



Release 8

NI-Director User Guide

July 16, 2013

The content of this document is subject to change without notice.

Copyright 2011 - 2013

Nakina Systems Inc., Nakina Systems, Nakina Integrity Solutions, NI-Guardian, NI-Collector, NI-Controller, NI-Director, NI-Framework, Nakina Open Console, Nakina Network Troubleshooting Console, Nakina Secure Network Access Client, Nakina Command Broker, Nakina Session Broker, Nakina Network Backup and Restore, Nakina Network Audit & Software Delivery, Nakina Network Commissioning, Nakina Domain Activation, Nakina Adapter SDK and Simply Profitable Networks are all trademarks or registered trademarks of Nakina Systems Inc. All other trademarks are property of their respective

All rights reserved.

Table of contents

1. Revision history	7
2. Vendor Files: Managing vendor configuration files	8
2.1 About vendor configuration files	8
2.2 Add a vendor configuration file to the database	10
2.3 List the vendor configuration files and view or modify the details.	11
2.4 Delete a configuration file from the database	12
3. Backup & Restore: Backing up and restoring NE data	13
3.1 About Backup and Restore	14
3.2 Configuring and performing network element backups	18
3.2.1 Configure the default settings for scheduled and immediate backups	18
3.2.2 Create a scheduled backup job for one or more NE Groups	20
3.2.3 Run a scheduled backup job immediately	24
3.2.4 Perform an immediate backup of one or more NEs	26
3.2.5 Re-run a backup job for one or more failed NEs	27
3.2.6 Copy a backup image from the file server to your PC	30
3.3 Managing scheduled backups	31
3.3.1 List the scheduled backups and view or modify details	32
3.3.2 Enable a backup schedule for one or more NEs	34
3.3.3 Disable a scheduled backup	34
3.3.4 Delete a scheduled backup from the database	35
3.4 Managing immediate NE backups	36
3.4.1 Search for NEs to view their backup status and details	36
3.4.2 Delete an NE backup image	40
3.5 Managing backup jobs	41
3.5.1 List all backup jobs and view job details	41
3.5.2 Delete an immediate backup job	43
3.6 Restore NE configuration data	44
4. Network Audit: Auditing the network before a software delivery	47
4.1 About hardware and alarm audits	49
4.2 Configuring and running hardware and alarm audits	50
4.2.1 Create a hardware component XML file	50
4.2.2 Create a hardware audit profile	52
4.2.3 Create an alarm audit XML file	57
4.2.4 Create an alarm audit profile	58
4.2.5 Perform an audit	62
4.3 Managing audit specifications and jobs	66

4.3.1	View the list of audit specifications	66
4.3.2	Modify an existing hardware audit specification	67
4.3.3	Modify an existing alarm audit specification	71
4.3.4	View a list of audit jobs and job details	74
4.3.5	Delete an audit job from the database	76
4.3.6	Delete an audit specification from the database	77
5. Software Delivery: Performing NE software delivery		79
5.1	Configuring and performing a software delivery	80
5.1.1	Create and run hardware and alarm audits	81
5.1.2	Copy software releases to the managed file server	81
5.1.3	Create a software image configuration file	82
5.2	Create a software release specification	83
5.2.1	Create a software delivery workflow	93
5.2.2	Create targets in a workflow	98
5.2.3	Perform a software delivery on workflow targets	101
5.2.4	Monitor the software release process	109
5.3	Managing software releases	111
5.3.1	Copy software releases to a managed file server	112
5.3.2	List of software releases and view or modify details I.	112
5.3.3	Delete a software release from the database	118
5.4	Managing software delivery workflows	119
5.4.1	List workflows and view or modify details	119
5.4.2	Delete a workflow from the database	124
5.5	Managing software delivery targets	125
5.5.1	List targets within a workflow and view or modify target details	125
5.5.2	Delete targets from a workflow	130
6. Fault Manager: Configuring NE fault collection and reporting		131
6.1	Configure fault collection for each network element	131
6.2	Configure the automatic fault reporting parameters	134
6.3	View archived historical events	135
7. Performance Monitoring: Configuring and managing performance monitoring		137
7.1	About Performance Monitoring	138
7.1.1	Adapter support for PM data collection	138
7.1.2	About PM collection configuration	139
7.1.3	About PM export collection and configuration	139
7.1.4	About PM jobs	140
7.1.5	About PM data removal configuration	141
7.1.6	PM report viewing and format.	141
7.1.7	Performance Monitoring search attributes	142
7.2	Configuring performance monitoring collection	142

7.2.1	Configure the PM groups to be collected for NEs or NE Groups	142
7.2.2	Configure a data cleanup policy and a data export server	146
7.2.3	Modify the PM Groups that are collected for an individual NE	147
7.2.4	Modify the PM groups to be collected for multiple NEs or NE Groups	150
7.3	View or modify NE performance monitoring details	153
7.4	Managing performance monitoring jobs	159
7.4.1	View PM jobs and job details	159
7.4.2	Delete a job from the database	160
7.4.3	Re-run a failed "PM Collection Configuration" job	161
8	NE Security: Managing network element credentials	163
8.1	NE Security prerequisites and considerations	164
8.1.1	NE Security Role and permission prerequisite	164
8.1.2	NE Security adapter considerations	164
8.1.3	NE Security and password rule considerations	165
8.2	Creating credentials on network elements	165
8.2.1	Create a credential on a single network element	167
8.2.2	Create a credential on multiple NEs	171
8.3	Deleting or changing credentials	178
8.3.1	Change or delete one or more credentials on a specific network element	179
8.3.2	Change or delete a specific credential on all NEs	181
8.4	About searching for credentials	182
8.5	Managing NE security jobs	184
8.5.1	View NE Security job details	184
8.5.2	Delete unwanted NE security jobs	186
9	Inventory: Performing and managing searches	187
9.1	Understanding searches	188
9.1.1	About the search screens	188
9.1.2	AND versus OR searches	190
9.1.3	Complete list of search attributes	191
9.1.4	Using wildcards in search criteria	199
9.1.5	Working with table data	199
9.2	Performing a search	201
9.3	Loading, saving and deleting search criteria	201
9.4	Saving search results to a file	202
10	Inventory Reports: Creating and managing inventory reporting	204
10.1	Create an inventory reporting schedule	204
10.2	Generate an inventory report immediately	211
10.3	List report tasks and view or modify details	213
10.4	Download an inventory report from the server	216
10.5	Delete an inventory report task from the database	217

