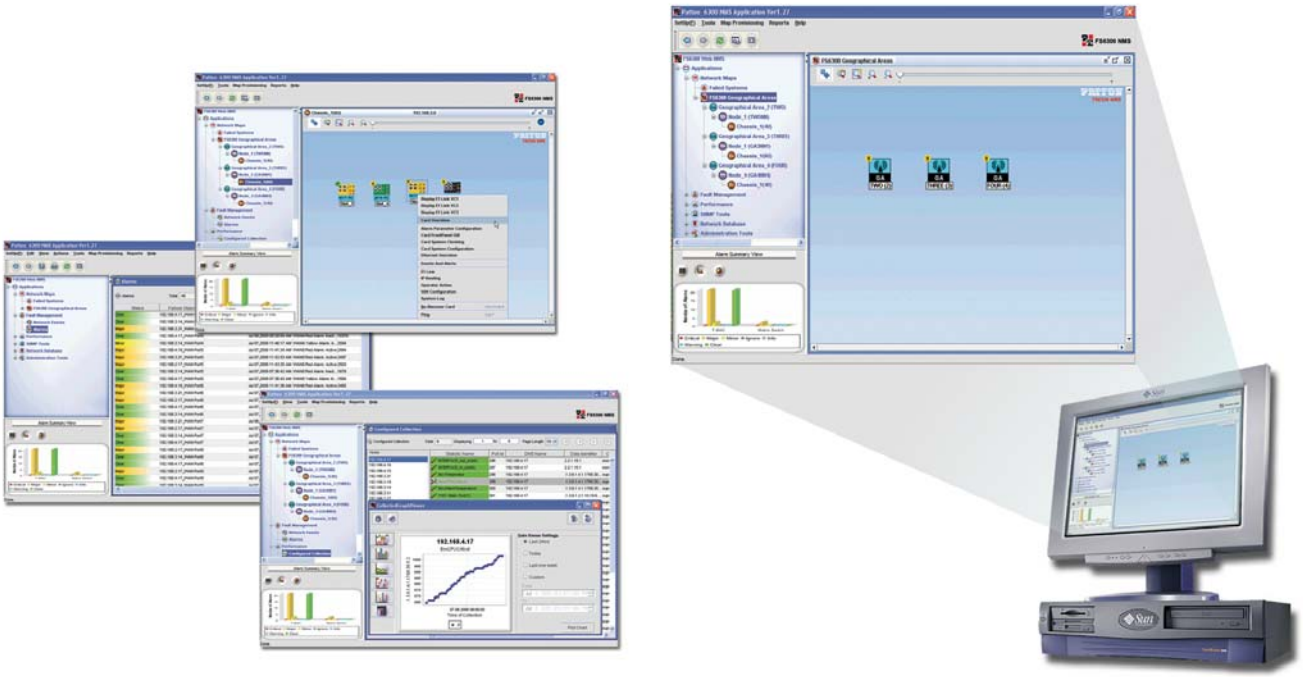
PATTON
let's Connect!™

ForeSight 6300
Network Management System

Administrator's Reference Guide



Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Part Number: **07MFS6300-ARG, Rev. B**
Revised: **February 29, 2012**

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
tel: +1 (301) 975-1000
fax: +1 (301) 869-9293
support: +1 (301) 975-1007
web: www.patton.com
e-mail: support@patton.com

Summary Table of Contents

Table of Contents

List of Figures

List of Tables

About this guide

This *FS6300 NMS Administrator's Reference Guide* provides detailed information for performing advanced operations in the FS6300 system. Instructions in this guide assume that configuration processes have already taken place. For information on installing and configuring devices in the FS6300 NMS, refer to the *FS6300 NMS User Manual*.

Audience

This guide is intended for the following users:

- System administrators
- Operators

Structure

This guide contains the following chapters and appendices:

Chapter 1 Managing System Operations

Chapter contents

Overview

This chapter introduces you to the features and benefits of the FS6300 NMS. It also includes basic information about logging in and out of the system, and working with the main toolbars and menus.

FS6300 NMS Features

- Integrated FCAPS
- Scalable NMS
- Configuration Management
- Alarm Management
- Security Management
- Administration Management
- Performance Management

Common User Tasks

The following are user tasks you will encounter when working with the FS6300 NMS:

- Discover the network (See "Discovering Your Network" on page 45)
- Configure alarms and clocking (Refer to the *FS6300 NMS User Manual*)
- Configure and manage individual devices in the network (Refer to the *FS6300 NMS User Manual*)
- Manage network events (See "Managing Alarms and Network Events" on page 94)
- Monitor performance data (See "Monitoring Performance Data" on page 105)

Bringing up the NMS Server from Linux

To start the server, from the */opt/FS6300/Server/<release #>* directory, double-click on the **WebNM-SLauncher.sh** file to open the launcher. To start and stop the server, in the splash screen window, right-click on the **Start 6300 NMS Server** icon and select **Run**. To initialize the database, right-click on the **Reintialize 6300 NMS** icon and select **Run**, then acknowledge the confirmation request in the pop-up window.

Bringing up the NMS Client from Windows XP

The NMS Windows Remote Application Client (WRAC) is the primary client for the FS6300 NMS. It is recommended that you use the WRAC. You can launch the WRAC by double-clicking on the **WebNM-SLauncher.bat** icon on the desktop. In the resulting splash screen window, right-click on the client icon and select **Run**. Then, enter the authentication information in the FS6300 NMS Authentication dialog box.

Logging into the Client

The FS6300 NMS Authentication box is displayed to provide an authenticated access to the FS6300 NMS. Enter a valid user name and password to access the Application Client.

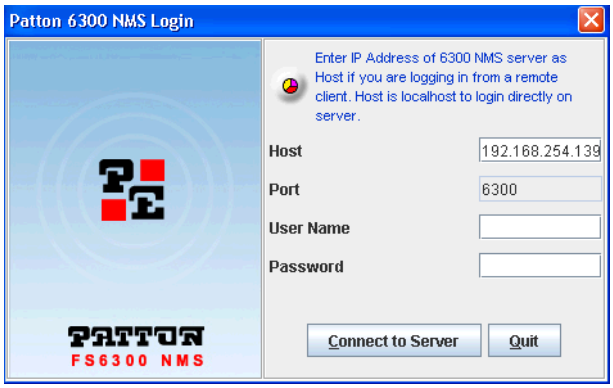


Figure 1. Logging in to the application client

1. In the **Host** field, enter **localhost** for the server address if you are logging in directly to the server. If you are logging in from the WRAC, enter the **IP address** of the NMS server.
2. Enter the **User ID** assigned to you in the User ID field. If you do not have a User ID, contact your system administrator. For unconfigured systems, the default User ID is **superuser.**
3. Enter the password assigned to you in the **Password** field. To learn how to configure your password, see "Configuring Your Password" on page 17. For unconfigured systems, the default password is **superuser**.
4. Click **Connect to Server**.

The splash screen with a progress bar displys until the Application Client has completely loaded.

Configuring Your Password

Configuring your password before connecting to the client

When you log on to the Application Client for the first time, a Password Confirmation dialog box is displayed(only if this has been enabled by the administrator - see "Enabling users to change password at first login" on page 20). If you do not see this dialog box, then ignore this section and perform the steps explained in the next section, "Configuring your password from the client" on page 17 .

To configure your password before connecting to the client:

1. In the Password Confirmation dialog box, click **Reuse** to continue using the same password for the same period as previously configured. To enter a new password, click **Configure** and perform further steps.
2. Enter the new password in the **Type new password** field.
3. Re-enter the same password in the **Confirm new password** field.
4. Enter the number of days you want your password to be valid in **Password expiry duration.** If no value or zero is entered in this field, then the password never expires.
5. Click **Connect**.

The new password is assigned to you and you are connected to the Application Client. You need to use this new password from the subsequent login.

Configuring your password from the client

1. After logging into the client, select **Security Administration** from the Tools menu. Select the user from the users list, and click **Edit** in the Menu bar. Select **Change Password**. The Password Configurator window is displayed.
2. Enter the new password in the **New Password** field.
3. Re-enter the same password in the **Confirm Password** field.
4. Click **OK**. The new password is assigned to the user.

Troubleshooting

Table 1 lists the messages that are displayed in certain situations during the login process.

Table 1. Troubleshooting messages

Message	Why am I getting this?	What do I do?
You are logged in for the first time; would you like to reuse the existing password or configure a new password? (See "Configuring your password before connecting to the client" on page 17).	This pop-up message is displayed when you log on to the Application Client for the first time (only if this has been enabled by the administrator - see "Enabling users to change password at first login" on page 20).	Refer to "Configuring your password before connecting to the client" on page 17 for the procedure.
Your password has expired. Would you like to reuse the old password or configure a New password?	Your password has expired.	• You can either set a new password or retain the old password. • Click Reuse to keep the same password and for the same expiration period configured before. • Click Configure to enter a new password. Refer to "Configuring your password before connecting to the client" on page 17 for the procedure. • If you do not have the permission to set your password, contact the system administrator. (Admins - see "Modifying User Permissions" on page 34)
This User account has Expired. Please contact the Administrator for further details	Your user account has expired. The user account is created by the system administrator. (Admins - see "Adding Users" on page 31)	Contact the system administrator to renew your user account. (Admins - see "Adding Users" on page 31)
This User account is Disabled. Please contact the Administrator for further details	• Your user account has been disabled by the system administrator. (Admins - see "Disabling Users" on page 35) • Also, if your consecutive login attempts fail for a certain number of retries (number is configured by the administrator), the user account is automatically disabled. (Admins - see "Disabling Users" on page 35)	Contact the system administrator to enable your user account. (Admins - see "Disabling Users" on page 35)

Table 1. Troubleshooting messages

Message	Why am I getting this?	What do I do?
Connection lost to the FS6300 NMS server at <host>. Do you want to shut-down the client?	This message is displayed if the connection between the client and server is lost due to network problems or if the server is shut down abruptly.	• Click Yes to shut down the client or No to continue working. • If you decide not to close the client even after the connection is lost, the screens, views, and data of the client remain the same, but you cannot perform any further operations in the client and no updates occur. You need to reopen the client and reconnect to the FS6300 NMS Server.
[Lock Screen dialog box] Please enter your password to unlock the client.	This dialog box is displayed when the Application Client is idle for more than a specific period, that is, when there is no interaction between the user and the Application Client (no mouse or keyboard events). (Admins - see "Enabling the lockout function when the client is idle" on page 20 to configure this feature).	• Enter a valid password in the Password field and click Unlock to resume working on the Application Client. • To disable this prompt every time the Application Client is idle (only for that session), select Don't show this dialog for the current session any more • Only specific number of unsuccessful logins are allowed. When exceeded, the session with Application Client is forcefully terminated and you need to reopen the Application Client.
FS6300 NMS Application Client has been terminated	• This message is displayed when the Application Client is idle for more than a specified period, that is, when there is no interaction between the user and the Application Client. • The Application Client is terminated. (Admins - see "Enabling the terminate function when the client is idle" on page 20 to configure this feature).	Bring up/reopen the client again.

Configuring Administrator Startup and Idle Options

This section describes how a system administrator can enable particular startup and idle options for the client.

Enabling users to change password at first login

By default, this option is disabled. To enable users to change their password when they log in for the first time:

1. Open the **NmsProcessesBE.conf** file located in the <*Web NMS Home*>/*conf* directory.
   <*Web NMS Home*> is the IP address where the NMS server is running.
2. Find the process for **com.adventnet.nms.security.authorization.NmsAuthManager** in the *conf* file.
3. In the command[...`change_password_for_firsttime_login false`...], replace ***false*** with **true**.
4. Save the *conf* file.

Enabling the lockout function when the client is idle

If the client is idle for a certain amount of time, you can enable the client to require a user ID and password to unlock the screen. By default, the lock screen function is disabled. To enable it:

1. Open the **clientparameters.conf** file located in the <*Web NMS Home*>/*conf* directory.
   <*Web NMS Home*> is the IP address where the NMS server is running.
2. Find the command [`ALLOWED_IDLE_TIME_BEFORE_LOCKOUT="0"`] and replace ***0*** with **the number of minutes** the client is allowed to be idle before the system locks user access.
3. In case of Applet and Web Start Clients, you will also need to edit the **java.policy** file present in <*Web NMS Home*>/*jre/lib/security* directory and include the following line for the function to work correctly:

   ```
   permission java.awt.AWTPermission
   "listenToAllAWTEvents";
   ```

4. Save the files.

Enabling the terminate function when the client is idle

If the client is idle for a certain amount of time, you can enable the client to shut down. By default, the terminate function is disabled. To enable it:

1. Open the **clientparameters.conf** file located in the <*Web NMS Home*>/*conf* directory.
   <*Web NMS Home*> is the IP address where the NMS server is running.
2. Find the command [`ALLOWED_IDLE_TIME_BEFORE_TERMINATION="0"`] and replace ***0*** with **the number of minutes** the client is allowed to be idle before the system shuts down.
3. Save the *conf* file.

Using the NMS Menus

The following menu items are always available at the top of the main window of the NMS:

- **SetUp(F):** Add Device | 6300 Container Definition | Back | Forward | Exit
- **Tools:** Schedule Tasks | Discovery Administration | View Exported Card Configuration | Firmware Upgrade | Multiple Card Configuration | Security Administration
- **Map Provisioning:** Create Inter-Chassis Links | Auto-Screen Maps and Channels | Create and Manage DS0 Maps | DS0 Availability by Ports | Chassis Diagnostics | InBand Channel Management
- **Reports:** Alarm Tracking | Chassis Checklist | Discovery Checklist | Device Checklist | NMS Summary
- **Help:** About FS6300 NMS

Additionally, some options in the menu tree have other toolbars at the top related to their function in the network:

- **Fault Management - Network Events - View:** Details | Alarms | Refresh
- **Fault Management - Network Events - Actions:** Save To File | Export Events | Print
- **Fault Management - Alarms - Custom Views:** Add | Remove | Modify
- **Fault Management - Alarms - Edit:** Delete | Pick Up/UnPick | Clear | Search
- **Fault Management - Alarms - View:** Delete | Details | Events | Refresh
- **Fault Management - Alarms - Actions:** Save To File | Export Events
- **Performance - Configured Collection - View:** Plot - Current Statistic | Plot - Collected Statistic | Refresh
- **Network Database - View:** Details | Events | Alarms | Statistics | Refresh
- **Network Database - Object:** *Varies depending on object type*
- **Administration Tools - Policies - Policy:** Add Policy | Search | Refresh
- **Administration Tools - Policies - Edit:** Update Policy | Delete Policy | Execute Policy | Stop Policy

Also, **right-clicking** on a device in the main window will display a menu of options available for that specific device.

Logging out of the Application Client

To log out, perform any of the following procedures:

- From the **SetUp(F)** menu at the top of the screen, choose **Exit**.
- Press **Alt+F4**.

A Confirmation Message dialog box is displayed. Click **Yes** to quit the client.

> **Note** Do not use the **X** button to close the client. Always use the **Exit** option. Using the **X** button may lock the user out of the system.

Backing Up the Database

The FS6300 NMS provides a tool for backing up the database. You may also create a policy to backup the database automatically based on a schedule.

Creating a backup file of the database

1. Click **Tools > Schedule Tasks** in the main window. In the **FS6300-Schedule Tasks** window, select the radio button for **Database Backup**.
2. Click **Execute Now**. A status message will display as the system completes the backup process.

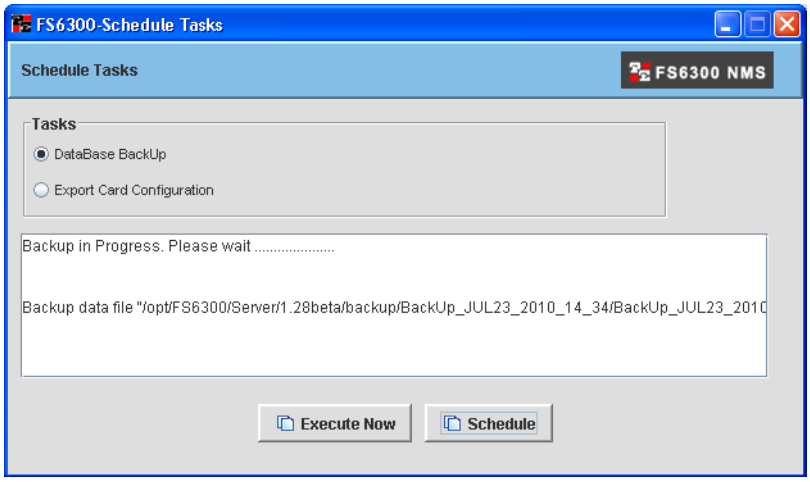


Figure 2. FS6300 Schedule Tasks window

3. The backup is saved to the *opt/FS6300/<version>/backup/* directory.

Scheduling a policy to backup the database

The **6300 NMS Backup** policy automatically backups the system to reduce the load on the server.

1. Click on **Administration Tools > Policies** in the NMS menu tree.
2. Select **Policy > Add Policy** from the menu at the top of the screen. The **Add Policy Details** window displays.

Figure 3. Add Backup Policy

3. Select **6300NMSBackupPolicy** from the drop-down menu. Enter a **Name** for the backup policy and click **Add**. The **Object Details** window displays.

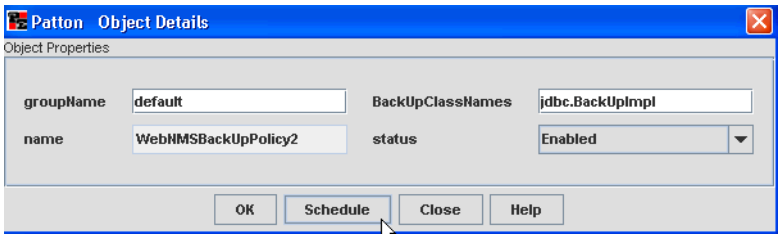


Figure 4. Policy Details

4. Table 2 describes the fields for adding a new **6300NMSBackup** policy.

Table 2. FS6300 NMS Backup Policy Properties

Property	Description
groupname	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. (You can execute different policies at the same time by associating them with a common group name).
name	Displays the name of the backup policy. *This field cannot be edited.*
BackUpClassNames	Specify the class name implementing the backup interface.
Status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when it is Enabled.

5. Click **Schedule** in the **Object Details** window. The **Policy Scheduler** window displays. Select the radio buttons for **Dates** or **Days**, depending on what your policy schedule will be based on. You can select all dates/days and hours, or specific selections. Click on the box of the day, date, or hour to make your selection. Then, click **OK**.

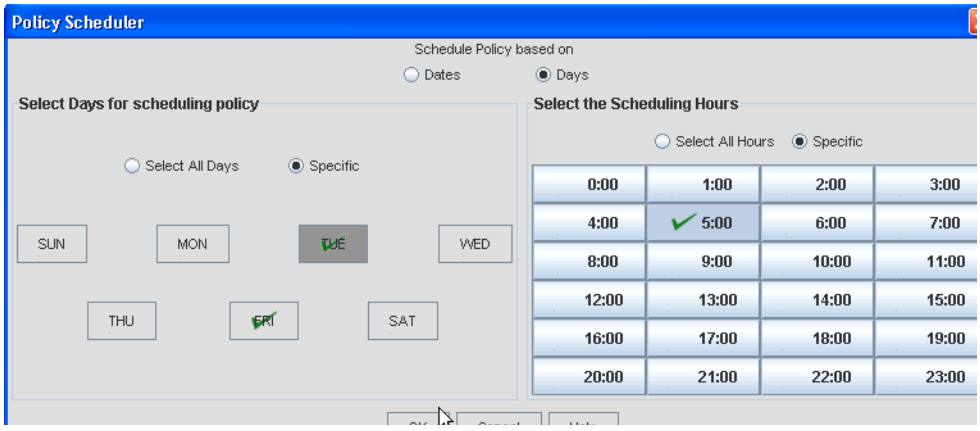


Figure 5. Policy Scheduler

6. Click **OK** in the **Object Details** window to save the policy. A confirmation message displays that the policy was added successfully.

Restoring the Database

The backed up data/configuration information can be restored into the database/configuration files using the **RestoreDB.bat/sh** file available in *.../backup* directory. Execute the **RestoreDB.bat** file with the filename of the backed up contents.

Data backed up in one database can be restored in another. For example, the data backed up in MySQL can be restored in Oracle database. The procedure to achieve this is the same.

For example, if the database backup file name is ***BackUp_JUL2_2002_3_11.data***, then you can restore the contents as shown below:

```
.../backup>RestoreDB BackUp_JUL2_2002_3_11.data
```

(Make sure that the filename is specified in the correct case since it is case-sensitive).

In case you have the file that contains the backed up contents under a directory other than *.../backup*, you need to specify the full path where the file exists.

> **Note** While specifying the full path for restoring the data using the **RestoreDB.bat** file, always use 'forwardslash' (for example like *.../backup/BackUp_JUL2_2002_3_11.data*). If you use, 'backslash', this command might throw a "File not found" error in Windows since in windows "\" (Backslash) is considered as "Esc".

For example, the backup file is present under *.../backup* directory, then you can restore the contents as shown below :

```
.../backup>RestoreDB
.../backup/BackUp_JUL2_2002_3_11.data
```

Managing Device Configurations

Operators may want to reboot a device or save the current configuration to memory, in case problems arise in the system.

Exporting the configuration for specific cards

To export the card configuration:

1. Click **Tools > Schedule Tasks** in the main window. In the **FS6300-Schedule Tasks** window, select the radio button for **Export Card Configuration**. Select the **Card Model** from the drop-down menu.

2. Click **Execute Now**. The **Export Card Configuration** window displays a list of cards.

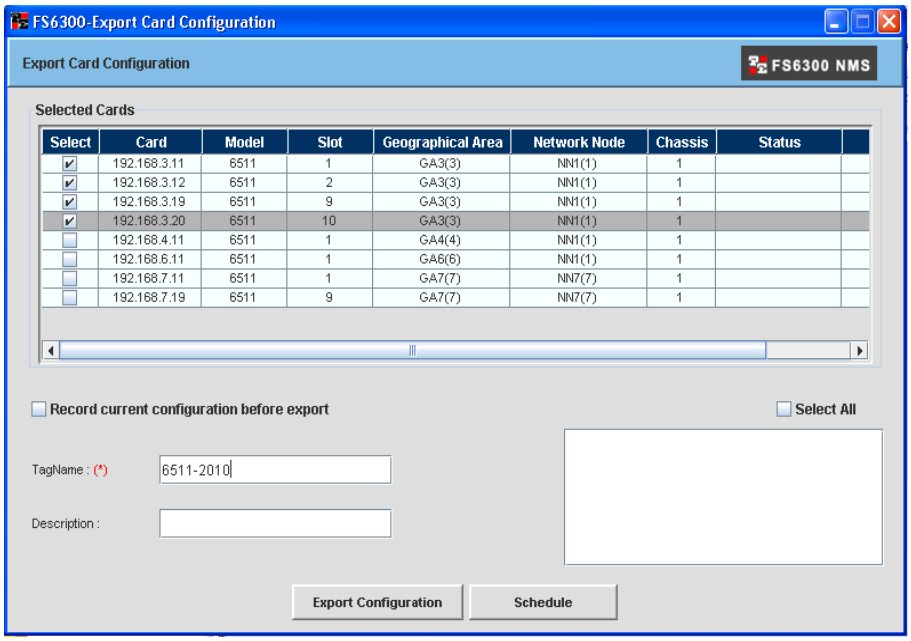


Figure 6. FS6300 Export Card Configuration window

3. Select the boxes of the desired cards. Enter a name for the configuartion in the **TagName** field. Then, click **Export Configuration**.

The window displays a "COMPLETED" status message after the system successfully exports the configuration file. Exported files are on the NMS in the directory: */opt/FS6300/Server/<nms version>/ExportedFiles/Device-Config/<card type>*.

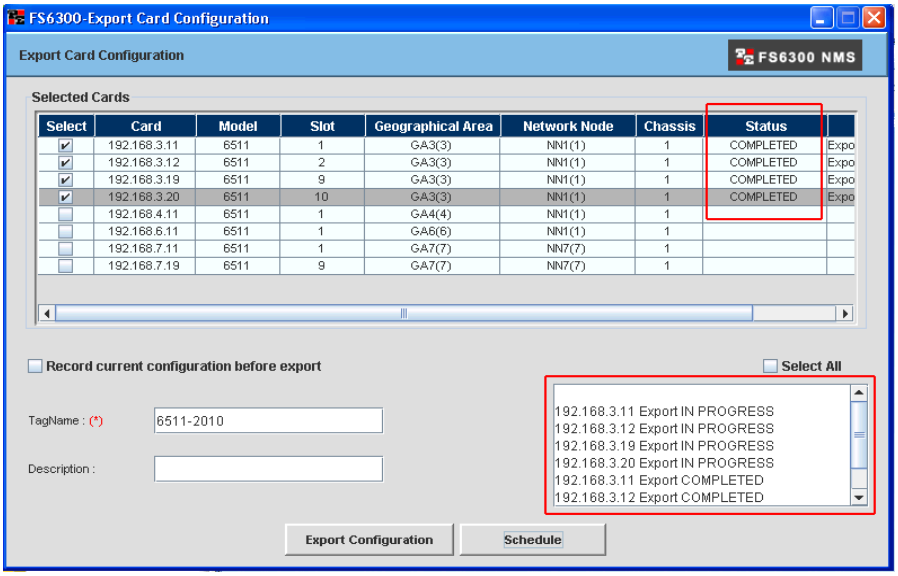


Figure 7. Export Complete

Importing the configuration for specific cards

To import a saved card configuration:

1. Click **Tools > View Exported Card Configuration** in the main window. The **Import Card Configuration** window displays.

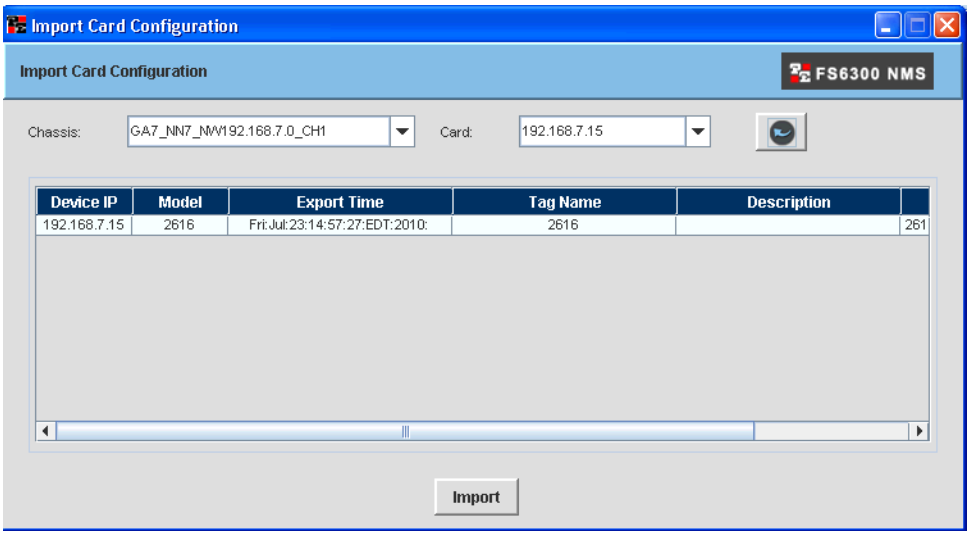


Figure 8. Import Card Configuration

2. Select the desired **Chassis** and **Card** IP address from the drop-down menus. Click the  button to refresh the available device configuration list.
3. Select the configuration file from the list and click **Import**. A confirmation message displays after the system successfully applies the configuration file.

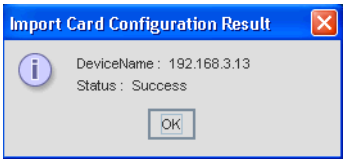


Figure 9. Successful Import

Recording the current configuration

To save the current configuration of a device to memory:

1. In the main menu tree under **Network Maps**, navigate to the **Chassis** or **Card/Slot.**
2. Right-click on the card's icon in the main window and select **Operator Action**. The **Reset Options** window appears. It shows the card model, IP address, and software revision of the card.

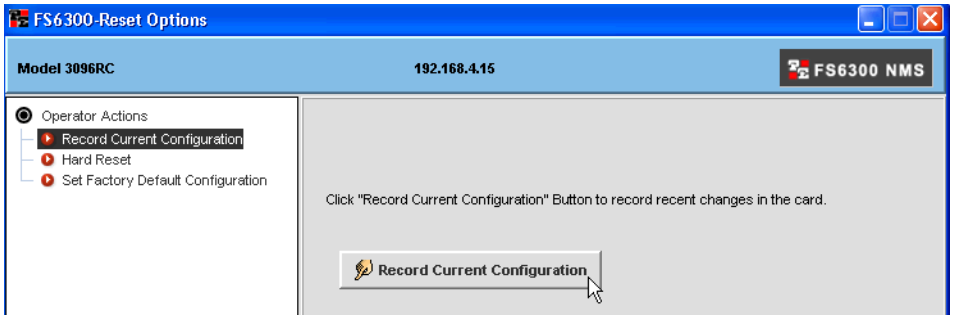


Figure 10. Record Current Configuration

3. Select **Record Current Configuration** from the menu tree in the Reset Options window.
4. Click the **Record Current Configuration** button.

Rebooting the device

To reboot a chassis or card:

1. In the main menu tree under **Network Maps**, navigate to the **Chassis** *or* **Card/Slot.**
2. Right-click on the card's icon in the main window and select **Operator Action**. The **Reset Options** window appears. It shows the card model, IP address, and software revision of the card.

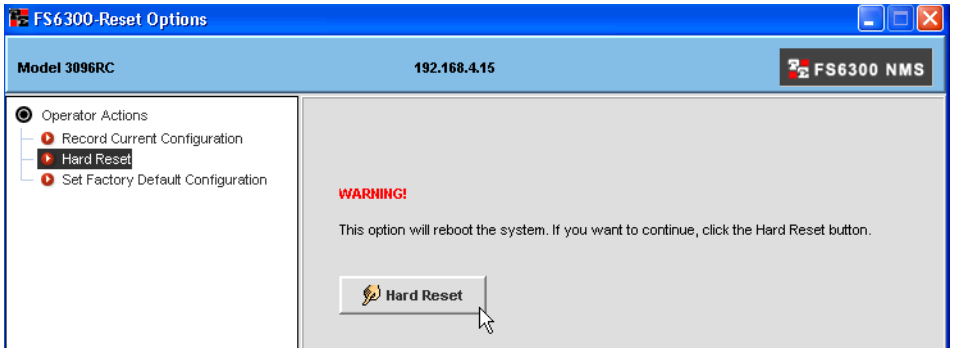


Figure 11. Hard Reset

3. Select **Hard Reset** from the menu tree in the Reset Options window.
4. Click the **Hard Reset** button.

IMPORTANT

The **Hard Reset** process will reset ALL of the system's values to the original factory settings. After resetting these values, the system will continue to function the same until the system is rebooted.

Setting the factory default configuration

To set the factory default configuration for a device:

1. In the main menu tree under **Network Maps**, navigate to the **Chassis** *or* **Card/Slot.**
2. Right-click on the card's icon in the main window and select **Operator Action**. The **Reset Options** window appears. It shows the card model, IP address, and software revision of the card.

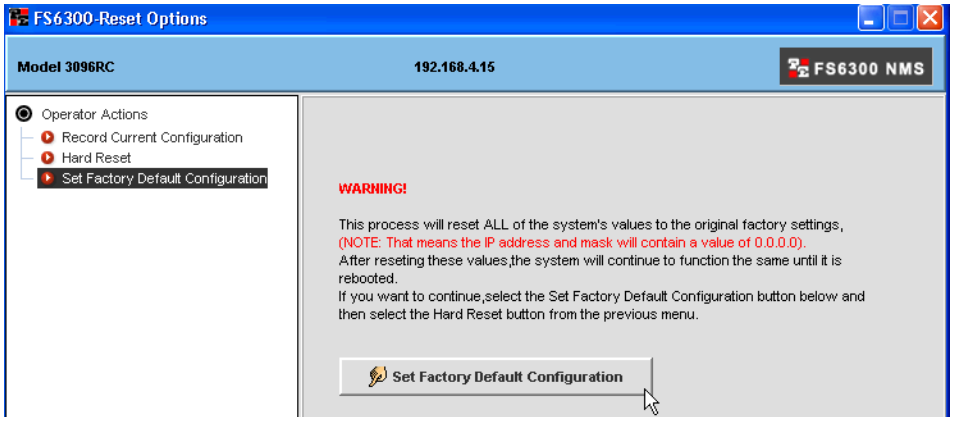


Figure 12. Set Factory Default Configuration

3. Select **Set Factory Default Configuration** from the menu tree in the Reset Options window.
4. Click the **Set Factory Default Configuration** button.
5. Click the **Hard Reset** button.

IMPORTANT

The **Hard Reset** process will reset ALL of the system's values to the original factory settings. After resetting these values, the system will continue to function the same until the system is rebooted.

Using Scripts for System Tasks

This section provides instructions for performing system tasks through scripts and CLI commands.

- **Backup the database and logs:** The NMS package includes a shell script for backing up the database contents and logs directory to the server. Refer to "Executing the script to backup the database and logs directory" on page 29.
- **Migrate the database:** The NMS package includes a shell script for using the current development build on an earlier database. Refer to "Executing the script to migrate the database" on page 29.
- **Backup card configurations:** The NMS package includes a shell script for using the current development build on an earlier database. This section explains how to set up the system to automatically save card configurations. Refer to "Executing the script to back up card configurations" on page 29.

Executing the script to backup the database and logs directory

The NMS package includes a shell script for backing up the database contents and logs directory to the server. This script will zip the logs directory and the database contents on the server. Also, this script is useful for uploading the required data from a customer network for further analysis.

To execute the script, go to the <*installed directory*> on the server machine. Enter the command:

```
sudo ./NMS_info.sh
```

Executing the script to migrate the database

The NMS package includes a shell script for using the current development build on an earlier database. To use this script, stop the NMS server but leave the MySQL server running.

To execute the script, go to the <*installed directory*>*/bin* on the server machine. Enter the command:

```
sudo dos2unix db_changes_1.27D.sh;sudo ./db_changes_1.27D.sh
```

Executing the script to back up card configurations

The NMS package includes a shell script for setting up automatic card configuration backups for cards managed by the NMS. This script supports the following card types: 2616RC, 3096RC, 3196RC, and 6511RC.

Place the script file in the following location: */opt/FS6300/pe_card_backup.pl*

Configuration backup files are saved in the following location: */opt/FS6300/card_cfg/[date of backup]/[ipaddress]-[date of backup]*

Backup configurations for all cards in the NMS

To backup the card configuration files for all of the cards in the NMS, enter the command:

```
./pe_card_backup.pl DB
```

This command obtains a list of IP addresses of all cards managed in the NMS database. It also checks availability of the backup location on the file system and creates the directory, if needed.

For each of the IP addresses, the script pings the card on the network. If the card is available, the script backs up the configuration. If the card does not respond to the ping request, the script skips the card and moves on to the next IP address in the list.

The script performs each card configuration backup sequentially and allows 5 minutes for completion. Immediately after a successful card backup, the script sends a network ping to the next card and repeats the process. If the backup does not complete in 5 minutes, the system purges the incomplete configuration for that particular card. Then, the system moves on to the next card.

Backup configuration for a specific card

To backup the card configuration files for a specific card in the NMS, enter the command:

```
./pe_card_backup.pl HOST 1.2.3.4
```

This script checks the availability of the backup location on the file system and creates the directory, if needed. If the card is available, the script backs up the configuration. If the card does not respond to the ping request, the script will not back up the configuration file. The script allows 5 minutes to complete the card backup. If the backup does not complete in 5 minutes, the system purges the incomplete configuration for the card.

Chapter 2 Managing User Access

Chapter contents

Overview

The Security Administration window is an important tool for managing users and groups, and for managing their permissions and actions in the FS6300 NMS. To reach the **Security Administration** window, click on **Tools > Security Administration** at the top of the screen.

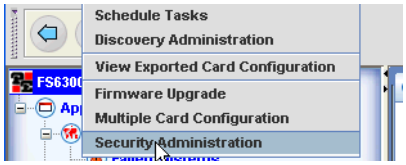


Figure 13. Tools > Security Administration

Managing Users

Before anyone has access to the FS6300 NMS Client, he or she must be added as a user to the FS6300 NMS Server database. After you have created users, you can add them to groups, and give them specific permissions.

Adding Users

To add a new user:

1. In the **Security Administration** window, do any of the following:

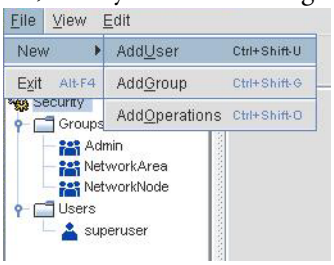


Figure 14. Add User from Security Window

– From the **File** menu, choose **New > AddUser.**

– Press **Ctrl+Shift+U**.

– Click the **Add User** icon  .

The **User Administration** window displays.

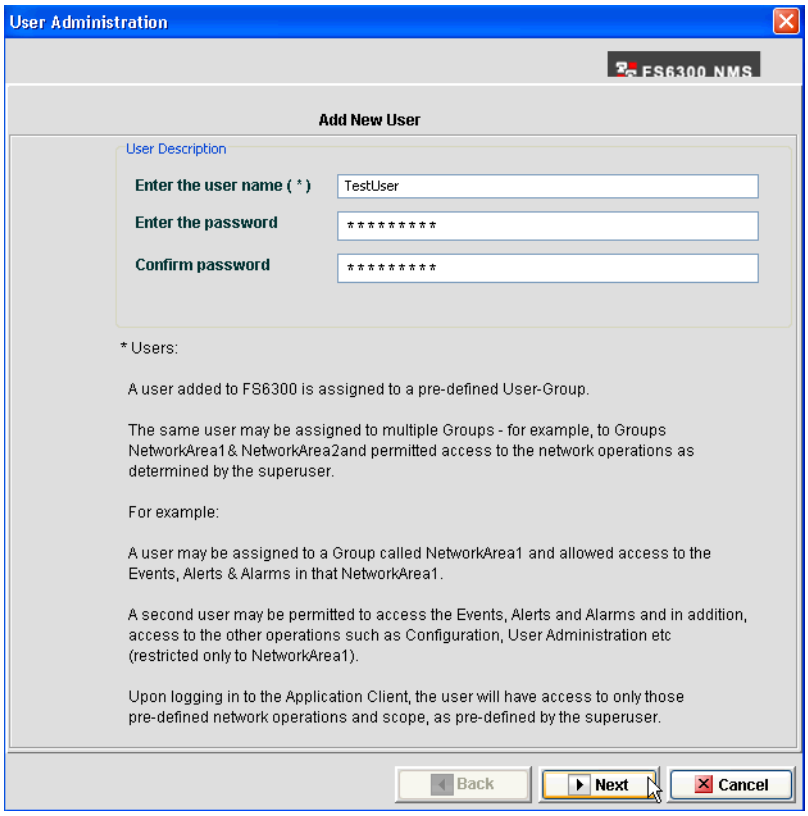


Figure 15. Add New User

2. Type the desired user name and password in the text fields and click **Next**.
3. If desired, you can set the account and/or password to expire after a certain amount of time. By default, the user account and password are set to never expire. Make the desired changes, then click **Next.**

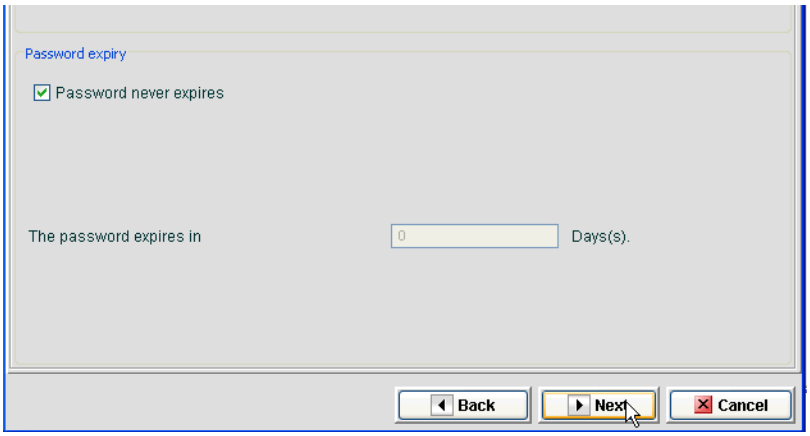


Figure 16. User Account Expiry Options

4. If you are associating the user to have permissions based on an existing group, select the **Group-based permissions** checkbox. Then, select the checkbox of the group that you want to add the new user to. Click on the arrow on the right side of the Group Names table to view permissions for a group.

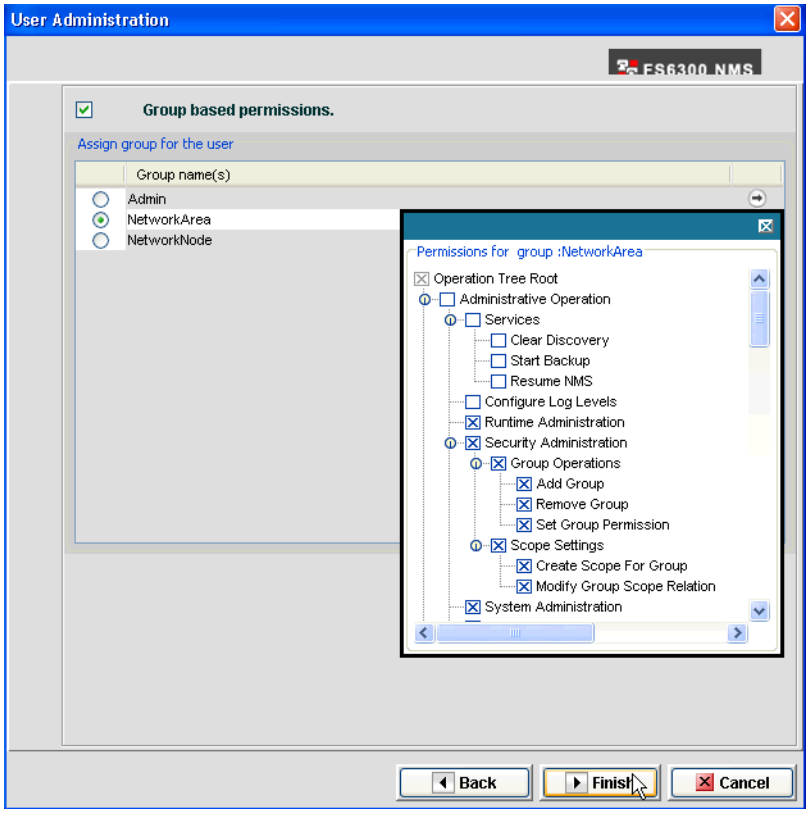


Figure 17. Adding a New User to a Group

If you did not select the checkbox for group-based permissions and want to set the user's permissions individually, click **Finish**, and see "Modifying User Permissions" on page 34.

