Basics Configuration Guide, Chapter 4, Configuring SNMP*. For more information about virtual routers, see *NMC-RX User Guide, Vol. 2, Chapter 3, Configuring Virtual Routers*.

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 32.

Table 32: User Profile Parameters (with SNMPv3)

Parameter	Description
User Name	Range 1–32 characters; must contain at least one alphabetic and one numeric character
User Authentication	
Mode	(See <i>Configuring User Authentication Settings</i> earlier in this chapter for more information.) Determines the type of login: <ul style="list-style-type: none"> ■ Local—Authenticates the user login locally ■ RADIUS—Authenticates the user login through a RADIUS server
Test Login	When enabled (checked) and user authentication mode is set to RADIUS, the remote login action is tested.
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 can be changed by the user.
Re-enter Password	Password must be typed again exactly as typed in the User Password field.

Table 32: User Profile Parameters (with SNMPv3) (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> <ul style="list-style-type: none"> ■ 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. ■ Device Maintenance—Allows access to all device-specific settings or features; default.
Device Administration	<p>Sets the level to determine what actions a user can take in regard to a particular object.</p> <ul style="list-style-type: none"> ■ View—Allows a user to view a device’s configuration. ■ Create—Allows a user to create configurations on a device. ■ Configure—Allows a user to configure a device’s configuration. ■ Delete—Allows a user to delete device configurations. ■ 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.
Remote Login	
SSH User Name Source	<ul style="list-style-type: none"> ■ 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 is active and you can edit the text. Type the user name in the text box. The username can be from 1 to 128 characters.
User Preferences	
Single Click Object View	Displays an object’s current configuration in view mode with a single click; default: disabled (cleared)
SNMPv3 User	
User Name	Name of the SNMP user; range 1-32 characters
SNMP Group	<p>The group of the SNMP user. Depending on the choice selected (Public, Private, Admin), different authentication and privacy parameters are available.</p> <p>NOTE: All SNMPv3 user attributes must match the attributes set up via the CLI on the router.</p>
Authentication	
Key	Secret authentication key used for messages sent on behalf of the user; range: 16 characters for MD-5 protocol, 20 characters for SHA protocol; default is empty
Protocol	Protocol used to authenticate the user; MD-5 or SHA
Privacy	
Key	Secret encryption key used for messages sent on behalf of the user; range: 16 characters
Protocol	Encryption protocol; DES



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

3. To save the settings, click OK.

Configuring Remote Login

From the NMC-RX application, you can log in to routers remotely through Telnet or SSH. The selection of either Telnet or SSH is an NMC-RX application-wide setting and is accessible only to users with security privileges. Although the NMC-RX application automatically defaults to Telnet, SSH is considered a more secure alternative to Telnet for logging in to 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 router. For more information, see *JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security*.
- Determine your Telnet policy before you configure SSH on your router. Effective use of SSH implies that you 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 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 the NMC-RX application, 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 the three tasks that are 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, users with security privileges must set this field to assign every user a username source for remote logins.

To set an SSH username source:

1. From the Configuration menu in either the Network Workshop or the Device Workshop, select Create, and click User Profiles.

The Create User Profile dialog box appears.

2. Set the parameters. See Table 31 (SNMPv2c) or Table 32 (SNMPv3).



When modifying the user that is set as the Config Sync Services user or the Polling Service user, all Config Sync Services or the Polling Service are updated with the SNMP settings for the configured user. You cannot remove a user who is set as a Config Sync Services user or a Polling Service user.

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

Configuring Remote Login Settings

Only a user with security privileges can configure remote login settings. Otherwise, this menu item is disabled.

To configure the remote login settings:

1. From the Configuration menu in either the Network Workshop or the Device Workshop, select NMC-RX Application Settings, then click Remote Login.

The Remote Login tab appears.

2. Set the parameters as shown in Table 33. For example:

The screenshot shows a configuration window for NMC-RX User Authentication. At the top, there are tabs for 'Config Sync Services', 'Polling Service', 'Remote Login', 'NMC-RX User Authentication', 'User Inactivity Timer', and 'Software Download'. The 'Login Type' is set to 'SSH ONLY'. Below this, the 'SSH Command Line' section is expanded, showing 'Available NMC-RX Arguments' with two buttons: '<HOST>' and '<USER NAME>'. The 'Command Line String' field contains the text 'ssh <USER NAME>@<HOST>'. A 'Test...' button is located at the bottom right of the section.