11.Command Broker: Configuring and managing TL1 command groups 219

11.1 About TL1 command groups. 220

11.1.1 How TL1 command groups are interpreted by the system. 220

11.1.2 About TL1 command formats 223

11.1.3 About TL1 input command filtering. 223

11.2 Create TL1 command groups 224

11.3 Managing TL1 command groups 226

11.3.1 List TL1 command groups and view or modify details 227

11.3.2 Copy and modify an existing TL1 command group 228

11.3.3 Delete a TL1 command group 229

1 Revision history

NI-Director User Guide: this guide is for NI-Director administrators and users. It contains procedures for using the NI-Director applications, which include:

- Backup and Restore
- Network Audit
- Software Delivery
- Performance Monitoring
- Fault Collection
- NE Security
- Vendor Files
- Inventory Reporting

Before using the NI-Director procedures, you must configure NI-Framework as described in the NI-Framework Configuration Guide.

The following table provides a summary of the major changes made to this document for NI-Director. Each new version of this document supersedes all earlier versions until re-issued.

Issue date	Description
July 16, 2013	Removed Device Configuration and added the new Vendor Files tool for 8.3.
May 22, 2013	Second issue of this document for NI-Director release 8.3 or higher unless re-issued.
March 20, 2013	First issue of this document for NI-Director release 8.3 or higher unless re-issued.



Note: You must familiarize yourself with the detailed operation of each managed network element. If an application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. The information in the Adapter Notes must be made available to the users so they know what to expect when managing network elements from the client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

2 Vendor Files: Managing vendor configuration files

This section contains the following NI-Director procedures for managing vendor configuration files used to automatically configure pre-provisioned CPEs in an ethernet service:

- [“About vendor configuration files” on page 8](#)
- [“Add a vendor configuration file to the database” on page 10](#)
- [“List the vendor configuration files and view or modify the details” on page 11](#)
- [“Delete a configuration file from the database” on page 12](#)

Read the adapter notes



Note: If an application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they know what to expect when managing network elements from the Network Integrity client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

2.1 About vendor configuration files

Vendor Configuration files are provided by an equipment vendor to configure parameters on a specific model of network element. They are used by Network Integrity to automatically activate a CPE that was previously pre-provisioned as part of an Ethernet Service, and is now physically installed and turned up.

Vendor configuration files must be imported into the Network Integrity database for use during activation.

For a given adapter, there should be one vendor configuration file for each supported common CPE configuration. For example, if the common CPE configuration varies by region, there should be one common vendor configuration file per adapter, per region; such as:

- "EasternRegion" (Adva 825)
- "EasternRegion" (Adva 114)
- "EasternRegion" (RAD 205)
- "WesternRegion" (Adva 825)

These configuration files should not manipulate CLI user ids or SNMP community names. These will be managed using NE security templates.

Sample vendor configuration file

The following example is for demonstration purposes only, and shows the content of a typical configuration file:

```
remark Template Version: 0.3
configure system
snmp-dying-gasp enable
security-strength low
clock timezone cst
security-banner "This system is restricted solely to authorized users
for legitimate business purposes only. The actual or attempted
unauthorized access, use or modification of this system is strictly
prohibited. Unauthorized users are subject to company disciplinary
proceedings and/or criminal and civil penalties under state, federal or
other applicable domestic and foreign laws."
  sntpclient mode unicast
  sntpclient server 192.168.0.1
  security-strength low
  syslogclient server 192.168.1.1
  cli-prompt testing-activation1
exit

configure interface e1000-wan-1
  adminstate enable
  speed auto1000full
  media fiber
  cpd-filter efm-oam discard
exit

configure mgmttnl e1000-wan-1
  ripv2 disable
  mode mac
  dhcp enable
  no ip access-group system in
exit

configure communications
  proxyarp disable
exit

config power-supply psu-2
  assignstate disable
exit

configure snmp
  traphost 172.16.1.37:162 2c public
exit
database save
```

About roles and permissions for vendor configuration files

Access to the Vendor Files application is controlled by the **Configuration Administration Role**, which has two permissions: “View Configuration Data” and “Manage Configuration Data”.

2.2 Add a vendor configuration file to the database

Use this procedure to add a vendor configuration file to the database and associate it with one or more compatible adapters. A vendor configuration file is used to automatically configure pre-provisioned CPEs in an ethernet service.

Before using this procedure, you must obtain the configuration file from the vendor and place it in a directory that can be navigated to.