5. Click **Finish**. The new user is displayed in the Security window menu tree under Users.

Modifying User Permissions

To add, delete, or modify permissions for an individual user:

1. In the **Security Administration** window, click on the user in the User section of the menu tree.

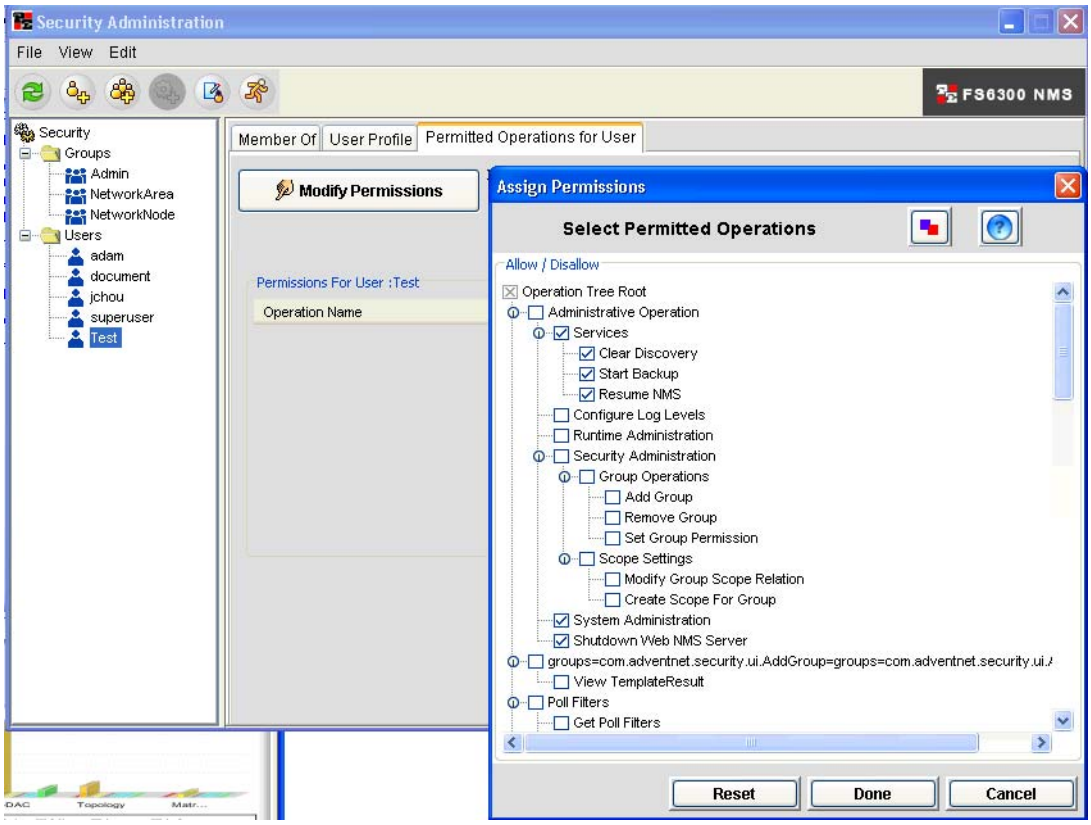


Figure 18. Modify User Permissions

2. Click on the **Permitted Operations for User** tab, then click on the **Modify Permissions** button.
3. In the **Assign Permissions** window, select the checkboxes of the allowed operations for the user. Then, click **Done**.
4. The permissions for the user are displayed in a table in the Permitted Operations for User tab. If desired, you may add a note for allowed operations. To ad a note, double-click on the Description column in the user's Permissions table.

Disabling Users

To temporarily disable a user from logging in and accessing the NMS:

1. In the **Security Administration** window, click on the user in the User section of the menu tree.

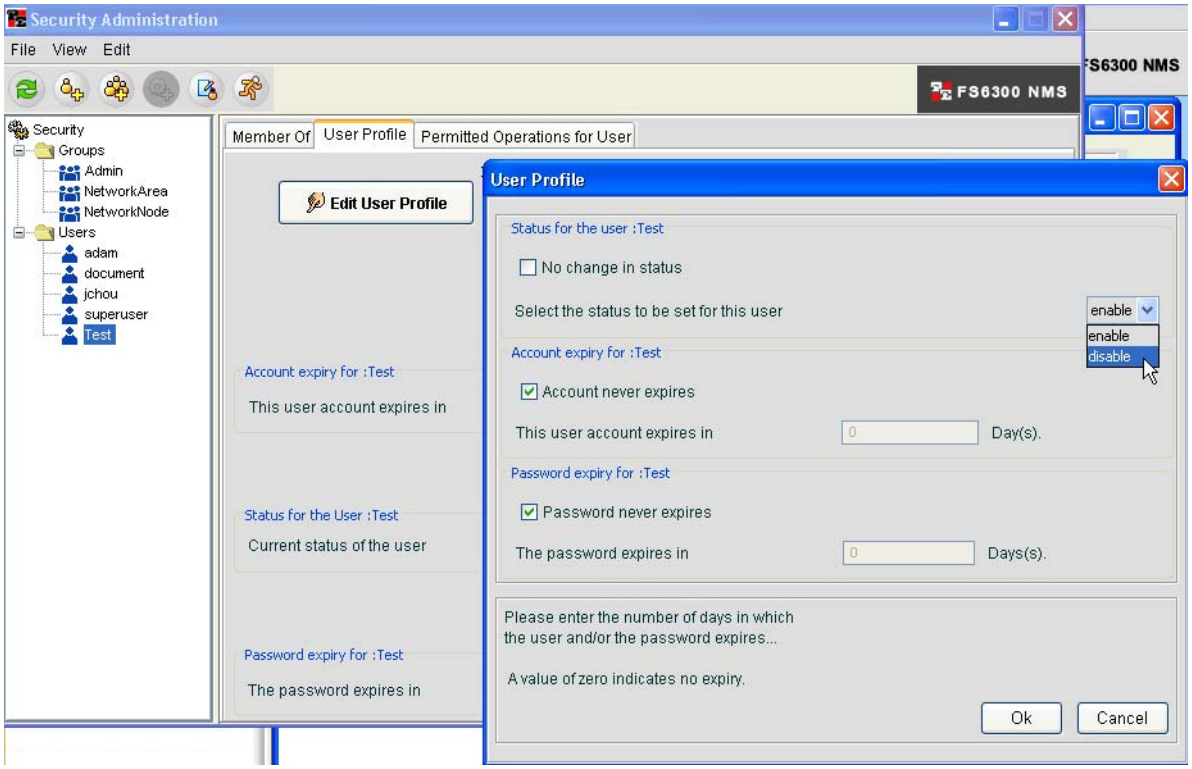
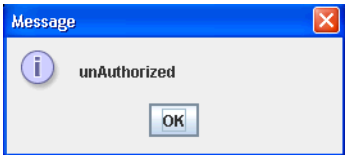


Figure 19. Disable User

2. Click on the **User Profile** tab, then click on the **Edit User Profile** button.
3. In the User Profile window, you can edit the status of the user, and when the user account and/or password expires.
4. To temporarily disable a user, de-select the **No change in status** checkbox, then choose **disable** from the status drop-down menu.
5. Click **OK**. A red circle with a white "x" will appear on the user's name in the Security window menu tree. When the user attempts to log in to the NMS, a message will display–"Unauthorized."



6. To re-enable a disabled user's account, repeat steps 1-4, except select **enable** from the status drop-down menu. Click **OK**.

Reinstating Users

To reinstate a disabled user account:

1. Log into the NMS as the administrator (The default login and password is *superuser*).
2. In the **Security Administration** window, select the disabled user account. Click on the **User Profile** tab.
3. Click **Edit User Profile**. The **User Profile** window displays. Modify the **Account Expiry** and **Password Expiry** fields as desired.
4. Uncheck the **No change in status** box. Select **enable** from the user status drop-down menu. Then, click **OK**. The user can now log into the system again.

Changing User Passwords

To change a user password:

1. In the **Security Administration** window, select the user in the menu tree. Then, do any of the following:
   - From the **Edit** menu, choose **Change Password.**
   - Press **Ctrl+Shift+C**.
   - Right-click on the user in the menu tree and select **Change Password**.
2. In the **Change Password** dialog box, type in the new password for the user. Then, type in the new password again.
3. Click **OK**.

Deleting Users

To delete a user:

1. In the **Security Administration** window, select the user in the menu tree.
2. Right-click on the user in the menu tree, and select **Delete**.

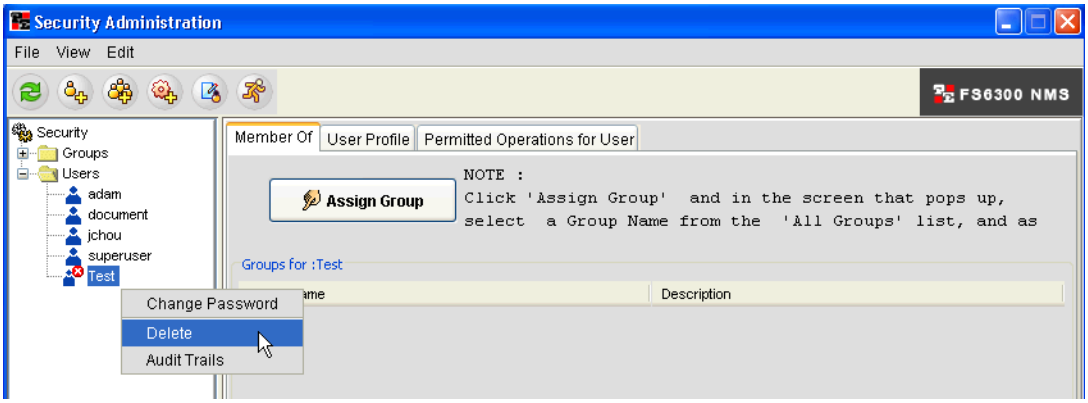


Figure 20. Delete User

3. A warning message will display. Click **Yes**.

Assign/Delete Users To/From Groups

To assign or delete a user to/from a group:

1. In the **Security Administration** window, select the user in the menu tree.
2. Click on the **Member Of** tab, and click the **Assign Groups** button.

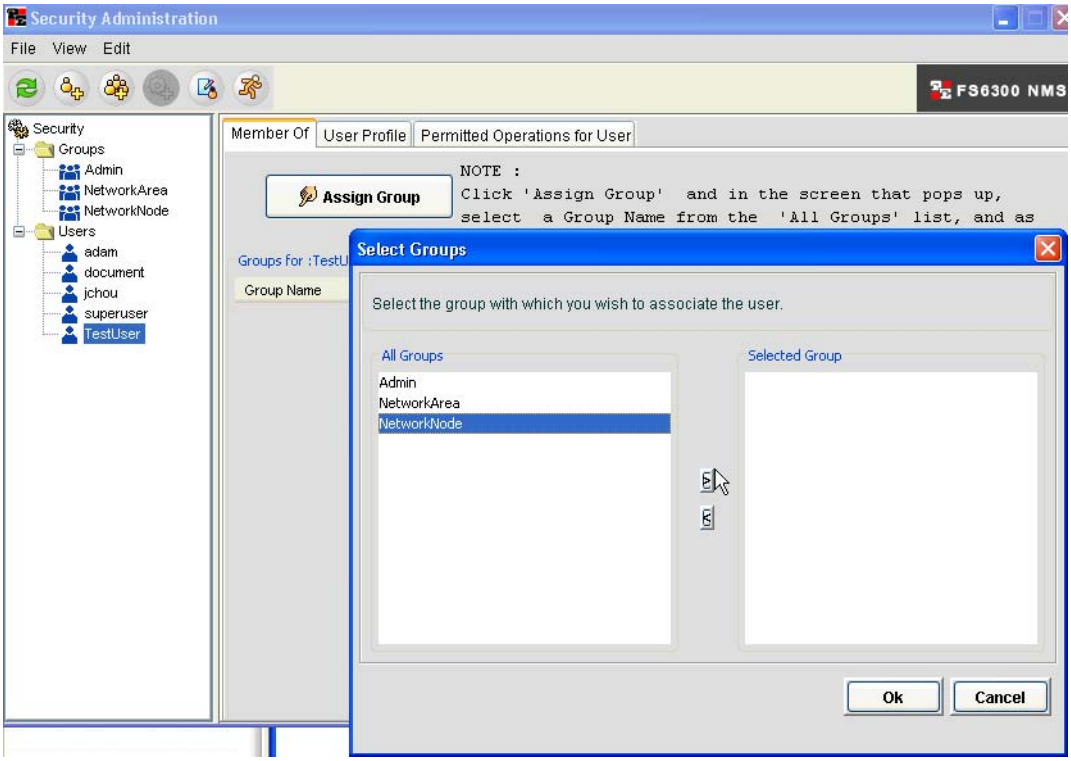


Figure 21. Assign User to Groups

3. In the **Select Groups** window, click on the group in the All Groups column, then click the ">" button to add the group to the user's list. Repeat this step if you want to add the user to multiple groups.
4. To remove a user from a group, click on the group in the Selected Groups column and click the "<" button.
5. Click **OK**.

> **Note** If you remove an Admin user from a group with administrative privileges, this will disallow some permissions for the user. To view/modify selected user permissions, click on the **Permitted Operations for User** tab, then click the **Modify Permissions** button. The included and excluded permissions are also listed in the Permissions for User table.

Managing Groups

In the FS6300 NMS, you can create groups with specific permissions for each group, and then assign users to these groups with specified operational tasks and permissions.

Adding Groups

To add a group:

1. In the **Security Administration** window, do any of the following:
   - From the **File** menu, choose **New > Add Group.**
   - Press **Ctrl+Shift+G**.
   - Click the **Add Group** icon  .

   The **Group Wizard** window displays.

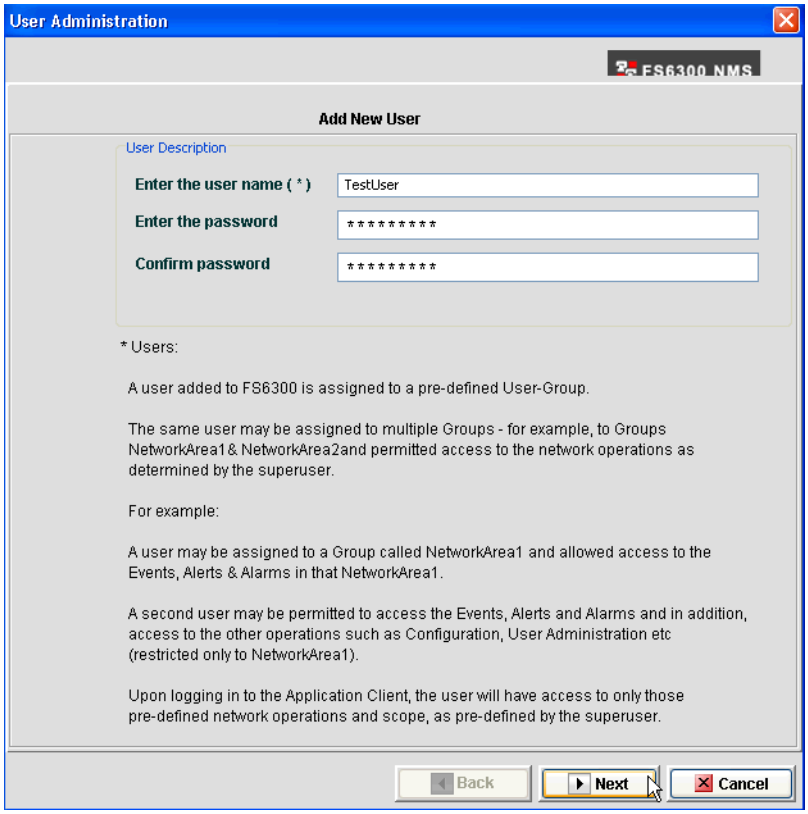


Figure 22. Add New Group

2. Type the desired group name in the text field and click **Next**.
3. Select the check boxes for the operations that users in the group will be allowed to do. Click **Finish**.

Assign/Delete Users To/From Groups

To assign or delete a user to/from a group:

1. In the **Security Administration** window, select the group in the menu tree.
2. Click on the **Operators** tab, and click the **Assign Users** button.

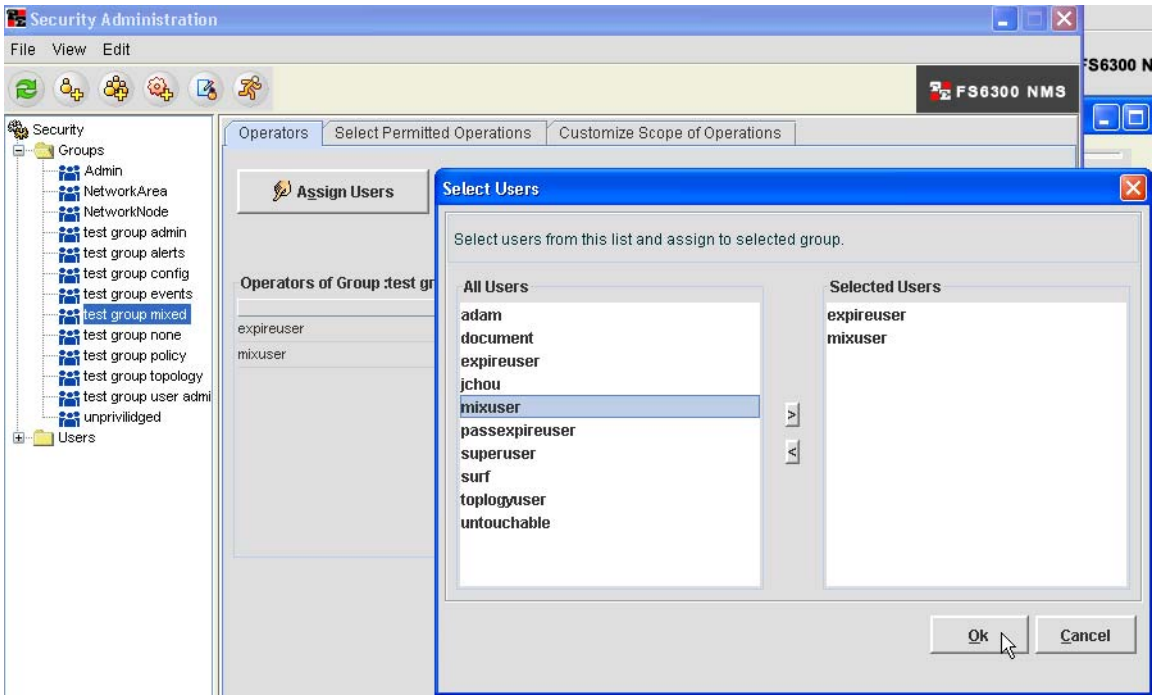


Figure 23. Assign Users to Groups

3. In the **Select Users** window, click on the user in the All Users column, then click the ">" button to add the user to the group's list. Repeat this step if you want to add multiple users to the group.
4. To remove a user from a group, click on the user in the Selected Users column and click the "<" button.
5. Click **OK**.

Deleting Groups

To delete a group:

1. In the **Security Administration** window, select the group in the menu tree.
2. Right-click on the group in the menu tree, and select **Delete**.
3. A warning message will display. Click **Yes**.

Managing Scopes for Groups

Scopes are associated with the actual operations of a group and with specific properties to which the users have access. Scopes are used to set limits to a permission by applying one or more properties to a group permission.

Adding Scopes

To add a scope:

1. In the **Security Administration** window, select the group in the menu tree.

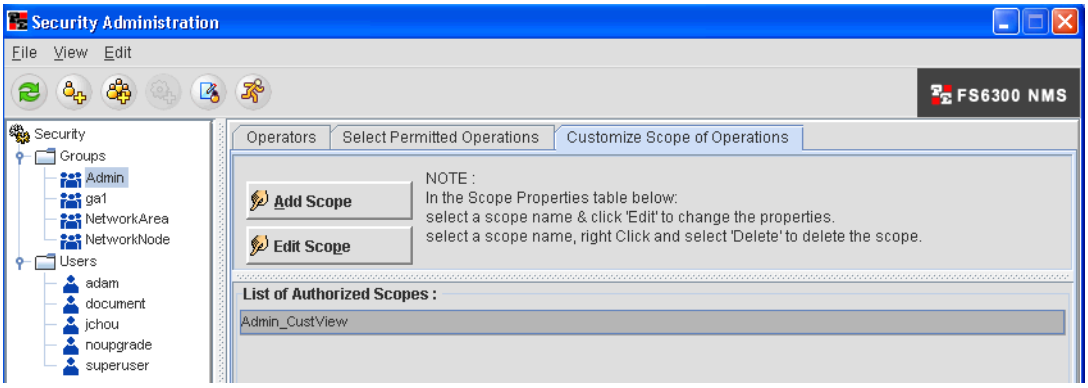


Figure 24. Add Scope to Group

2. Click on the **Customize Scope of Operations** tab, and click the **Add Scope** button.

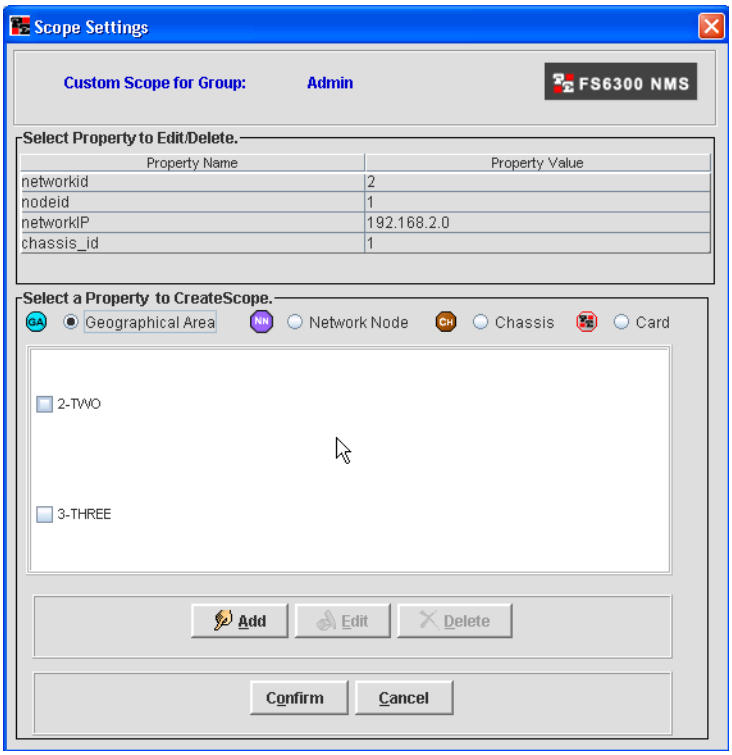


Figure 25. Scope Settings

3. Select the property that you would like to add for the group. You can select from Geographical Area, Network Node, Chassis, Card, and Port.
4. Click the **Add** button. The Property value will appear in the table in the Scope Settings window.
5. Click the **Confirm** button to add the scope.

Deleting Scopes

To delete a scope:

1. In the **Security Administration** window, select the group in the menu tree.
2. Click on the **Customize Scope of Operations** tab.

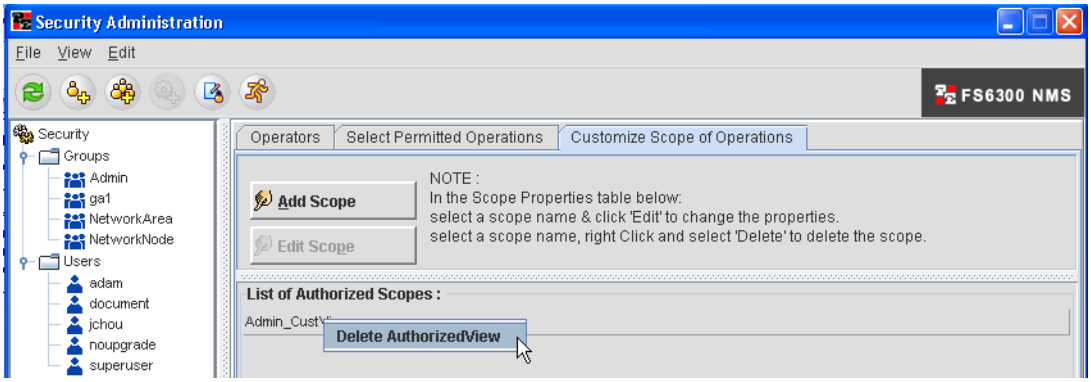
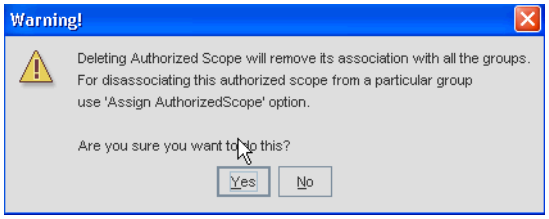


Figure 26. Delete Scope

3. Right-click on the scope in the **List of Authorized Scopes** table, and select **Delete AuthorizedView**.
4. A warning message will display. Click **Yes**.



Managing Operations

The Operations Tree contains a list of operations (also referred to as permissions) that is provided by default in FS6300 NMS. The operations are logically arranged in a tree structure with parent and child operations. You can add new operations when they are needed and delete obsolete operations. For example, if you add new applications, you may want to add specific operations for users to use with the new applications.

Adding Operations

To add new operations to the operations tree so that users/groups can add it to their permissions:

1. In the **Security Administration** window, do any of the following:
   - From the **File** menu, choose **New > Add Operations.**
   - Press **Ctrl+Shift+O**.
   - Click the **Add Operation** icon  .
2. In the **Operations** window, select the top of the operation group in the tree where you want to add the new operation.

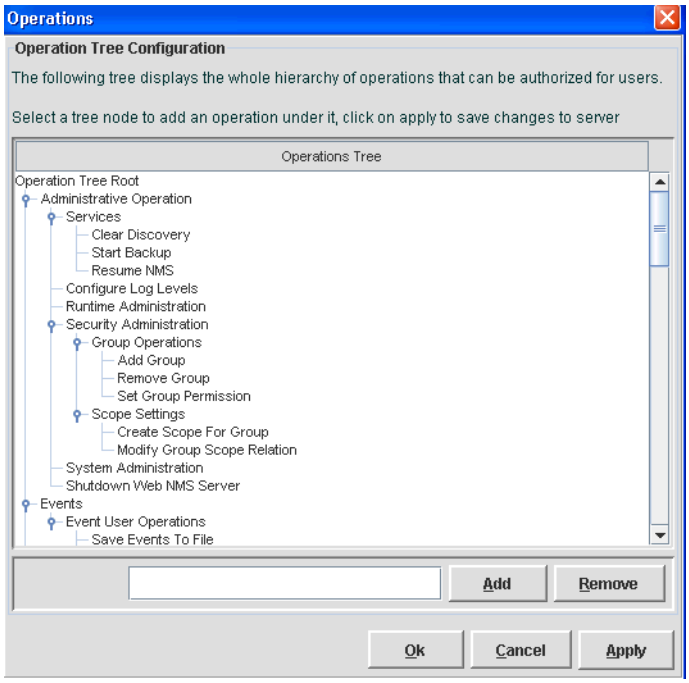


Figure 27. Add Operation

3. Type in the name of the new operation in the text field and click **Add**.
4. Click **Apply**.
5. Repeat steps 2-4 to add more new operations. Then, click **OK**.

Deleting Operations

To delete operations in the operations tree:

1. In the **Security Administration** window, press **Ctrl+Shift+O** to open the **Operations** list.
2. In the **Operations** window, select the operation in the tree that you want to delete.
3. Click **Remove**.
4. A warning message will display. Click **Yes.**
5. Click **OK**.

Managing Audit Trails

Audit trails allow you to view the operations that have been performed by a user. The audit trail identifies all operations that have been performed, the time, whether it was successful, category, and audited object. You should periodically clear the trails after they have been reviewed.

Viewing Audit Trails

To view audit trails:

1. In the **Security Administration** window, do any of the following:
   - From the **View** menu, click **Audit Trails**.
   - Press **Ctrl+Shift+A**.
   - Click the **Audit Trails** icon .

The **Auth Audit Screen** displays.

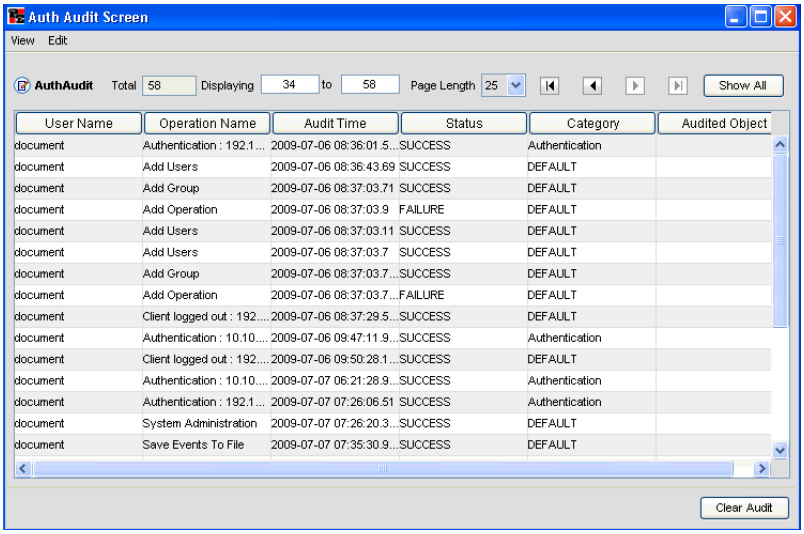


Figure 28. Auth Audit Screen

2. To view details of a specific audit, select the operation in the Auth Audit table, then click **View > Audit Details** at the top of the window.
3. Click the **Clear Audits** button at the bottom of the window to delete all of the audits in the table.

Searching Audits

To search for audits matching certain criteria:

1. In the **Security Administration** window, do any of the following:
   - From the **View** menu, click **Audit Trails**.
   - Press **Ctrl+Shift+A**.
   - Click the **Audit Trails** icon .

The **Auth Audit Screen** displays.

2. Select **Edit > Search** (or **Ctrl+F**) from the top of the screen. The **Search** box displays.

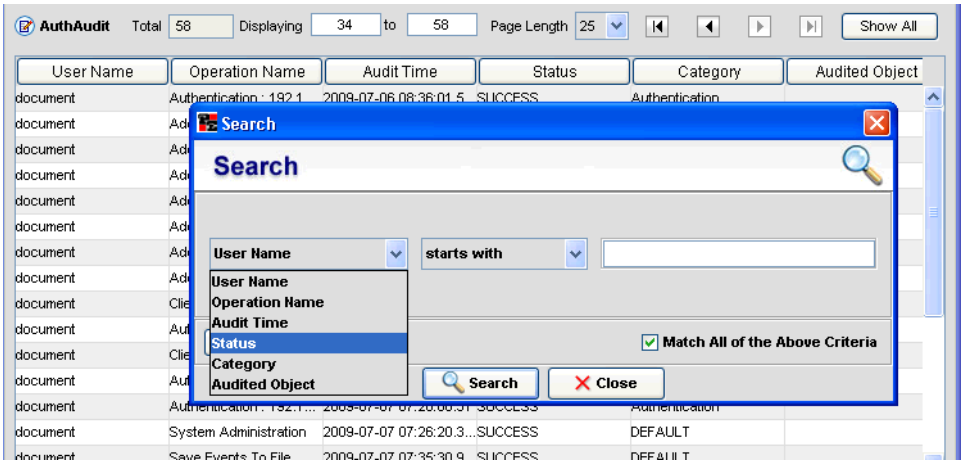


Figure 29. Search Audits

3. Select and enter your search criteria and click the **Search** button. You can search the audits by User, Operation, Time, Status, Category, or Object.

Chapter 3 Discovering Your Network

Chapter contents

Overview

The Discovery process is the most important step in working with the NMS. This chapter describes how to add containers before discovering your network, how to schedule rediscovery processes, and how to add a device manually to the system.

To open the **Discovery** window, click on **Tools > Discovery Administration** at the top of the screen.

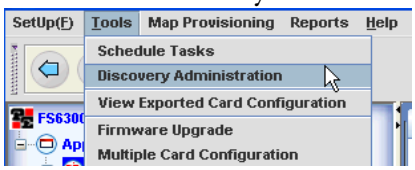


Figure 30. Tools > Discovery Administration

Note The FS6300 supports Patton Models 2616RC, 3096RC, 3196RC and 6511.

Note The FS6300 currently only supports all devices with same community strings and networks with 24 bit masking.

Defining Containers

Containers are unique identification details about the Geographical Areas, Network Nodes, and Chassis in your network. You may pre-define and create a master list of containers before initial discovery of your network, or you may define containers while configuring multiple cards.

Pre-Defining Containers Before Initial Discovery

Before starting discovery, you may create a master list of pre-defined details for the Geographical Areas, Nodes, and Chassis in your network. When you configure multiple cards later, you can refer to your master list of containers. To reach the **Container Definition** window, click on **SetUp(F) > 6300 Container Definition** at the top of the screen.

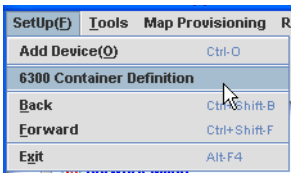


Figure 31. SetUp(F) > 6300 Container Definition

Adding Pre-Defined Containers

To add containers in the NMS:

1. In the Container window, click on **Add** in the menu tree.

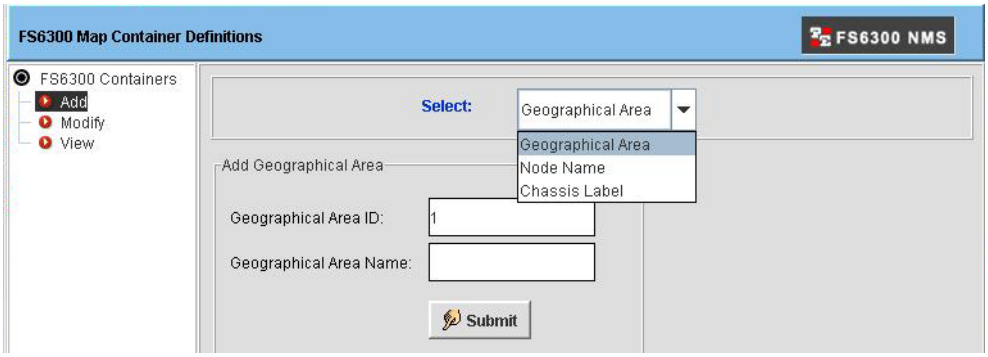


Figure 32. Add Container

2. From the drop-down menu, select which type of container you want to add. You should add the Geographical Areas first, then add the Nodes in that area, then add the Chassis Labels in the Nodes. Each Geographical Area-Node-Chassis combination is unique, and may only be applied to cards in one chassis-subnet.

   – **Geographical Area (GA):** The Geographical Area ID must be numerical, and cannot be changed once it is added to the system. However, the Name may be modified at any time.

   – **Node Name (NN):** Add nodes in the network to a Geographical Area. You may also add details such as system manager and system location.

   – **Chassis Label:** The Chassis ID must be numerical, but the Label Name is optional.

   Note The GA ID must be unique across the entire NMS. The NN ID must be unique across the entire Geographical Area it is under. The Chassis ID must be unique across the entire Network Node it is under.

3. Click **Submit**.

Modifying Pre-Defined Containers

To modify pre-defined containers:

1. In the Container window, click on **Modify** in the menu tree.

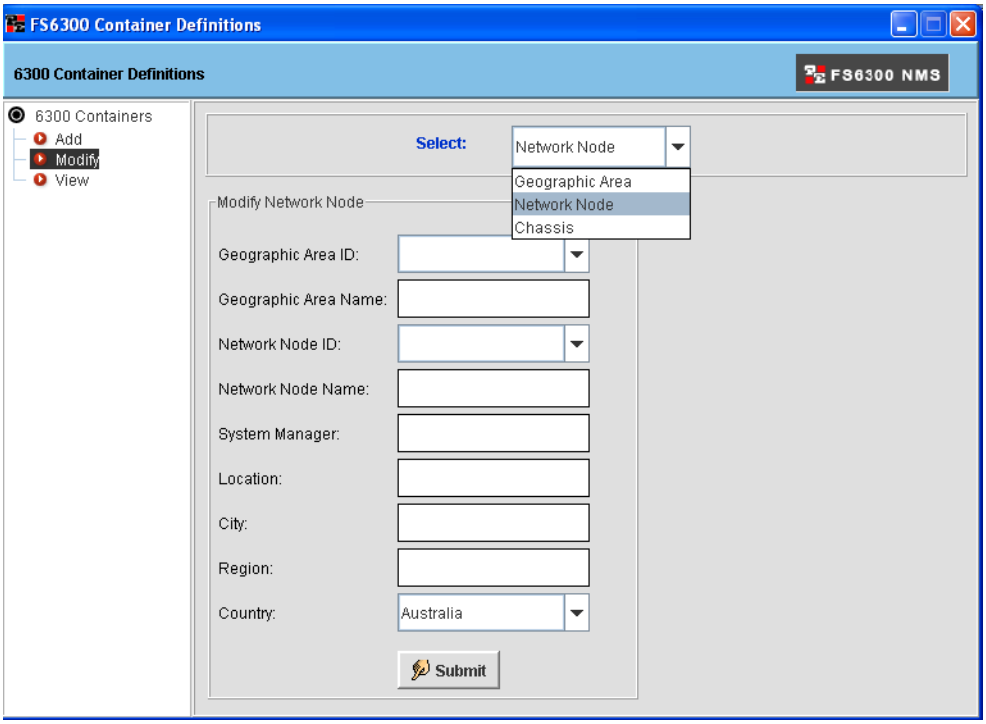


Figure 33. Modify Container

2. From the drop-down menu, select which type of container you want to modify. Some items, such as ID, are permanent and cannot be modified.
3. Click **Submit**.

Viewing and Deleting Containers

To view or delete containers:

1. In the Container window, click on **View** in the menu tree.

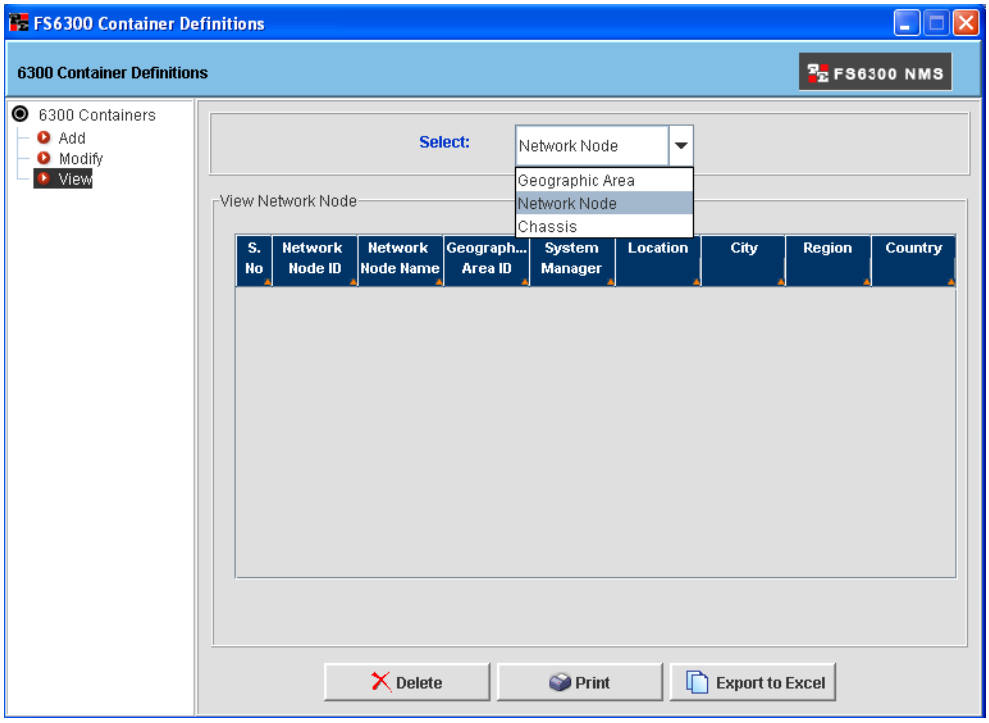


Figure 34. View Containers

2. From the drop-down menu, select which container type you want to view.
3. The table displays a list of containers. This table includes details that were added or modified during multiple card configuration, but it does not reflect the list of Geographical Areas, Network Nodes, or Chassis IDs existing on discovered cards. You can rearrange columns in the table by clicking and dragging the column to the desired order.
4. To delete a container, select the row of the container in the table, and click **Delete**. A container may be deleted ***only*** if the container is **not assigned** to any card in the NMS.
5. If desired, click **Print** to send the list to a printer or **Export to Excel** to save the list to a Microsoft Excel spreadsheet.

Defining Containers During Multiple Card Configuration

You may wish to define containers after all of the chassis in your network have been discovered. In this case, you may add IDs, details, and labels during the multiple card configuration process. To reach the **Multiple Card Configuration**. window, click on **Tools** > **Multiple Card Configuration**. at the top of the screen.

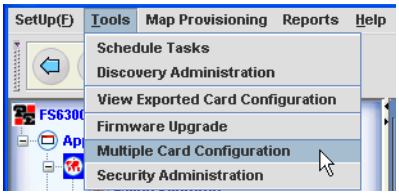


Figure 35. Tools > Multiple Card Configuration

1. Click on **Card Parameters** in the menu tree on the left side of the screen.

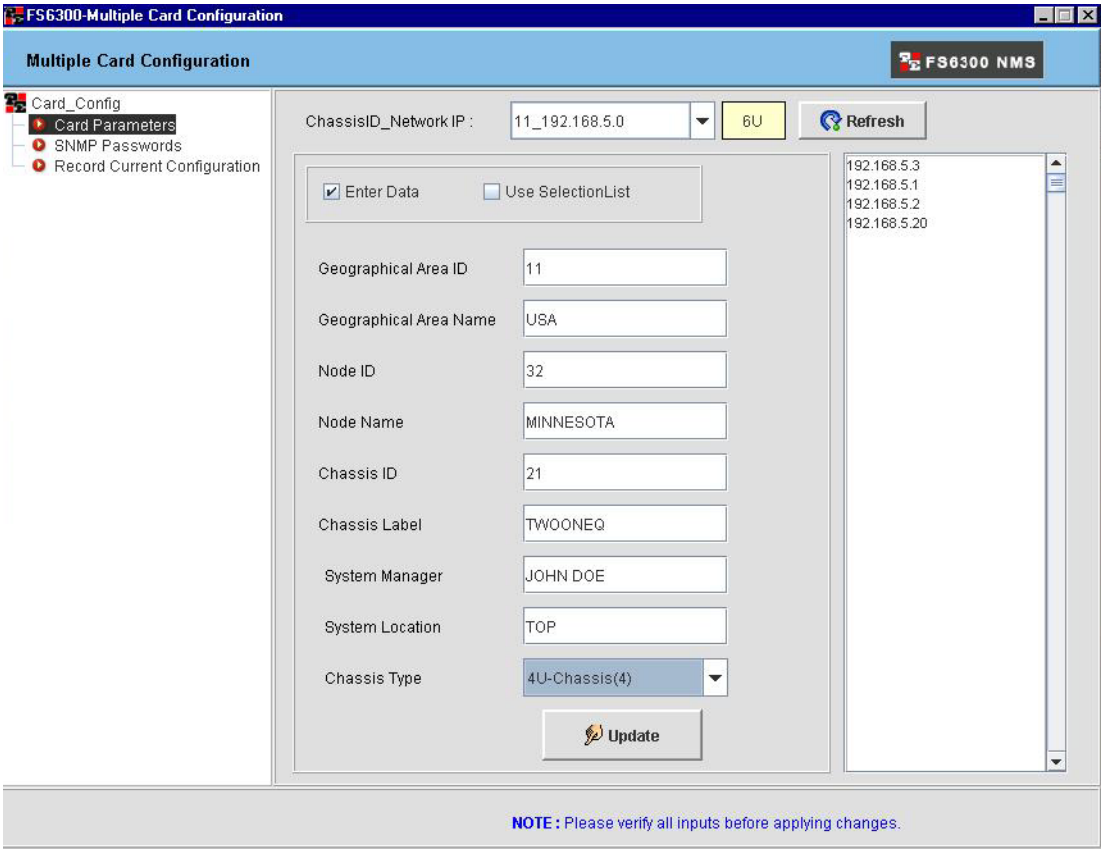


Figure 36. Multiple Card Configuration > Card Parameters

2. Select the network address for the chassis in the drop-down menu at the top of the window.
3. You can modify containers by typing in the data or using drop-down menus. Select the checkbox at the top of the Card Parameters window for the option you want to use.
4. Enter the information you want to update on the subnet for the following fields, or if you are using the Selection List, you may select containers from the pre-defined master list.