Table 33: Remote Login Parameters

Parameters	Description
Login Type	<p>Determines the type of login specified through the NMC-RX application:</p> <ul style="list-style-type: none"> ■ 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.
Available NMC-RX Arguments	<ul style="list-style-type: none"> ■ < 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). ■ < USER NAME > —Specifies the username, which is the SSH username set in the NMC-RX user profile. You can use either the NMC-RX username or another username specified by the administrator. When clicked, the < USER NAME > token is added to the command-line string (see below).
Command Line String	<p>Specifies what is executed when the remote login action starts. The string contains arguments that are necessary for SSH authentication. Syntax example:</p> <pre>ssh2 <USER NAME>@<HOST></pre> <ul style="list-style-type: none"> ■ ssh2—SSH executable ■ < USER NAME > —Parameter syntax for username ■ < HOST > —Parameter syntax for IP address
Test	When clicked, the remote login action is started with the command-line string that you specified.

3. Click Save.

Testing Remote Login Action

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

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

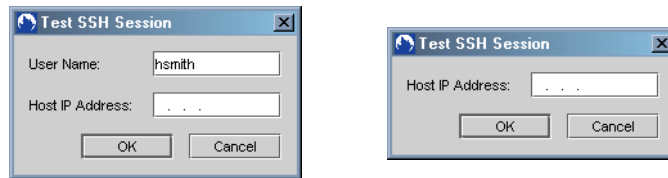
translates to:

```
ssh2 hsmith@10.5.129.39
```

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

1. Click Test.

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



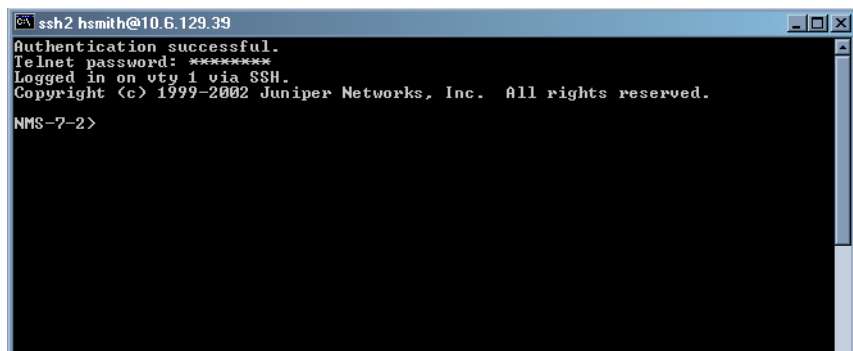
2. (Optional) Specify a username.



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 command-line interface (CLI) of the router.



Logging In

After you configure SSH, you can remotely log in to the E-series router through the Tools menu. To log in:

1. Select Device Utilities and Remote Login.

The SSH Sessions dialog box appears.

2. Enter the host IP address, and click OK.

The CLI of the E-series router appears. For more information, see *NMC-RX User Guide, Vol. 2, Chapter 13, Using Device Utilities*.

Creating Group Security

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

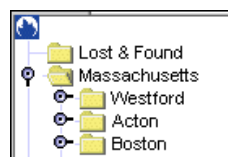
The NMC-RX application does not support security at the device level. To establish security for a particular device, the user with device administration privileges can create the device as a member of a group and apply a security setting and, if needed, a security filter to the group.