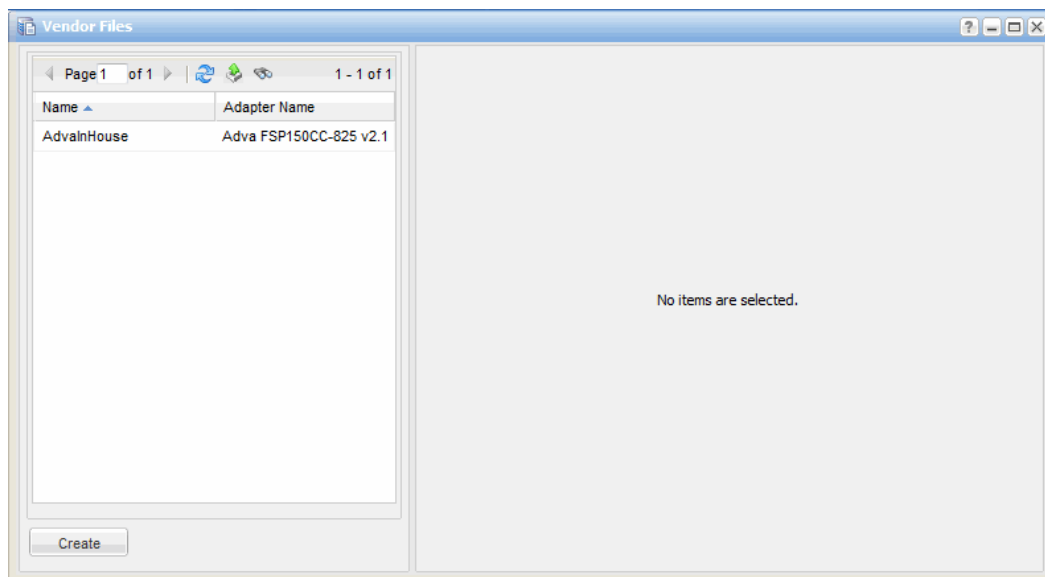


CAUTION: The data provided in the configuration file must be entered and tested by experienced administration personnel who fully understand the NEs and the parameters they are provisioning. Network Integrity validates the file against the associated adapter, but it does not validate the data within the file. Failure to test and validate all aspects of the configuration file can lead to unintended NE configuration.

1. Launch **Vendor Files**.

The system displays the Vendor Files screen which lists the currently imported files.

The system displays the list of vendor files and the associated adapters.



2. Click **Create**.

The system displays the vendor file details.

3. In the **Name** field, type a name to describe the file you are importing.
4. Click **Browse** and select the desired vendor configuration file. When the file has been selected, click **Open**.
5. From the Adapter Name list, select the adapter to associate with the configuration file.
6. Click **Save**.

The system stores the vendor configuration details in the Network Integrity database.

2.3 List the vendor configuration files and view or modify the details

Use this procedure to view a list of the configuration files that have been added to Network Integrity. From the list of configuration files, you can select one to view or modify the associated adapters and file details.



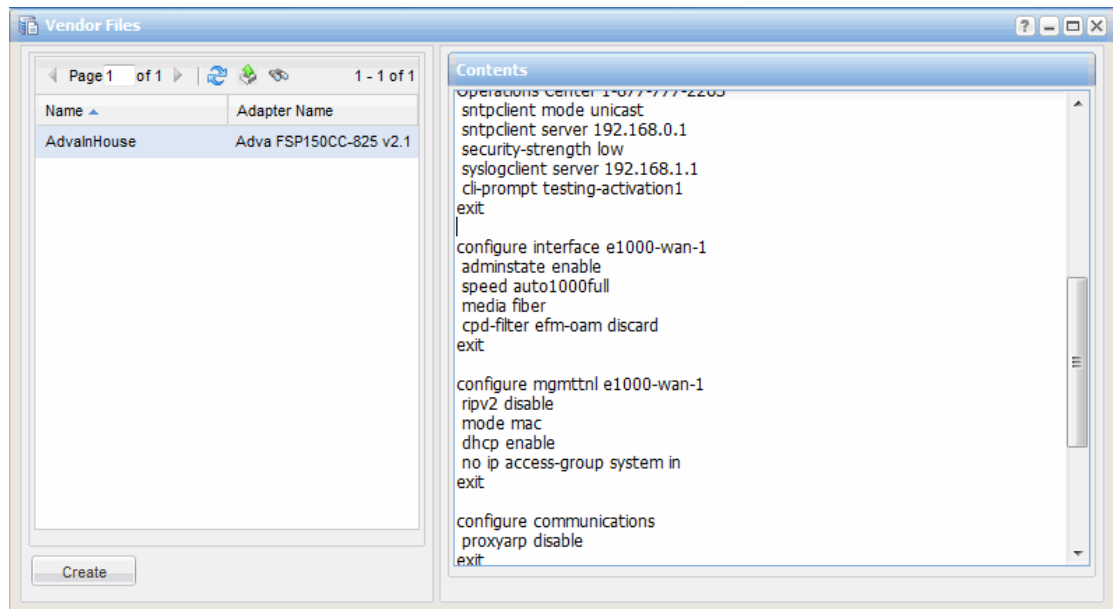
CAUTION: The data provided in the configuration file must be entered and tested by experienced administration personnel who fully understand the NEs and the parameters they are provisioning. Network Integrity validates the file against the associated adapter, but it does not validate the data within the file. Failure to test and validate all aspects of the configuration file can lead to unintended NE configuration.



Note: When a configuration file is modified, a copy is created and modified in the database, but the original file that was imported remains unchanged on the managed server.

1. Launch **Vendor Files**.
The system displays the Vendor Files screen which lists the currently imported files.
2. To view the details of the configuration file, click on the name.