   – **Geographical Area ID** *(This is permanent and cannot be modified).*

– **Geographical Area Name** (Descriptive name of the geographical area)

– **Node ID** *(This is permanent and cannot be modified).*

– **Node Name** (Descriptive name of the node)

– **Chassis ID** *(This is permanent and cannot be modified).*

– **Chassis Label** (Descriptive label for the chassis)

– **System Manager** (Name of the person managing this subnet on the network)

– **System Location** (Description of where the system is located)

– **Chassis Type** (Choose a chassis type from the drop-down menu)

5. Click **Update** to save the information for all of the cards on that subnet.

If the same CH ID exists on cards in a different chassis unit but with the same subnet address, an alert is displayed asking if the cards need to be merged into one unit.

If the same CH ID exists on cards in a different chassis unit and with different subnet address, an alert is displayed that Chassis ID already exists.

This is to ensure uniqueness of Chassis IDs in the NMS.

The following details are also checked when modifying containers during multiple card configuration:

- If there is already an entry for the GA ID and GA Name entered by the Admin
- If not, a new record is added to the master-list.
- If the master-list instead has an entry for GA-101-Michigan or GA-105-Maryland, an alert is displayed requesting the admin to re-enter the ID/Name

The NMS also verifies containers to prevent duplication of ID and name for the Network Node.

- If the values entered are successfully verified and found to be unique, these values are auto-updated in the master-list table (mentioned with Option A above), in the background.
- 6300 NMS does not allow these records to be deleted from the 6300-Conatiner definition interface.
- All cards in the selected chassis are configured with the new container IDs.

Figure 37 shows a visual representation of container IDs in the NMS.

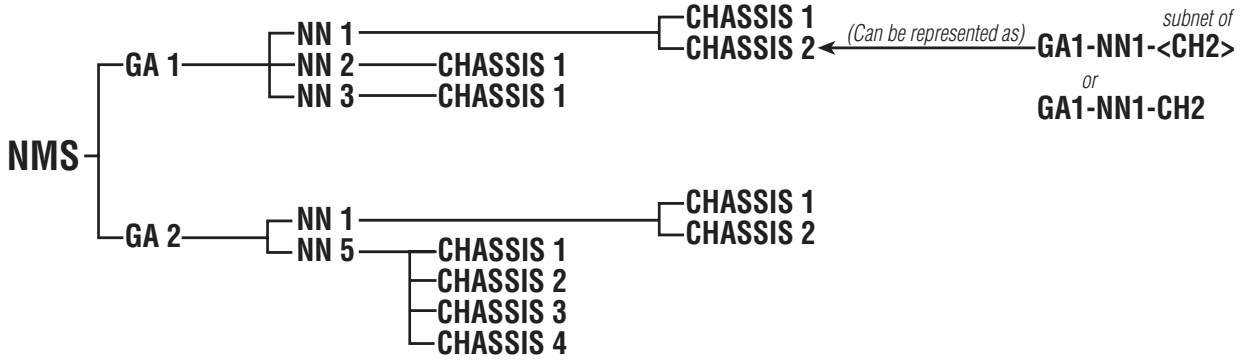


Figure 37. Container IDs in the NMS

Configuring Initial Discovery Parameters

The **Initial Discovery** process is the first discovery process that is started as soon as the FS6300 NMS server loads.

To set initial discovery parameters:

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Initial Parameters** button.

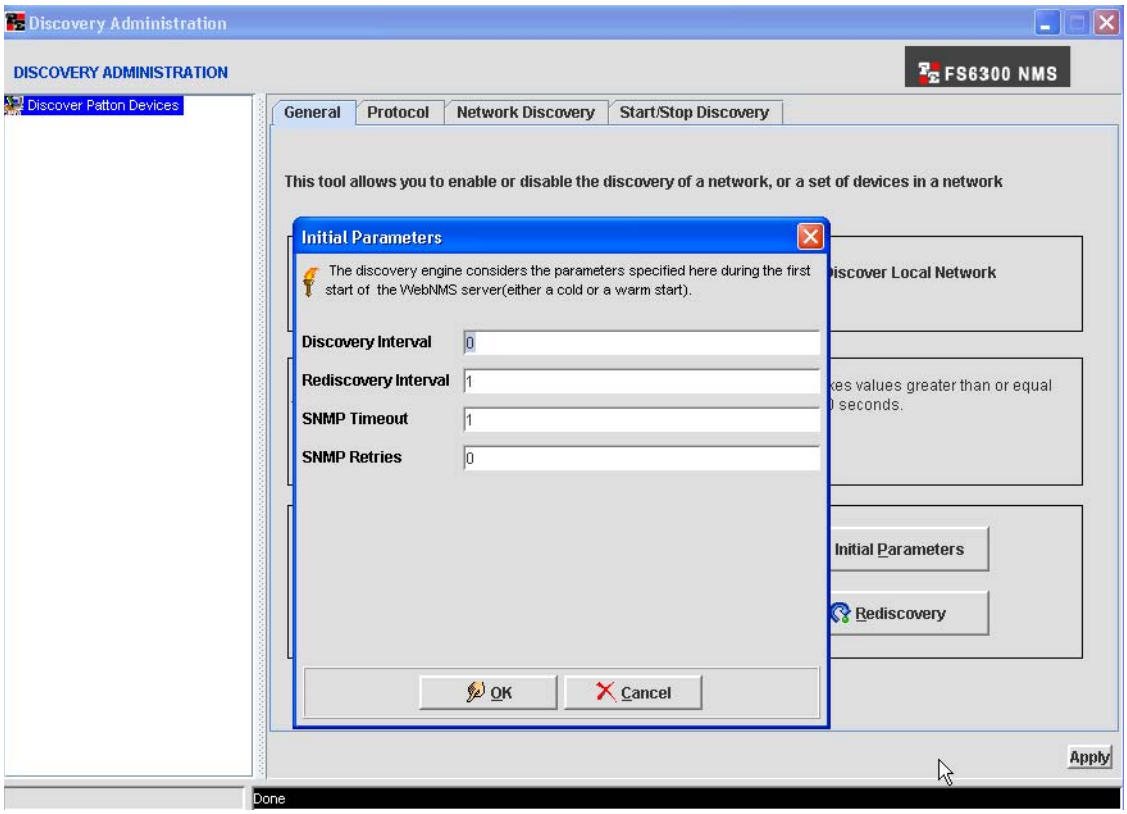


Figure 38. Set Initial Parameters

3. The initial parameters are:
   - **Discovery Interval:** Interval (in seconds) between the discovery of any two devices in the network.
   - **Rediscovery Interval:** Interval (in hours) between two complete discoveries of a network.
   - **SNMP Timeout:** Threshold value, in seconds, for all the SNMP requests.
   - **SNMP Retries:** Number of SNMP retries for discovery, status polling, and data collection.
4. Click **OK**. Then, click **Apply** in the Discovery Administration window.

Starting the Discovery Process

Before starting the Discovery process, at least one node must be deployed, powered up, and connected to the network.

Enabling AutoDiscovery

To start Discovery:

1. From the **Tools** menu at the top of the screen, select **Discovery Administration**. The Discovery Window displays.
2. Click on **Discover Patton Devices** in the tree on the left side of the screen.
3. Click on the **Auto-Discovery** checkbox.

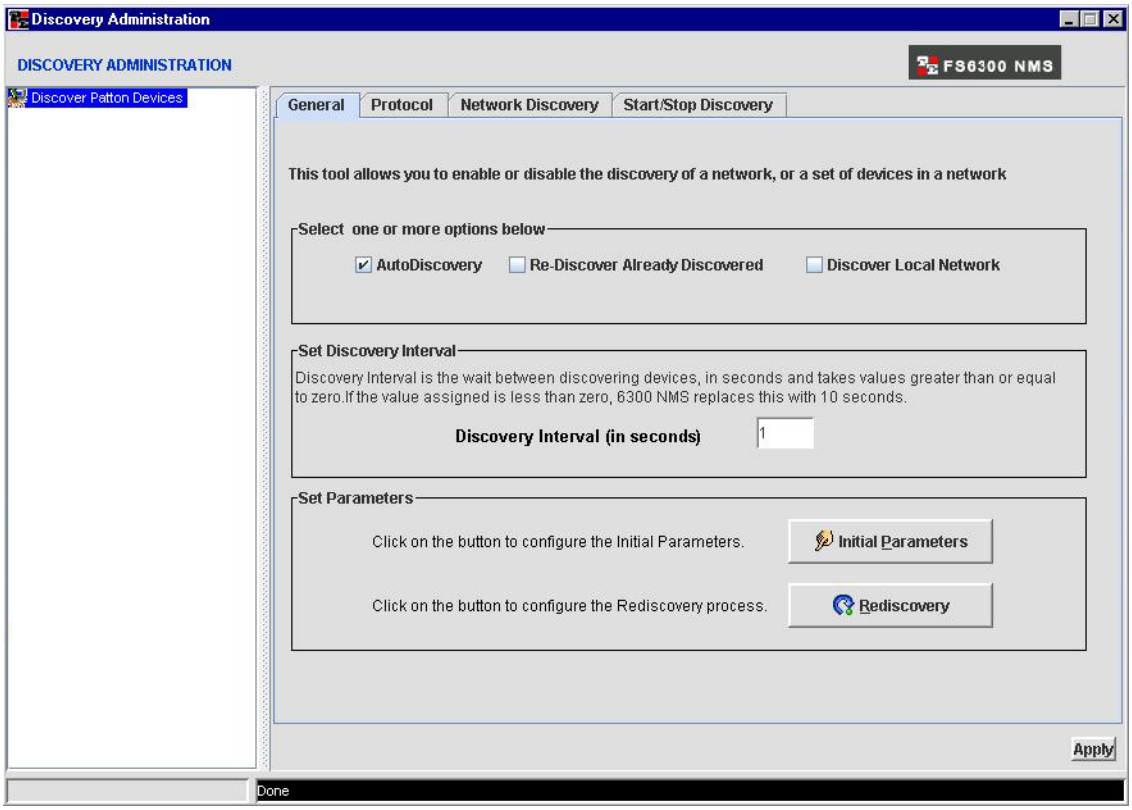


Figure 39. Discovery Window

Configuring Discovery of Specific Networks

4. Click on the **Network Discovery** tab at the top of the Discovery Administration window.

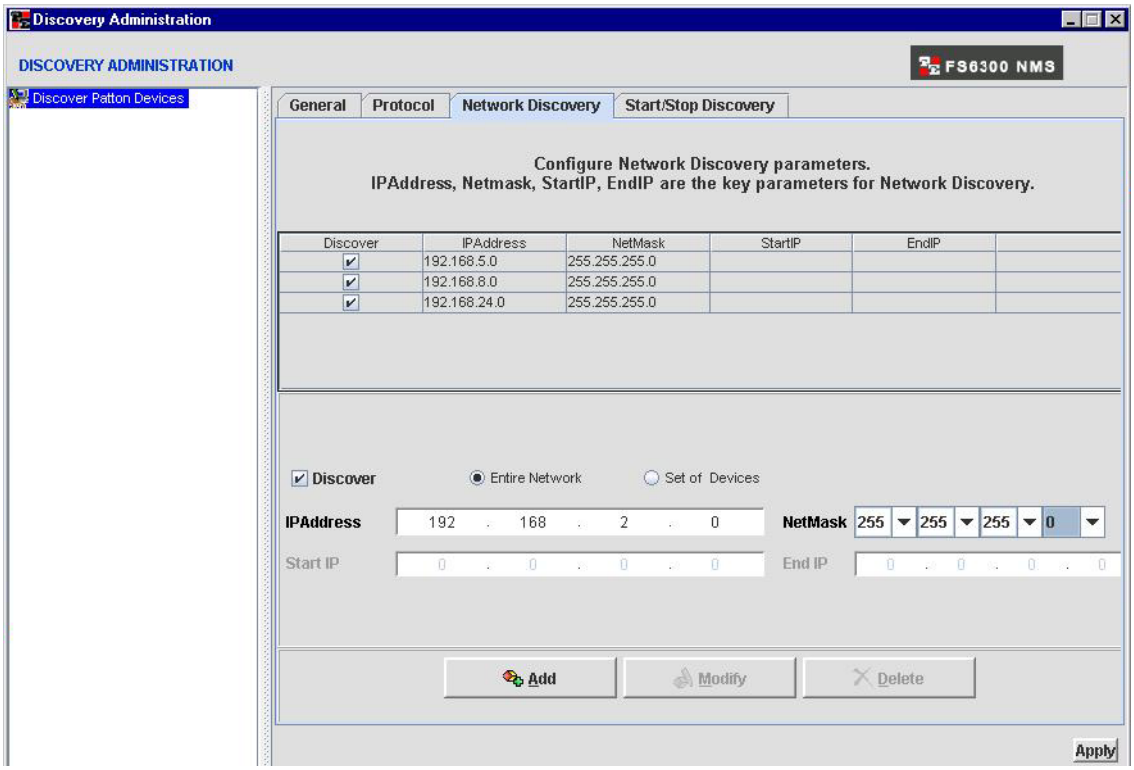


Figure 40. Network Discovery tab

5. Enter the **IP Address** of the network or set of devices you want the FS6300 NMS to discover. Click **Add**. Repeat this step to add more networks for the NMS to discover.

6. Click **Apply** to begin the Discovery process.

7. Returning to the main window, click on **Networks** (under *Network Database*) in the menu tree to see if the IP subnet has already been entered into the Networks table for discovery.

Note The discovery process may take some time, depending on how many nodes there are to discover on your network. During the Discovery process, a blue icon with an actively spinning wheel will be in the upper right-hand corner of the main window.

IMPORTANT

It is very important that you do not attempt to configure any parameter during the Discovery process. Attempting to do so could corrupt the data being collected during Discovery.

When the NMS has collected enough information to identify the node, the node will be listed in the Nodes table (under Network Database). As more information is collected through the Discovery process, entries will appear in the **FS6300 Geographical Areas** section (under *Network Maps*).

When the Discovery process is complete, the spinning wheel icon is replaced with a blue box containing a white checkmark. Once Discovery is complete, a new subnet can be entered into the Network Discovery window (**Tools > Discovery Administration**).

Setting Discovery Interval

You can set the wait time between discovering devices by configuring the Discovery Interval.

To set the discovery interval:

1. In the **General** tab of the Discovery Configurator,

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.

2. Click on the **General** tab, then enter the interval value (in seconds) in the **Discovery Interval** box. The value can be greater than or equal to zero and the default value is 1 second.

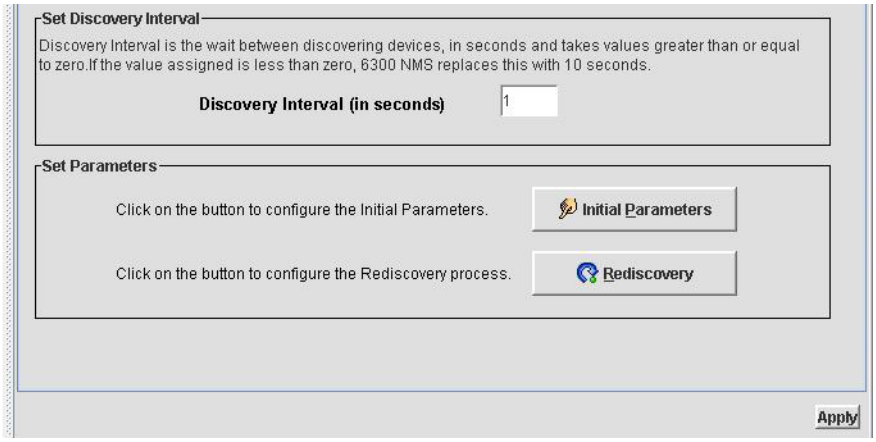


Figure 41. Set Discovery Interval

3. Click **Apply**.

Configuring Discovery of SNMP Devices

SNMPdevices may not be discovered through the default discovery process. To enable discovery of SNMP devices:

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **Protocol** tab, then click the **Edit Properties** button. The **SNMP Properties** window opens.

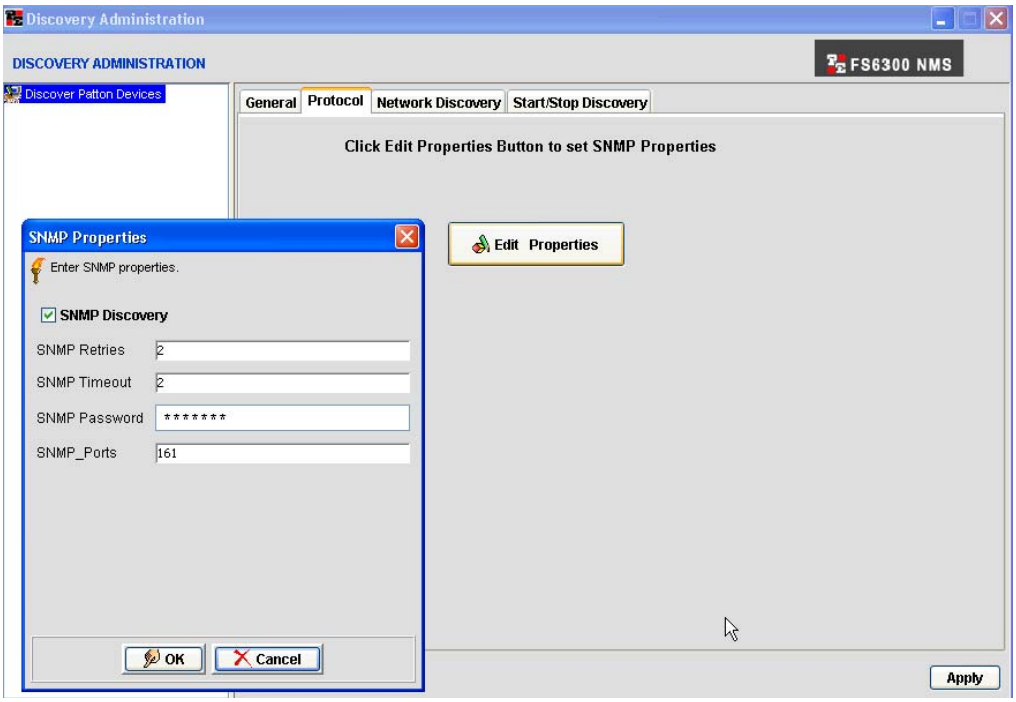


Figure 42. Configure Discovery for SNMP Devices

3. Enter information for the following parameters:

- **SNMP Discovery:** Select the checkbox to enable or disable discovery of SNMP devices.
- **SNMP Retries:** Specify the number of times the system will attempt to query the device if it does not respond to the first query.
- **SNMP Timeout:** Specify how many seconds the system will wait for a response before attempting to contact the device again.
- **SNMP Password:** Enter your password for configuring the SNMP device.
- **SNMP Ports:** Specify the ports to use to communicate with the SNMP agents.

4. Click **OK** to close the SNMP Properties window. Then, click **Apply** to save your changes to the server.

Adding a Device Manually

To add a single device to the NMS database:

1. Click on **SetUp(F)** > **Add Device** at the top of the screen.

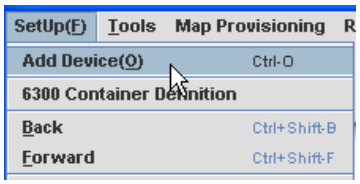


Figure 43. SetUp > Add Device

2. The **Add SNMP Device** window displays.

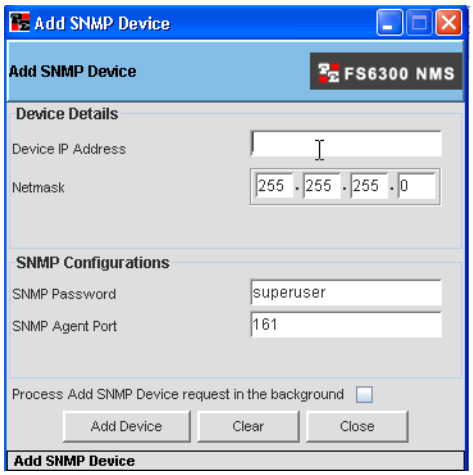


Figure 44. Add SNMP Device

Enter information for the following fields:

– **Device IP Address:** Enter the IP address of the device you want to add.

– **Netmask:** Enter the netmask for the device IP address. Default = 255.255.255.0

– **SNMP Password:** Enter the password to access the device.

– **SNMP Agent Port:** Enter the port number where the SNMP Agent is running. Default = 161

– **Process Add SNMP Device request in the background:** Select this box if you want continue with other operations in the NMS while the discovery process for the device runs in the background.

3. Click **Add Device**. If the device has been added to the system previously, a message will display that the node already exists in the database.

Stopping/Restarting a Discovery Process

You may want to stop a discovery cycle that is already in process to add or modify a network or set of devices.

> **Note** You cannot use the stop/restart discovery feature if the discovery process has already completed. This feature is only for discovery cycles that are in progress.

To stop/restart a discovery in progress:

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **Start/Stop Discovery** tab. **Select the network** that you want to edit from the drop-down menu. If the network is able to be paused in the discovery process, the **Start Discovery** and **Stop Discovery** buttons will be lit.

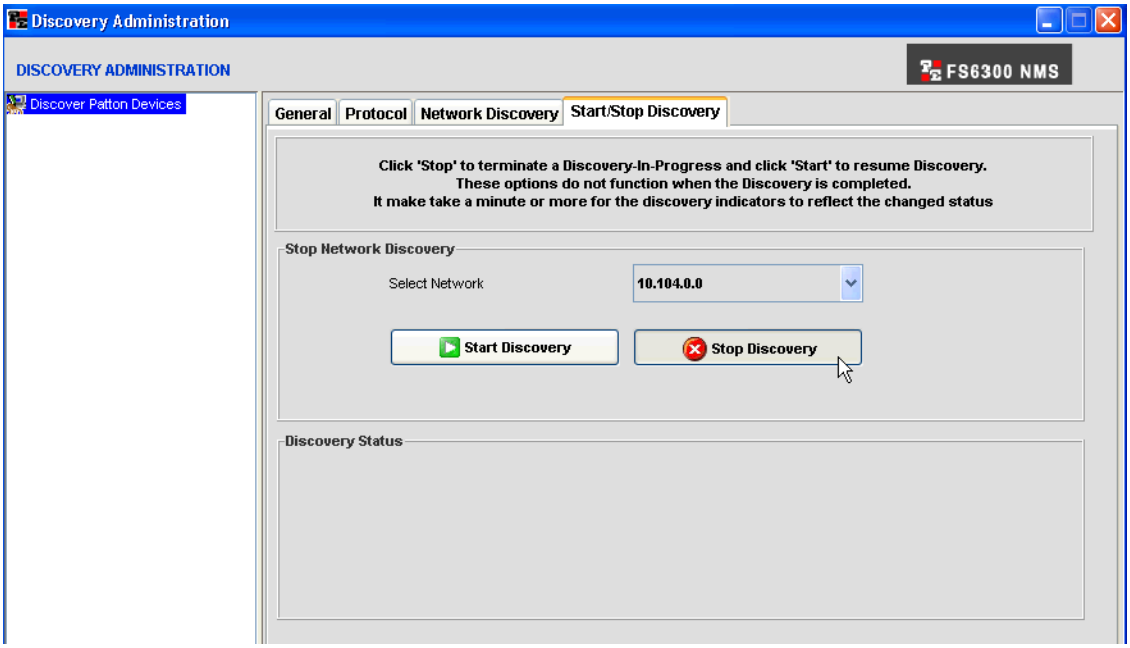


Figure 45. Stop Discovery in progress

3. A message will display in the **Discovery Status** area that discovery is currently disabled for the network.
4. Make the desired changes in the **Network Discovery** and/or **Protocol** tabs and click **Apply**.
5. Return to the **Start/Stop Discovery** tab. Select the network from the drop-down mneu and click **Start Discovery**. The discovery process will continue.

Re-Discovering Already Discovered Devices

By default, the rediscovery process discovers only devices that were not discovered previously. It does not rediscover the already discovered devices. To rediscover already discovered devices:

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then select the checkbox for **Re-Discover Already Discovered.** By default, this option is disabled.

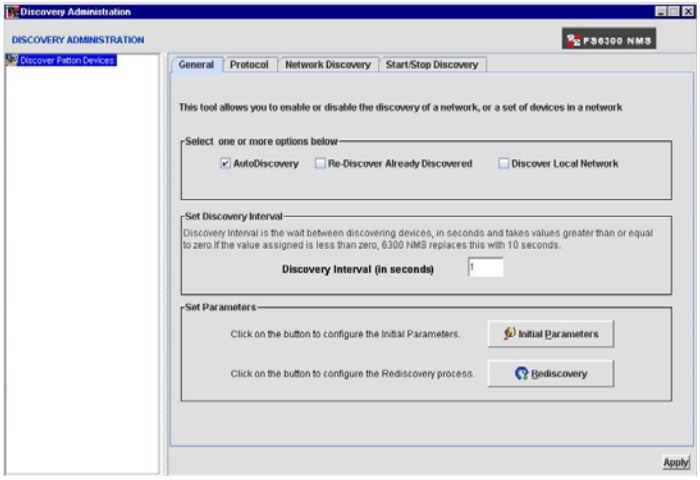


Figure 46. Re-Discover Already Discovered

3. Click **Apply**. This change will take place the next time the NMS goes through the re-discovery process. (See "Scheduling Rediscovery" on page 60).

Re-Discovering Cards Manually

You should re-discover cards after changing a card's configuration, or if you have added a new chassis or devices to the network. To manually re-discover cards:

1. Right-click on the device icon. You can do this in the Geographical Area, Network Node, Chassis, or Card sections of Network Maps.
2. Select **Re-Discover Cards** from the drop-down menu. A window displays with information about the card(s), including IP address, netmask, and SNMP Agent port.
3. Click **Re-Discover**. A message displays at the bottom of the box: "This action will take a few minutes. Please watch the status message. Status: Re-discovering..."

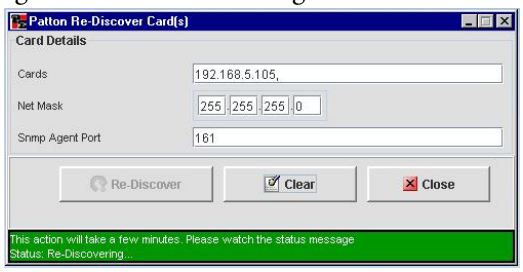


Figure 47. Re-Discover Cards

Scheduling Rediscovery

You can configure and schedule how often the network goes through the re-discovery process. The rediscovery process can also be configured to run at a specific hour on a specified date of the month or specified day of the week.

You can set the Rediscovery Interval using one of the following options:

- Regular Interval
- Specific Dates
- Days of the Week

Regular Interval

To schedule re-discovery for a regular interval (for example, every 24 hours):

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Rediscovery** button. The **Rediscovery Scheduler** window opens.

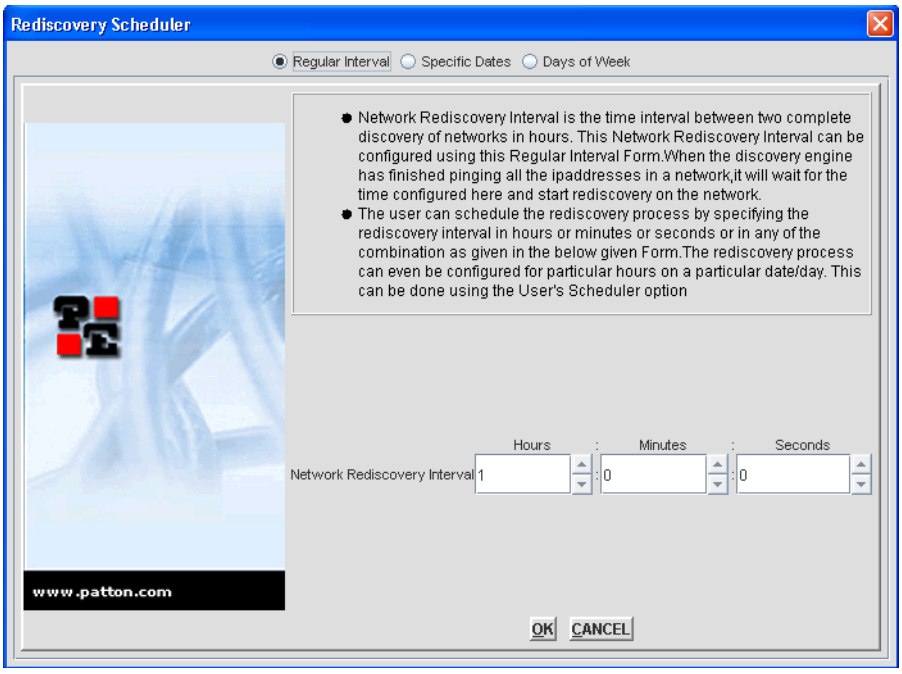


Figure 48. Schedule Re-Discovery for Regular Intervals

3. Select the **Regular Interval** radio button at the top of the window.
4. Specify the rediscovery interval in Hours, Minutes, and Seconds. By default, the interval is set as 24 hours. You can set any value from 1 to 24 in the hours field.
5. Click **OK**.

Note If the Rediscovery Interval is set using Regular Interval option, then the values set for Specific Dates and Days of Week options will not take effect.

Specific Dates

To set rediscovery on specific dates:

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Rediscovery** button. The **Rediscovery Scheduler** window opens.

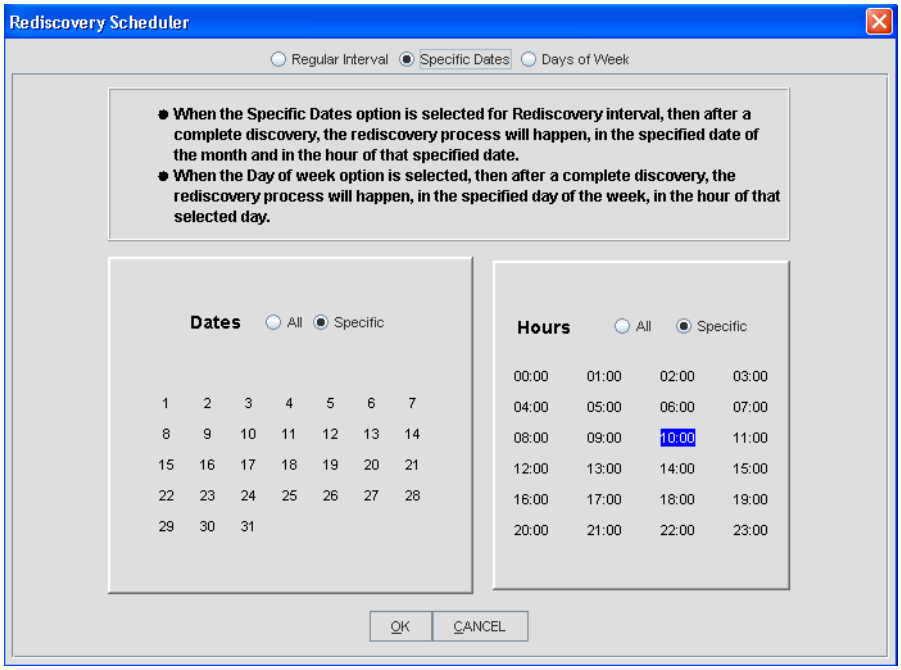


Figure 49. Schedule Re-Discovery for Specific Dates

3. Select the **Specific Dates** radio button at the top of the window.
4. Select the dates that you want re-discovery to occur:
   - **All Dates:** Select the radio button for **All**. Re-Discovery will occur every day.
   - **Specific Dates**: Select the radio button for **Specific**. Then, click on all of the dates in the month that you want re-discovery to occur. For example, if you select 5 and 15, then the rediscovery will take place on the 5th and 15th of every month.
5. Select hours for the selected dates:
   - **All Hours:** Select the radio button for **All** for re-discovery to occur every hour on the specified date(s).
   - **Specific Hours:** Select the radio button for **Specific.** Then, click on all of the hours that you want re-discovery to take place on the specified date(s).
6. Click **OK**.

Days of the Week

To set re-discovery on specific days:

1. Click on **Tools > Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Rediscovery** button. The **Rediscovery Scheduler** window opens.

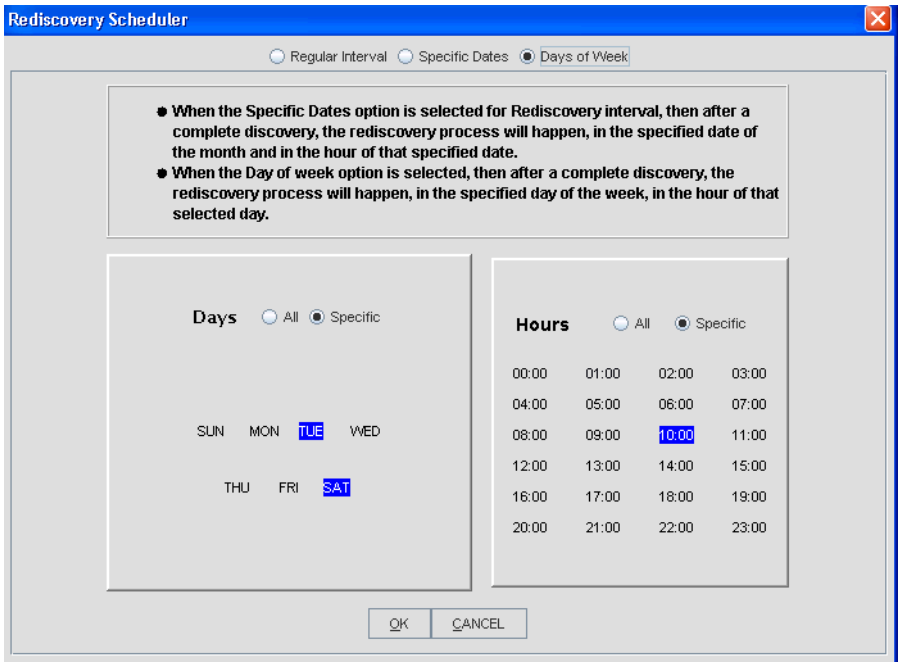


Figure 50. Schedule Re-Discovery for Days of the Week

3. Select the **Days of the Week** radio button at the top of the window.
4. Select the day(s) that you want re-discovery to occur:
   - **All Days:** Select the radio button for **All**. Re-Discovery will occur every day.
   - **Specific Days:** Select the radio button for **Specific**. Then, click on all of the days of the week that you want re-discovery to occur. For example, if you select MON TUES WED, the re-discovery occurs only on those days, every week.
5. Select hours for the selected days:
   - **All Hours:** Select the radio button for **All** for re-discovery to occur every hour on the specified day(s).
   - **Specific Hours:** Select the radio button for **Specific.** Then, click on all of the hours that you want re-discovery to take place on the specified day(s).
6. Click **OK**.

Note When both dates and days are configured, then the **Specific Dates** settings will take place and the Days of the Week settings will be ignored.

Configuring Multiple Cards

If you have separate subnets that are supposed to be in the same Geographical Area but in a specifically named Node and Chassis, you will want to update the subnet information so that is displayed as it actually is located in the network.

Updating the Configuration

To configure multiple cards:

1. Select **Tools** from the menu at the top of the screen, then **Multiple Card Configuration**. The Multiple Card Configuration window appears.

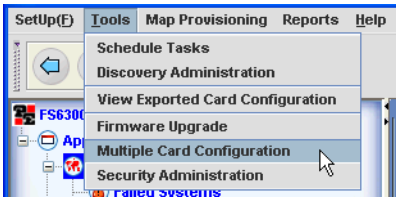


Figure 51. Tools > Multiple Card Configuration

2. Click on **Card Parameters** in the menu tree on the left side of the screen.

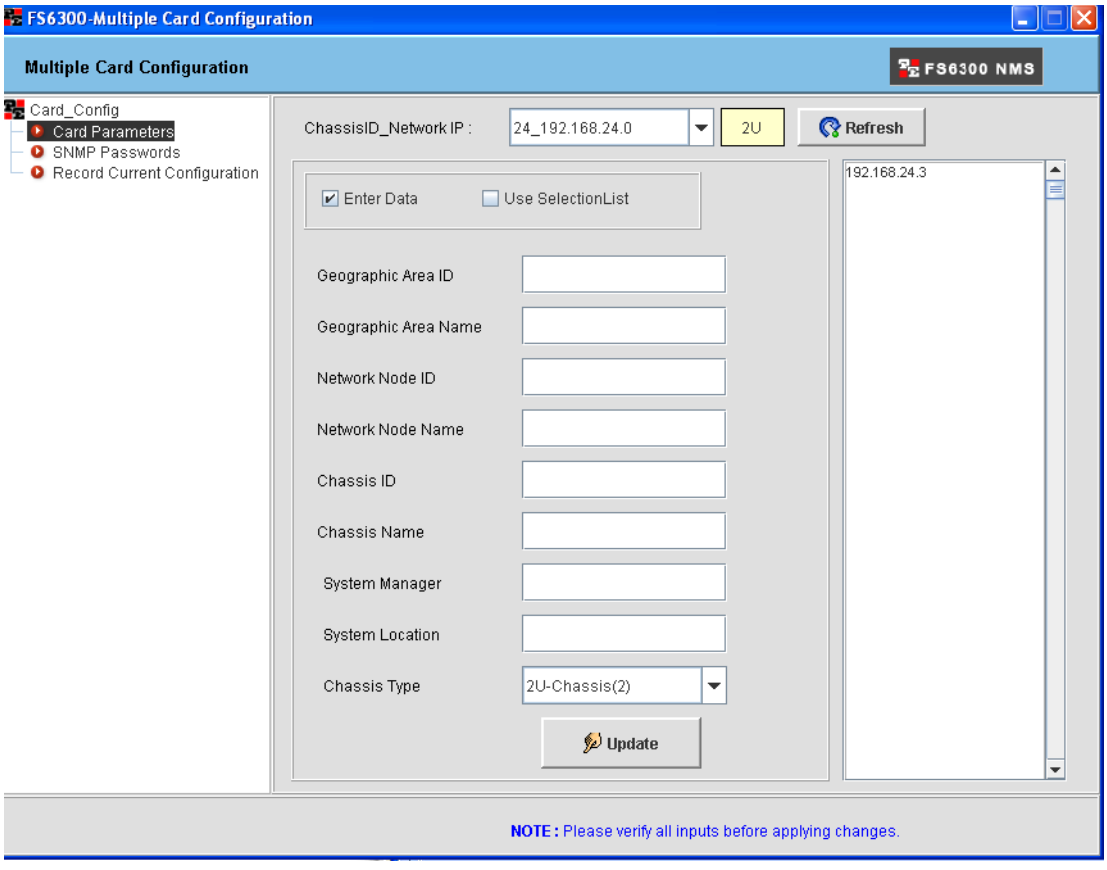


Figure 52. Multiple Card Configuration > Card Parameters

3. Select the subnet you would like to update from the **Network IP** drop-down menu. The list on the right side of the screen shows the IP addresses of all the devices discovered on that specific subnet.
4. Enter the information you would like to update on the subnet for the following fields:
   - Geographical Area ID (Integer that identies the geographical area)
   - Geographical Area Name (Descriptive name of the geographical area)
   - Network Node ID (Integer used to identify the node on the network)
   - Network Node Name (Descriptive name of the node)
   - Chassis ID (Integer used to identify the chassis on the network)
   - Chassis Name (Descriptive label for the chassis)
   - System Manager (Name of the person managing this subnet on the network)
   - System Location (Description of where the system is located)
   - Chassis Type (Choose a chassis type from the drop-down menu)
5. Click **Update** to save the information for all of the cards on that subnet.

Note After clicking Update, it is very important to save this information in the cards' non-volatile memory so that the values will not be lost in case of a power failure or card reboot.

Saving the Configuration

To save the information to non-volatile memory:

1. Click on **Record Current Configuration** in the menu tree on the left side of the screen. This will save all current configurations in non-volatile memory for the devices listed in the panel on the right side of the screen.

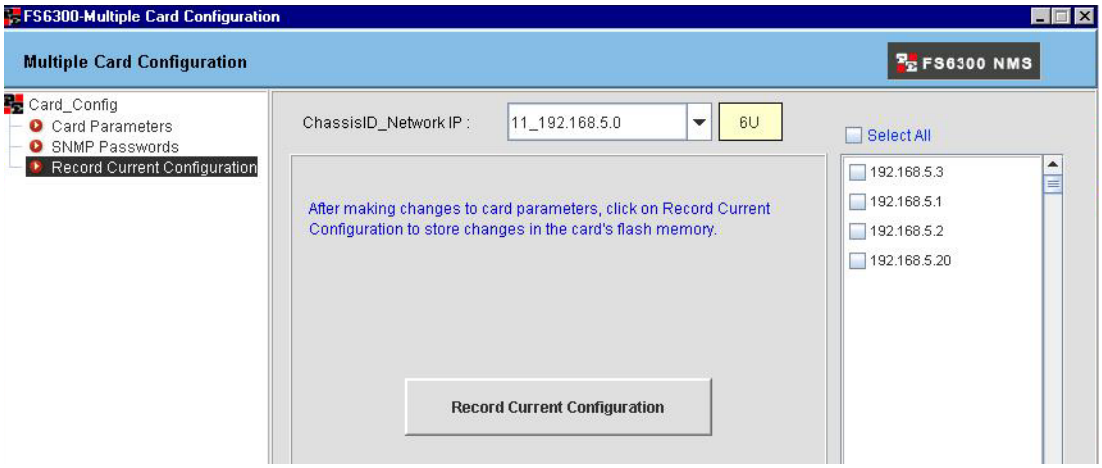


Figure 53. Multiple Card Configuration > Record Current Configuration

Forcing Discovery for Selected Cards

Though the cards have the updated information saved, the NMS will not display the changes until the cards have been re-discovered. To re-discover specific cards and not the entire subnet, see "Re-Discovering Cards Manually" on page 59.