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

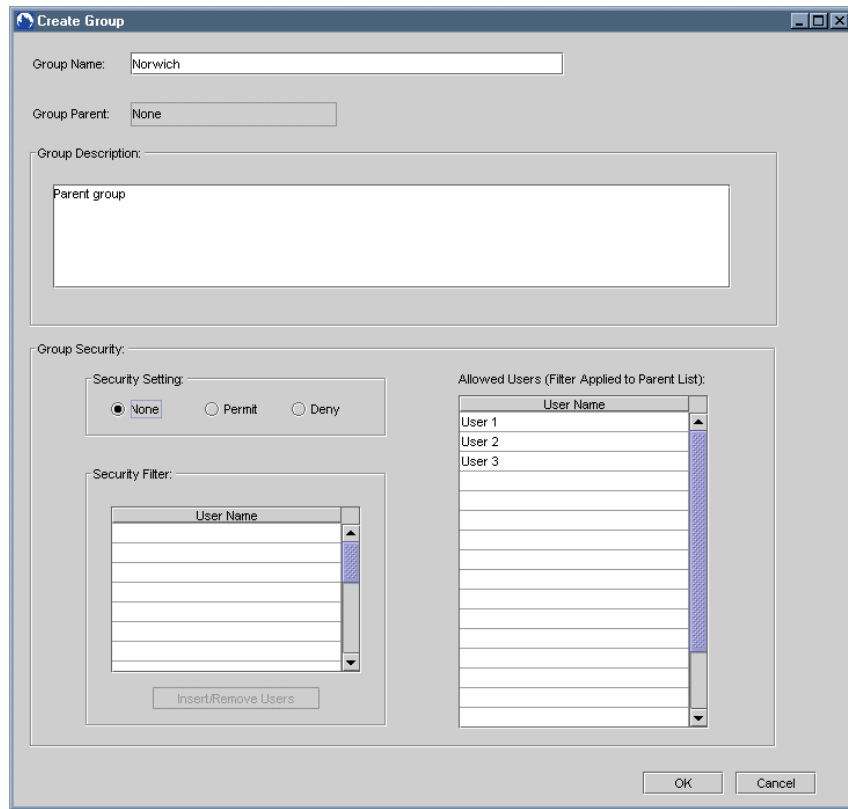
To create a group:

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 (Table 34).

Table 34: Create Group Parameters

Parameter	Description
Group Name	Name of the group; cannot exceed 32 alphanumeric characters and may include spaces.
Group Parent	Name of the parent for the new group. If the new group does not have a parent, the Group Parent text box reads None, which means the group is at the top level.
Group Description	Descriptive or contextual information up to 255 alphanumeric characters. The resulting description appears whenever you access its associated group. You can easily change or delete a description at any time.

4. Select a Security Setting option (Table 35).

Table 35: 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 privilege level of the group. The group is visible to any user who is in the access list of the parent group to which this group belongs or is available systemwide.

Table 35: Security Settings (continued)

Setting	Description
Permit	Also known as private access. This group is visible to users who are in the filter list of the group, provided that the users are also in the access list of the parent group to which this group belongs.
Deny	This group is visible to anyone in the access list of the parent group to which this group belongs, except those users to whom the group's own filter denies access.



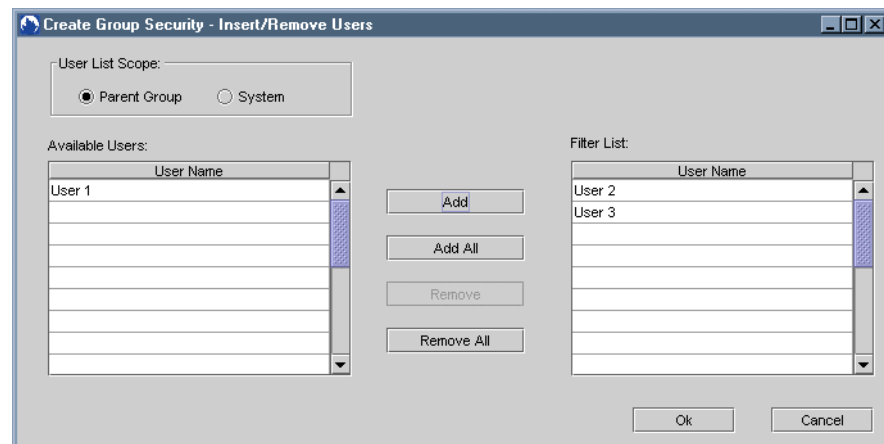
NOTE: The access list for a group is derived by filtering the access lists from the top level of the navigational tree down to the given group.

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 contains 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, which lets you 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 the users 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 name and folder icon appear in the list in the context area of the Network Workshop.



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

Removing Devices

Only a user with device administration privileges who has access to all the parent groups for this group is able to delete the group or device. A user who does not have such access is 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 that you want to delete.
2. Right-click, and select 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.

Security Summary

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

Groups

Group 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, the child group is also accessible to the user because the user has access to the parent.
- If the child group security setting is Permit, the child group is displayed if the user is in the filter list for the child group because this is a list of users who are permitted access.
- If the child group security setting is Deny, the child group is displayed if the user is not in the filter list for the child group because this is a list of users who are denied access.

Devices

To view a list of devices, click the All Elements tab in the Network Workshop. The elements that this 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. The NMC-RX application secures a device through the security of the group to which the device belongs.

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