The system displays the details in the Contents panel.



3. To modify a vendor configuration file, right-click and select **Modify**. You can change the Name, choose a different configuration file, or change the adapter.
4. When the desired changes have been made, click **Save**.
The system updates the database.

2.4 Delete a configuration file from the database

Use this procedure to delete a configuration file from the Network Integrity database.

1. Launch **Vendor Files**.
The system displays the Vendor Files screen which lists the currently imported files.
2. Select one or more vendor configuration files to be deleted.
3. Click **Delete**.
The system prompts for confirmation.
4. Click **OK** to delete the file.
The system removes the configuration file from the database.

3 Backup & Restore: Backing up and restoring NE data

The NI-Director **Backup And Restore** application is used to capture and restore NE configuration data. Data backups use a file transfer protocol to securely transfer and maintain network element configuration data. If a network element has a system crash or the existing data becomes corrupted, authorized users can restore a previously backed up image to one or more NEs.



Note: If an application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they know what to expect when managing network elements from the Network Integrity client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.



Note: It is recommended that you store at least two backup images for every network element in your network. This is to ensure that if a backup is lost or fails, or a restore operation fails, a second backup image is available.

This section contains the following procedures for Backup and Restore:

“About Backup and Restore” on page 14

This section provides an overview of the Backup and Restore features.

“Configuring and performing network element backups” on page 18

This section contains all the procedures to configure and run scheduled and immediate backups of NE data.

- [“Configure the default settings for scheduled and immediate backups” on page 18](#)
- [“Create a scheduled backup job for one or more NE Groups” on page 20](#)
- [“Run a scheduled backup job immediately” on page 24](#)
- [“Perform an immediate backup of one or more NEs” on page 26](#)
- [“Re-run a backup job for one or more failed NEs” on page 27](#)
- [“Copy a backup image from the file server to your PC” on page 30](#)

“Managing scheduled backups” on page 31

This section contains the procedures for managing scheduled NE backups that have already been configured.

- [“List the scheduled backups and view or modify details” on page 32](#)
- [“Enable a backup schedule for one or more NEs” on page 34](#)
- [“Disable a scheduled backup” on page 34](#)
- [“Delete a scheduled backup from the database” on page 35](#)

“Managing immediate NE backups” on page 36

This section contains the procedures for managing immediate NE backups.

- [“Search for NEs to view their backup status and details” on page 36](#)
- [“Delete an NE backup image” on page 40](#)

“Managing backup jobs” on page 41

This section contains the procedures for managing backup jobs.

- [“List all backup jobs and view job details” on page 41](#)
- [“Delete an immediate backup job” on page 43](#)

“Restore NE configuration data” on page 44

3.1 About Backup and Restore

The Backup and Restore application greatly simplifies complex backup and restore procedures by providing operator-oriented features from a common user interface for all managed network elements.

Time-consuming manual backup procedures are eliminated through automated, scheduled backups. You can maintain as many backups as required, and if a network failure occurs, the network can be quickly restored from any image with minimal manual intervention.

The Backup and Restore user interface is designed to allow operators to focus their efforts on problem areas without wasting precious resources on successful backup jobs. Flexible searching and filtering options allow network operators to easily identify consecutive failures and to drill down and troubleshoot problems.

Operators can search for one or more NEs, filter the results, and compare backup and restore data on the same screen. For example, operators can search for a specific type

of NE and compare the last successful backup to the last failed restore operation. The following example shows a search for all failed backups on Nortel NEs.

The screenshot shows the 'Backup and Restore' application window. The 'Backup Search Criteria' section has 'Last Backup Result' set to 'Failed'. The 'NE Search Criteria' section has 'Vendor/Model/Version' set to 'Nortel'. The 'Search Result' section shows a table with 2 items.

Select	NE Name	Backup				Restore		
		Last Result	Current State	Consecutive Failures	Last Successful	Last Result	Current State	Last Restored Image Name
<input type="checkbox"/>	OM3500-3-NP	Failed	Idle	1		Unstarted	Unstarted	
<input type="checkbox"/>	OM3500-1-SP	Failed	Idle	1		Unstarted	Unstarted	

For each backup and restore task on each NE the following information is provided on the same screen so that comparisons can be made:

- **Last Backup Result:** search results can be filtered on the status of the last backup: Unstarted, Success, or Failed
- **Current Backup State:** - search results can be filtered on the status of the current backup: Unstarted, InProgress, Idle, Stopped, Success, Failed, or Pending
- **Consecutive failures:** the number of consecutive backup failures. The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.
- **Last Successful:** the date and time of the last successful backup
- **Last Restore Result:** search results can be filtered on the status of the last restore: Unstarted, Success, or Failed
- **Current Restore State:** search results can be filtered on the status of the current restore: Unstarted, InProgress, Idle, Stopped, Success, Failed, or Pending

- **Last Restored Image Name:** the name of the image that was last restored successfully

If a scheduled or immediate backup job fails, it can be re-run on just the failed NEs with the click of a button without wasting resources on the successful backups. Each job provides a link to the job logs which contain additional troubleshooting information about the task.

The image shows two screenshots from a software interface. The top screenshot is titled "Backup Job Status Details" and displays job information for a failed backup. It includes fields for Job Name, Schedule, File Server, Last Successful Backup Time, Last Backup Time, Current State (Failed), and counts for Passed, Fail, In Progress, and Pending. Below this is a table of NE Information with one item: ZON1, Adtran, OPTI-6100, and State Failed. A button "Run immediate backup on failed NEs" is circled in red. The bottom screenshot is titled "Log Details" and shows log information for the failed backup, including Log ID, Log Time, Application Name, Activity, and a detailed error message: "Error: NE: VERN1, Cause: Command failed on NE: Error code: OperationFailed Error message: OPTI6100 BACKUP/RESTORE ERROR: The FTOT_SNMP Management Credential does not exist." A red arrow points from the "Failed" state in the top window to the "Log Details" window, with the text "Drill down for log details".