Upgrading Firmware

The FS6300 NMS supports the following Patton models:

Supported Rack Cards	Supported CPE Devices
6511	3201
3196RC	3088
3096RC	3086
2616RC	1082 (C/D/I/F)

The rack cards must have the following minimum firmware version installed in order to operate properly:

Card	Minimum Firmware Version Required
6511	6511RC-1.2.9.img
3196RC	3196RC-1.3.9.img
3096RC	3096RC-1.5.16.img
2616RC	2616RC-1.3.9.img

To update the firmware for a rack card:

1. Click on **Tools** > **Firmware Upgrade** at the top of the screen.

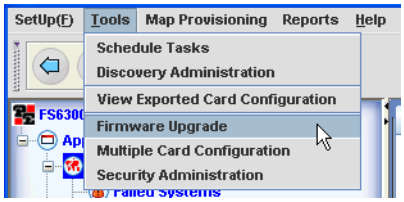


Figure 54. Tools > Firmware Upgrade

2. The **FS6300 Firmware Upgrade** window displays.

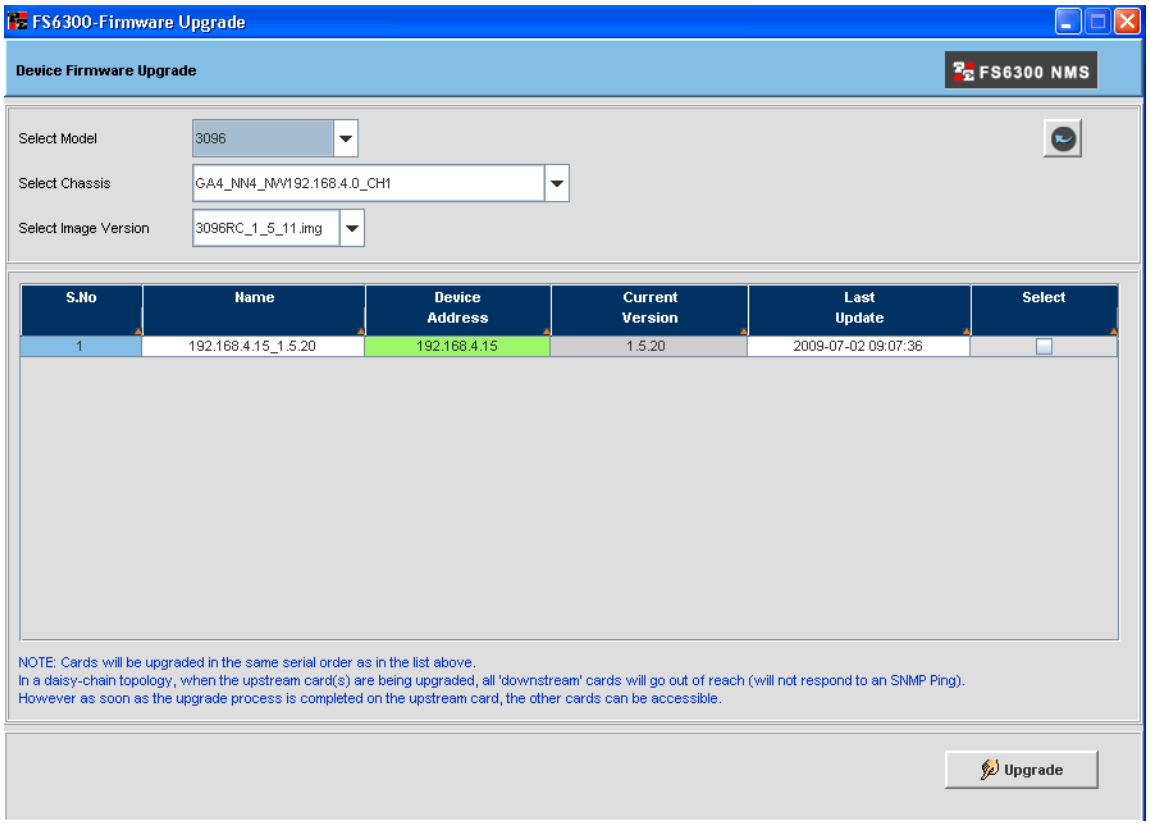


Figure 55. Firmware Upgrade window

3. Select the desired **Model**, **Chassis**, and **Image Version** from the drop-down menus. Available cards will display in the firmware table.
4. **Select the checkbox** in the table for the card(s) you want to upgrade.

> **Note** The NMS will upgrade the cards in the same order that they are listed in the table. In a daisy-chain topology, when the upstream card(s) are being upgraded, all "downstream" cards will be temporarily unavailable and will not respond to an SNMP ping request. However, the other cards will be accessible as soon as the upgrade is completed for the upstream card.

5. Click **Upgrade**.

Chapter 4 Configuring Maps

Chapter contents

Introduction

To route traffic from one device to another device in the NMS, you must define DS0 maps (also called an internal connection or cross-connection). An internal cross-connection carries traffic between the two external devices via a card in the system. The external devices can be (but are not limited to) a T1/E1 NTU, a G.SHDSL customer premise equipment (CPE) modem, or another blade in the same cPCI chassis in which the card(s) in the NMS is installed.

External devices can connect to a device in the NMS via a T1/E1 WAN port, a DSL port, an STM-1 trunk, or an H.110 port. (A device will connect to an H.110 port via the card's interface to the H.110 bus in the cPCI chassis midplane). Each DS0 mapping defines a one-to-one connection between a selected number of timeslots on one port and a corresponding number of timeslots on a different port.

Click on **Map Provisioning** at the top of the main screen to view options for configuring DS0 maps.

Map Types in the FS6300

There are three types of maps in the FS6300 NMS.

- **Same-Card Maps:** A map created between any two TDM ports (T1E1, GSHDSL, iDSL) on the same card.
- **Inter-Card Maps:** A pair of maps created between two TDM ports on two different cards, in the same 2U or 4U chassis unit, or on two different cards in the same segment of a 6U chassis unit.

  Inter-card maps use the H.110 back plane ports and time slots.

  H.110 Tx Port number and Time slots used by one map are used as Rx Port Number and Time slots by the second map. Similarly, the Rx Port and Time slots used in one map are used for Tx on the second map.

  To create inter-card maps, FS6300 auto-allocates H.110 time slots from the chassis back plane.
- **End-to-End Maps:** A map between ports of any two cards placed in different ForeFront chassis/chassis segments.

Displaying Map Details in the FS6300 Network Maps View

By default, the **Network Maps > FS6300 Geographical Areas** view displays maps between areas and devicesin the NMS. Right-click on a link to view link details and properties such as alarm severity level, connection type, source and destination information, and time slots.

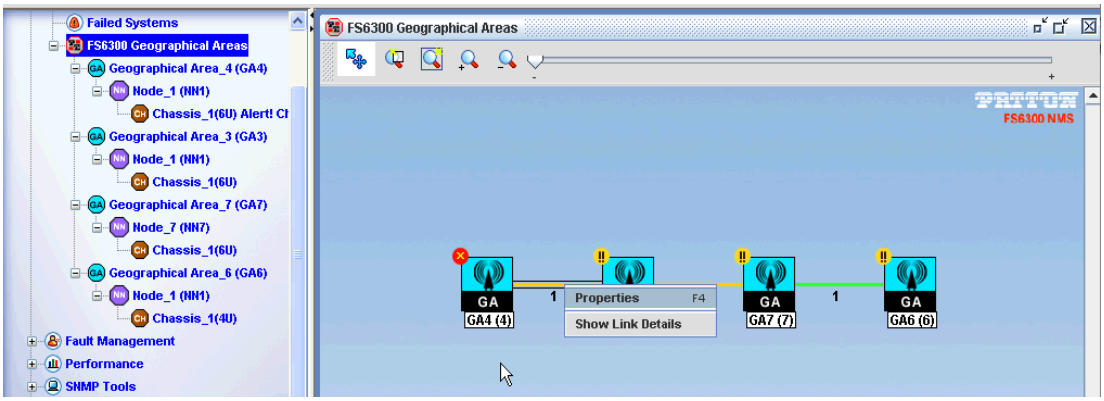


Figure 56. Link Details in the Network Maps View

Auto-Screening DS0 Maps

The FS6300's AutoScreening feature can automatically detect maps that are discovered from an existing network setup that has cards running any firmware version. The Auto-Screening function also internally segregates maps into same-card and valid inter-card DS0 maps. Then, it automates the task of generating a unique Map Description/System ID for every DS0 map, and setting the ID on the card and in the FS6300 database, without any user intervention.

To automatically screen for DS0 maps:

1. Select **Map Provisioning > Auto-Screen Maps And Channels** from the menu at the top of the screen.

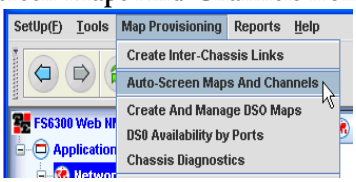


Figure 57. Tools > Discovery Administration

2. The **AutoScreening** window displays the discovery status of the FS6300 managed network (Discovery: completed / in-progress).

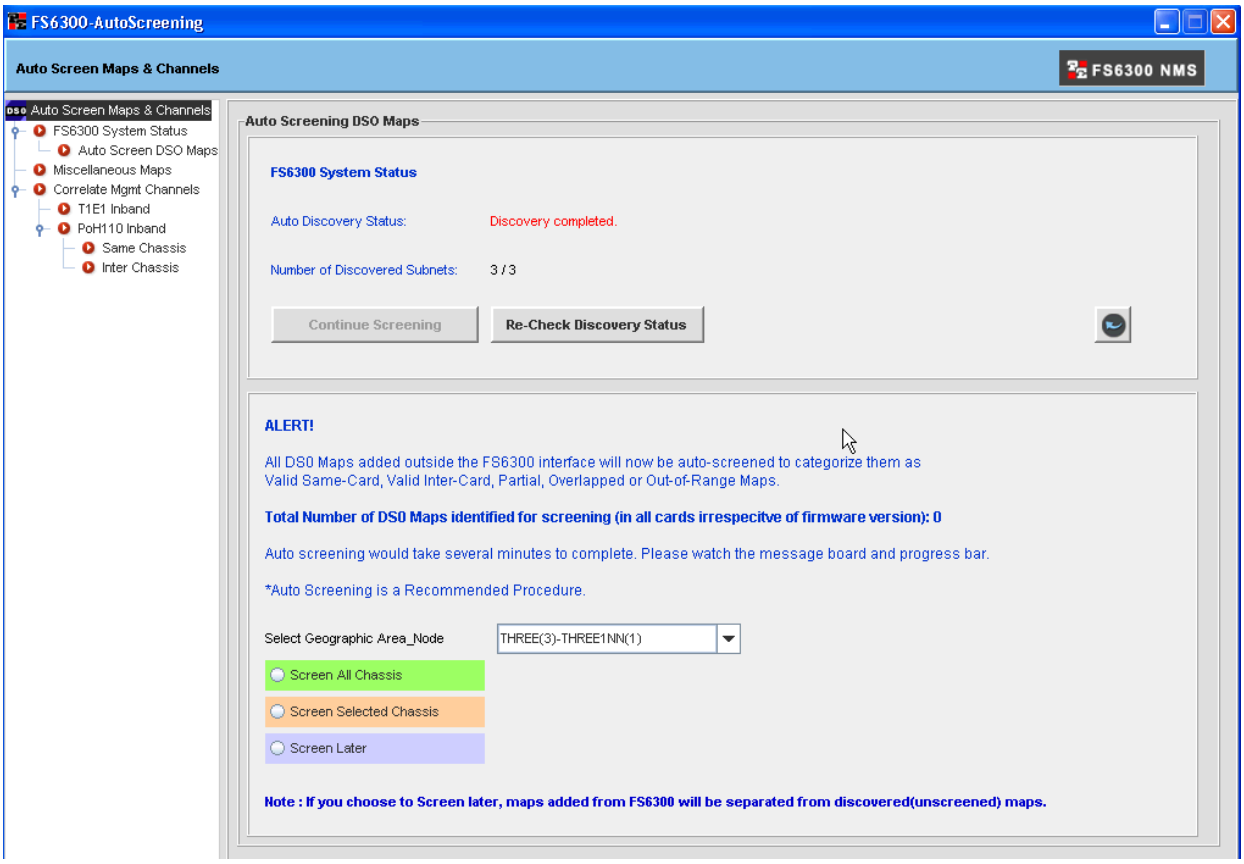


Figure 58. Auto-Screening window

– If auto-discovery is in-progress, the screening procedure is stalled until discovery of at least one subnet is completed. You cannot select a screening option at this time.

– When one subnet is discovered, you may proceed with screening of that subnet or wait until discovery is completed for other subnets. When discovery of at least subnet is completed, you may select a screening option (**Screen All Chassis / Screen Selected Chassis / Screen Later**).

3. Select a screening option:

– **Screen All Chassis**– Automatically screen all cards on all chassis' in the system

– **Screen Selected Chassis**– Select a chassis from the drop-down menu to screen. You also have the option to re-discover cards in that chassis before screening, so that any new maps added outside the FS6300 interface (after the last discovery), are also included for screening.

– **Screen Later**– No maps will be screened at this time. The unscreened maps are displayed under **Miscellaneous Maps**. These maps are not classified as same-card, inter-card, partial, etc.. You can review the list but cannot delete any map in the FS6300 database until they are screened.

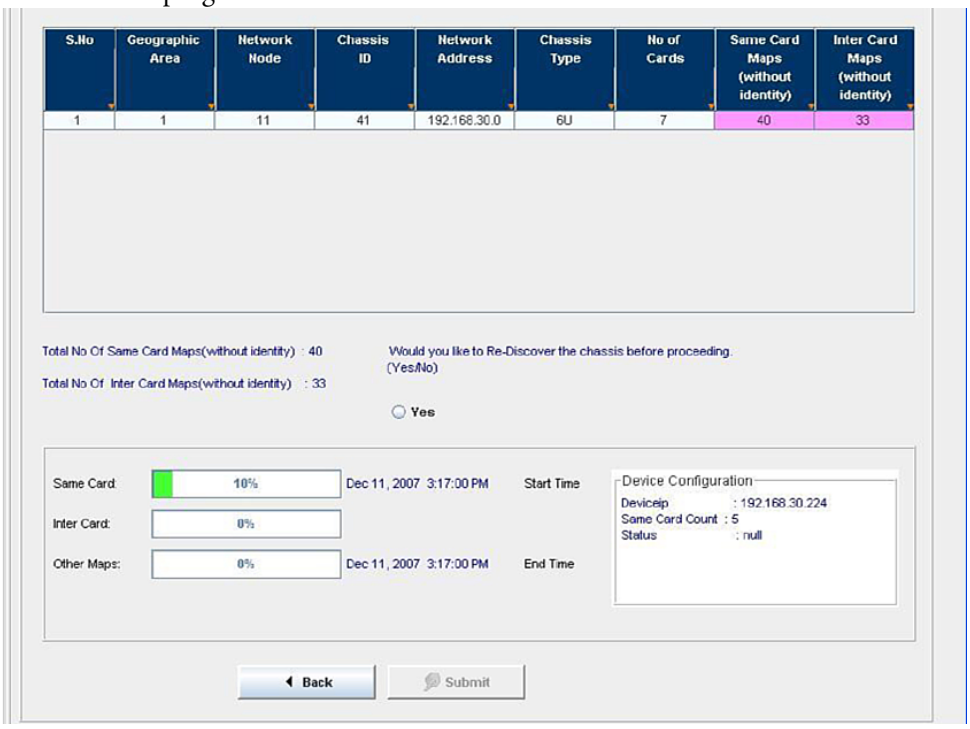
4. After selecting a screening option, the maps identified for screening are organized into same-card, inter-card, partial, overlap and out-of-range maps and displayed in a table format for review.

– *Out-of-range map***s** are those that have time slots specified beyond the permissible range - T1E1 > 32, GsDSL > 36, iDSL >3.

– *Overlapped maps* are those that use the same H.110 Ports and Time slots in two or more DS0 maps on different cards in the same chassis.

– *Partial maps* are those that use H.110 Ports and Time slots without a complementary map created on another card in the same chassis.

5. Click **Submit**. The identified maps are assigned an FS6300 System ID, which is set in the database and also configured on the cards. The various stages of processing are displayed in the user interface in a message board and also as progress bars.



6. When screening is completed, a success message is displayed and the user interface is re-initialized. Screened maps which are Same-Card, Inter-Card or Partial, are displayed in the **View-Delete Maps** section. Out-of-range maps and Overlapped maps are displayed in the **Miscellaneous Maps** section.

Managing Miscellaneous Maps

In the FS6300 AutoScreening menu, the **Miscellaneous Maps** section displays Out-of-range, Overlapped maps and Unscreened maps, if any, in a selected chassis.

Out-of-Range Maps

Out-of-range maps should be deleted first; in order to free the system of incorrectly defined maps.

Overlapped Maps

- If the auto-screening program finds a valid DS0 map pair and in addition, one or more DS0 maps on some other cards in the same chassis using exactly the same H.110 Tx and Rx Port numbers and Timeslots, all the maps are tagged as overlap.

  You will need to manually examine the multiple DS0 maps, and select the correct pair (if any). Then, submit the valid pair back into the system.

  FS6300 internally verifies that the selected pair is valid - That the two maps have the same Chassis ID, are in the same subnet, are created on two different cards, the H.110 Tx and Rx Ports and Timeslots on the two maps are exactly complementary.

  After the verification, FS6300 auto-generates a new map description and updates the map on the card and in the database. The valid pair gets auto-appended into the appropriate 'View Delete' section.

  In this process of manually pairing some correct maps, some maps may be left over. You have to carefully select and delete the extra maps to correct the overlap condition.

- If one or more T1E1 timeslots are used in a same-card DS0 map and also in a T1E1 in-band, FS6300 displays a T1E1 overlap condition.

  In such a scenario, you will need to first delete the incorrect record - either the DS0 map or the in-band channel. Then, select the DS0 map and submit back into this system.

  FS6300 internally verifies the correctness of the record and assigns an auto-generated system id. The card is configured and if successful, the database is updated.

In the AutoScreening window, click on **Miscellaneous Maps** in the menu on the left. Select **Overlapped Maps**. There are two tables in this section that show overlapping DS0 maps.

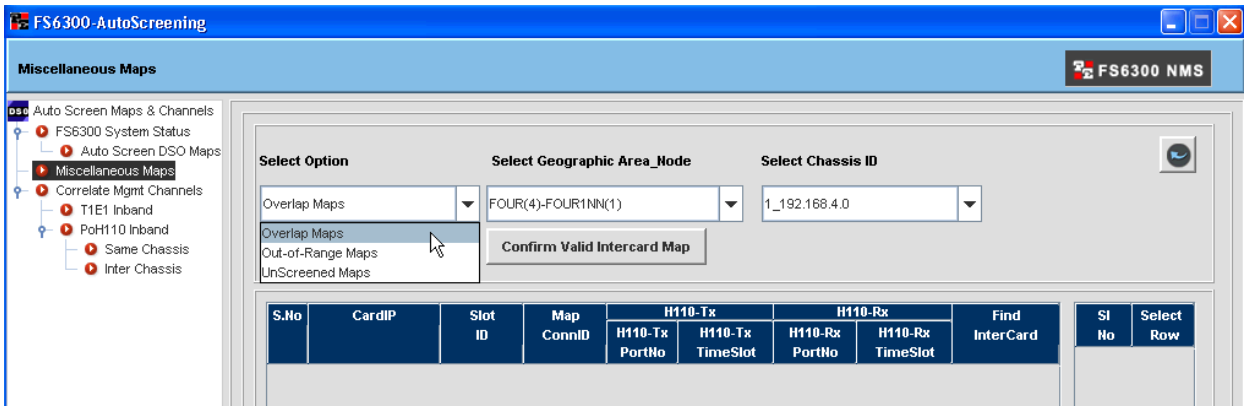


Figure 59. Miscellaneous Maps window

To identify overlapping maps:

1. Select **Overlap Maps** from the Miscellaneous Maps window.
2. The table will display all of the overlapped maps. Select a row of an overlapped map, and click **Delete Overlap**.
3. Next, select the two rows that are highlighted green and click **Confirm Valid Intercard Map**. If the request is processed successfully, the two identified maps are now assigned a new Inter-Card System ID, which is updated in the database and also configured on the cards. The rows are cleared from the Overlapped Maps table.
4. The paired DS0 maps are now displayed in the View-Delete section under Inter-Card maps.

Managing Maps

In the NMS, you can create DS0 map connections on the same card, inter card, or inter chassis. Click on **Map Provisioning > Create and Manage DS0 Maps** to bring up the DS0 Mapping window.

Creating Same Card Maps

To create maps on the same card:

1. Click on **Same Card** (under Provision Maps) in the menu tree of the Map Provisioning window.

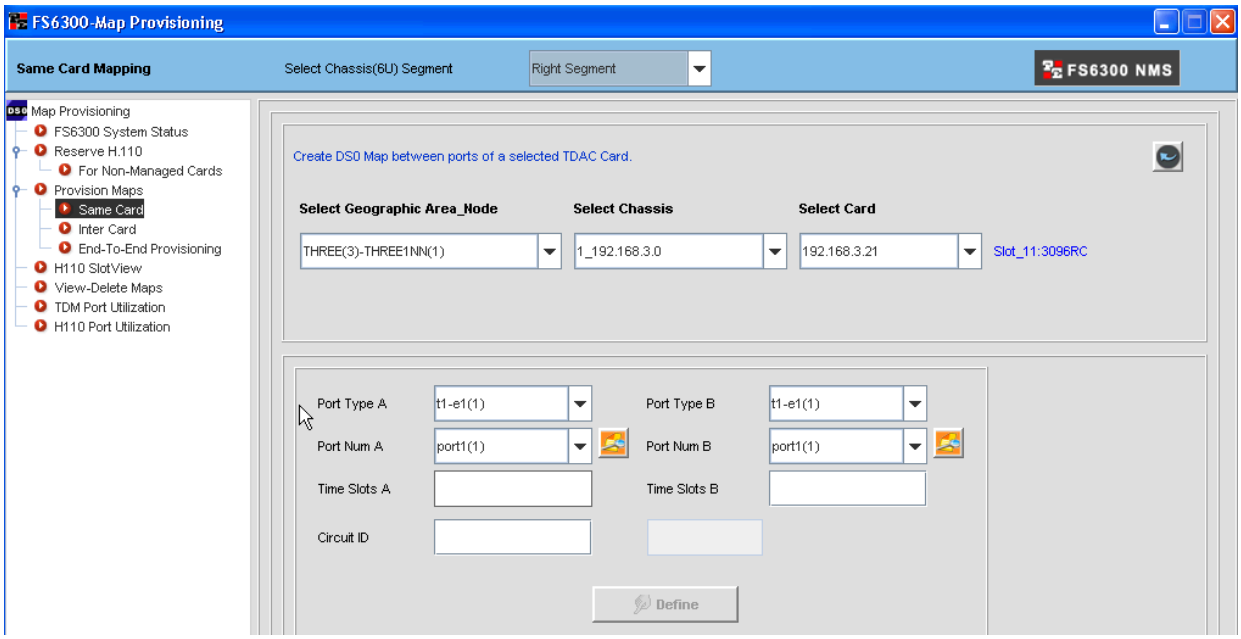


Figure 60. Same Card window

2. Select a chassis from the **Select Chassis** drop-down menu. If the selected chassis is type **6U**, select the right or left segment from the drop-down menu in the blue section at the top of the window.
3. Select a card in the chassis from the **Select Card** drop-down menu.
4. Choose the device type to use from the **Dev Type A** and **Dev Type B** drop-down menus. The available options for device types will vary, depending on the card's model.

5. Select which ports to use on the device from the **Dev Num A** and **Dev Num B** drop-down menus. Select the orange square icon to view available ports. A pop-up window will display.
6. Enter the range of time slots to use on the card in the **Dev Slots A** and **Dev Slots B** text fields.
7. Enter a **Circuit ID** for the map.
8. Click **Define**.
9. The new map will be added to the table in the **View-Delete Maps** section.

Creating Inter Card Maps

To create maps between cards in the same chassis:

1. Click on **Inter Card** in the menu tree of the Map Provisioning window.

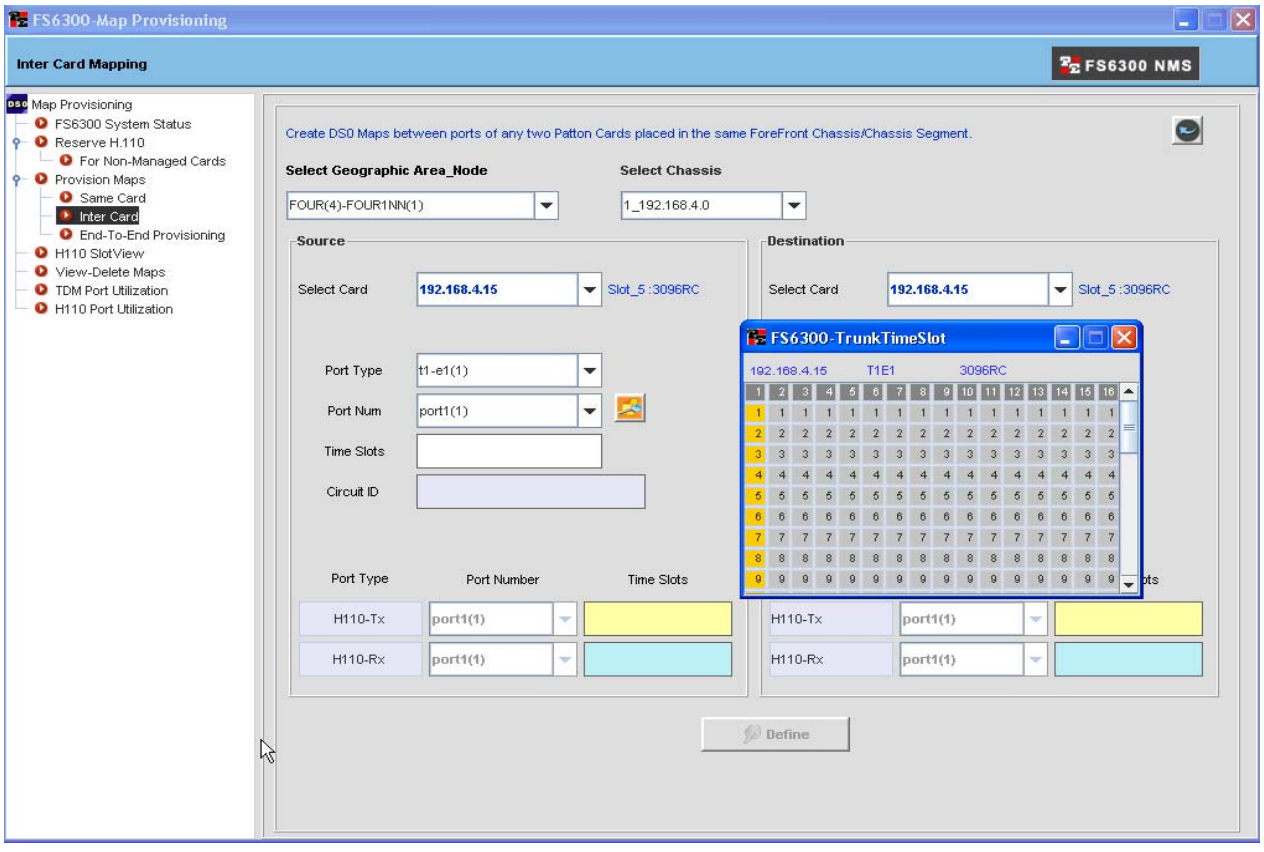


Figure 61. Inter Card window

2. Select a chassis from the **Select Chassis** drop-down menu. If the selected chassis is type **6U**, select the right or left segment from the drop-down menu in the blue section at the top of the window.
3. Select a card in the chassis where you want to start the mapping in the **Select Card** drop-down menu in the **Source Card** section (left side) of the window.
4. Select a port type for the source card from the **Port Type** drop-down menu.

5. Select which port to use on the device from the **Port Num** drop-down menu.

   Select the orange square icon to view available ports. A pop-up window will display.

6. Enter the range of time slots to use on the card in the **Time Slots** text field.

7. (optional) Enter a Circuit ID or Description if needed. The same description is assigned to the two cards.

8. Repeat Steps 3-6 for the **Destination Card** on the right side of the window.

9. Click **Define**.

10. The new map pair will be added to the table in the **View-Delete Maps** section.

Creating End-to-End Maps

End-to-end maps are DS0 maps the FS6300 creates based on available time slots on two different cards in two different chassis in the same Network Node. Pre-defined **Reserved Pools** must exist between the two chassis to create an end-to-end map (see Reserving Pools on page 77). Also, the pools reserved between the two inter-connected chassis must have free timeslots that can be used for creating end-to-end maps.

To create maps between different chassis:

1. Click on **Map Provisioning > Create and Manage DS0 Maps** from the top of the screen. The FS6300 Map Provisioning window displays.

2. Click on **End-to-End Provisioning** (**under Provision Maps**) in the menu tree of the Map Provisioning window.

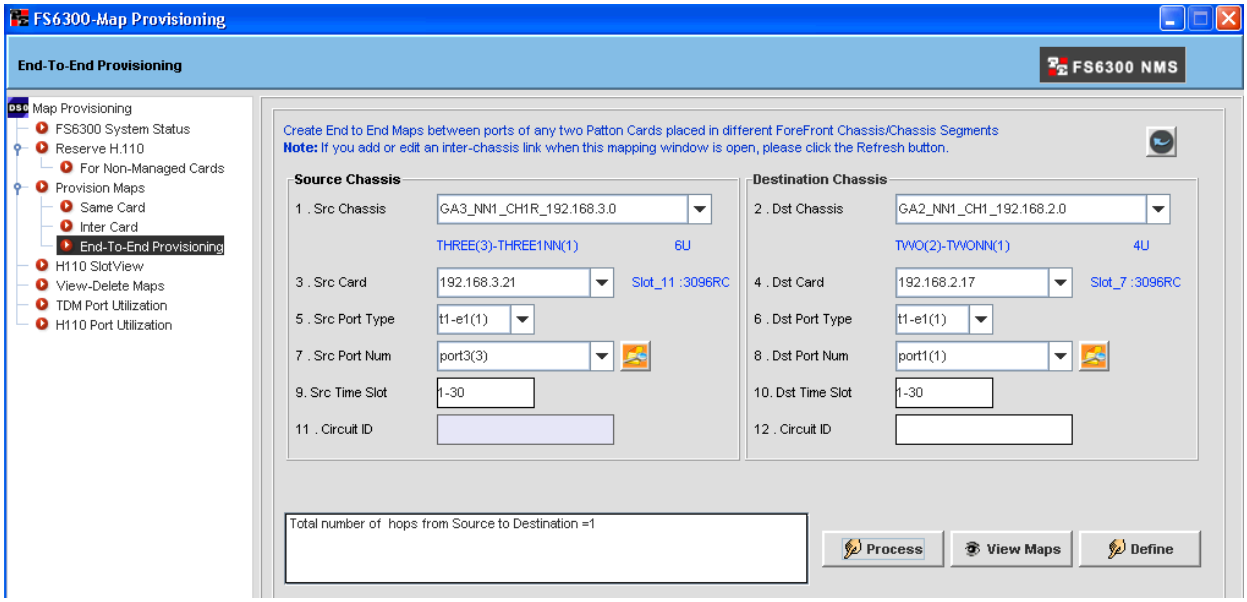


Figure 62. Map Provisioning > End-to-End Provisioning

3. Select a **Source** and **Destination** chassis.

4. All cards discovered in the selected Source and Destination chassis are listed in the drop-down menu. Select a **Source Card** and a **Destination Card**.

5. All Port Types discovered on the selected Source and Destination cards are listed in the **Port Type** drop-down menu. Select the **Source Port Type** and **Destination Port Type**.
6. Select **Ports** on the source and destination cards.

   Use the orange square icon to view available ports. A pop-up window will display. If you select **T1-E1**, as the **Port Type**, the port number that has a pre-defined trunk on the selected card is excluded from the selection list.
7. Enter the **Time Slot range** on **Source Port** followed by **Time Slot range** on **Destination Port**.
8. (optional) Enter a **Circuit ID** (Description) if needed. The same description is assigned to all of the cards you are mapping.
9. Click **Process** to preview the map. The FS6300 will display the number of hops between the source and destination chassis.
10. Click **View Maps** to see details of the new end-to-end map.
11. Click **Define** to save the map to the card configuration. A confirmation message will display if the configuration is successful.

Removing Maps

To delete maps between different elements (GA, NN, and CH):

1. Click on **Map Provisioning > Create and Manage DS0 Maps** from the top of the screen. The FS6300 Map Provisioning window displays.
2. Click on **View-Delete Maps** in the menu tree of the Map Provisioning window.

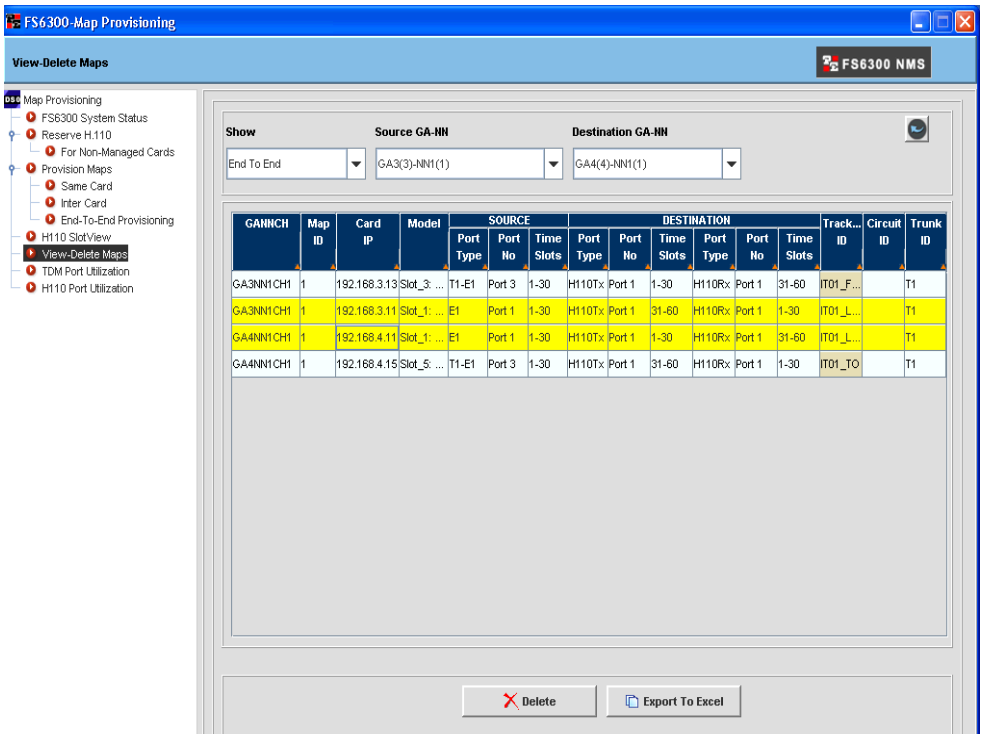


Figure 63. Map Provisioning > View-Delete Maps

3. Select the desired map type from the **Show** drop-down menu. Then, select the **Source** and **Destination** elements to view maps.
4. Select the rows of the desired maps to delete, or hold down Shift and click the top and bottom rows to select all of the maps shown in the table.
5. Click **Delete**. A confirmation message displays. Click **OK**.

Managing Inter-Chassis Links

Reserving Pools

You can create *reserved pools* between chassis or between chassis segments by identifying time slots on selected T1E1 or STM-1 Ports for purposes of inter-chassis mapping.

1. Click on **Map Provisioning > Create Inter-Chassis Links** from the top of the screen. The FS6300 Inter-Chassis Links window displays.
2. Click on **Manage Reserve Pools** in the menu tree of the Inter-Chassis Links window.

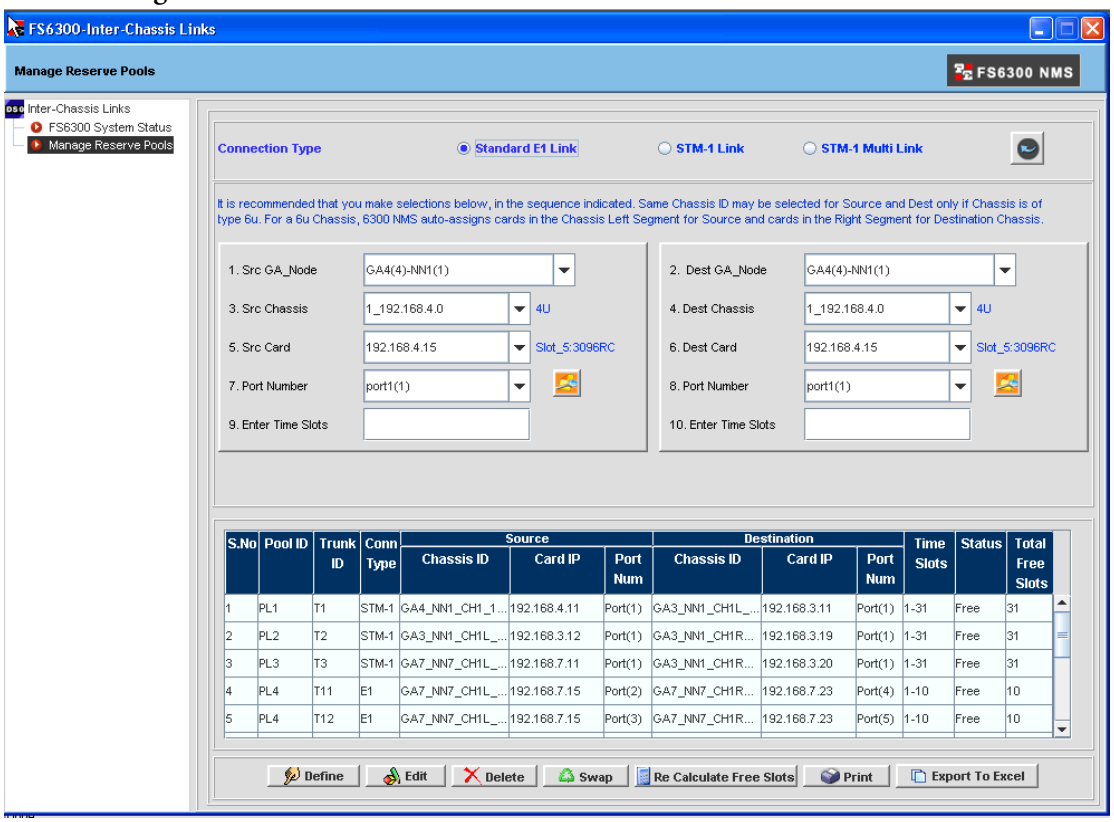


Figure 64. Reserve Pools

3. Select a **Connection Type**: - **Standard T1E1** (for all cards except 6511), **STM-1 or STM-1 Multi Link** (6511 cards only).
4. Select the **Network Node** name from the drop-down menu.
5. Select the **Source Chassis** and **Destination Chassis.**

6. Select the **Source Card** and **Destination Card**.
7. Identify **Trunk Ports** on the source and destination cards.

   Select the orange square icon  to view available ports. A pop-up window will display. Available ports will be shaded in gray.
8. Enter exactly the matching time slots for Source and Destination Trunk ports. While adding time slots from the trunk ports into the Pool, FS6300 verifies that the timeslot specification is exactly matching. The acceptable input for time slot specification is either a number or a range of numbers.
9. Click **Define**.

The FS6300 assigns a Pool ID and Trunk ID for the newly created pool. The record is listed in a table in the Reserve Pools window. You cannot change the Pool and Trunk IDs.

You may repeat steps 2 through 8 to add more trunks and timeslots into the pool from the same source and destination cards; or, to add new trunks and timeslots from different cards in the selected chassis.

The reference to Source and Destination chassis is for the purpose of tracking the two inter-connected chassis and does not imply that one is the actual Source chassis and the other is the Destination chassis. For example:

If Trunk T1 is created between two chassis, CH1 and CH2 (Source and Destination), and Trunk T2 is created between CH2 and CH1 (Source and Destination), only one Pool is created called CH1-CH2 for both T1 and T2.

If the selected Chassis ID is a 6U on one side or both sides, a suffix, L (Left) or R (Right), is added to the end of the Chassis ID.

The order in which you create the reserved pools is the order the FS6300 will use to prioritize the inter-chassis links.

The status of the Pool is initially 'Free'. Based on utilization of reserved slots, FS6300 updates the status to "Partial' or 'Used'. You are allowed to:

- Remove an unused Pool
- Add more timeslots from an already reserved Trunk Port to the Reserve Pool.
- Remove/cancel timeslots added from a Trunk to a pool if not already used.

Synchronizing Maps and Trunks

Due to database backups, restores or manual configurations, the number of free slots available in the NMS database may not accurately correspond with the source or destination cards in the trunk. The NMS updates the number of available slots during the discovery/re-discovery process. The **Re-Calculate Free Slots** feature compares the timeslot utilization between two cards of the trunk.

> **Note** If incorrect but matching map configurations exist on both of the cards, the re-calculation feature will not display those configurations. For example, it will not show a partial map on each of the cards that utilizes the same timeslot created initially by the NMS. Also, currently the re-calculation feature does not consider the timeslots on the trunk that are used for In-band or PPP links.

To view number of free slots between devices:

1. Click on **Map Provisioning > Create Inter-Chassis Links** from the top of the screen. The FS6300 Inter-Chassis Links window displays.
2. Click on **Manage Reserve Pools** in the menu tree of the Inter-Chassis Links window.
3. Select the row of a trunk in the table and click **Re-Calculate Free Slots**.
4. A detailed confirmation message displays if the trunk is utilized correctly.