Backup Job Status Details

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Backup Job Status Details

Job Name ZON1 Failed#1 01:24 04:11:26 PM GMT

Schedule

File Server ftp naksf01

Last Successful Backup Time

Last Backup Time 2008.01.24 04:24:12 PM GMT

Current State Failed

Passed 0

Fail 1

In Progress 0

Pending 0

Any Status Search Reset Rows per page: 10

NE Name	Vendor	Model	State
ZON1	Adtran	OPTI-6100	Failed

Run immediate backup on failed NEs Close

Log Details

Log ID SYSLOG-1601

Log Time 2008.01.24 04:24:07 PM GMT

Application Name Backup And Restore

Activity Backup

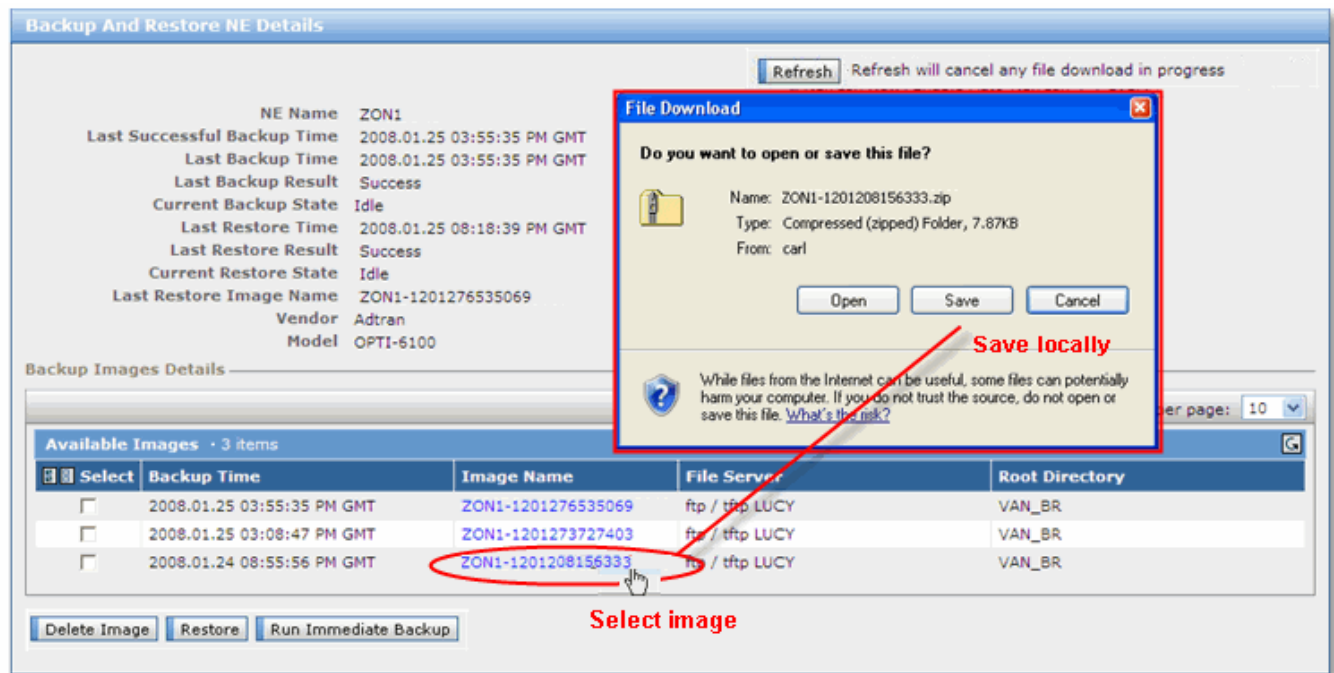
Message Error: NE: VERN1, Cause: Command failed on NE: Error code: OperationFailed Error message: OPTI6100 BACKUP/RESTORE ERROR: The FTOT_SNMP Management Credential does not exist.

Close

Drill down for log details

Operators can quickly and easily locate and obtain a copy of a backup image for an NE, by clicking the NE Name in the search results, which displays the list of images. With a

single click on the image name, the operator can copy the compressed image file from the backup server to the local PC for additional troubleshooting.



Access to Backup and Restore is controlled through the user roles and permissions, which define the tasks that can be performed and the NEs that can be accessed. To use the Backup And Restore application, a user account must be assigned to the Backup and Restore Administration Role and have the correct permissions and NE Groups assigned. Without the correct permissions and NE group assignments, users can not access some or all of the features or NEs.



Note: Each network adapter comes with an Adapter Note that identifies any special considerations or limitations with the NE or the adapter. Read the notes to make sure that Backup and Restore is supported for your NEs, and to see if there are any vendor-specific NE issues that you need to be aware of.

Backup and Restore search attributes

The [Backup and Restore search attributes](#) allow you to search for all attributes associated with Backup and Restore searches.

Table 3–1: Backup and Restore search attributes

Attribute	Searches for
Last Backup Result	NEs based on the status of the last backup: Unstarted, In Progress, Stopped, Success, Failed, or Pending.

Attribute	Searches for
Current Backup State	NEs based on the status of the current backup: Unstarted, Success, Failed, InProgress, Pending or Idle.
Last Restore Result	NEs based on the status of the last restore: Unstarted, Success, or Failed.
Current Restore State	The status of the current restore: <ul style="list-style-type: none">• Unstarted: restore job has not started• Success: restore job has completed successfully• Failed: restore job failed• InProgress: restore job is currently in progress• Pending: restore job is waiting to run• Idle: no restore action being performed on the NE

3.2 Configuring and performing network element backups

This section contains the procedures to configure scheduled backups and perform immediate backups on NEs.

- [“Configure the default settings for scheduled and immediate backups” on page 18](#)
- [“Create a scheduled backup job for one or more NE Groups” on page 20](#)
- [“Enable a backup schedule for one or more NEs” on page 34](#)
- [“Run a scheduled backup job immediately” on page 24](#)
- [“Perform an immediate backup of one or more NEs” on page 26](#)
- [“Re-run a backup job for one or more failed NEs” on page 27](#)
- [“Copy a backup image from the file server to your PC” on page 30](#)



Note: For NEs that use TFTP, you must configure the TFTP server on a Unix system so that Backup and Restore features function properly. For details see the Network Integrity Installation and Administration Guide.

3.2.1 Configure the default settings for scheduled and immediate backups

Use this procedure to set the defaults for all scheduled and immediate NE backups. The system displays the default information each time you configure a backup and allows you to make changes if required.

Table [Backup configuration parameters](#) lists the backup configuration defaults that can be configured.

Prerequisites

You must add a managed file server to the database so that it is available for selection in the following procedure.

1. Launch **Backup And Restore**.
2. If not already selected, click the **Default Configuration** tab.
The system displays the following configuration screen.

The screenshot shows the 'Backup and Restore' window with the 'Default Configuration' tab selected. The window has a blue header bar with the title 'Backup and Restore'. Below the header are four tabs: 'Current NE Status', 'Scheduled Backups', 'Jobs', and 'Default Configuration'. The 'Default Configuration' tab is active. The configuration area is divided into two sections: 'Default Configuration' and 'File Server'. The 'Default Configuration' section contains four input fields: 'Backup Root Directory' (text box with 'backups/current'), 'Number of Backups per-NE, per-job' (text box with '10'), 'Maximum Concurrent Backups' (text box with '3'), and 'Maximum Concurrent Backups per GNE' (text box with '3'). Each of these four fields has a red asterisk to its right, indicating it is mandatory. The 'File Server' section contains four fields: 'Server Name' (dropdown menu with 'local' selected), 'IP Address' (text box with '172.16.1.58'), 'Port Number' (text box with '21'), and 'User Name' (text box with 'temp'). The 'Server Name' field also has a red asterisk to its right. At the bottom left of the configuration area is a 'Save' button.

3. Configure the backup defaults as described in the [Backup configuration parameters](#) table. Fields marked with a red asterisk are mandatory.

Table 3–2: Backup configuration parameters

Field	Description
Default Configuration	
Backup Root Directory	The path relative to the user's root directory on the managed server. Do not begin the path with / or \. If the directory does not exist, the system creates one automatically relative to the user root directory.
Number of Backups per-NE, per-job	The maximum number of images to keep on the file server for each NE for each job.
Maximum Concurrent Backups	The maximum number of NEs to be backed up concurrently (at the same time) during the job.
Maximum Concurrent Backups per GNE	The maximum number of subtending NEs per GNE to be backed up concurrently (at the same time) during the job.
File Server	
Server Name	The name of the managed file server where the backups are stored.

Field	Description
IP Address	This is a read-only field. The IP address of the file server based on the selection from the Server Name list.
Port Number	This is a read-only field. The port number on the file server being used for the backup.
User Name	This is a read-only field. The user name used to log on to the file server being used for the backup.

- When the required fields have been configured, click **Save**.

These values appear as the defaults when you create a scheduled backup job, but the values can be changed during the creation procedure.

3.2.2 Create a scheduled backup job for one or more NE Groups

Use this procedure to create a scheduled backup job for one or more NE groups. After a scheduled backup job is created, it can be run immediately or left to run at the scheduled time and frequency.



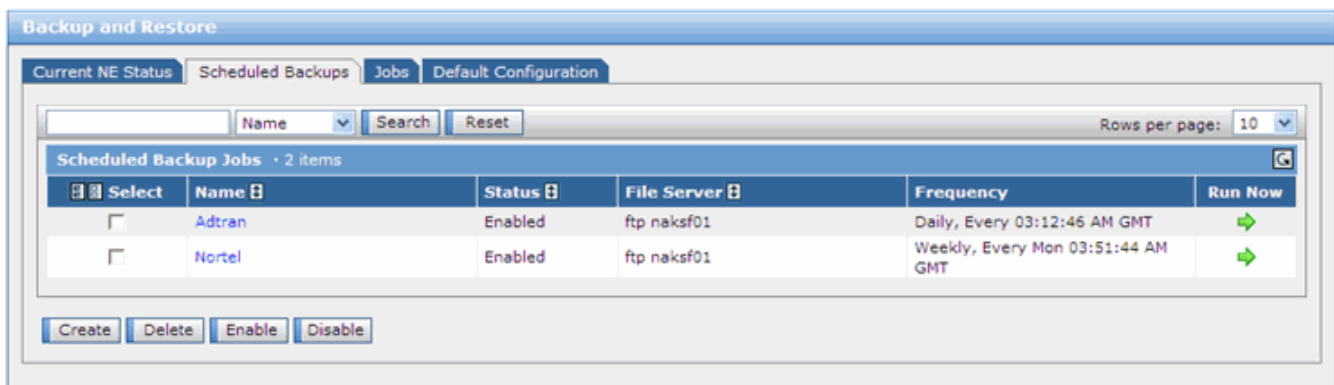
Note: The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.