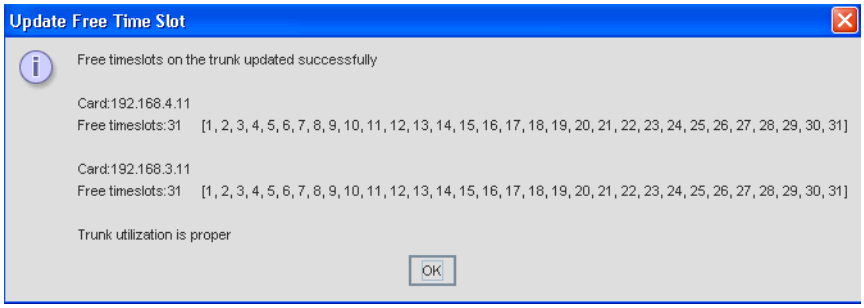


Figure 65. Trunk Utilization Confirmation Message

5. If the NMS finds a conflict with the trunk, a detailed message displays.

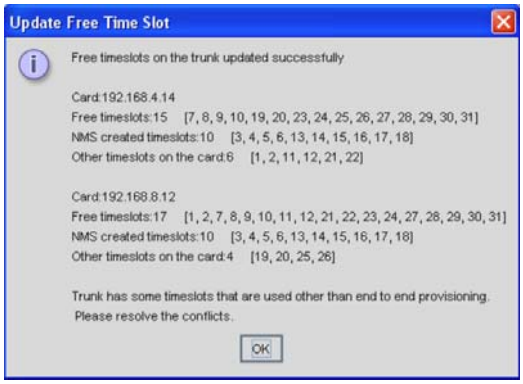


Figure 66. Trunk Utilization Conflict Message

Removing Inter-Chassis Links

To delete degraded inter-chassis links from the system:

1. First, confirm that all related end-to-end maps have been removed from the system (see Removing Maps on page 76). Click on **Map Provisioning > Create Inter-Chassis Links** from the top of the screen. The FS6300 Inter-Chassis Links window displays.
2. Click on **Manage Reserve Pools** in the menu tree of the Inter-Chassis Links window (Figure 64 on page 77). The table at the bottom of the **Inter-Chassis Links** window displays all of the inter-chassis links in the NMS.
3. In the table, click the **Source > Card IP** column to organize the links. Click the rows of the desired links to remove. To select multiple consecutive links, hold down the Shift key and click the first row and the last row in the group. Confirm that each link's **Status** is marked as **Free**. Then, click **Delete**.

Managing H.110 Slots

Reserving H.110 Slots for Non-Managed Cards

Note FS6300 does not support management of 6081, 3125, or 3101card(s). Consequently H.110 Time Slots utilized for mapping between two unsupported cards is not reported in the application interface.

The **Reserve H.110 For Non-Managed Cards** section serves two purposes:

- To explicitly let the FS6300 know that certain Time Slots on the H.110 back plane are already used for mapping between two unsupported card(s), so that these Time Slots are not auto-provisioned for other inter-card maps.
- To block identified H.110 Time Slots exclusively for future mapping between unsupported cards.

Note You do not need to reserve H.110 slots in this user interface if DS0 maps are created between unsupported and FS6300-supported cards.

- Since the unsupported card is not modeled in FS6300, the DS0 Mapping interface does not offer the facility to create maps between any discovered card and an unsupported card.
- All such DS0 maps requiring interfacing with an unsupported card must be added directly on the cards outside of the FS6300 interface.
- Upon returning to the DS0 mapping menu, maps added on supported cards are auto-detected; and, when screened, they are accepted as partial maps into the FS6300 system.

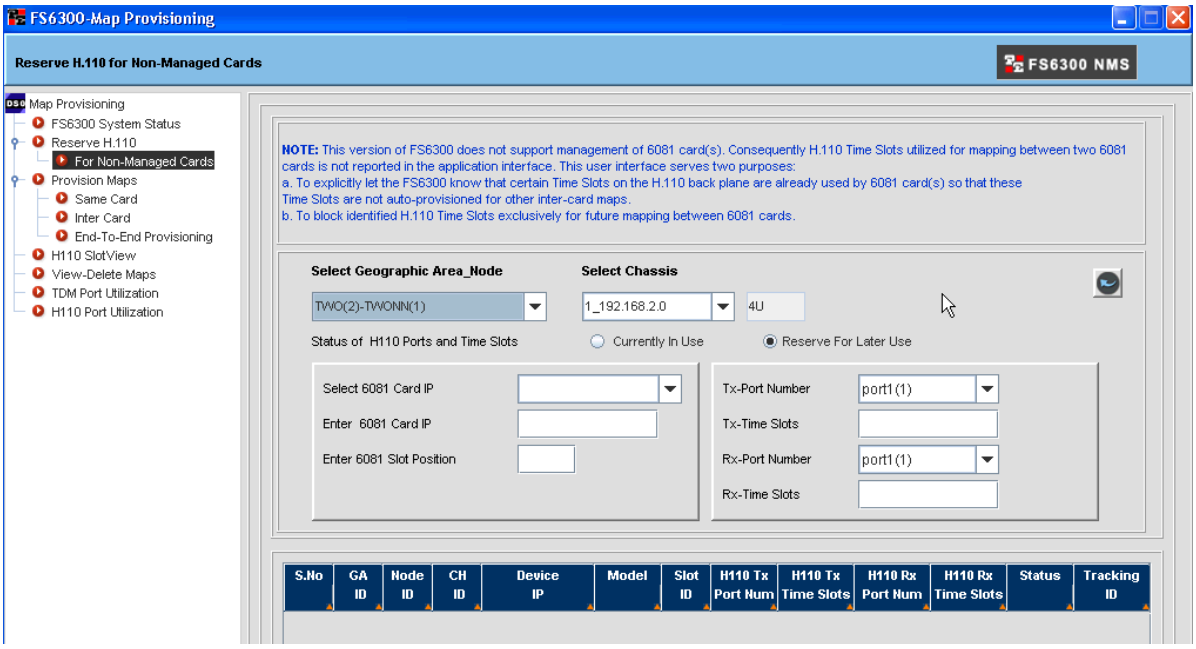


Figure 67. Reserve H.110 Slots for Non-Managed Cards

To reserve H.110 slots for unsupported cards:

1. Click on **For Non-Managed Cards** (under **Reserve H.110**) from the menu on the left. Select the **Geographic Area Node** and **Chassis** holding the unsupported card(s) from the corresponding drop-down menus.
2. Specify the purpose of blocking the H.110 ports (**Status of H.110 Ports and Time Slots**)–
   - Select **Currently In Use** if you are you providing details of H.110 ports and time slots already used between two unsupported cards in the chassis.
   - Select **Reserve for Later Use** if you are reserving H.110 ports in the chassis for future use between two unsupported cards.
3. Enter the **IP Address** of (or select from the corresponding drop-down menu) the unspported card and the **Slot Number** in which it currently exists. Once a card IP is entered into the system, it is listed for selection so that you may not re-enter the same address.
4. Next, select the **Tx-Port Number** and enter the **Tx-Time Slots**. Repeat for the **Rx-Port Number** and **Rx-Time Slots**.

   Note It is not required to *precisely* specify the Tx and Rx Port Numbers and Time Slots because this is only a 'reservation mechanism' (an interim solution). However, it is essential to specify the slots actually in use or slots that need to be reserved.

5. Click **Submit**. The information you entered will display in a table. You may delete or edit information in this table by seclecting the row of the information you would like to modify and clicking the **Edit** or **Delete** buttons.

Viewing H.110 Time Slot Utilization

You can view the utilization of H.110 time slots from the H.110 SlotView or the H.110 Port Utilization links in the Map Provisioning window (**Map Provisioning > Create and Manage DS0 Maps**).

The **H.110 SlotView** window shows information about time slots that are one-sided (Tx or Rx) or used. One-sided (Tx/Rx) slots have partial or inter-card maps to unsupported cards. Used slots have inter-card maps to FS6300-supported cards. The table also shows in-band slots and detected overlaps.

The **H.110 Port Utilization** window shows how many time slots are being used on all the ports in a chassis.

Viewing H.110 Time Slots through H.110 SlotView

To view H.110 time slots through H.110 SlotView:

1. Click on **H.110 SlotView** in the menu tree of the Map Provisioning window.

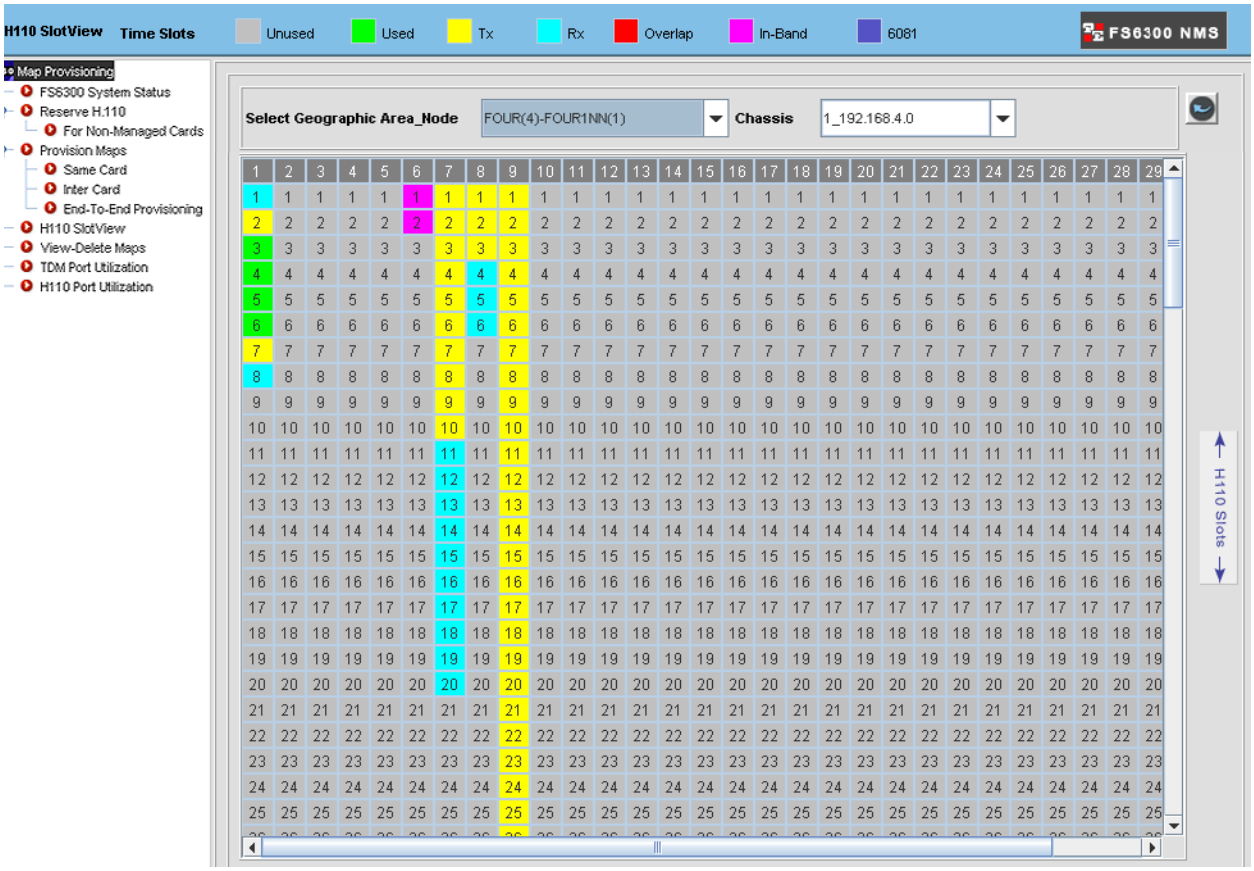


Figure 68. H.110 SlotView

2. Select the **Geographic Area Node** and **Chassis** that you want view in the corresponding drop-down menus.
3. **Used Time Slots** will be highlighted in green in the table. **Unused Time Slots** will be highlighted in gray. The key for all highlighted codes for times slots is at the top of the window.

The blue text in the lower-left corner of the window shows the number of **Total Time Slots Used by DS0**.

Viewing H.110 Time Slots through H.110 Port Utilization

To view H.110 time slots through H.110 Port Utilization:

1. Click on **H.110 Port Utilization** in the menu tree of the Map Provisioning window.

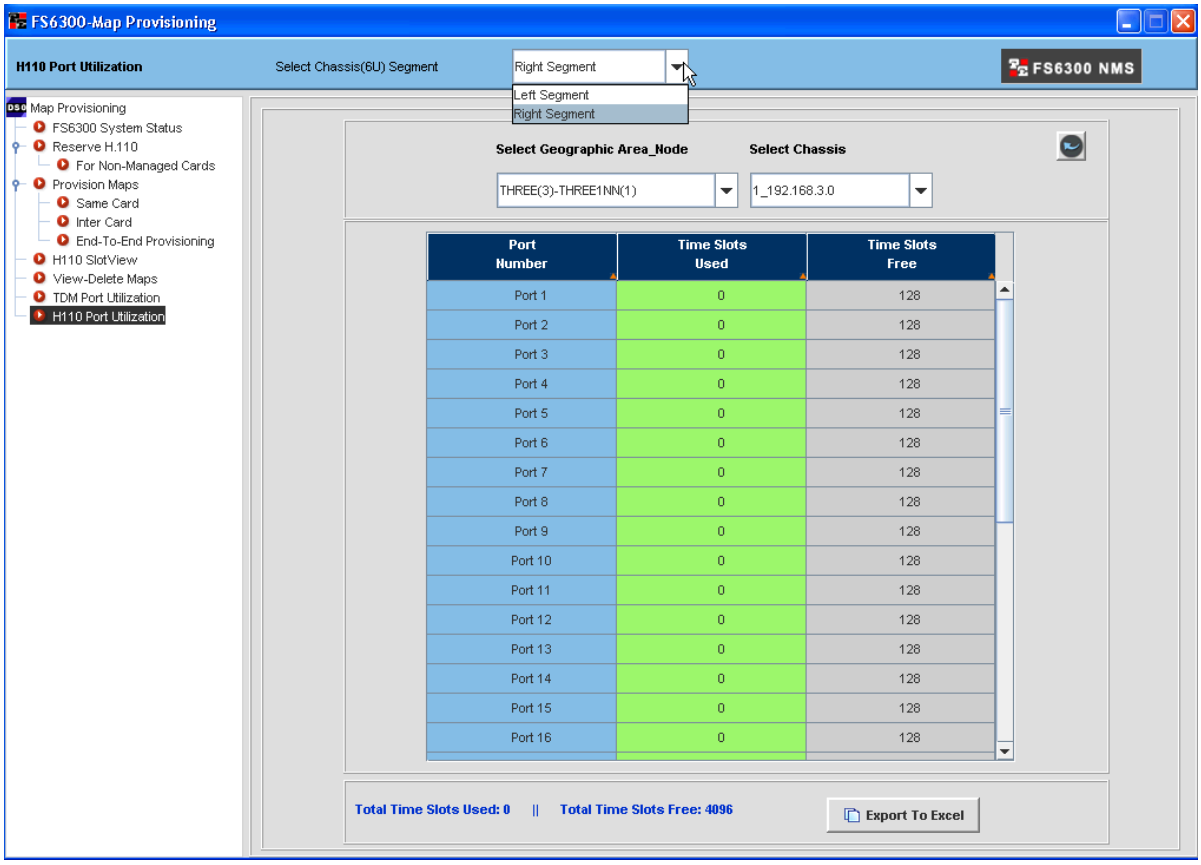


Figure 69. H.110 Port Utilization

2. Select the node of the chassis you want to view from the **Select Geographic Area Node** drop-down menu.
3. Select the chassis that you want view in the **Select Chassis** drop-down menu. If the selected chassis is type **6U**, select the right or left segment from the drop-down menu in the blue section at the top of the window.
4. The table lists all of the ports in the chassis, and lists the number of used time slots and unused time slots for each port. To view *which* time slots are used or unused in a chassis, see Viewing H.110 Time Slots through H.110 SlotView on page 82.

Viewing TDM Port Time Slots

You can view time slots that are used on G.SHDSL, iDSL, T1or E1 ports on a card through the Map Provisioning window.

To view time slots on TDM ports:

1. Click on **TDM Port Utilization** in the menu tree of the Map Provisioning window.

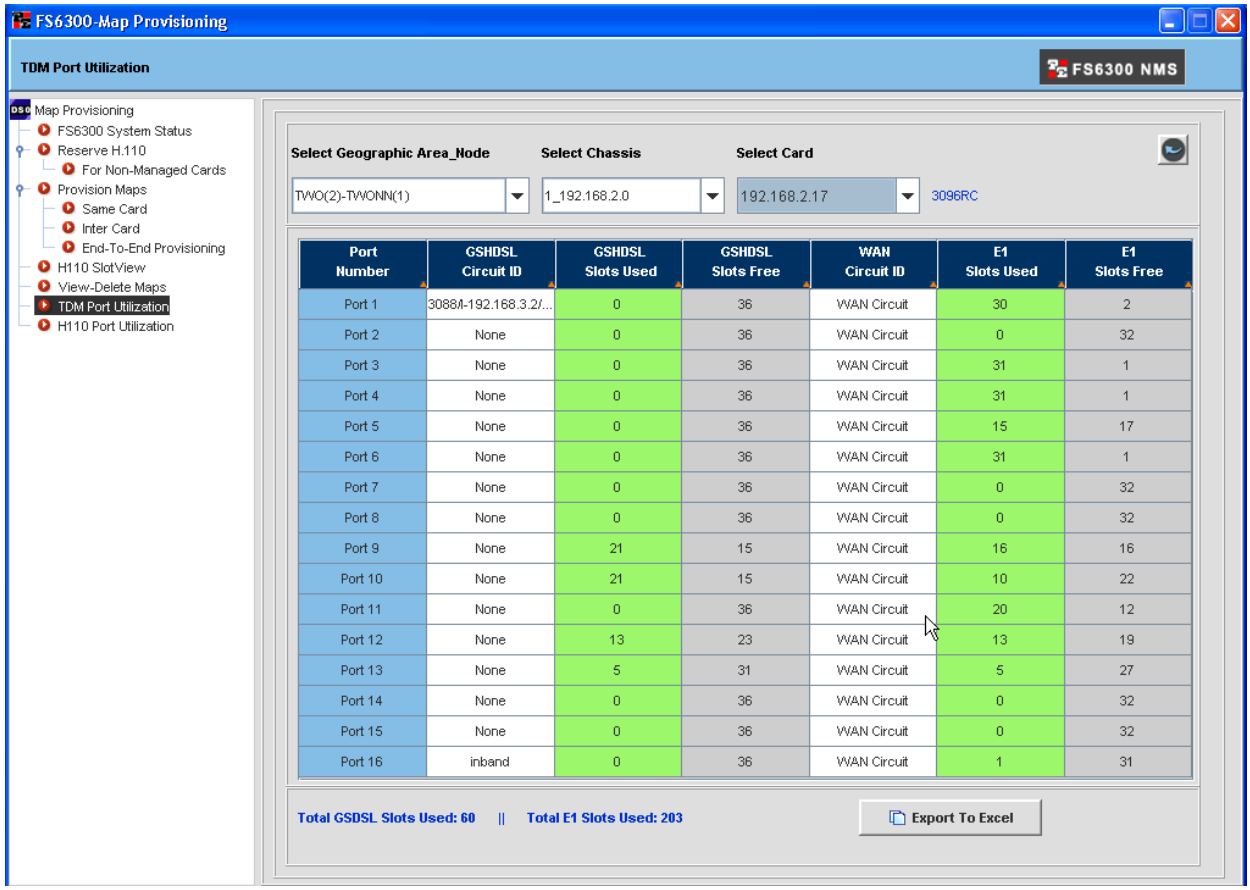


Figure 70. TDM Port Utilization

2. Select the node of the chassis you want to view from the **Select Geographic Area Node** drop-down menu.
3. Select the chassis that you want view in the **Select Chassis** drop-down menu. If the selected chassis is type **6U**, select the right or left segment from the drop-down menu in the blue section at the top of the window.
4. Select the card in the chassis that you want to view from the **Select Card** drop-down menu.
5. The table lists all of the TDM ports on the card, and lists the number of used and unused TDM interface time slots for each port.

Viewing DS0 Availability on Ports

You can view time slots that are used on all ports on a card through the Time Slot Utilization window.

To view time slots on all ports on a card:

1. Click on **Map Provisioning** at the top of the screen and select **DS0 Availability by Ports**.

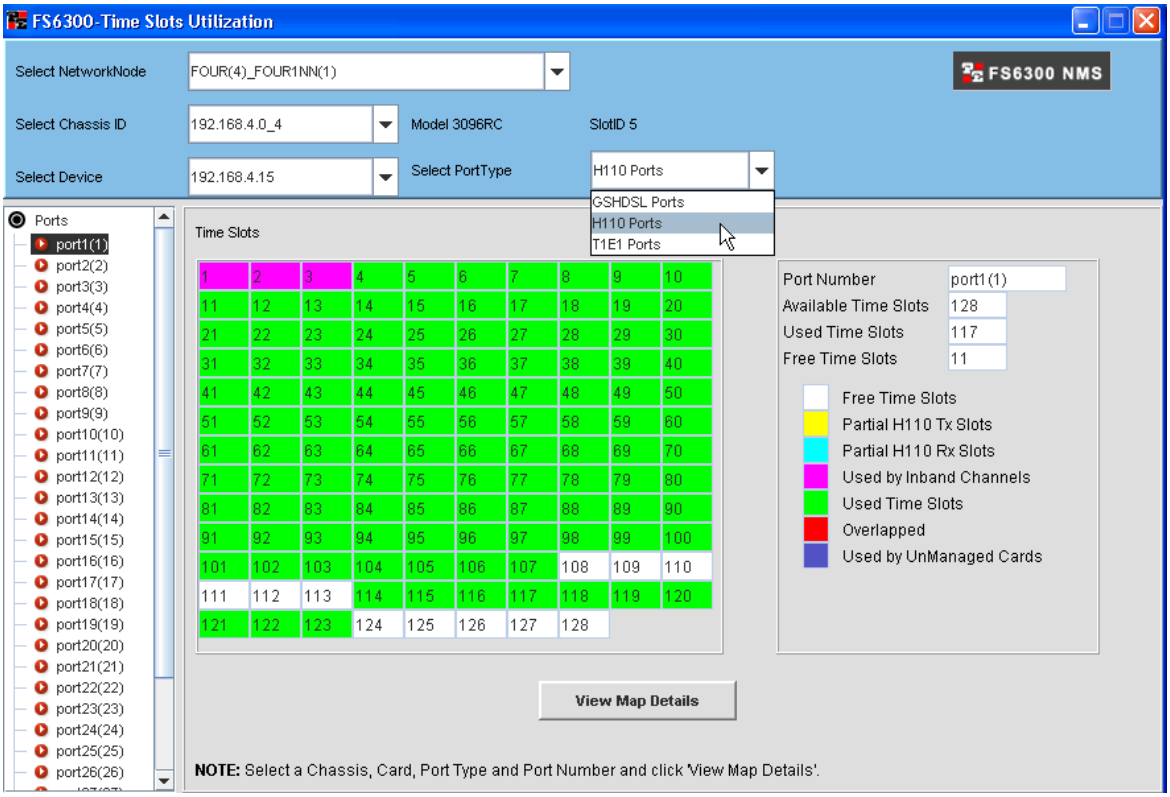
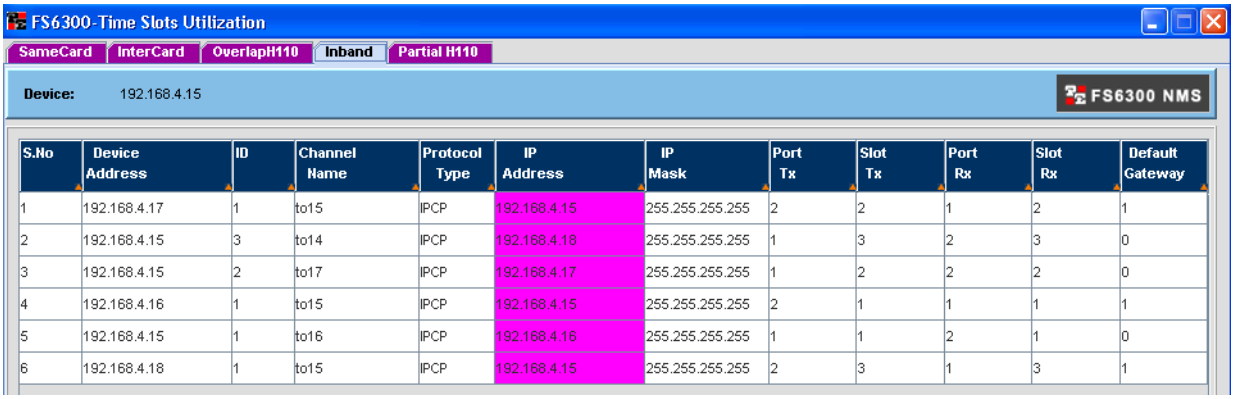


Figure 71. DS0 Availability by Ports

2. Select the node of the chassis you want to view from the **Select Network Node** drop-down menu.
3. Select the chassis that you want view in the **Select Chassis ID** drop-down menu.
4. Select the card in the chassis that you want to view from the **Select Device** drop-down menu.
5. Select a **Port Type** on the card.
6. Click on a port in the menu tree of the window to view which time slots are being used on that port on that card, and how they are being used (inband, one-sided, overlapped, ect).

7. Click on **View Map Details** to determine how the time slots are being used on a specific port. The Time Slot Details window will show information about used and overlapped timeslots.



S.No	Device Address	ID	Channel Name	Protocol Type	IP Address	IP Mask	Port Tx	Slot Tx	Port Rx	Slot Rx	Default Gateway
1	192.168.4.17	1	to15	IPCP	192.168.4.15	255.255.255.255	2	2	1	2	1
2	192.168.4.15	3	to14	IPCP	192.168.4.18	255.255.255.255	1	3	2	3	0
3	192.168.4.15	2	to17	IPCP	192.168.4.17	255.255.255.255	1	2	2	2	0
4	192.168.4.16	1	to15	IPCP	192.168.4.15	255.255.255.255	2	1	1	1	1
5	192.168.4.15	1	to16	IPCP	192.168.4.16	255.255.255.255	1	1	2	1	0
6	192.168.4.18	1	to15	IPCP	192.168.4.15	255.255.255.255	2	3	1	3	1

Figure 72. Time Slot Details

Viewing Chassis Diagnostics

Users regularly create and delete the DS0 maps. Users can also create these maps directly on the card using the card web page. This might result in conflicting configurations with the existing maps on the other cards. Also, users might restore an earlier configuration backup file on the card that may conflict with other map configurations. The **Chassis Diagnostics** view provides a way to easily identify and correct conflicting configurations. Benefits of the chassis diagnostic view include:

- View all chassis available in the system and view details of a specific chassis
- View all chassis level DS0 map configurations from all of the cards in the selected chassis
- Analyze the DS0 maps and detect the conflicting configurations between the maps
- View all configured trunks and reserved H110 maps on the selected chassis
- View complete port and timeslot utilization details
- View details about conflicts on the DS0 maps
- Navigate directly to conflict areas using highlighted tabs
- Manage conflicting configurations and update information

To view chassis diagnostics:

1. Click on **Map Provisioning** at the top of the screen and select **Chassis Diagnostics**. The **Chassis Diagnostics** window displays (Figure 73 on page 87).

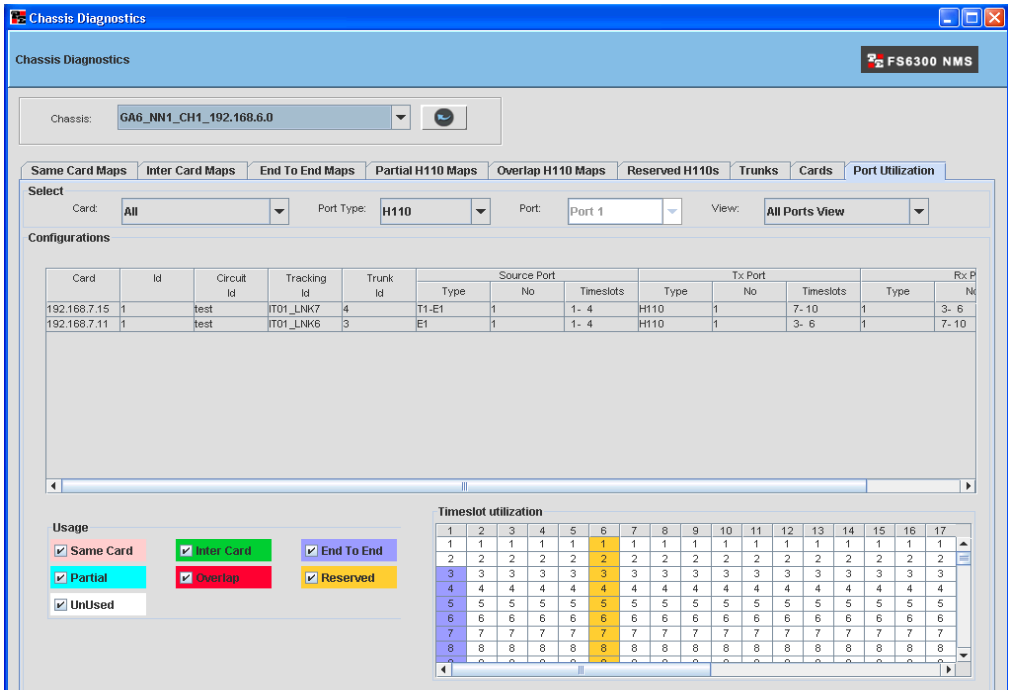


Figure 73. Chassis Diagnostics > Port Utilization tab

2. Select the desired **Chassis** from the drop-down menu and click the  button to view configuration details.
3. Select a tab to view specific chassis information. The window highlights conflicts in each tab.
   - **Same Card Maps:** This tab lists DS0 maps on the same card.
   - **Inter Card Maps:** This tab lists DS0 maps between different cards in the same chassis.
   - **End to End Maps:** This tab lists DS0 maps between different chassis.
   - **Partial H110 Maps:** This tab lists DS0 maps that use H110 timeslots on the card but do not have corresponding maps on any other card in the chassis.
   - **Overlap H110 Maps:** This tab lists multiple DS0 maps that use the same H110 timeslots. If there are a large number of overlapped H110 DS0 maps, select any DS0 map from the top table (*Configurations)* to view the maps that are conflicting with the H110 utilization in the bottom table (*Details*).
   - **Reserved H110s:** This tab lists all of the reserved H110 timeslots on the chassis. Select a device to view details of corresponding DS0 maps for each reserved H110 configuration and any conflicting configurations (i.e. any DS0 map using these reserved H110 timeslots).
   - **Trunks:** This tab lists all of the trunks on the chassis. Select a trunk to view if the trunk is used by any map (other than end-to-end provisioning).
   - **Cards:** This tab lists all of the cards and details for the selected chassis.
   - **Port Utilization:** This tab shows the port and timeslot utilization for various DS0 maps.

Chapter 5 Managing Logs and Reports

Chapter contents

Overview

Logs and reports are tools that help you monitor and manage events in the FS6300 NMS. This chapter explains how to view and save different logs and reports.

Managing Logs

When you first start the application client for the NMS, a log window will open and monitor server messages during your FS6300 session.

Saving Log Files

To save messages displayed in the log window:

1. In the **Logs** window, click the **Save To File** button.

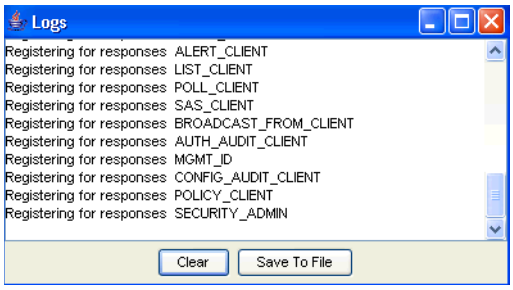


Figure 74. Logs window

2. Navigate to the folder where you want to save the log file.
3. Type in a file name for the log. Be sure the filename has the **.txt** extension.

Clearing the Log

To clear the log, click the **Clear** button in the Log window (Figure 74).

Managing Reports

In the FS6300 NMS, you can keep track of alarms and view summaries of each area (i.e. geographical areas, nodes, devices, maps, chassis, ect...) of the network. The Report menu also contains checklists for monitoring Chassis, Devices, and Discovery.

For information on generating graphs and reports for current and past performance data, see the Performance chapter in the *FS6300 NMS User Manual*.

To view the **Reports** menu, click on **Reports** in the toolbar at the top of the main screen.

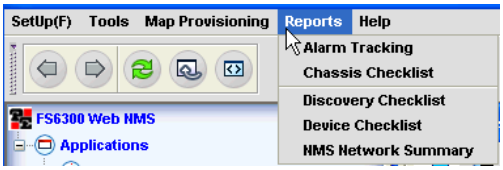
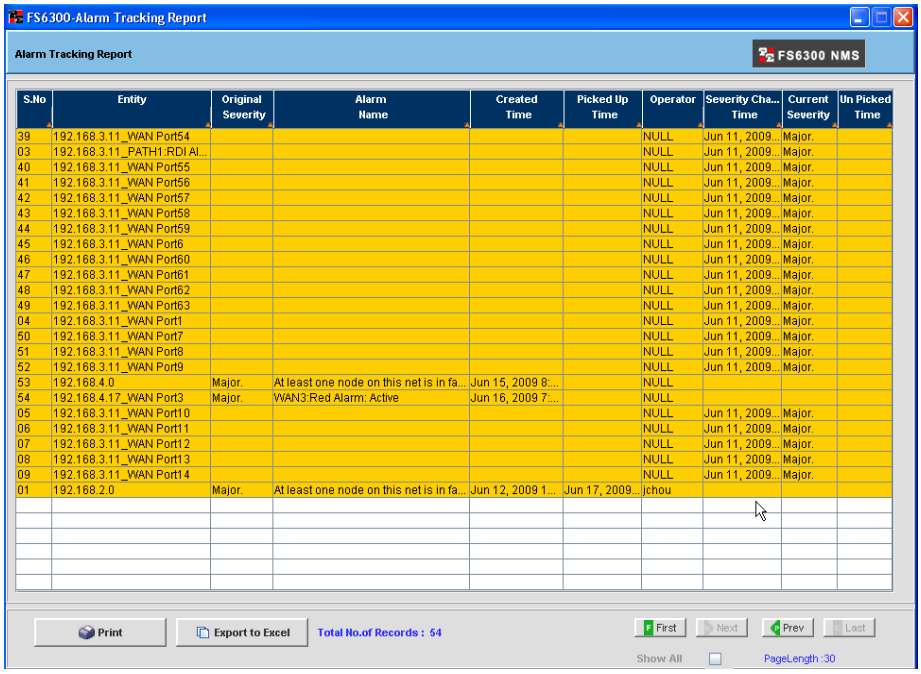


Figure 75. Reports Menu

Alarm Tracking Report

The **Alarm Tracking Report** displays a list of all the alarms in the networks monitored by the NMS.



S.No	Entity	Original Severity	Alarm Name	Created Time	Picked Up Time	Operator	Severity Cha... Time	Current Severity	Un Picked Time
39	192.168.3.11_WAN Port54					NULL	Jun 11, 2009...	Major.	
03	192.168.3.11_PATH1:RDI Al...					NULL	Jun 11, 2009...	Major.	
40	192.168.3.11_WAN Port55					NULL	Jun 11, 2009...	Major.	
41	192.168.3.11_WAN Port56					NULL	Jun 11, 2009...	Major.	
42	192.168.3.11_WAN Port57					NULL	Jun 11, 2009...	Major.	
43	192.168.3.11_WAN Port58					NULL	Jun 11, 2009...	Major.	
44	192.168.3.11_WAN Port59					NULL	Jun 11, 2009...	Major.	
45	192.168.3.11_WAN Port6					NULL	Jun 11, 2009...	Major.	
46	192.168.3.11_WAN Port60					NULL	Jun 11, 2009...	Major.	
47	192.168.3.11_WAN Port61					NULL	Jun 11, 2009...	Major.	
48	192.168.3.11_WAN Port62					NULL	Jun 11, 2009...	Major.	
49	192.168.3.11_WAN Port63					NULL	Jun 11, 2009...	Major.	
04	192.168.3.11_WAN Port1					NULL	Jun 11, 2009...	Major.	
50	192.168.3.11_WAN Port7					NULL	Jun 11, 2009...	Major.	
51	192.168.3.11_WAN Port8					NULL	Jun 11, 2009...	Major.	
52	192.168.3.11_WAN Port9					NULL	Jun 11, 2009...	Major.	
53	192.168.4.0	Major.	At least one node on this net is in fa...	Jun 15, 2009 8:...		NULL			
54	192.168.4.17_WAN Port3	Major.	WAN3:Red Alarm: Active	Jun 16, 2009 7:...		NULL			
05	192.168.3.11_WAN Port10					NULL	Jun 11, 2009...	Major.	
06	192.168.3.11_WAN Port11					NULL	Jun 11, 2009...	Major.	
07	192.168.3.11_WAN Port12					NULL	Jun 11, 2009...	Major.	
08	192.168.3.11_WAN Port13					NULL	Jun 11, 2009...	Major.	
09	192.168.3.11_WAN Port14					NULL	Jun 11, 2009...	Major.	
01	192.168.2.0	Major.	At least one node on this net is in fa...	Jun 12, 2009 1...	Jun 17, 2009...	jchou			

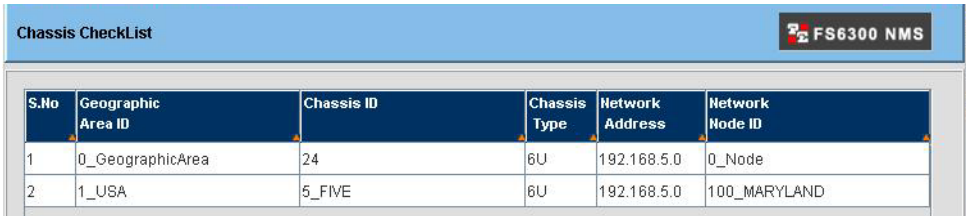
Figure 76. Alarm Tracking Report

To sort the columns, click on the column title. Click on the **Export to Excel** button to save the table to a Microsoft Excel spreadsheet.

The **Alarm Summary View** window always appears in the bottom left corner of the screen under the main menu tree. It offers a quick glance at the status of alarms that are currently occurring in the system. You can change how the Alarm Summary View is displayed by clicking on the icons in the Alarm Summary View window. The **Alarm Tracking** function shows a detailed report of the occurring alarms.

Chassis Checklist

The **Chassis Checklist** displays a list of all of the Chassis IDs and details in the NMS.



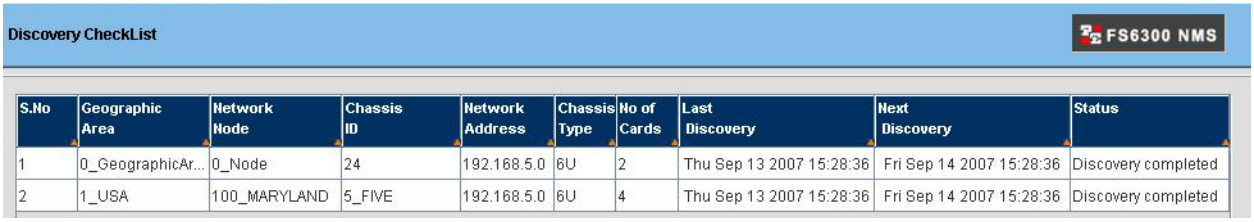
S.No	Geographic Area ID	Chassis ID	Chassis Type	Network Address	Network Node ID
1	0_GeographicArea	24	6U	192.168.5.0	0_Node
2	1_USA	5_FIVE	6U	192.168.5.0	100_MARYLAND

Figure 77. Chassis Checklist

To sort the columns, click on the column title. Click on the **Export to Excel** button to save the table to a Microsoft Excel spreadsheet.

Discovery Checklist

The **Discovery Checklist** displays a list of geographical areas, network nodes, and chassis IDS, and the status of the discovery schedules for each item.



S.No	Geographic Area	Network Node	Chassis ID	Network Address	Chassis Type	No of Cards	Last Discovery	Next Discovery	Status
1	0_GeographicAr...	0_Node	24	192.168.5.0	6U	2	Thu Sep 13 2007 15:28:36	Fri Sep 14 2007 15:28:36	Discovery completed
2	1_USA	100_MARYLAND	5_FIVE	192.168.5.0	6U	4	Thu Sep 13 2007 15:28:36	Fri Sep 14 2007 15:28:36	Discovery completed

Figure 78. Discovery Checklist

To sort the columns, click on the column title. Click on the **Export to Excel** button to save the table to a Microsoft Excel spreadsheet.

Device Checklist

The **Device Checklist** displays a list of network addresses for a certain model of card or all models in the network. Select the model to view from the drop-down menu.

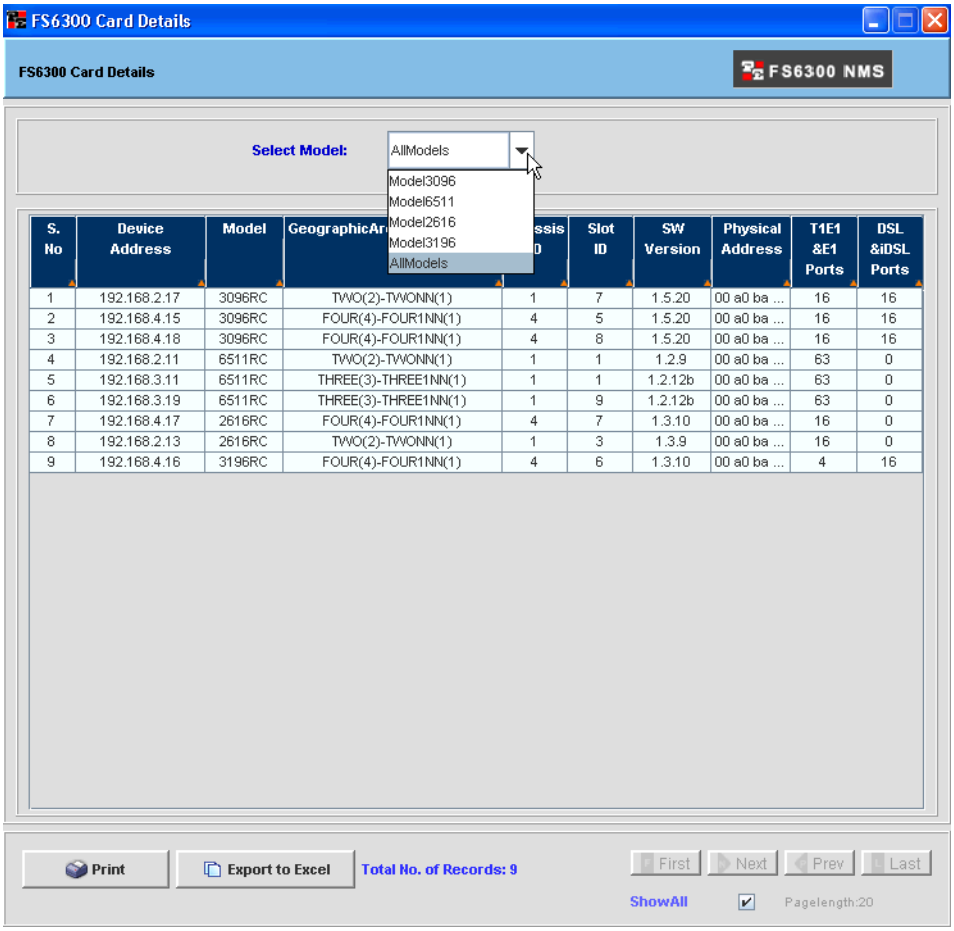


Figure 79. Device Checklist

To sort the columns, click on the column title. Click on the **Export to Excel** button to save the table to a Microsoft Excel spreadsheet.