Prerequisites

Follow the procedure in the NI-Framework Configuration Guide to “Configure file servers for your products” and add a remote server for NI-Director.

- Launch **Backup And Restore**.
- If not already selected, click the **Scheduled Backups** tab.

The system displays the list of existing backup jobs.



- Click **Create**.

The system displays Step 1 of the Create Backup Job wizard where you define general parameters and file server for the scheduled backup.

The screenshot shows the 'Create Schedule Backup' wizard, Step 1: General Information. The window has a blue title bar and a left sidebar with a blue arrow pointing left and the text 'Step 1: General Information'. The main area contains the following fields:

- Backup Job Name: [Empty text box] *
- Backup Root Directory: R7
- Number of Backups per-NE, per-job: 10 *
- Maximum Concurrent Backups: 3 *
- Maximum Concurrent Backups per GNE: 3 *
- Description: [Empty text box]
- User ID: sysadmin

Below these fields is a section titled 'File Server' with a horizontal line. Under this line are the following fields:

- Server Name: MyServer (dropdown menu) *
- IP Address: 172.16.1.58
- Port Number: 21
- User Name: temp

At the bottom right of the window are two buttons: 'Next >>' and 'Cancel'.

4. In the **Backup Job Name** field, provide a name for the backup job. This name identifies the backup in the list of Scheduled Backups and in the list of Jobs.
5. If required, change the remaining defaults as described in table [“Backup configuration parameters” on page 19](#). Fields marked with a red asterisk are mandatory.
6. When the general information has been specified, click **Next**.

The system displays Step 2 of the Create Backup Job wizard where you select the NE Groups on which to run the schedule.

The screenshot shows the 'Create Backup Job' wizard at Step 2: Choose NE Group. The left sidebar indicates the current step. The main area is divided into two sections: 'Available NE Group' and 'Added NE Group'. The 'Available NE Group' section contains a search bar, a 'Search' button, and a list of 14 NE Groups. The 'Added NE Group' section is currently empty, showing 'no entries' and a 'Remove' button. The 'Group_Fujitsu_FLM600_1.0' is selected in the available list. Navigation buttons at the bottom include '<< Back', 'Next >>', and 'Cancel'.

Available NE Group
<input type="checkbox"/> 3535
<input type="checkbox"/> All NEs
<input type="checkbox"/> Group_Alcatel_1603_1.0
<input type="checkbox"/> Group_Cisco_15454_1.0
<input type="checkbox"/> Group_Cisco_2600_1.0
<input type="checkbox"/> Group_Cisco_2924-XL Switch_1.0
<input checked="" type="checkbox"/> Group_Fujitsu_FLM600_1.0
<input type="checkbox"/> Group_HP_HP4600_1.0
<input type="checkbox"/> Group_Nakina_TestServer_1.0
<input type="checkbox"/> Group_Nortel_3500_1.0

Added NE Group
no entries

7. From the list of **Available NE Groups**, select the NE Groups to be backed up.
If the list contains a large number of NE Groups, you can filter the list to view a subset. Select the criteria, type the filter term in the text field, and then click **Search**. You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#).
8. Click **Add** to move the selected NEs from the Available NE Group list to the Selected NE Group list.
9. When the NE groups have been selected, click **Next**.

The system displays Step 3 of the Create Backup Job wizard.

Create Schedule Backup

Step 1: General Information
Step 2: Choose NE Group
Step 3: Schedule And Status ←

Time Zone: UTC-12:00
Start Day: Jan 23, 2008
Start Time: 02:16 PM
Frequency: ☒ Once
☐ Daily
☐ Weekly on: Sunday
☐ Monthly on Day: 23
☐ Monthly on: First Sunday
Status: ☐ Enabled
☒ Disabled

<< Back Go Cancel

10. Specify the schedule and status for the backup as shown in the [Backup schedule and status](#) table.

Table 3–3: Backup schedule and status

Selection	Meaning
Time Zone	The time zone to associate with the start time.
Start Date	The date on which the backup begins.
Start Time	The start time for the schedule. Note: You must set the Start Time to be 10 minutes or more ahead of the current time or else the backup fails. For example, if the current time is 1:30 PM, set the scheduled time for 1:40 PM or later.
Frequency	How often the backup runs: <ul style="list-style-type: none"> • Once: the backup is performed only once at the specified Start Date and Start Time • Daily: the backup is performed each day at the specified Start Time • Weekly on: the backup is performed each week on the specified day (Sunday through Saturday) • Monthly on Day: the backup is performed once a month on the specified day. • Monthly on: the backup is performed once a month on the (First, Second, Third or Fourth) specified day (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday or Sunday)

Selection	Meaning
Status	<p>When Enable is selected, the schedule runs at the specified date, time and frequency (and can also be run manually).</p> <p>When Disable is selected, the backup does not run at the scheduled time, and it can not be run manually.</p> <p>A user log is generated each time the scheduled backup status is modified.</p>

- Click **Go** to complete the procedure.

The system adds the newly created schedule to the list of scheduled backup jobs. If the job is enabled, the system performs the backup at the scheduled time.

- To view the details of a scheduled job that has run, "[List all backup jobs and view job details](#)" on page 41 and click the name of the scheduled job in the **Name** column.
- To bypass a schedule and run a job immediately, see "[Run a scheduled backup job immediately](#)" on page 24.