NMS Network Summary

The **NMS Network Summary** window displays a map of managed objects icon. Click on an icon to view a summary of details for that managed object type. In the **Data Column** window on the left, you can select which details you want displayed in the report, then click the **Preview** button to display the report. Click the **Export to Excel** button to save the table to a Microsoft Excel spreadsheet.

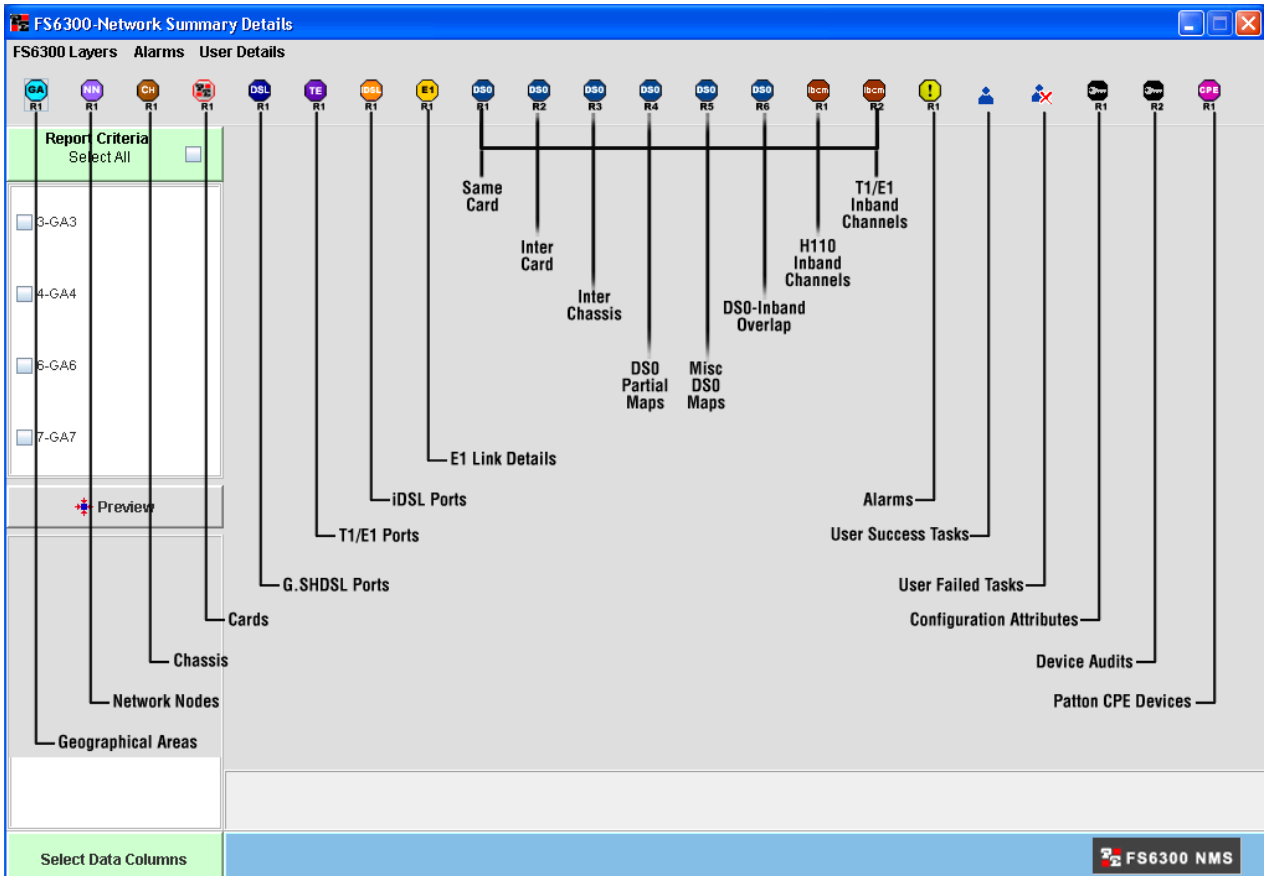


Figure 80. NMS Network Summary Window

Chapter 6 Managing Alarms and Network Events

Chapter contents

Introduction

The **Fault Management** section of the NMS application allows you to manage alarms and network events. Alarms indicate errors occuring on a network or device. Network events relate to occurrences in the network , such as discovery, status updates, or a device failure. This chapter describes how to manage alarm indications, view network events, configure trap and event parsers, configure event filters, and save the current list of network events.

Configuring Alarm Indications

In order to configure alarms, you need to configure the IP address of the NMS server which traps the alarm reports from each of the cards in the network. By default, the Alarm Trap IP address is 0.0.0.0, so no alarms are detected by the NMS.

You can configure the Alarm Trap Manager in two different ways, by right-clicking on a network node in the Geographical Areas section, or by right-clicking on a card in the Chassis section.

Configuring Alarms through the Network Node

To configure the IP address for the Alarm Trap field for each card:

1. From the menu tree on the left side of the screen, select the **Geographical Area** for the node that you want to configure.
2. In the main window, right-click on the **Network Node**, then select **Alarm Trap Manager.**
   The **Configure Alarm Trap Manager** window dispalys. You may configure the Alarm Trap Manager for any particular card in the chassis' subnet or you can configure all of the cards in the subnet at once.

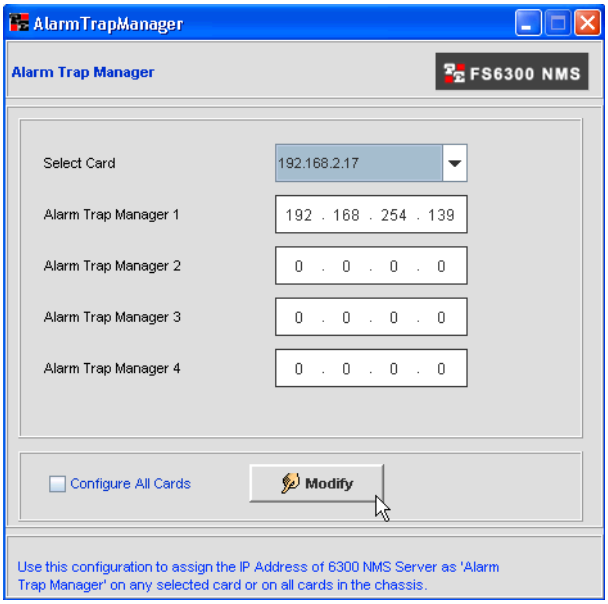


Figure 81. Alarm Trap Manager

3. Select the card that you would like to configure from the **Select Card** drop-down menu. If you would like to configure all of the cards at the same time, select the **Configure All Cards** checkbox at the bottom of the screen.

4. Enter the IP address of the NMS server in the **Alarm Trap Manager 1** field.
5. Click the **Modify** button.
6. If the configuration was successful, a "Configuration Result" window displays. Click **OK**.

Configuring Alarms through a Card in the Chassis

To configure the IP address for the Alarm Trap field for each card:

1. From the menu tree on the left side of the screen, select the **Chassis** for the card that you want to configure.
2. In the main window, right-click on the **Card**, then select **Alarm Parameter Configuration.** The **FS6300 Alarm Details** window appears. Click on the **Alarm System Overview** to view information about the alarms.

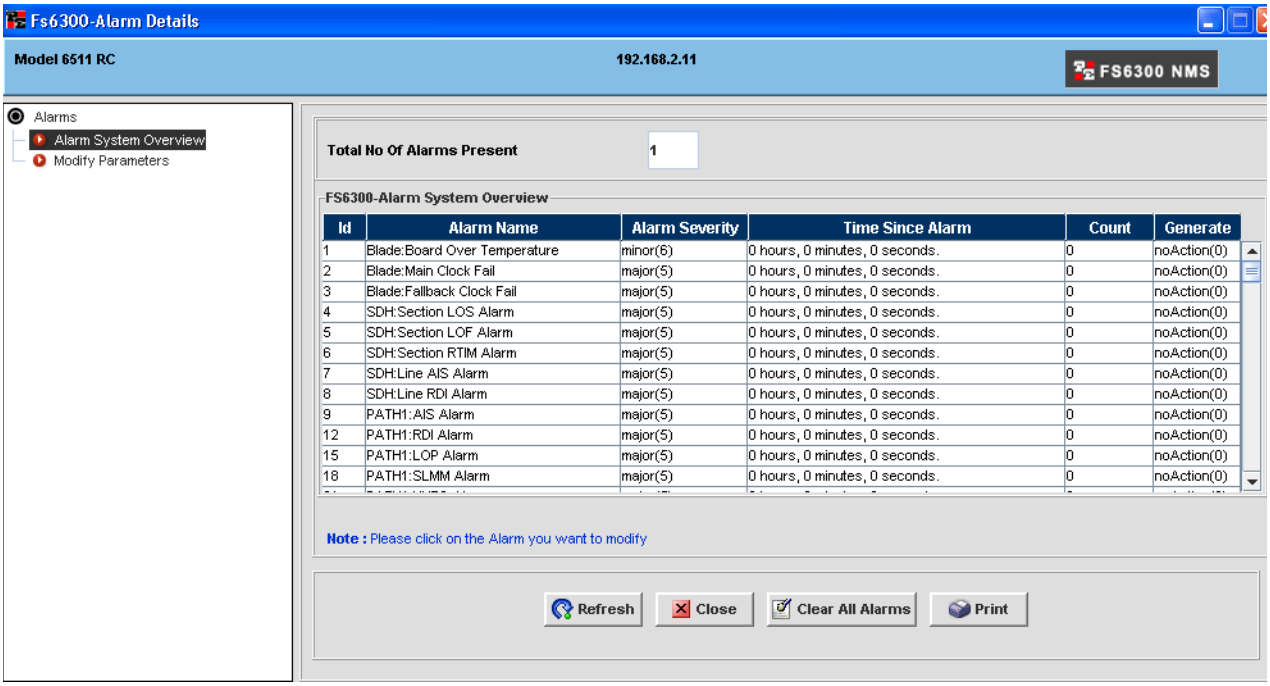


Figure 82. View Alarm Details

Alarm System Overview: The Alarm System Overview window shows the entire alarm system, including the following information for each alarm:

– Alarm Name

– Alarm Severity

– Time Since Alarm

– Count– the number of times this alarm has occurred since being cleared

3. Click on **Modify Parameters** to configure the alarms.

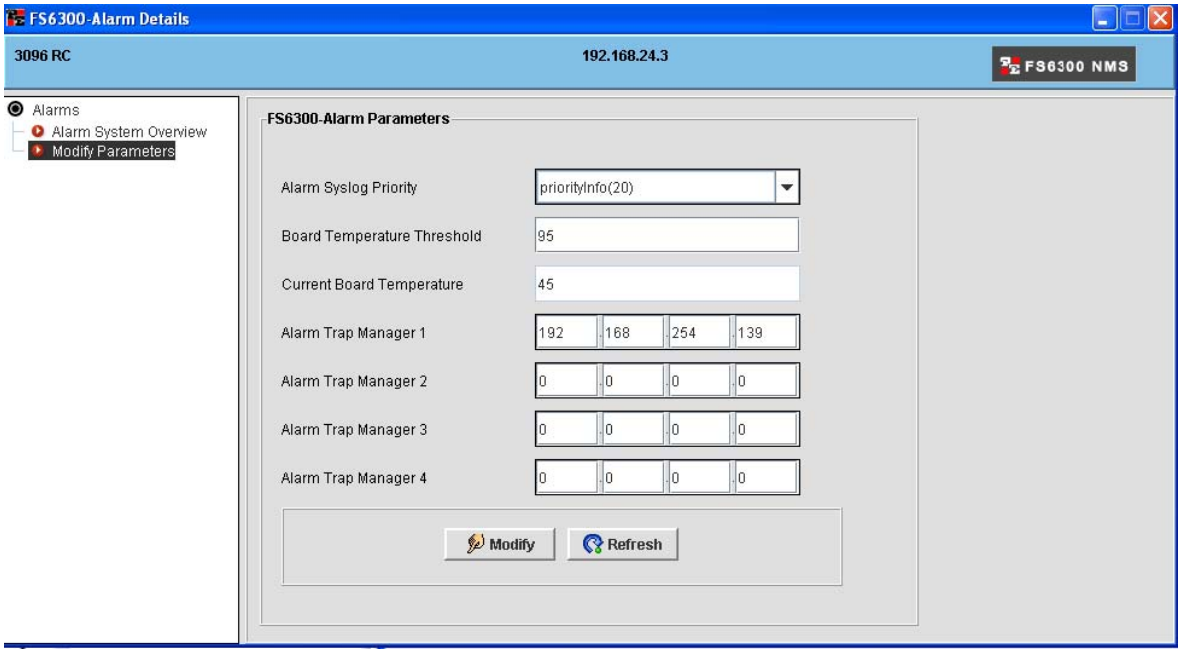


Figure 83. Modify Alarm Details

Modify Parameters: Configure the FS6300 Alarm Parameters through the Modify Parameters window.

– Alarm Syslog Priority

– Board Temperature Threshold

– Current Board Temperature

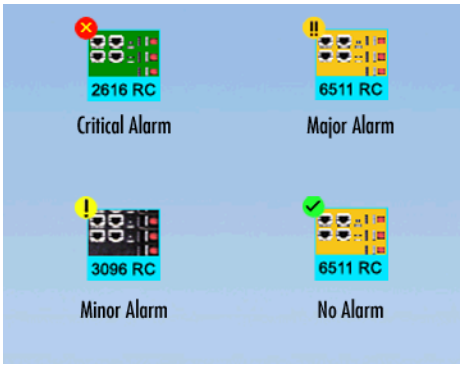
– Alarm Trap Managers 1-4

4. Click **Modify** to save your configuration in the card's volatile memory.
5. Return to the **Alarm Systems Overview** screen. Before the most severe active alarm is propagated to the icons in the NMS, you must first do Steps 6-7.
6. Click on the **Clear All Alarms** button. You should receive a "Configuration Result" window indicating success.
7. Click on the **Refresh** button.
8. Close the Alarm Details window.
9. Repeat Steps 2-8 for each card in the chassis. After this is completed, return to the view of the chassis in the main NMS window.

Alarm Indicator Icons

The following are symbols that appear on a card or node icon when the NMS receives an alarm:

- **Critical:** Red circle with a yellow "X"
- **Major:** Orange circle with two black exclamation points
- **Minor:** Yellow circle with a single black exclamation point
- **No Alarm/Informational:** Green circle with black checkmark



Alarms are propagated up to the next level throughout the **Network Maps** section in the menu tree.The **Chassis** icon indicates an alarm alert if one or more of the cards have an alarm. On the **Geographical Area** level, a network node will also display alarm alerts if a card in a chassis has an alarm.

Viewing Alarms

Viewing a Summary of Alarms

To view a summary of all systems with an alarm, click on **Failed Systems** (under Network Maps) in the menu tree on the left side of the screen. The Failed Systems map shows all the cards that have alarm alerts.

The **Alarm Summary View** window always appears in the bottom left corner of the screen under the main menu tree. It offers a quick glance at the status of alarms that are currently occurring in the system. You can change how the Alarm Summary View is displayed by clicking on the icons in the Alarm Summary View window. There are three different view options:

- Tabular View
- Graphical View
- Pie Chart View

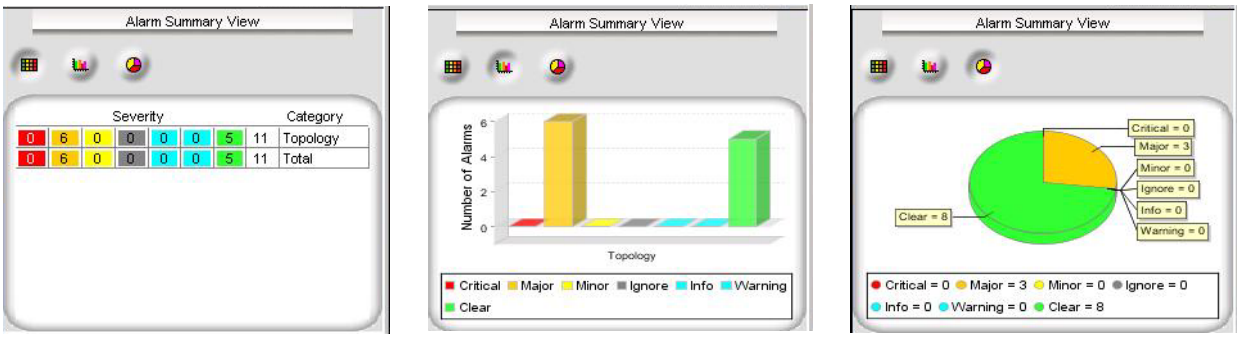


Figure 84. Alarm Summary View options (Tabular, Graphical, and Pie Chart)

Managing Alarm Custom Views

The NMS provides the ability to create custom views for specific alarms. Use custom views to display all alarms in a certain state or to view all alarms from one card or network.

Adding an Alarm Custom View

1. From the menu tree on the left side of the screen, select **Alarms** under **Fault Management**.
2. Select **Custom View** > **Add Custom View** from the top of the screen. The object properties window displays.

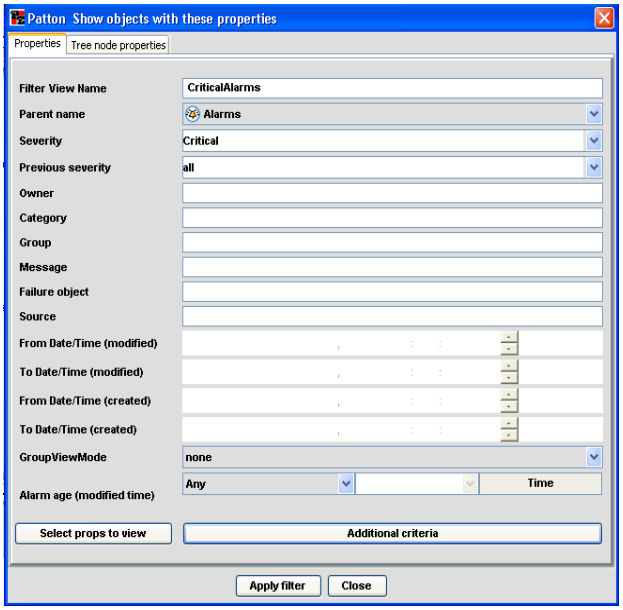


Figure 85. Example: Custom Alarm View for Critical Alarms

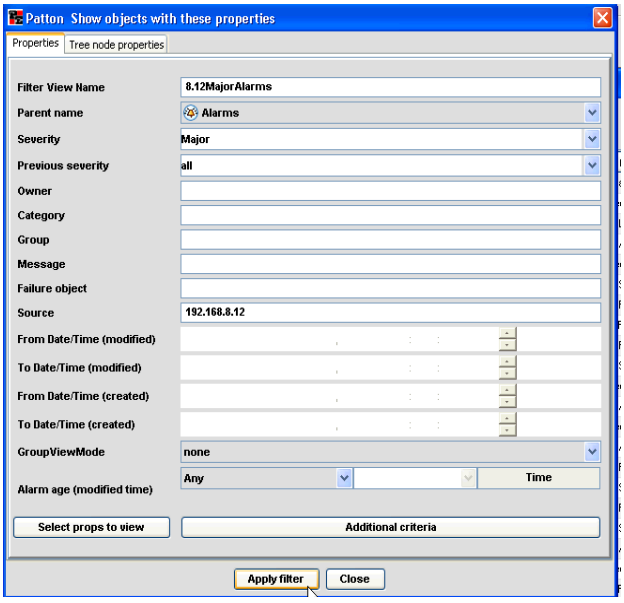


Figure 86. Example: Custom Alarm View for Specific Card

3. Enter the desired criteria for the custom view, then click **Apply Filter**. The new table displays and the NMS will automatically include the custom view as a submenu item under **Alarms** in the main menu tree.

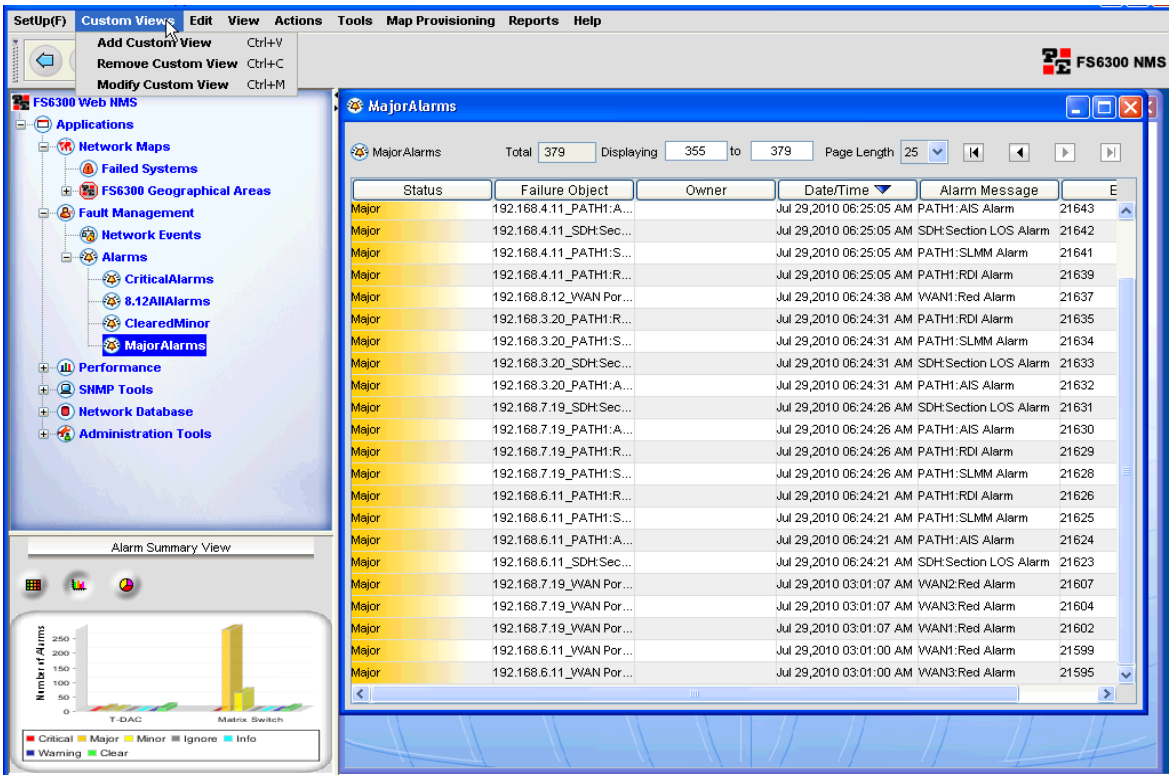


Figure 87. Alarm Custom Views

Modifying an Alarm Custom View

To modify an existing custom view:

1. Select the custom view in the menu on the left side of the screen.
2. Click **Custom Views > Modify Custom View** from the top of the screen.
3. Make the desired changes, then click **Apply Filter**.

Deleting an Alarm Custom View

To remove an existing custom view:

1. Select the custom view in the menu on the left side of the screen.
2. Click **Custom Views > Remove Custom View** from the top of the screen.
3. A confirmation message displays. Click **Yes** to delete the custom view.

Viewing Network Events

Viewing the current list of events

To view a current list of network events:

1. Click on **Fault Management** in the menu tree on the left side of the screen.
2. Click on **Network Events**.

A list of current events in the network will display in the main window.

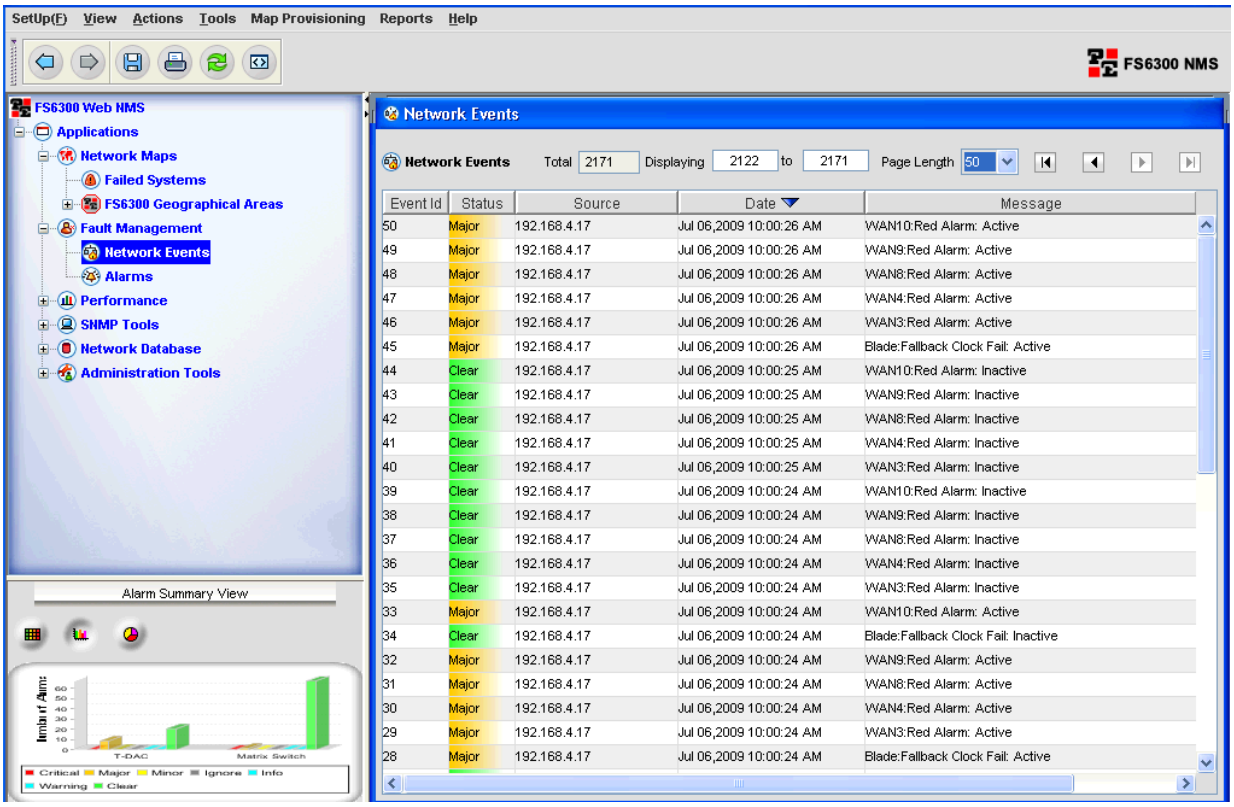


Figure 88. Fault Management > Network Events

Viewing details of an event

You can view the details of a network event in the list in several ways:

- Select a row in the table. Click on the **View** menu at the top of the screen, then select **Details**.
- Right-click on a row in the table, and select **Details** from the pull-down menu.
- Select a row in the table, then press **Alt+D**.
- Double-click on a row in the table.

Table 3 shows information about network event details.

Table 3. Network Event Details

Property	Description
Index	Specifies a unique ID created for each of the events that are generated.
Severity	Specifies the severity of the event, such as Critical, Major, Minor, Clear, Warning, Info.
Message	Specifies the message associated with the event.
Category	Specifies the category to which the event belongs. Example: Topology.
Domain	Specifies the domain-specific information which is based on physical location, functional categorization, or logical categorization of the source of the event.
Network	Specifies the network to which the event belongs to.
Node	Specifies the node to which the event belongs to. For example, if the event is for an interface, the node value is specified as interface parent node.
Failure Object	Specifies the specific entity (in the source) that has failed and is primarily responsible for the event.
Source	Specifies the exact source (network, node, interface) of the event.
Help URL	Specifies the URL for locating the help documentation on clicking the Help button in the same dialog box.
Date/Time	Specifies the date and time when the event was generated.
GroupName	Specifies the group name to which the event belongs.

Viewing alarms related to an event

To view alarms related to an event:

1. Click on **Network Events** (under Fault Management) in the menu tree.
2. Select the row of the event that you would like to view alarms for in the table.
3. Click on the **View** menu at the top of the screen, and select **Alarms**;
   OR, Right-click on the row and select **Alarms** from the pull-down menu;
   OR, Press **Ctrl+L**.
4. A window will display showing only the alarms for that selected event.

Saving Network Events

There are several actions you can take to save the current list of network events. These options are:

- "Saving Events to File" on page 103
- "Exporting Events" on page 103
- "Printing Events" on page 103

Saving Events to File

To save the current list of events that are displayed on the screen to a file:

1. Click on **Network Events** (under Fault Management) in the menu tree.
2. Click on the **Actions** menu at the top of the screen, and select **Save To File**;

   OR, press **Ctrl+I; OR** click  on the toolbar. The **Properties** window displays.
3. Enter a name for the file in the **File Name** field.
4. Click **Save File**. A confirmation message displays.

By default the saved file is located in <FS6300 NMS Home>/state directory. <FS6300 NMS HOME> is the IP address where the FS6300 NMS is installed.

> **Note** To view the saved file, click  on the toolbar or open a Web browser and access the URL - **http://<machine_name>:6300/state/<name of saved file>** [<machine_name> is the IP address where the FS6300 NMS Server resides].

Exporting Events

You can use the **Export Events** option to save the Event Custom View data as a CSV (comma-separated values) file in the FS6300 NMS server. An option is provided to export the entire Custom View data or only the data that is currently displayed in the Custom View.

To save the current list of events as a CSV file:

1. Click on **Network Events** (under Fault Management) in the menu tree.
2. Click on the **Actions** menu at the top of the screen, and select **Export Events**;
   OR, Press **Ctrl+Shift+E**. The **Export Data** window displays.
3. Select **Export Entry Custom View Data** or **Export Displayed Data**.
4. Enter a name for the file in the **File Name** field.
5. Click **Export**. A status message displays.

The exported custom view data file will be saved in the <FS6300 NMS Home> directory.

Printing Events

To print the current range of events displayed in the table:

1. Click on **Network Events** (under Fault Management) in the menu tree.
2. Click on the **Actions** menu at the top of the screen, and select **Print**;

   OR, Press **Ctrl+P; OR**, click  on the toolbar. .
3. The current list of network events is printed.

> **Note** If you are getting the message '**server printing not configured**', this means that the FS6300 NMS Server is not configured to execute the printing operation from the Application Client. See "Enabling Printing" on page 104.

Enabling Printing

By default, the option to print events and alarms in the NMS Application Client is disabled. To enable printing, you must configure the **NmsProcessesBE.conf** file. The printer must be connected in the same network as the NMS server. To enable printing in the NMS Application Client:

1. Open the **NmsProcessesBE.conf** file located in the <*Web NMS Home*>*/conf* directory. <*Web NMS Home*> is the IP address where the NMS server is running.
2. Configure the **PRINT_COMMAND** parameter for the **EventMgr**. The specific command may differ based on your operating system.

Win NT. The value for the PRINT_COMMAND parameter is based on the command given for the Print option in the command prompt in that machine. For example, if printing a file "*x.txt*" is invoked using *print x.txt* from command prompt, then the entry for the PRINT_COMMAND should be similar to:

```
SAVE_DIR state

PRINT_COMMAND "print .\\state\\printfile.tmp"
```

where:

printfile.tmp - The temporary file where the data to be printed will be saved.

state - Refers to the directory where the temporary file *printfile.tmp* is saved.

Windows 2000. The entry for the PRINT_COMMAND should be similar to:

```
PRINT_COMMAND "lpr -S Server -P printername <filename>"
```

where:

-S Server - Server Name of the host which is providing lpd service.

-P printername - name of the print queue, which will be maintained by the printer to put the job in the print queue and process.

<filename>- Referred from the SAVE_DIR directory; Give the filename as <*value of SAVE_DIR*>*printfile.tmp*

Linux. The entry for the PRINT_COMMAND should be similar to:

```
PRINT_COMMAND "lpr <filename>"
```

where:

<filename> - Referred from the SAVE_DIR directory. Give the filename as <*value of SAVE_DIR*>*//printfile.tmp*

Solaris. The entry for the PRINT_COMMAND should be similar to:

```
PRINT_COMMAND "/usr/ucb/lpr <filename>"
```

where:

<filename> - Referred from the SAVE_DIR directory. Give the filename as <*value of SAVE_DIR*>*//printfile.tmp*

Chapter 7 Monitoring Performance Data

Chapter contents

Introduction

The FS6300 NMS monitors performance of your network by collecting data from devices and providing reports. The performance is measured based on various factors, such as number of bytes of data received/sent (over a period) by a particular interface of a device, the interface's current bandwidth in bits per second, etc. After discovery, FS6300 NMS begins to collect data (by default, 5 minutes after a device is discovered) from each of the devices in the network and adds it to the database. Then, data collection occurs every 600 seconds (default interval). The data collected from a device in the network is called Performance Data.

This chapter describes how to view current and collected data. The FS6300 NMS collects data from a device based on statistics that are defined for that device. The FS6300 NMS can generate graphs and reports based on current performance data or collected (historical) performance data.

Viewing Configured Collection Data

To view data collection details:

1. Click on **Configured Collection** (under **Performance**) in the menu tree on the left side of the screen.
2. The **Configured Collection** table displays in the main window.

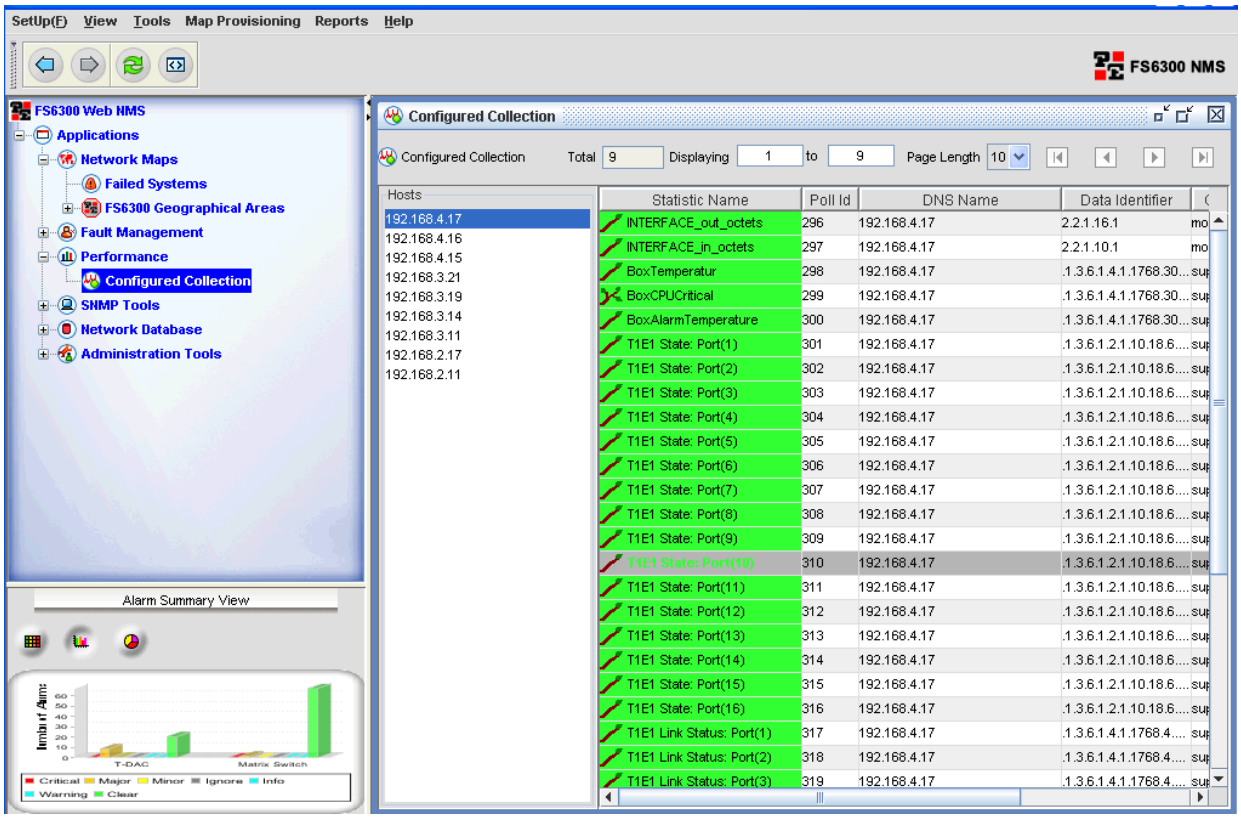


Figure 89. Performance > Configured Collection

Table 4 describes the Configured Collection properties:

Table 4. Configured Collection Properties

Property	Description
Statistic Name	A description to identify the Statistic.
Poll Id	A unique number generated automatically and associated with each Statistic.
DNS Name	Host name (device name) that the Statistic is associated with.
Data Identifier	A unique identification number of the device interface from which data about the device is to be collected.
Community	The community to be used when sending the SNMP request for collecting the Statistic.
Interval	The interval at which data should be collected for the Statistic. For example, the value 600 indicates that after every 600 seconds, data has to be collected.
Active	Specifies whether data collection for the selected device is active or not. If it is set to false, data collection is not performed for that device.
Multiple	Specifies the type used to poll columnar value of the tables

Viewing Current Performance Data

Current performance data is collected from a device instantly. To view the current data of a statistic:

1. Click on **Configured Collection** (under **Performance**) in the menu tree on the left side of the screen.
2. Select a host from the **Hosts** column in the **Configured Collection** window.
3. Select the row of the statistic that you want to view current performance data for.
4. Select **View** at the top of the screen, then choose **Plot** > **Current Statistic**;
   OR, Right-click on the row and choose **Plot** > **Current Statistic**;
   OR, Press **Ctrl+Shift+P**.
5. The **Current Graph Viewer** window appears, which shows a line chart (by default) of the current performance data for the selected statistic.

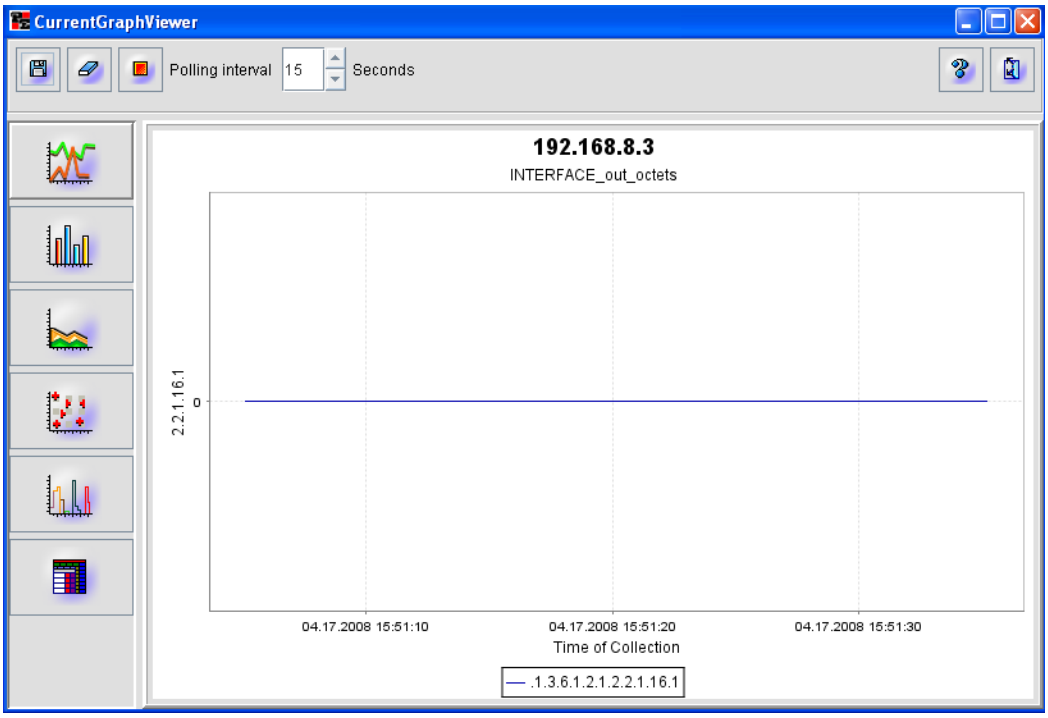


Figure 90. Plot Current Statistic

6. Click on an icon on the left side of the **Current Graph Viewer** window to change the type of chart. There are five types of graphs that you can view:
   - Line Chart
   - Bar Chart
   - Area Chart
   - Scatter Chart
   - X-Y Chart
7. By default, the **Current Graph Viewer** updates the information in the chart every 15 seconds. To change the **Polling Interval**, click **Stop Poller** at the top of the **Current Graph Viewer**. Enter a new value in the **Polling Interval** box, then click **Start Poller**.
8. To **Save** the current graph, click the disk icon .
9. To **Clear** current graph, click the eraser icon .
10. To **Print** the current graph, right-click on the graph and select **Print**.

Viewing Collected Performance Data

Collected performance data is data that was collected and stored in the database. To view the collected data of a statistic:

1. Click on **Configured Collection** (under **Performance**) in the menu tree on the left side of the screen.
2. Select a host from the **Hosts** column in the **Configured Collection** window.
3. Select the row of the statistic that you want to view collected data for.
4. Select **View** at the top of the screen, then choose **Plot** > **Collected Statistic**;
   OR, Right-click on the row and choose **Plot** > **Collected Statistic**;
   OR, Press **Ctrl+O**.
5. The **Collected Graph Viewer** window appears, which shows a line chart (by default) of the collected performance data for the selected statistic.

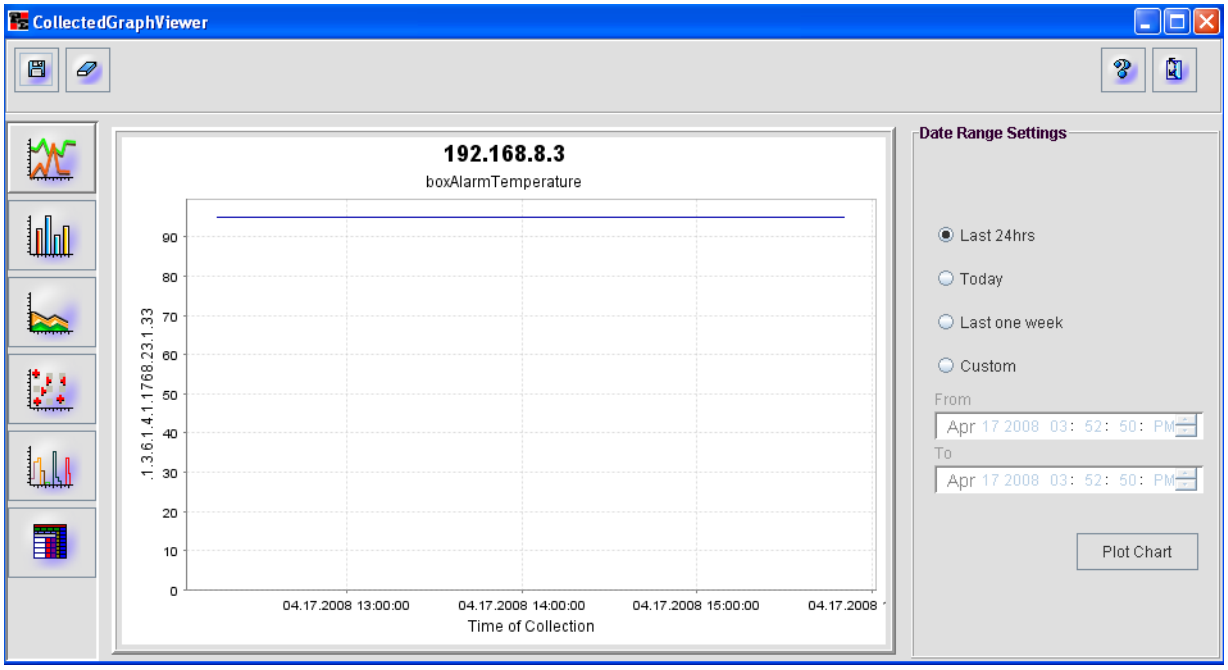


Figure 91. Plot Collected Statistic

6. Click on an icon on the left side of the **Collected Graph Viewer** window to change the type of chart. There are five types of graphs that you can view:
   - Line Chart
   - Bar Chart
   - Area Chart
   - Scatter Chart
   - X-Y Chart

7. By default, the **Collected Graph Viewer** shows information from the last 24 hours. Choose **Today**, **Last One Week**, or **Custom** based on the range of data you want to display. For **Custom**, set the **From** and **To** range in "**Month: Date: Year: Hour: Seconds: AM/PM**" format. Then, click **Plot Chart**.

8. To **Save** the current graph, click the disk icon  .

9. To **Clear** current graph, click the eraser icon  .

10. To **Print** the current graph, right-click on the graph and select **Print**.

Chapter 8 Monitoring SNMP Devices

Chapter contents

Overview

FS6300 NMS includes a MIB application for managing SNMP devices. The MIB Manager enables loading and searching MIBs, performing SNMP operations, and viewing data from SNMP-managed devices.

Note For information on how to discover/add SNMP devices in the NMS, see "Configuring Discovery of SNMP Devices" on page 56 and "Adding a Device Manually" on page 57.

To access the MIB application, click on **SNMP Tools** > **MIB Manager** in the menu tree on the main screen.

Navigation

Icons

Figure 92 describes the icons in the MIB Manager.

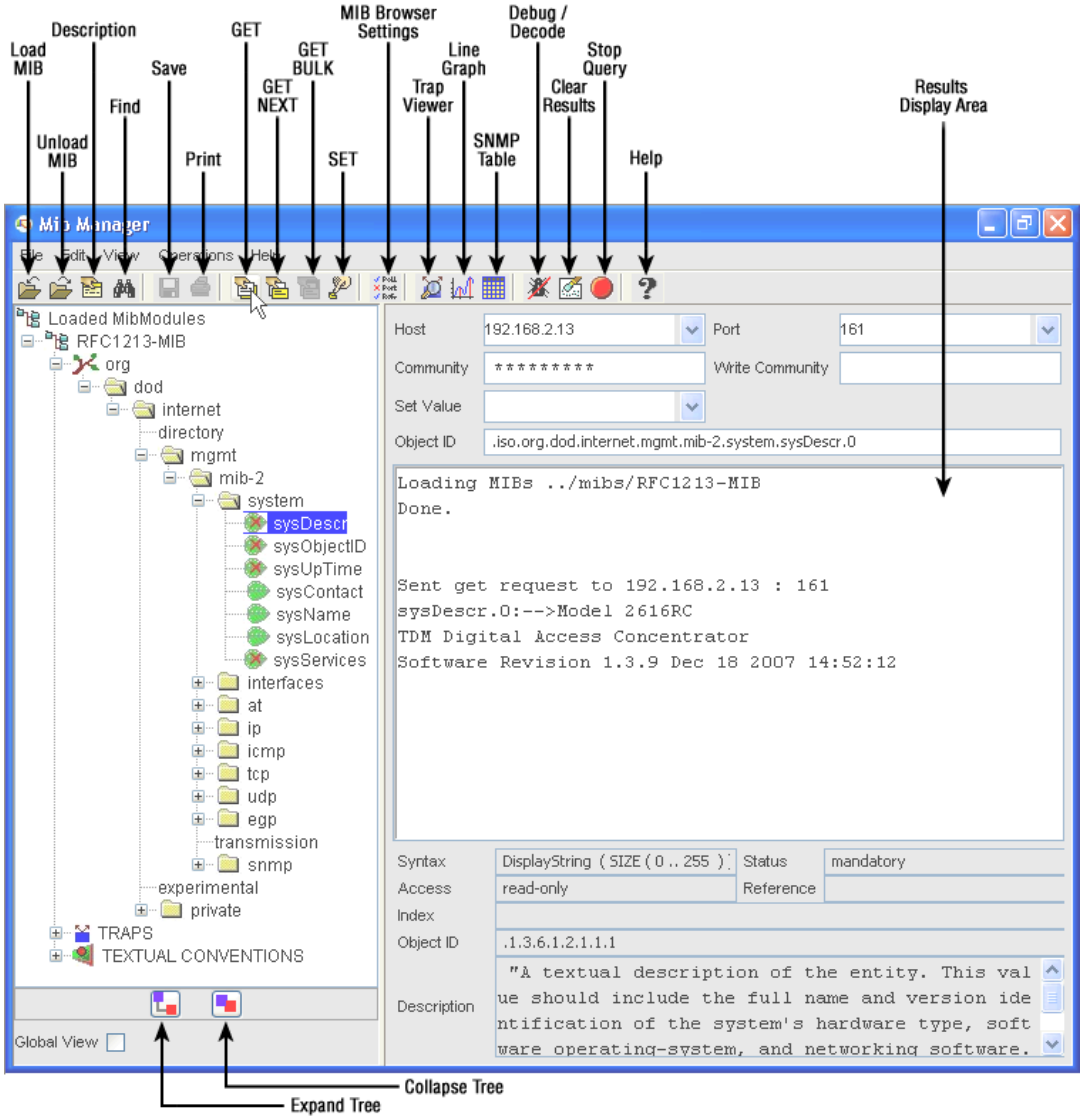


Figure 92. Buttons in the MIB Manager

Menus

You can also access icon functions and additional tools from the menus at the top of the screen:

Table 5. MIB Manager Menus

Menu	Option	Description
File	**Load**	Select a MIB file to add to the MIB Manager
	Unload	Remove a MIB file from the MIB Manager
	Load All	Add all MIB files to the MIB Manager at the same time
	Unload All	Remove all MIB files from the MIB Manager at the same time
Edit	**Settings**	Open the MIB Manager General Settings window
	Find Node	Perform a search for a specific MIB element
View	**Trap Viewer**	Open the tool to view traps received from SNMP agents
	Line Graph	Create a line graph from real-time SNMP data
	Bar Graph	Create a bar graph from real-time SNMP data
	SNMP Table	Open the tool to track data from selected table elements
	Description	View details for a MIB element
	Debug	Open the debug/decoder window
	Toolbar	Show/hide the icon toolbar at the top of the MIB Manager
	Display	Change the way the primary window is displayed
Operations	**Get**	Retrieve information for a selected MIB object
	Get Next	Retrieve information for the next MIB object in the object tree
	Get Bulk	Retrieve information from a large table for a specified OID (GETBULK only works for SNMPv2 and SNMPv3 versions)
	Set	Change and save information for a selected MIB object
	Stop	Cancel an SNMP operation in progress
	Clear	Clear the results display area

Configuring the MIB Manager

Setting Common Parameters

In order to perform SNMP operations correctly, it is important to set common parameters for the MIB manager first.

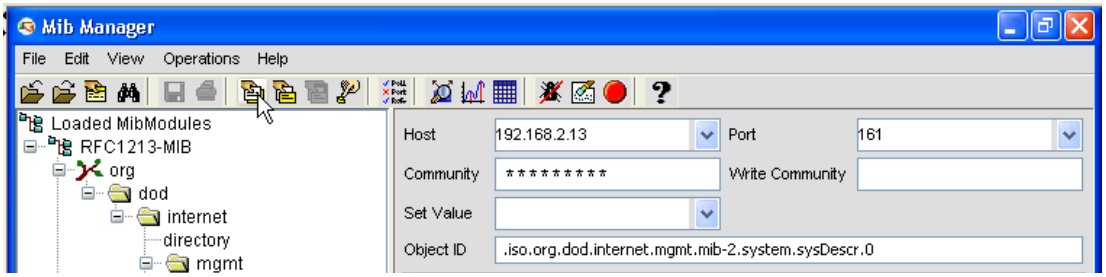


Figure 93. CommonMIB parameters in the main window

You can set the following parameters in the MIB manger's main window:

- **Host:** Enter the IP address of an NMS-managed card
- **Port:** Enter the port number to receive SNMP request messages. Default = *161*
- **Community:** Enter the same community strings that are configured for the system parameters on the card itself. Default for read/write access = *superuser*. Default for read-only access = *monitor*.
- **Set Value:** When you are performing the SET operation for a read/write MIB object, use the **Set Value** field to enter changes.

Setting General MIB Parameters

To set the SNMP version and other MIB settings, click on **Edit > Settings** or click  on the toolbar.

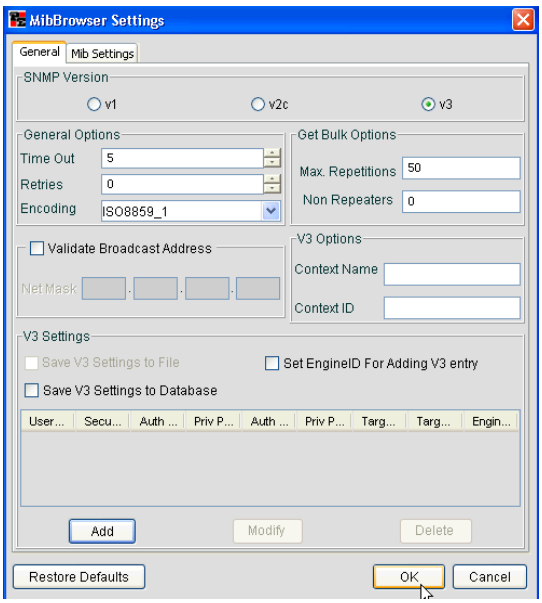


Figure 94. General MIbBrowser Settings

The **General** tab of the MIBBrowser Settings window allows you to make changes to the SNMP version used in the MIB Manager. (The **MIB Settings** tab applies to loading MIB modules. See "Configuring MIB Loading Options" on page 116 for more information).

- **SNMP Version:** Default = *v1*, Other options are SNMPv2 or SNMPv3
- **General Options:**
  - **Timeout:** The amount of time the application waits for a response message. Default = *5 seconds*
  - **Retries:** The number of times the application resends a request after a timeout occurs. Default = *0*
  - **Encoding:** The required transmission format for modifying information. Default = *ISO8859_1*
- **Get Bulk Options (*SNMPv2 or v3 only):**
  - **Max Repetitions:** The number of consecutive values that the application retrieves. Default = *50*
  - **Non Repeaters:** The number of values from the variable-bindings list that the application returns. Default = *0*
- **ValidateBrodcast Address:** Enable this option to check the validity of the netmask address you provide.
- **V3 Options (Required for SNMPv3 requests):**
  - **Context Name:** The name of the collection of management information used to identify the SNMP entity
  - **Context ID:** The identifier of an SNMP entity that may recognize an instance of a context with a specific context name
- **V3 Settings (Required for SNMPv3 requests):**

  The V3 Settings section is for managing security features for SNMPv3. You may add, modify or delete user entries. Click **Add** or **Modify** to open the **SNMP Parameter Panel**.
  - **Target host:** Enter any host with an SNMPv3 agent or proxy agent. Default = *localhost*
  - **Target port:** Enter a port that can receive SNMP requests. Default = *161*
  - **User name:** Enter/modify the name for the user
  - **Security level:** Default = *noAuth noPriv*; Select from the following security access options:
    noAuth noPriv = No additional parameters are requred
    Auth noPriv = Authentication password and protocol are required
    Auth Priv = Authentication password, protocol, and privacy password are required
  - **Auth Protocol:** Select MD5 or SHA. Default = *MD5*
  - **Auth Password:** Enter a secure password if user security level is set to *Auth Priv, Auth noPriv*
  - **Priv Protocol:** Default = *CBC-DES*, Required only is user security level is set to *Auth Priv*
  - **Priv Password:** Enter a secure password if user security level is set to *Auth Priv*
  - **Context Name:** Enter the context name you set under V3 options

  Click **Apply** to save your settings.

Loading MIB Modules

To add a MIB module to the MIB Manager:

1. Click on **File > Load MIB** or click  on the toolbar. The **Load a MIB File** window displays.

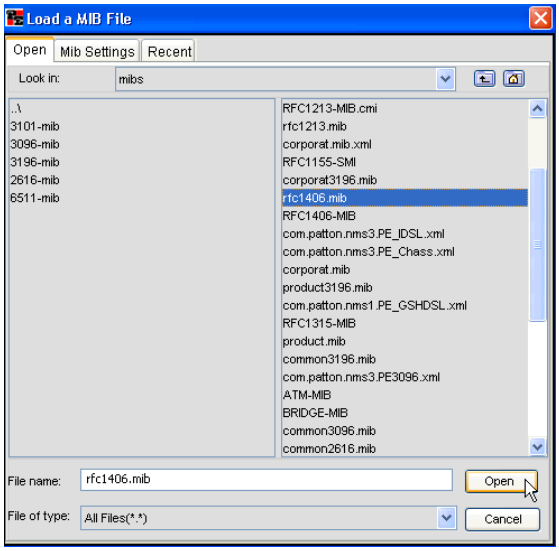


Figure 95. Load a MIB file

2. Browse to the **mibs** folder and select the file you want to load.Click **Open**.
3. The MIB file appears in the menu tree of the MIB Manager window.

If you want to load *all* available MIB files into the menu tree, click **File > Load All MIBs**.

Configuring MIB Loading Options

You can change the MIB loading options by clicking on the **MIB Settings** tab in the **Load a MIB File** window, or by clicking on the **MIB Settings** tab in the **MIBBrowser Settings** window.

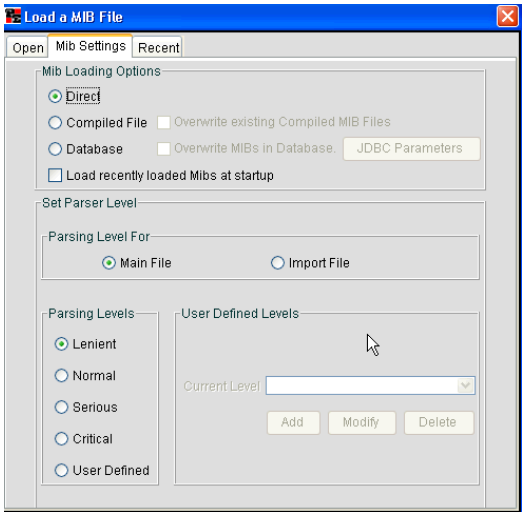


Figure 96. Loading options for MIB files

- **MIB Loading Options**
  - **Direct:** Load and parse a MIB file before displaying it in the MIB tree
  - **Compiled File:** Load a MIB file as a compiled file (*.cmi or *.cds). The MIB Manager parses the compiled file the first time you load it, and creates module files to optimnize loading time and performance.
  - **Database:** Load a MIB file from a database. Enter the drivername, URL, and user name and password for accessign the database where the MIB file is stored.
  - **Load recently loaded MIBs at startup:** Check this box to add recent MIB files to the **Recent** tab of the **Load a MIB Module** window for quick access

Note You must load MIB files in sequence into the MIB Manager to access the information correctly.

Setting Parser Levels

The MIB Manager always parses MIB files if you perform any of the following actions: load the MIB file directly, load the MIB file from a compiled file for the first time, select to overwrite existing compiled MIB files, or load the MIB file from a database for the first time.

There are different levels for parsing MIB files. To set the parser level, click on the **MIB Settings** tab in the **Load a MIB File** window, or click on the **MIB Settings** tab in the **MIBBrowser Settings** window (see Figure 96 on page 116).

- **Parsing Levels**

  Lenient: This level accepts all types of MIB files; No checks

  Normal: This level conforms to obsolete standards; Default checks

  Serious: This level strictly follows the current standard; Most checks throw exceptions on first misbehavior.

  Critical: This level completely follows SMIv1 and v2 standards; All possible checks throw exceptions on first misbehavior.

  User-Defined: Define your own parsing levels.

- **User Defined Levels:** Select **Add** to create a new, custom parsing level. The **Customize Level** box displays. Slect/deselect the options for your custom level, then click **OK**.

Unloading MIBs

To add a MIB module to the MIB Manager:

1. Select the file in the MIB menu tree that you want to unload.
2. Click on **File > Unload MIB** or click  on the toolbar.
3. A confirmation box displays. Click **Yes** to remove the MIB file.

If you want to unload *all* MIB files from the tree, click **File > Unload All MIBs**.

Peforming SNMP Operations

You can use the MIB Manager to retrieve and alter data from SNMP devices. GET, GETNEXT, and GET-BULK are operations for receiving data. SET is the operation for modifying MIB information. Traps are unsolicited messages you may receive from SNMP devices.

GET / GETNEXT

The GET and GETNEXT operations allow you to view information from a specific SNMP variable.

1. Load the MIB module (see "Loading MIB Modules" on page 116).
2. Select the desired element in the MIB tree.
3. Click **Operations > Get** or click  on the toolbar.
4. The requested information displays in the main MIB Manger window.
5. To view information from the next variable in the MIB tree, click **Operations > Get Next** or click  on the toolbar.
6. The requested information displays in the main MIB Manger window.

GETBULK

The GETBULK operation allows you to retrieve volumes of information from a large table. It may only be performed using SNMPv2 or SNMPv3.

1. Click on **Edit > Settings** or click  on the toolbar to set the MIB Manger to use SNMPv2 or SNMPv3. (See "Setting General MIB Parameters" on page 114).
2. Load the MIB module (see "Loading MIB Modules" on page 116).
3. Select the desired element in the MIB tree.
4. Click **Operations > Get Bulk** or click  on the toolbar.
5. The requested information displays in the main MIB Manger window. The number of different object results depends on the value entered in the **Max Repetitions** field in Step 1.

SET

The SET operation allows you to modify an SNMP variable with read-write access.

1. Load the MIB module (see "Loading MIB Modules" on page 116).
2. Select the desired element in the MIB tree.
3. Enter the new value for the object in the **Set Value** field.
4. Click **Operations > Set** or click  on the toolbar.

Managing Tables

The MIB Manager allows you to view and manage SNMP table data in the user-friendly **SNMP Table** tool.

To access the **SNMP Table** tool, select a valid object from the MIB tree and click on the toolbar or click **View > SNMP Table**. Valid objects will have a table symbol in the MIB tree.

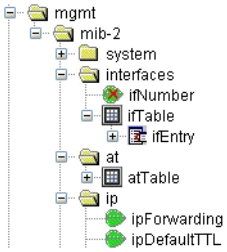


Figure 97. Table objects in MIB tree

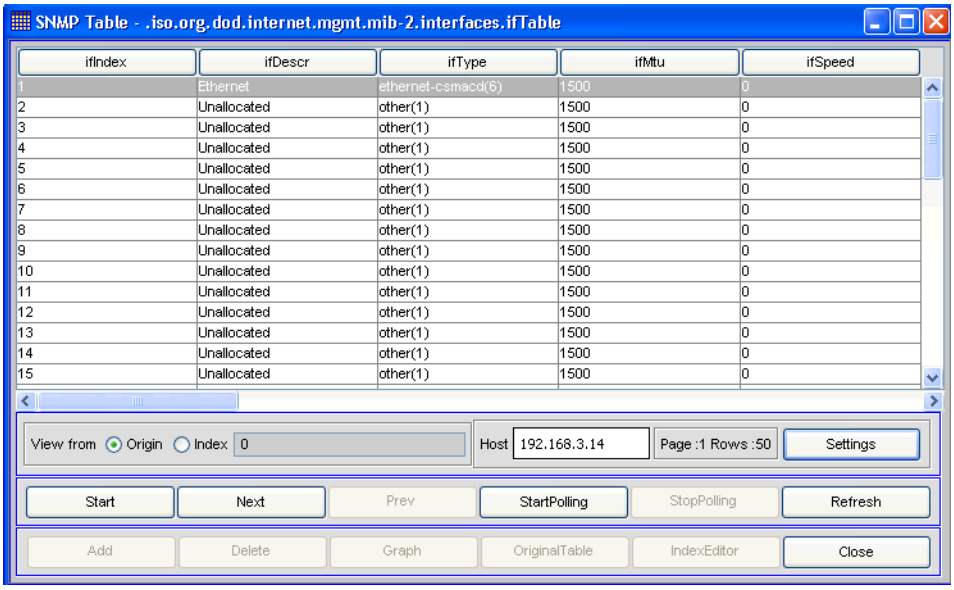


Figure 98. SNMP Table Tool

Gathering Table Data

1. Click **Start** in the SNMP table tool to begin collecting data for the selected table object.
2. Click **Start Polling** to begin polling data based on the polling interval in the **Settings** (see "SNMP Table Settings" on page 120).
3. Click **Stop Polling**.
4. If you are not using the polling option, click **Refresh** to update the table.

SNMP Table Settings

Click **Settings** in the SNMP Table window to change table options.

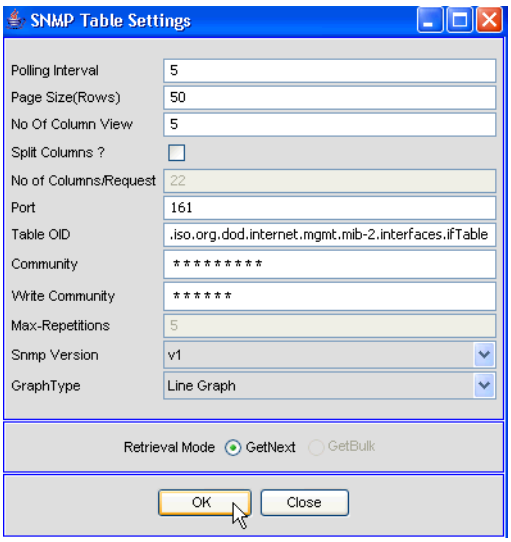


Figure 99. SNMP Table Settings

- **Polling Interval:** Specify the time interval between each retrieval of data. Default = *5 seconds*
- **Page Size (Rows):** Set the number of rows to retrieve from the table. Default = *50 rows*
- **No. of Column View:** Specify the number of columns to display in the SNMP Table window. Default = *5*
- **Split Columns:** When the size of the PDU exceeds the limit, the agent sends the error message "Too Big PDU Error". Check this box to split the PDU.
- **No. of Columns/Request:** If you check the box to **Split Columns**, use this field to specify the number of columns to split.
- **Port:** Specify the port where you want to request table data from.
- **Table OID:** Specify the Object Identifier for the table
- **Community:** Set the community string for the MIB
- **Write Community:** Enter the password for read/write access
- **Max-Repetitions:** ***(Applies only for GETBULK retrieval mode)*** The number of consecutive values that the table retrieves. Default = *5*
- **SNMP Version:** Switch SNMP version (v1, v2c, v3)
- **Graph Type:** Select a graph type (**Line Graph** or **Bar Graph**)
- **Retrieval Mode: GETNEXT** is the default retrieval mode. You may enable **GETBULK** mode for SNMP versions, v2c or v3.

Viewing and Graphing Table Data

You may view detailed information about specific table data in the SNMP Table window. To view more details about an individual column, right-click on the **Column Header** and select **View Column Node Details**. You may also select another column from the drop-down menu in the **Mib Description** window to view description details.

To create a graph of table details, select the entire row(s) and click **Graph**.

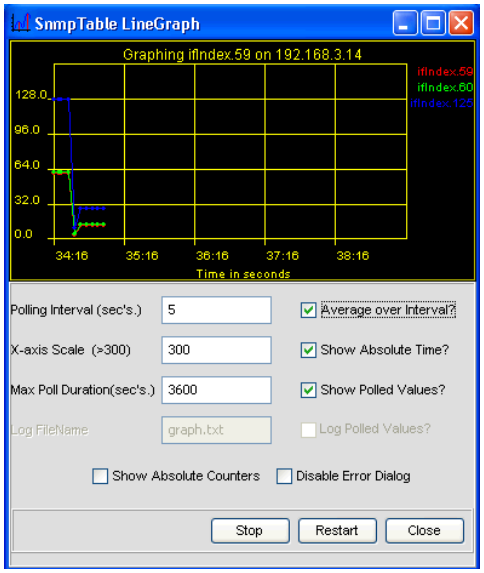


Figure 100. SNMP Table Graph

Move your cursor over the graph to view data values. You may modify the graph settings:

- **Polling Interval:** Specify the time interval between each retrieval of data. Default = *5 seconds*
- **Average over Interval:** By default, the graph shows the values of the specified OID for different hosts for the given polling interval. Select this option to plot the average of the values at a given polling interval.
- **X-axis Scale:** Specify the time value (in seconds) for the X-axis. You must enable the **Show Polled Values** option to modify the **X-axis Scale**. Default = *300 seconds*
- **Show Absolute Time:** Select this option to show time values in the graph as hours:secs.
- **Max Poll Duration (secs):** Specify the time period to show all polled values for that time. You must enable the **Show Polled Values** option to modify the **Max Poll Duration**.
- **Show Polled Values:** Enable this option to display all polled values for a specific time period, and to enable other graph options. Default = *Disabled*
- **Log Filename:** Specify the name for the log file. **You cannot create a log file from a graph when the Mib Manager is running as an applet because of security restrictions.**
- **Log Polled Values:** Enable logging for polled values. **You cannot enable this option when the Mib Manager is running as an applet because of security restrictions.**
- **Show Absolute Counters:** Enable this option to plot all absolute values.
- **Disable Error Dialog:** Enable this option to hide error messages when requests time out.

Debugging Output

The Mib Manager provides a tool for debugging and decoding output from SNMP operations. The **Debug** window logs messages between the PDU manager and PDU agent. The **Decoder** window translates SNMP debug messages.

Debug/Decode Windows

To view the **Debug** window:

1. Click **View** > **Debug** or click  on the toolbar. The **Debug** window displays.
2. As long as the **Debug** window is open, debugging is enabled and will show output messages.

To open the **Decoder** window:

1. The **Debug** window must be open. Select the data in the **Debug** window that you want to decode.
2. Click  . The **Decoder** window displays.
3. The selected data will display in the **Hex PDU** field. Click **Decode** to begin translating.
4. The decoded message displays in the bottom panel of the **Decoder** window.

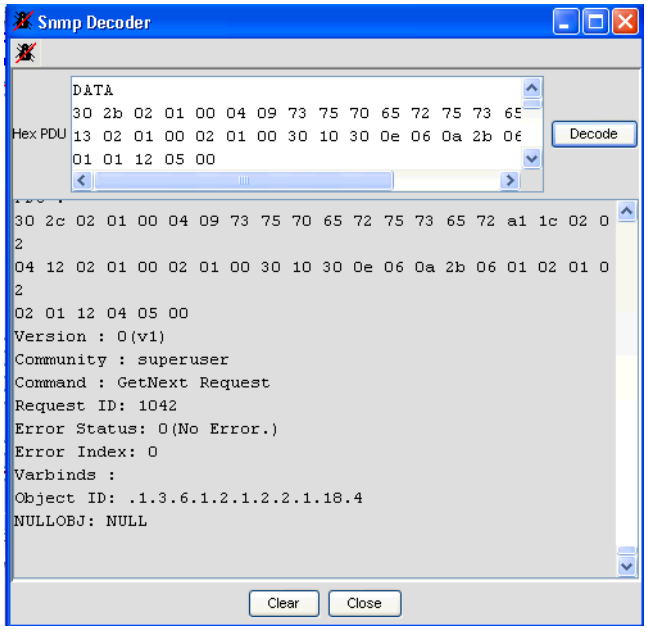


Figure 101. SNMP Decoder

5. Click  to return to the **Debug** window.

Troubleshooting SNMP Error Messages

Table 6 shows a list of error messages and why they might occur.

Table 6. SNMP Error Messages

Error Message	Description
No ObjectID Specified.	Error occurs if the OID is not specified before making a request.
No Host Specified.	Error occurs if the host name is not specified before making a query.
Host Name Should Be Entered.	Error occurs if an SNMP Table is loaded without specifying the host name.
Invalid OID Format	Error occurs if the specified OID is not a valid. It should be an Integer type or String type.
Invalid Table OID	Error occurs if an SNMP Table is loaded after specifying an invalid OID in the OID text field.
Table OID should be specified	Error occurs if an SNMP Table is loaded without specifying any Table OID.
Error Loading MIB: xyz	Error occurs if an invalid file is loaded in the LoadMibDialog text field.
RequestFailed: Error: Request TimedOut To LocalHost	Error occurs during GET, GETNEXT, and SET operations and while creating an SNMP Table, Line Graph or BarGraph: • If the agent does not implement the OID that is queried. • If the agent queried is not present in the network. • If the port number set is not valid for the agent queried. • If the Community and Write Community specified are not correct. • If the OID queried does not contain any data. • If for v3 agents security parameters are not set.
RequestFailed: Get Response PDU received from 192.168.1.001 **Error Indication In Response: There is no such variable name in this mib.** **ErrIndex:**	Error occurs during the SET operation: • If the OID is not instrumented by the agent for which it is setting value • If the agent queried is not present in the network. • If the WriteCommunity specified is not right one. • If the Syntax of the value you are setting is not as that required by the OID. The same error may occur when ploting a graph for a leafNode that is not instrumented by the agent for which it is setting value, and also when querying for data in an SNMP Table if data is not available.

Table 6. SNMP Error Messages

Error Message	Description
RequestFailed: Get Response PDU received from 192.168.1.001 **Error Indication In Response: A not writable error occurred.** **ErrIndex: 1**	Error occurs if the leafNode or OID that you are setting the value for has no read/write access.
ErrorSending Set Request : com.patton.snmp.beans.DataException: Error: OID not a leafnode.	Error occurs during a SET operation, if the OID selected is not a leaf node.
Error sending set request: com.patton.snmp.beans: DataException: Error: Creating Variable	Error occurs if setting a value for a columnnode of a table that does not have rowstatus.
LineGraphBean Error: cannot plot string value Root.....	Error occurs when plotting a graph for a leafNode, if the value of the selected OID is not an Integer/TimeTicks/ type.
LineGraphBean Error: cannot plot these values **.1.3..6.1.2.1.....: value** **.....: value** **.....: value**	Error occurs while plotting a Line/Bar Graph, if the selected OID/LeafNode has syntax: PhysAddress, NetworkAddress, IP Address, OBJECT IDENTIFIER.
Error: com.patton .snmp.beans.DataException: InvalidTable OID:(oid choosen)	Error occurs if the SNMP Table is loaded with an OID that is not a Table OID.
ErrorSendingPDU: Failed to Authenticate the Security Parameters, for user SnmpEngineEntry not found for address(hostname) port(portNo.)	Error occurs while creating an SNMP Table, if the host name specified, or is a different version other than v3 in the settings table.
LineGraphBeanError: cannot plot string value xyz.	Error occurs if the OID/LeafNode chosen for plotting a graph is a String type.
Discovery failed for address (hostname) port (portno.)	Error occurs if the wrong port number is set in the MibSettings panel.
Time Sync Failed for user (user name)	Error occurs if the wrong username/user password/priv password/ TargetHost/SecurityLevel is set in the MibSettings panel.
Error in Getting DataBase Connection:Please check the jdbc parameters: com.patton.snmp.beans.MibException: java.lang.ClassNot FoundException:	Error occurs if DriverName/URL/User Name/Password has been set incorrectly when loading MIBs from database.
Error in Getting DataBase Connection:Please check the jdbc parameters: java.lang.ClassNotfoundException: **(DriverName set)**	Error occurs if the mysql.jar class is not present in the classes directory.
Please enter the UserName	Error occurs if the Username is not set for the v3 User.

Table 6. SNMP Error Messages

Error Message	Description
Sent request to hostName:port no. **Request Failed :SNMPv3 Error in Response. usmStatsUnknownUser-Names(.1.3.6.1.2.1.1...) Counter value = 2HostName**	Error occurs if security parameters are set after setting the version v3 for a v1/v2 agent and a request is made.
Enter the FileName of MibModule	Error occurs while loading the MIBs file if OK button is clicked without selecting any file in "LoadMibDialog".
Error Loading MIB:(filename) **java io FileNotFoundException: Couldn't open stream for filename.cmi**	Error occurs if any file is chosen from outside the MIBs directory.
Error Loading MIB:(filename with full path from home dir).cds **com.patton.snmp.mibs.MibException:The .cds file could not be loaded.**	Error occurs if an invalid .cds file is loaded.
Error Sending PDU: Failed to Authenticate the Security Parameters for user authUser USMUserEntry not found for this user. TimeSynchronizationFailure could have occurred.	Error occurs if the ContextName/ContextEngineID is not set before making a query for SNMP Table.(Database Mode).
Error in (get/getNext/getBulk)request to hostName:port no. **Failed to Authenticate the Security Parameters for user authUser USMUserEntry not found for Address hostname: 161**	Error occurs if the ContextName/ContextEngineID is not set before making a GET/GETNEXT/GETBULK request.
Error in get request from < hostname >: 161 **Unable to encode PDU**	Error occurs during a GET request for a v3 User(Database mode)AuthProtocol: MD5 if Context Name and ContextEngineID are not specified. The same error may also occur GETNEXT and GETBULK operations(for AuthProtocol MD5&SHA).
Error in get request from < hostname >: 161 **Failed to authenticate the security parameters for user privuser authKey length has to be 20.**	Error occurs during a GET request for a v3 User(Database mode)AuthProtocol: SHA if Context Name and ContextEngineID are not specified.
can not plot the chosen variable: iso.org.dod.internet.mgmt.mib2.interfaces.ifTable	Error occurs if the IfTable OID chosen for plotting a graph is not a leaf OID.
sent get request to tonyjpaul:161 **Request Failed: SNMPv3 Error in Respopnse: usm Stats Not InTimeWindows(.1.3.6.1.6.3.1.5.1.1.2.0) CounterValue =13 tonyjpaul**	Error occurs during GET request for a v3 user if Context Name and ContextEngineID are not specified. The same error may also occur for GETNEXT and GETBULK operations.

Table 6. SNMP Error Messages

Error Message	Description
sent getbulk request to localhost:161 **Request Failed: Get Response PDU recieved from 127.0.0.1.** **Error Indication in response : This is a end of MIB View.** **ObjectID: .1.3.6.1.2.1.1.9.1.4.9** **NULLOBJECT:NULL**	Error occurs if the GETBULK operation is performed for "org".(setting version v2/v3 for a v1 host) and/or if the OID/LeafNode selected is the last node of the mib.The same error may also occur for GETNEXT and GET operations.
Error Sending set Request: com.patton.snmp.beans.DataException: Error: Mib node unavailable for OID.	Error occurs while setting value for an OID that does not have a leafnode. It occurs if selecting any OID from "enterprises".
sent get request to < hostname >:161 **Request Failed: Get Response PDU received from 192.168.1.182** **Error Indication in response : There is no such instance in this MIB.** **ObjectID: .1.3.6.1.2.1.1.9.1.4.9** **NULLOBJECT:NULL**	Error occurs during a GET operation on sysServices node for a v3 agent if the leafnode sysServices is not implemented by the agent.
sent get request to <hostname>:161 **Request Failed: Get Response PDU received from 192.168.1.182** **Error Indication in response : A no creation error occurred.** **Errindex:1**	Error occurs during a SET operation on ipRouteDest which has read-write access & syntax of datatype:IP Address for a v3 user. It occurs because values cannot be set if the column is not of Row-Status type.
sent get request to <hostname>:161 **No data available in this subtree**	Error occurs during a GET request for a v2 agent at OID "transmission"(.1.3.6.1.2.1.10) when no data is available for that particular instance of OID.
Error in getting Database Connection . Please check the jdbc Parameters: **com.patton.snmp.mibs.MibException: java.sql.SQL Exception: No suitable Driver.**	Error occurs when connecting to the database for an agent of any version, if the DriverName set is not correct.
Error in Getting DataBase Connection:Please check the jdbc Parameters: java.sql.SQLException: No suitable Driver.	Error occurs when the URL set is not a valid URL for connecting to database.(mysql->msql)
Error in Getting DataBase Connection:Please check the jdbc Parameters: java.sql.SQLException: Cannot connect to MYSQL sever on smplinux:3306. Is there a mysql server is running in the machine/port you are trying to connect to? **(java.net.UnknownHostException)**	Error occurs when the URL set is not a valid URL for connecting to database.(snmplinux->smplinux)

Table 6. SNMP Error Messages

Error Message	Description
Error in Getting DataBase Connection:Please check the jdbc Parameters: java.sql.SQLException: General error: **Unknown database "<tst>"**	Error occurs when the URL set is not a valid URL for connecting to database.(test->tst)
sent set request to <hostname>:161 **Request Failed: SNMPv3 Error in Response : usmStatsNotInTimeWindows(.1.3.6.1.6.3.15.1.1.2.0)Counter value = 75 <hostname>**	Error occurs if the request is made after a certain interval of time.
sent get request to <hostname>:161 **Request Failed: Get Response PDU received from 192.168.1.182** **Error Indication in response : There is no such object in this MIB.** **ObjectID: .1.3.6.1.2.1.8.1.0** **NULLOBJECT:NULL**	This OID is not instrumented for the agent you are querying for or no data is available in this OID.

Chapter 9 Monitoring Managed Objects

Chapter contents

Introduction

Managed objects save information about an element in the network database. The NMS also monitors status polling, data collection & threshold collection for managed objects. You can view a list of managed objects by clicking on **Network Database** in the menu tree on the left side of the screen, and then **Managed Objects**.

This chapter describes viewing the various properties of managed objects. It also covers other aspects of the **Network Database** section of the NMS interface, such as Other Objects which includes DS0 Maps and Inband Channels.

Working with Managed Objects

Click on **Network Database > Managed Objects** in the main menu tree to view a full list of managed objects in the network. Right-click on a device in the Managed Objects table to view a device-specific menu for configuring that device. The device-specific menu also appears as a toolbar at the top of the screen when you select a device in the table. All Managed Objects have a sub-menu with an option to **UnManage** and device-specific tasks.

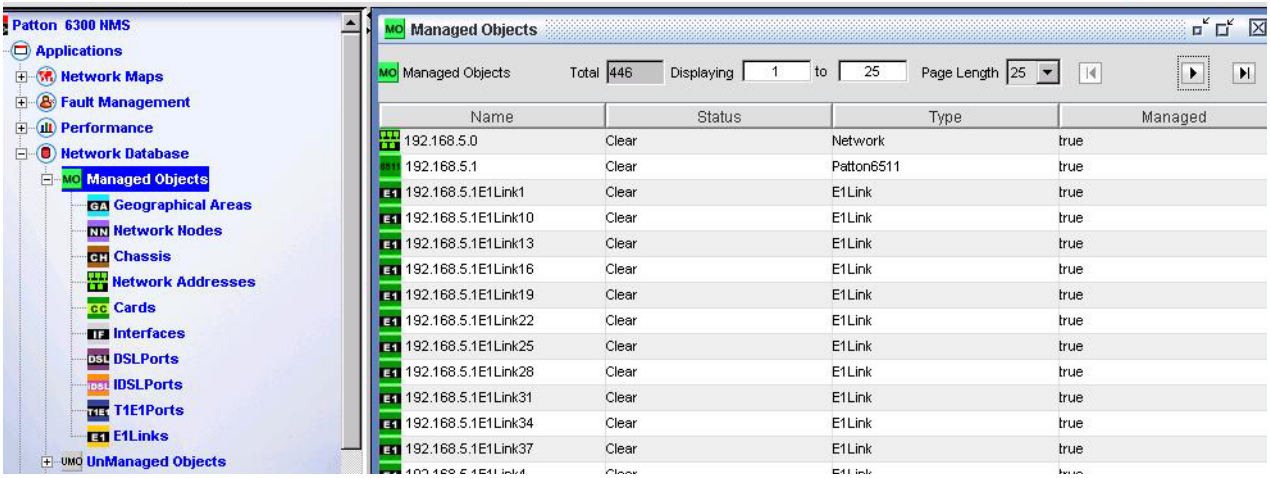


Figure 102. Managed Objects Table

Expand the Managed Objects selection in the menu tree to view specific object categories.

- "Geographical Areas" (See page 130)
- "Network Nodes" (See page 130)
- "Chassis" (See page 130)
- "Network Addresses" (See page 131)
- "Cards" (See page 131)
- "Interfaces" (See page 132)
- "DSL Ports" (See page 132)
- "IDSL Ports" (See page 132)
- "T1/E1 Ports" (See page 132)
- "E1 Links" (See page 133)

Geographical Areas

Navigate to **Network Database > Managed Objects > Geographical Areas** in the menu tree to view a list of all managed geographical areas in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that geographical area.

The configuration menu for a geographical area has the following options:

- **Delete Objects and Traces** – Deletes elements that no longer need to be managed
- **Geographical Area Overview** – Displays a summary of the area name, ID, number of nodes, # of chassis, number of subnets, alarm status.
- **UnManage** – Moves the area to the UnManaged Objects table. Select this option if you no longer want to manage the area, but you do not want to delete it from the client.

Network Nodes

Navigate to **Network Database > Managed Objects > Network Nodes** in the menu tree to view a list of all managed nodes in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that node.

The configuration menu for a network node has the following options:

- **Delete Objects and Traces** – Deletes elements from the NMS that no longer need to be managed
- **Network Node Overview** – Displays a summary of the node, including geographical area name and ID, node name and ID, system manager, and location info.
- **Alarm Trap Manager** – See "Configuring Alarms through the Network Node" on page 95 in Chapter 4.
- **UnManage** – Moves the node to the UnManaged Objects table. Select this option if you no longer want to manage the node, but you do not want to delete it from the client.

Chassis

Navigate to **Network Database > Managed Objects > Chassis** in the menu tree to view a list of all managed chassis in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that chassis.

The configuration menu for a chassis has the following options:

- **Delete Objects and Traces** – Deletes elements that no longer need to be managed
- **Chassis Overview** – Displays a summary of the chassis, including geographical area name and ID, node name and ID, chassis name, ID, and type, network address, number of each card model, and alarm status.
- **Chassis Unit GUI** – Displays the front panels of all of the cards in the chassis in real-time.
- **Chassis Clocking Sync**– See the ***Configuring Chassis*** chapter in the *FS6300 NMS User Manual*.
- **UnManage** – Moves the chassis to the UnManaged Objects table. Select this option if you no longer want to manage the chassis, but you do not want to delete it from the client.

Network Addresses

Navigate to **Network Database > Managed Objects > Network Addresses** in the menu tree to view a list of all managed addresses in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that address.

The configuration menu for an address has the following options:

- **Managed Object Properties** – Displays and modifies details about the managed object related to status monitoring and relationships to other objects.
- **Delete Objects and Traces** – Deletes elements that no longer need to be managed.
- **UnManage** – Moves the network address to the UnManaged Objects table. Select this option if you no longer want to manage this network address, but you do not want to delete it from the client.

Cards

Navigate to **Network Database > Managed Objects > Cards** in the menu tree to view a list of all managed cards in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that card. Each card has different configuration options in the menu, depending on the model of the card you select.

The configuration menu for any card includes the following options:

- **Delete Objects and Traces** – Deletes elements that no longer need to be managed.
- **Card Overview** – Displays a summary of the card, including box information, card information, and alarm status.
- **Alarm Parameter Configuration** – See "Configuring Alarms through a Card in the Chassis" on page 96 in Chapter 4.
- **Card Front Panel GUI** – Displays the front panel of the card in real-time.
- **Card System Clocking** – See the ***Configuring Alarms and Clocking*** chapter in the *FS6300 NMS User Manual*.
- **Card System Configuration** – Displays current configuration settings for the card.
- **Ethernet Overview** – Displays current Ethernet settings for the card.
- **Events and Alerts** – Displays a color-coded chart of events and alarms for the card.
- **Operator Action** – See "Managing Device Configurations" on page 24 in Chapter 1.
- **System Log** – See the ***Configuring and Managing Devices*** chapter in the *FS6300 NMS User Manual*.
- **Ping** – Displays a status message after pinging the interface.
- **UnManage** – Moves the card to the UnManaged Objects table. Select this option if you no longer want to manage the card, but you do not want to delete it from the client.

Interfaces

Navigate to **Network Database > Managed Objects > Interfaces** in the menu tree to view a list of all managed interfaces in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that interface.

The configuration menu for an interface includes the following options:

- **Interface Monitor > Ping** – Displays a status message after pinging the interface.
- **Managed Object Properties** – Displays and modifies details about the managed object related to status monitoring, relationships to other objects, and SNMP attributes.
- **UnManage** – Moves the interface to the UnManaged Objects table. Select this option if you no longer want to manage the interface, but you do not want to delete it from the client.

DSL Ports

Navigate to **Network Database > Managed Objects > DSL Ports** in the menu tree to view a list of all managed G.SHDSL ports in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that DSL port.

The configuration menu for a port includes the following options:

- **G.SHDSL Link Configure** – Displays the G.SHDSL Port Configuration window, where you can view information and edit the desired state and test mode for a specific DSL port.
- **UnManage** – Moves the DSL port to the UnManaged Objects table. Select this option if you no longer want to manage the DSL port, but you do not want to delete it from the client.

IDSL Ports

Navigate to **Network Database > Managed Objects > IDSL Ports** in the menu tree to view a list of all managed IDSL ports in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that port.

The configuration menu for a port includes the following options:

- **IDSL Link Configure** – Displays the IDSL Port Configuration window.
- **UnManage** – Moves the IDSL port to the UnManaged Objects table. Select this option if you no longer want to manage the IDSL port, but you do not want to delete it from the client.

T1/E1 Ports

Navigate to **Network Database > Managed Objects > T1E1 Ports** in the menu tree to view a list of all managed T1/E1 ports in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that T1/E1 port.

The configuration menu for a port includes the following options:

- **Configure T1/E1 Link** – Displays the T1/E1 Configuration window.
- **UnManage** – Moves the T1/E1 port to the UnManaged Objects table. Select this option if you no longer want to manage the T1/E1 port, but you do not want to delete it from the client.

E1 Links

Navigate to **Network Database > Managed Objects > E1 Links** in the menu tree to view a list of all managed E1 links in the network. Select a row and click the new menu in the toolbar at the top of the screen (or right-click on the row) to view the configuration menu for that link.

The configuration menu for an E1 link includes the following options:

- **E1 Port Link Configuration** – Displays the SDH Test Overview window, where you can view information and edit line interface and test paramters.
- **UnManage** – Moves the E1 link to the UnManaged Objects table. Select this option if you no longer want to manage the E1 link, but you do not want to delete it from the client.

Working with Other Objects

Click on **Network Database > Other Objects** to view a list of all of the objects that exist in the network although the NMS does *not* provide fault management (such as status polling, data collection, trap processing, and alarm propagation).

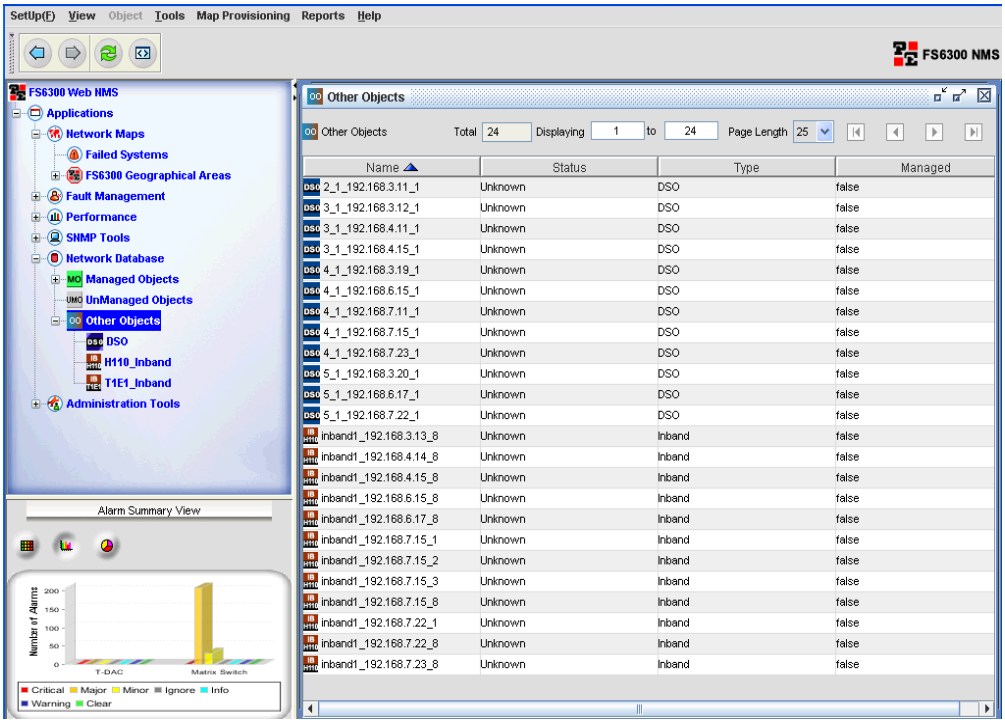


Figure 103. Other Objects Table

To change an object's status from unmanaged to managed:

1. Right-click on the row of the object in the **Other Objects** table.
2. Select **Manage** to move the device to the **Managed Objects** table.
3. Select **Managed Object Properties** to view management details about the device.

Chapter 10 **Managing Database Policies**

Chapter contents

Overview

Policies are specific tasks that are executed at a certain time based on a set of specified conditions. Policies are used for cleaning up tables, backing up the NMS, and configuring automatic alerts.

To reach the Policies screen, click on **Policies** (under Administration Tools) in the main menu tree. When Policies is selected in the menu tree, the **Policy** toolbar appears at the top of the screen. From the Policy toolbar menu, you can:

- Add Policy (Ctrl+P)
- Search Policies (Ctrl+F)
- Refresh Policies (F5)

Figure 104. Policy Menu

When you click on **Policies** in the menu tree, a table displays in the main screen which shows a list of all policies that exist in the NMS. The policies in the table are color-coded– Green policies are enabled, Red policies are disabled, and Orange policies are enabled but are either not fully configured, or there was an error during execution.

There are four types of policies that can be added to the NMS:

- Table Cleanup
- 6300 NMS Backup
- Alert Delete
- Alert Action

Adding Policies

There are four different types of policies and each policy have different requirements that need to be configured. However, the first steps of adding a policy are the same, regardless of the type of policy.

To add a new policy:

1. In the main menu tree, click on **Policies** (under Administration Tools).
2. Select **Policy > Add Policy** from the toolbar at the top of the screen (Figure 104 on page 135).
3. Select the type of policy you want to add from the drop-down menu.

Figure 105. Policy drop-down menu

4. Enter a unique name for the policy in the **Interface Name** field. Note that the **Instance Name** cannot be the same as the **Policy** name.
5. Click **Add**.
6. A window will display with specific configuration details for the policy you selected. See the following sections for more information about configuring specific policies:
   - "Table Cleanup Policy" on page 137
   - "6300 NMS Backup Policy" on page 138
   - "Alert Delete Policy" on page 139
   - "Alert Action Policy" on page 140

Table Cleanup Policy

The **Statistics Table Cleanup** policy automatically cleans statistical information from the database. Table 7 describes the fields for adding a new **StatsTableCleanup** policy.

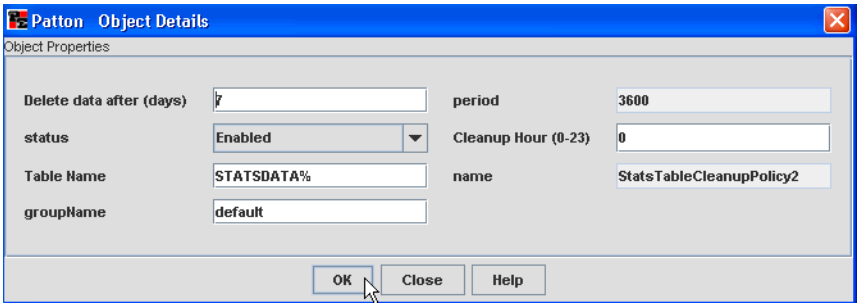


Figure 106. Adding Table Cleanup Policy

Table 7. Table Cleanup Policy Properties

Property	Description
Delete data after (days)	Specify how long to store the data in the database before it is deleted. Default = 7days
status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when it is Enabled.
Table Name	Specify the name of the table that stores the statistical data. Default = STATSDATA%, unless you have changed the data collection parameters. If you have specified your own table name in the data collection parameters, that table name should be specified in this field.
groupName	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. (You can execute different policies at the same time by associating them with a common group name).
Period	Displays the interval (default interval - 3600 seconds) at which the policy checks whether it is time for cleanup. *This field cannot be edited.*
Cleanup Hour (0-23)	Specify the hour of the day to clean up the statistics. Default = 0 (i.e., between Midnight and 1 A.M.).
name	Displays the name of the policy. *This field cannot be edited.*

6300 NMS Backup Policy

The **6300 NMS Backup** policy automatically backups the system to reduce the load on the server.

1. Click on **Administration Tools** > **Policies** in the NMS menu tree.
2. Select **Policy** > **Add Policy** from the menu at the top of the screen. The **Add Policy Details** window displays.

Figure 107. Add Backup Policy

3. Select **6300NMSBackupPolicy** from the drop-down menu. Enter a **Name** for the backup policy and click **Add**. The **Object Details** window displays.

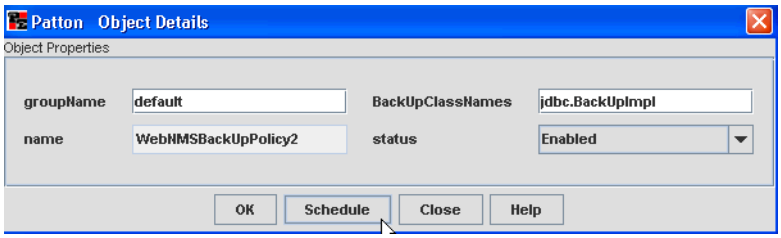


Figure 108. Policy Details

4. Table 8 describes the fields for adding a new **6300NMSBackup** policy.

Table 8. FS6300 NMS Backup Policy Properties

Property	Description
groupname	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. (You can execute different policies at the same time by associating them with a common group name).
name	Displays the name of the backup policy. *This field cannot be edited.*
BackUpClassNames	Specify the class name implementing the backup interface.
Status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when it is Enabled.

5. Click **Schedule** in the **Object Details** window. The **Policy Scheduler** window displays. Select the radio buttons for **Dates** or **Days**, depending on what your policy schedule will be based on. You can select all

dates/days and hours, or specific selections. Click on the box of the day, date, or hour to make your selection. Then, click **OK**.

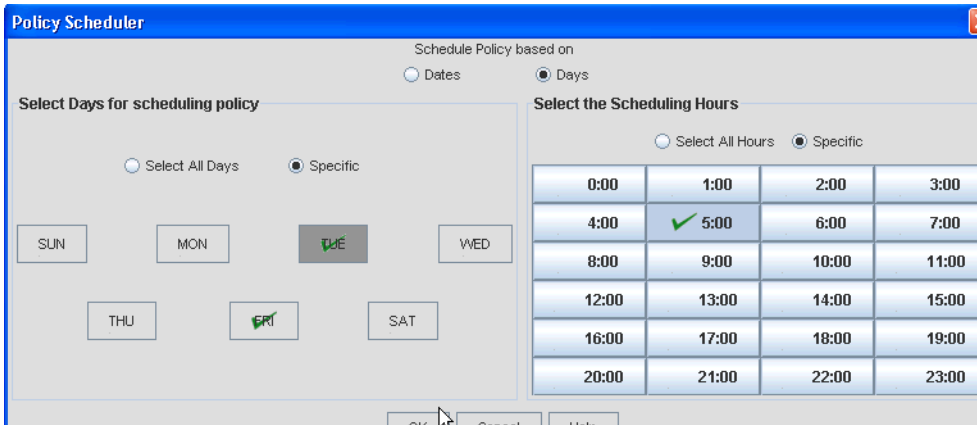


Figure 109. Policy Scheduler

6. Click **OK** in the **Object Details** window to save the policy. A confirmation message displays that the policy was added successfully.

Alert Delete Policy

The **Alert Delete** policy automatically backups the system to reduce the load on the server.

Table 8 describes the fields for adding a new **AlertDelete** policy.

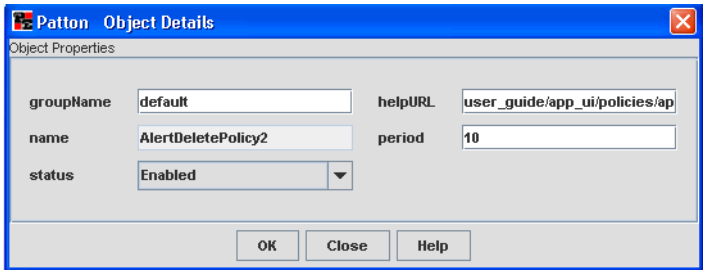


Figure 110. Adding Alert Delete Policy

Table 9. Alert Delete Policy Properties

Property	Description
groupName	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. (You can execute different policies at the same time by associating them with a common group name).
name	Displays the name of the policy. *This field cannot be edited.*
status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when it is Enabled.
helpURL	Links to a corresponding help file.
period	Displays the interval at which the policy checks whether it is time for backup.

Alert Action Policy

The **Alert Action Policy** checks alarms in the database. If an alarm is in the same state for a certain amount of a time without any change in severity, an action (set by the administrator) will be taken. Table 10 describes the fields for adding a new **AlertAction** policy.

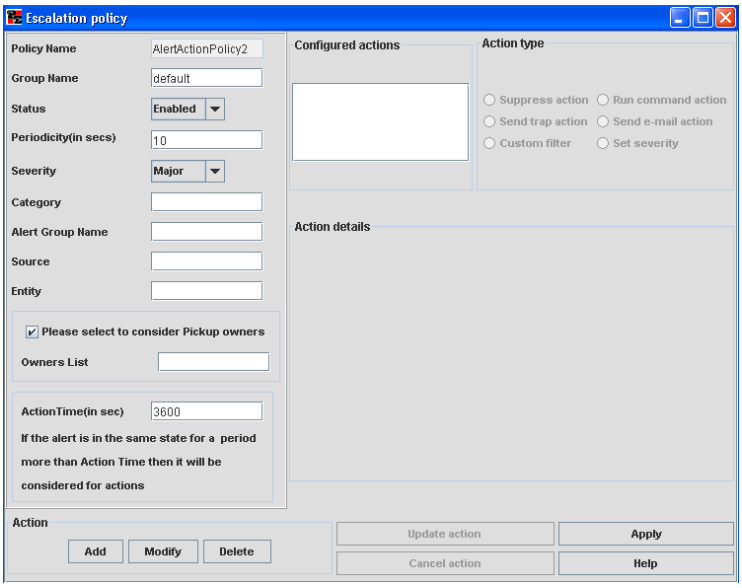


Figure 111. Adding Alert Action Policy

Table 10. Alert Action Policy Properties

Property	Description
Policy Name	Displays the name of the policy. *This field cannot be edited.*
Group Name	Displays the default group name. Edit this field to change the group name. Default = deault
Status	Specify whether the policy is Enabled or Disabled. The policy can be executed only if it is Enabled.
Periodicity (secs)	Specify the interval (in seconds) between two successive execution of the policy. Default =10 seconds
Severity	Specifies the severity of an alarm that causes an action to take place if the severity state hasn't changed in a certain amount of time.
Category	Specify the category which serves as a match criterion.
Alert Group Name	Specify the name of the alert group.
Source	Specify the name of the source whose alerts are to be picked.
Entity	Specify the name of the interface the source (whose alerts are to be picked) communicates with.
Owner's List	Specify the e-mail IDs that picked alerts are e-mailed to. *Applies to the 'Send E-mail Action'.*
Action Time (in secs)	Specify the maximum time limit for an alarm to remain in a particular state. If an alarm remains in the same state for more than the specified period, then an action is triggered.

Action Types

There are several types of actions that can be configured when the severity of alarm has been in the same state for a certain amount of time:

Suppress Action. This action suppresses alarms matching a particular criteria– either all together, or multiple alarms of the same type within a given interval. When an alarm occurs, you can suppress all the alarms that match a particular filter.

To suppress alarms:

1. In the Escalation Policy window, select **Suppress Action** (under **Action Type**).

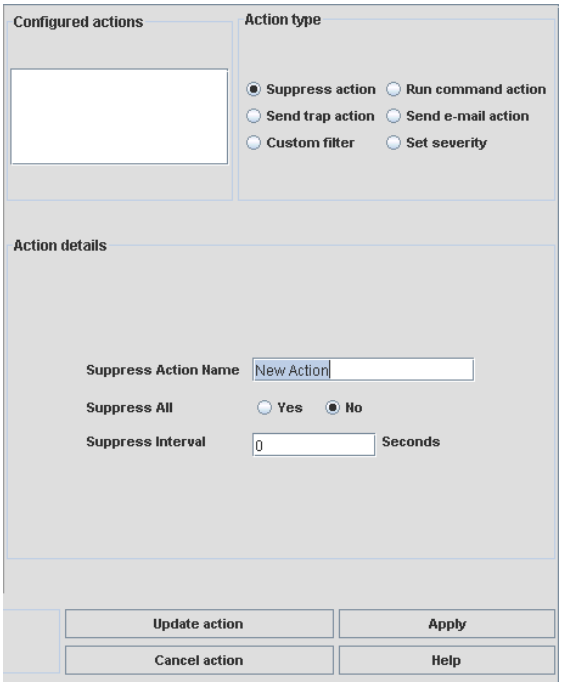


Figure 112. Suppress Action

2. In the Action details section, enter a unique name in the **Suppress Action Name** field.
3. To suppress all the events and alarms, select **Yes** in the **Suppress All** field. To suppress multiple alarms for a given interval, select **No**. Specify the interval in seconds in the **Suppress Interval** field.
4. Click the **Update Action** button to add the action to the Configured Actions list.
5. If you are finished adding actions, click the **Apply** button.

Send Trap Action. This action sends SNMP v1 or v2c traps for the alarms matching the specified criteria.

To send traps:

1. In the **Escalation Policy** window, select **Send Trap Action** (under **Action Type**).

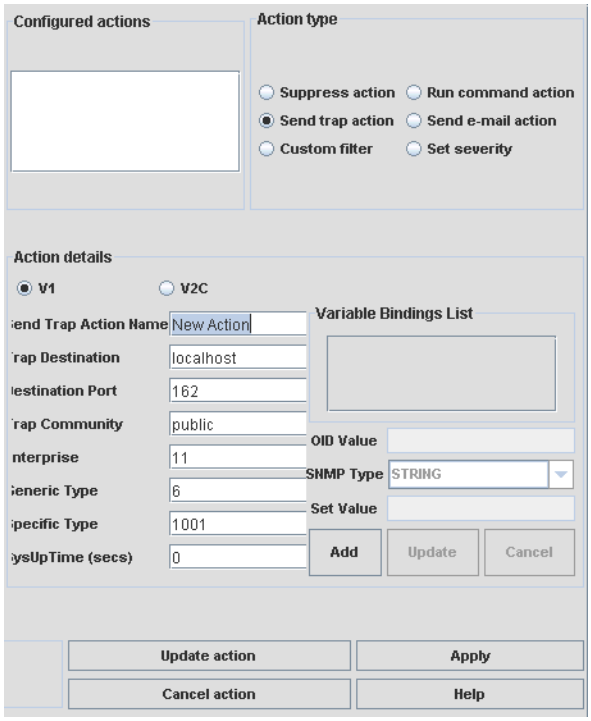


Figure 113. Send Trap Action

2. In the **Action details** section, specify values for the following:
   - **V1** or **V2C**: Select SNMP trap type.
   - **Send Trap Action Name:** Specify a name for the trap action.
   - **Trap Destination:** Specify the host to send the trap to.
   - **Destination Port:** Specify the destination host port to send the trap to.
   - **Trap Community:** Specify the community to be set for the generated trap.
   - **Enterprise:** Specify the enterprise OID of the trap.
   - **Generic Type:** Specify the generic type number to use for the trap.
   - **Specific Type:** Specify the type number to use for the trap.
   - **SysUpTime:** Specify the sysuptime value to use in the trap.
3. You can also set variable bindings to the trap. To add a variable biding, click **Add**. Specify the **OID Value**, **SNMP Type**, and **Set Value**. Click **Update**.
4. Click **Update Action**. Then, click **Apply**.

Send E-mail Action. This action sends an e-mail on receiving an alarm of a specific kind (specified in the filter match criteria).

To set up an e-mail action:

1. In **Escalation Policy** window, select **Send e-mail action** (under **Action Type**).

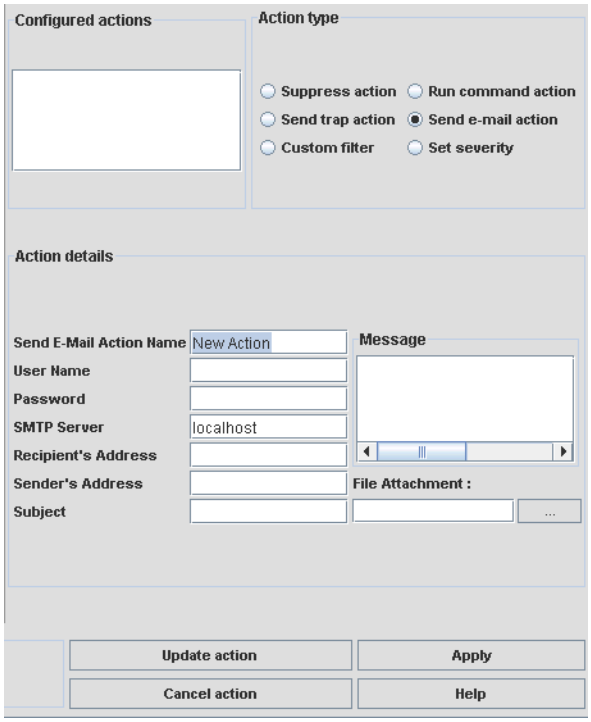


Figure 114. Send E-mail Action

2. In the **Action Details** section, specify the following:
   - **Send Email Action Name:** Specify a name for the e-mail action.
   - **User Name:** Specify the user name for the mail server that will authenticate you to send the e-mail.
   - **Password:** Specify the password for the mail server that will authenticate you to send the e-mail.
   - **SMTP Server:** Specify the SMTP server name.
   - **Recipient's Address:** Specify the e-mail address for the user that will receive the e-mail.
   - **Sender's Address:** Specify the e-mail address that will show in the From field of the e-mail.
   - **Subject:** Specify the subject of the e-mail.
   - **Message:** Specify the message to be sent in the e-mail.
   - **File Attachment:** Specify the location of a file to be attached in the e-mail.
3. Click **Update Action**. Then, click **Apply**.

Custom Filter. You can create your own custom filter and define rules for processing alarms. To use custom filters, write your own filter class in JAVA. The custom filters that you implement must be compiled and placed in the CLASSPATH of the FS6300 NMS Java Virtual Machine.

To use custom filters:

1. In **Escalation Policy** window, select **Custom Filter** (under **Action Type**).

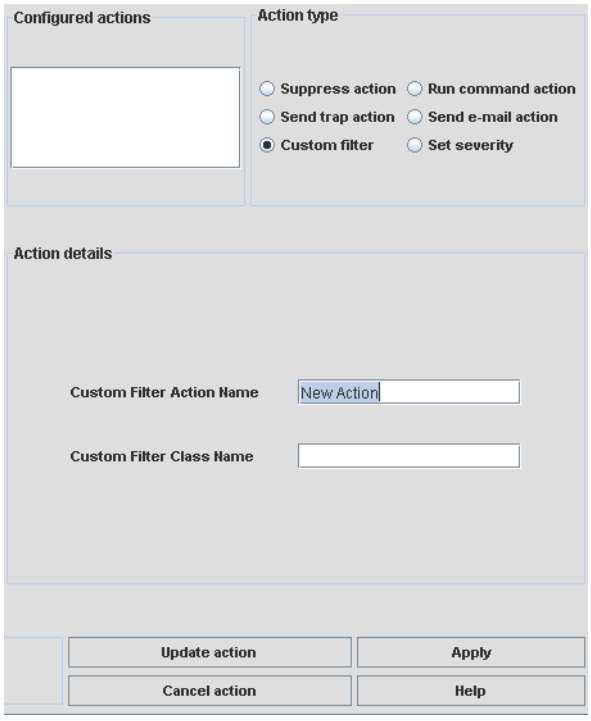


Figure 115. Add Custom Filter

2. In the **Action Details** section, specify the following:
   - **Custom Filter Action Name:** Enter a name for the custom filter.
   - **Custom Filter Class Name:** Enter the custom filter class name.
3. Click **Update Action**. Then, click **Apply**.

Run Command Action. This action triggers a specific command when an alarm is received.

To run a command:

1. In **Escalation Policy** window, select **Run Command Action** (under **Action Type**).

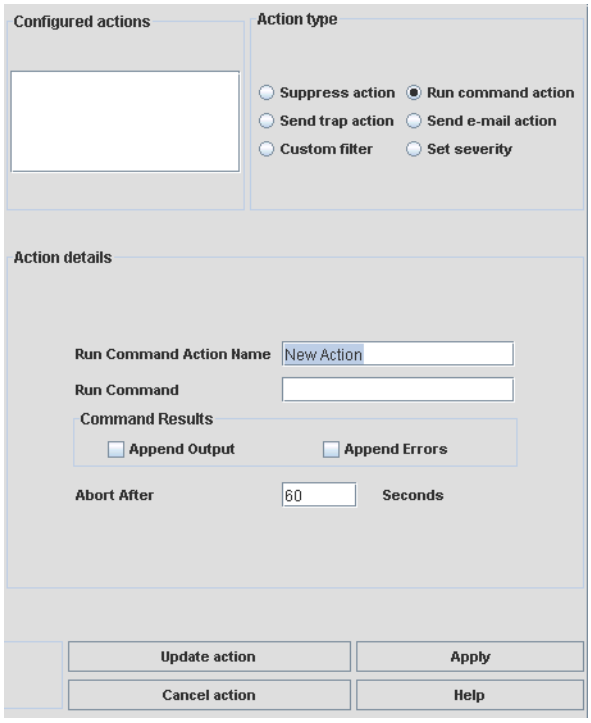


Figure 116. Run Command Action

2. In the **Action Details** section, specify the following:
   - **Run Command Action Name:** Enter a name for the run command action.
   - **Run Command:** Specify the command string to be executed. The command string should be a machine executable program on the server that does not require a shell, i.e., it cannot be a batch or shell file. To use shell scripts or commands, you must invoke the shell as a part of the command string. The command string should be specified with the full path of the shell, where the server has been started.
   - **Command Results:** To append the output or errors from the command to the event message text, select Append Output or Append Errors. Selecting either option will run the command synchronously in the main event processing thread. This delays all alarms, following the alarm being processed, until the command execution completes or is terminated by the timeout option.
   - **Abort After:** Enter the timeout for the command. After the time specified in this field has passed, the command execution is stopped. This is important, if you are appending the output or errors, since all alarm processing is held up by the command execution.
3. Click **Update Action**. Then, click **Apply**.

Set Severity. This action escalates or de-escalates the severity of an alarm.

To set severity:

1. In **Escalation Policy** window, select **Set Severity** (under **Action Type**).

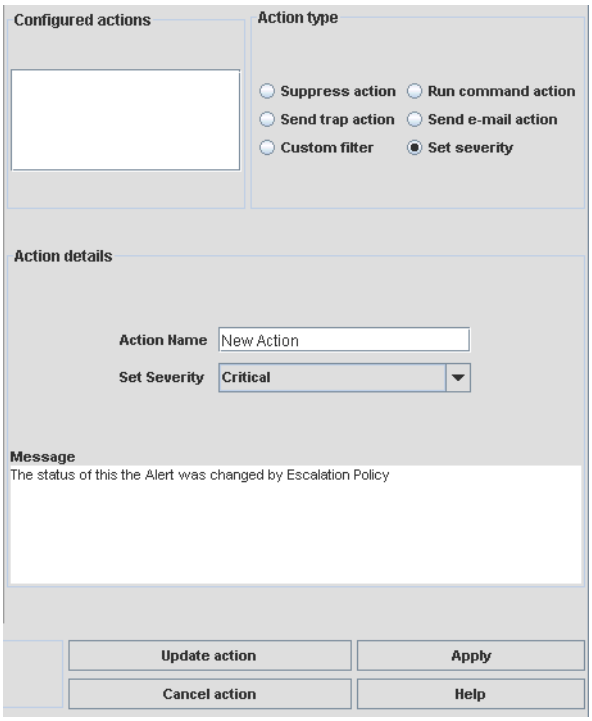


Figure 117. Set Severity

2. In the **Action Details** section, specify the following:
   - **Action Name:** Enter a name for the set severity action.
   - **Set Severity:** Select the severity (Critical, Major, Minor, ect...) from the drop-down box.
   - **Message:** Enter a message in this field to send when the severity level changes (optional).
3. Click **Update Action**. Then, click **Apply**.

Modifying Policies

To edit an existing policy:

1. Click on **Policies** in the menu tree (under **Administration Tools**).
2. Select the row of the policy in the **Policies** table.
3. **Right-click** on the selected policy, or press **Ctrl+U**.
4. Make the desired changes, then click **OK**.

Deleting Policies

To delete a policy:

1. Click on **Policies** in the menu tree (under **Administration Tools**).
2. Select the row of the policy in the **Policies** table.
3. **Right-click** on the selected policy, or press **Ctrl+C**.
4. A message will display, asking if you are sure that you want to delete the policy. Click **Yes**.
5. A confirmation message will display– "Policy deleted successfully." Click **OK**.

Executing Policies

To manually start a policy:

1. Click on **Policies** in the menu tree (under **Administration Tools**).
2. Select the row of the policy in the **Policies** table.
3. **Right-click** on the selected policy, or press **Ctrl+X**.
4. A confirmation message will display. Click **OK**.

Stopping Policies

To stop a policy while it is running:

1. Click on **Policies** in the menu tree (under **Administration Tools**).
2. Select the row of the policy in the **Policies** table.
3. **Right-click** on the selected policy, or press **Ctrl+T**.
4. A message will display, asking if you are sure that you want to stop the policy. Click **Yes**.
5. A confirmation message will display– "Policy stopped successfully." Click **OK**.

Chapter 11 Contacting Patton for assistance

Chapter contents

Introduction

This chapter contains the following information:

- "Contact information"—describes how to contact PATTON technical support for assistance.
- "Warranty Service and Returned Merchandise Authorizations (RMAs)"—contains information about the RAS warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

- Online support—available at **www.patton.com**.
- E-mail support—e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support—standard telephone support is available Monday through Friday, from 8:00 A.M. to 5:00 P.M. EST (8:00 to 17:00 UTC-5), Monday through Friday by calling **+1 (301) 975-1007**

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at **www.patton.com**
- By calling **+1 (301) 975-1000** and speaking to a Technical Support Engineer
- By sending an e-mail to **returns@patton.com**

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company
RMA#: xxxx
7622 Rickenbacker Dr.
Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

Appendix A **Recovering the NMS Server from Disk**

Chapter contents

Introduction

This chapter describes how to upgrade the server firmware and how to restore the NMS server if the disk fails.

To restore the NMS server, perform the following sections in order:

- "Upgrading the RAID Controller" on page 152
- "Assigning Spare Drives" on page 154
- "Rebuilding the NMS Server" on page 155

Upgrading the RAID Controller

To upgrade the server firmware:

1. Place the **Highpoint RR3120 firmware upgrade 1.2.25.8 bootable** CD into the optical drive of the NMS server. Restart the system. The NMS server will boot from the firmware upgrade CD.

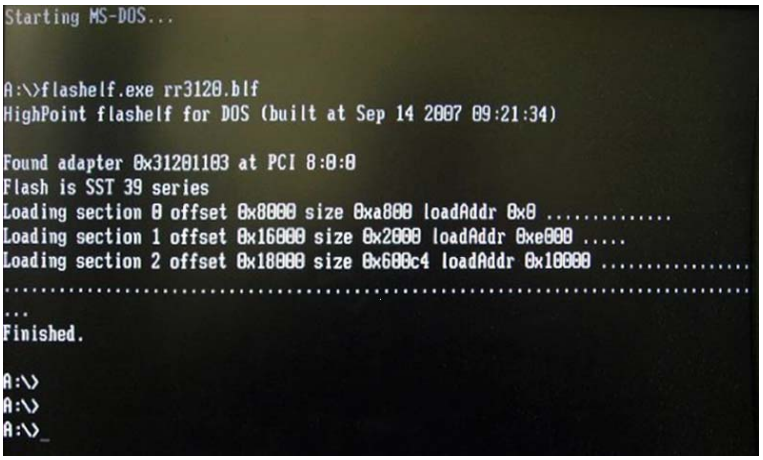


Figure 118. Boot from firmware upgrade CD

2. Once the Flash process completes, remove the CD from the optical drive. Then, power off the NMS server and turn it back on. At the RAID initialize screen, press the **CTRL** and **H** keys at the same time to start the BIOS Setting Utility.

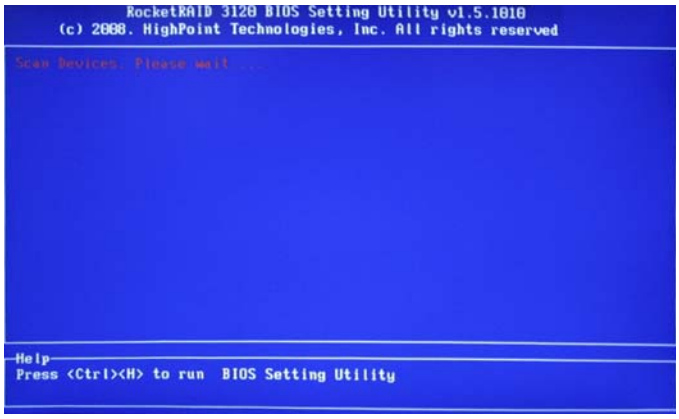


Figure 119. BIOS Setting Utility

3. To show the server's firmware version, select **View > Controller** from the top of the screen.

Figure 120. View > Controller

4. Verify that the firmware version is "**v1.2.25.8**" as shown in Figure 121.

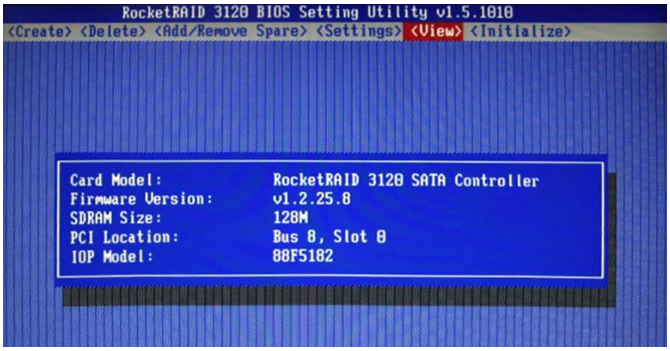


Figure 121. Firmware Version

5. Select **Settings > Parameter Setting** from the top of the screen. Enable **Auto Rebuild** (if disabled).

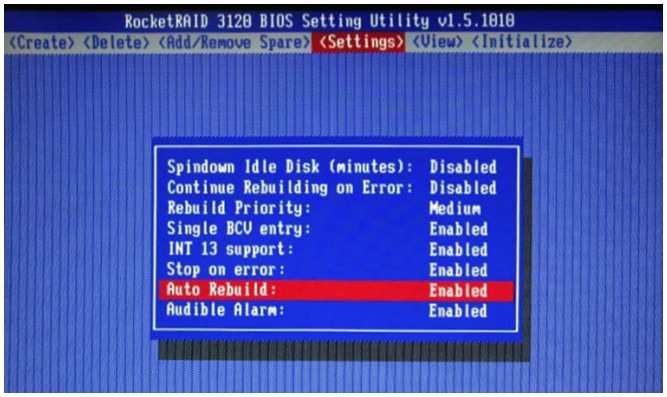


Figure 122. Enable Auto Rebuild

Note If the intention is to only upgrade the RAID controller and not restore the NMS server, restart the system now and resume normal use. To continue the procedure for restoring the NMS server, follow the instructions in the next section, "Assigning Spare Drives".

Assigning Spare Drives

Creating a spare drive is the next procedure in the process to restore the NMS server from disk. Ensure that you have verified the firmware version and enabled auto rebuild in the BIOS Setting Utility (as instructed in the section "Upgrading the RAID Controller" on page 152) before assigning spare drives.

1. In the BIOS Setting Utility, select **Delete** at the top of the screen. Select the **FS6300NMS** entry and press **Enter**. The Array list should now be empty.

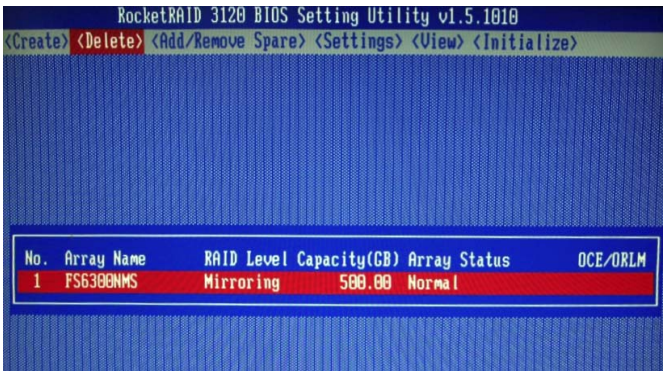


Figure 123. Delete FS6300NMS Array

2. Select **Add/Remove Spare** from the top of the screen. Assign each drive in the list as a spare for array use later in the process.

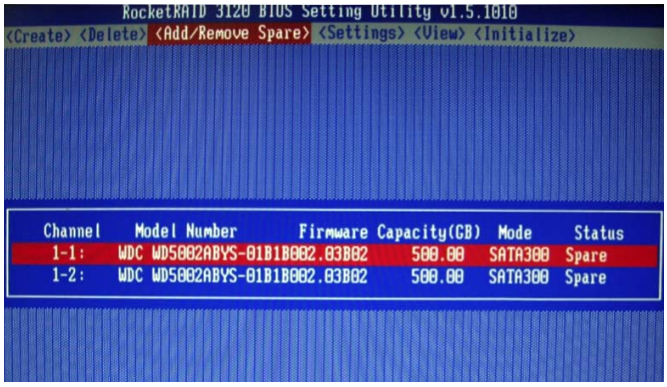


Figure 124. Assign Both Drives as Spares

3. Press the Power button to shut down the NMS server. Remove one of the disks and label the drive as "**system1 spare**". Then, replace the empty bay with the provided "**RMA recovery drive**."
4. Continue the process with the procedure in the next section, "Rebuilding the NMS Server".

Rebuilding the NMS Server

Before following the steps in this section, ensure that you have assigned the spare drives and have removed and replaced one of the drives with the **RMA recovery drive** (as instructed in the section "Assigning Spare Drives" on page 154).

To rebuild the NMS server:

1. Press the power button to turn on the NMS server. At the RAID initialize screen, press the **CTRL** and **H** keys at the same time to start the BIOS Setting Utility (Figure 119).
2. The RAID Controller automatically begins the rebuilding process. To view the progress, select **View > RAID Array** from the top of the screen.

Figure 125. View > RAID Array

Leave the system on the **RAID Array** screen (Figure 126) and wait for the rebuilding progress to reach 100%. The rebuilding process usually takes about 1.5 hours. When the progress finishes, the array status will change to "**Normal**".

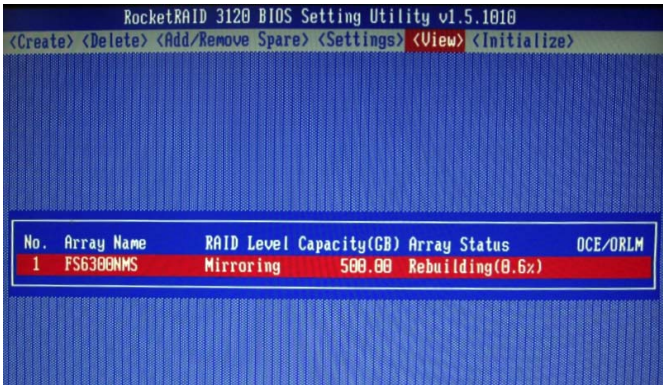


Figure 126. Rebuild Progress

3. After the rebuild process reaches 100%, leave the system running and pull out the "**RMA recovery drive**" from the NMS server. Label the drive as "**reference for server 2**".
4. Insert the "**system1 spare**" drive into the empty drive bay. The rebuild process will start again.
5. While system 1 is performing the rebuild process, repeat the above process to rebuild server 2.
6. When the re-build process finishes on both servers, reboot the servers. Remember to provision the IP address and host files in FC6.

At this point, the NMS servers are restored and ready for normal operation.