3.2.3 Run a scheduled backup job immediately

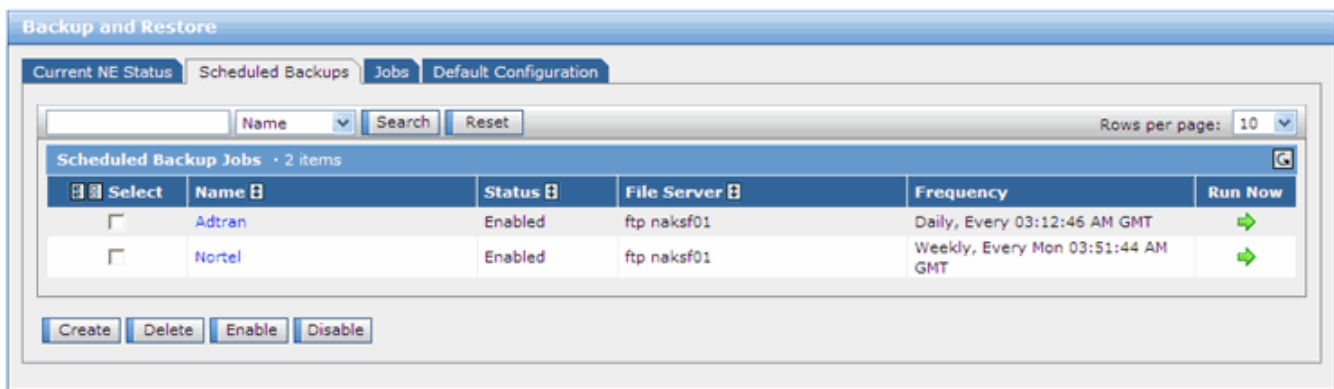
Use this procedure to bypass a backup schedule and immediately run a scheduled job.



Note: Only one backup at a time can run on an NE. If a second backup is attempted while another backup is already running, the system displays an error message explaining the condition.


The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.

- Launch **Backup And Restore**.
- If not already selected, click the **Scheduled Backups** tab.
The system displays the list of scheduled backup jobs.



- Determine the status of the scheduled job:

If the status is	Then go to
Disabled	Step 4.
Enabled	Step 5.

- Select the Disabled scheduled backup job and then click the **Enable** button to change the status.
- Click the green arrow  in the **Run Now** column beside the desired scheduled backup job.

The system prompts for confirmation.

- Click **OK** to run the backup job immediately. If the system indicates the job is Disabled, repeat [Step 4.](#)

Note: If the system displays the message “The current job is running. Please wait.” it usually indicates that another user ran the same job just before you did.

The system displays the details about the job. For each NE, the current backup state is displayed. To update the displayed status, click the **Refresh Now** button.

Backup Job Status Details

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Backup Job Status Details

Job Name: Nortel
 Schedule: Weekly, Every Mon 03:51:44 AM GMT
 File Server: MyServer
 Last Successful Backup Time:
 Last Backup Time: 2008.02.06 01:43:04 PM GMT
 Current State: Failed
 Passed: 2
 Fail: 7
 In Progress: 0
 Pending: 0

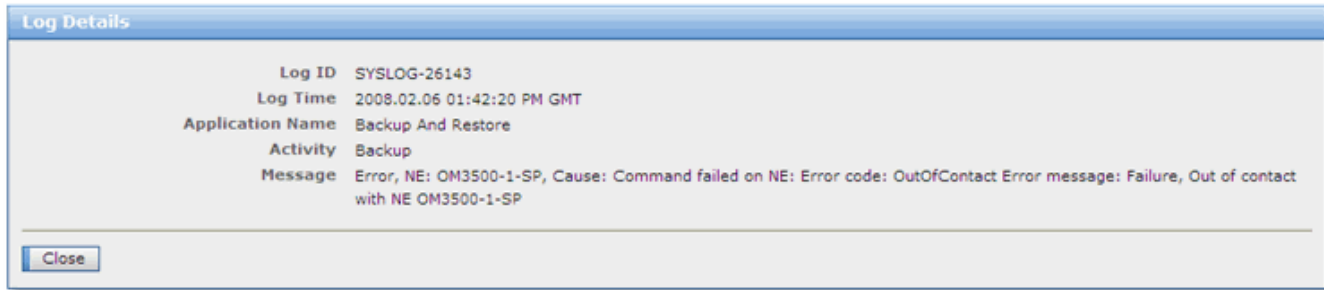
Any Status Search Reset Rows per page: 10

NE Name	Vendor	Model	State
OM3500-133SP	Nortel	OPTera Metro 3500 MSP	Success
OM3500-3-10.3	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-22 SP	Nortel	OPTera Metro 3500 MSP	Success
OM3500-13-17	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-SP	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-3-17	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-3-SP	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-3-10	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-SP2	Nortel	OPTera Metro 3500 MSP	Failed

Click for log

Run immediate backup on failed NEs Close

7. To troubleshoot a failed NE and view the log, click the **Failed** link in the **State** column.



8. To return to the previous screen, click **Close**.
9. From the job details screen, you can [“Re-run a backup job for one or more failed NEs” on page 27](#).

3.2.4 Perform an immediate backup of one or more NEs

Use this procedure to perform an immediate backup of one or more NEs. (This a different procedure than [“Run a scheduled backup job immediately” on page 24](#) because it does not require an existing scheduled job.)



Note: Only one backup job at a time can run on an NE. If a second backup job is attempted while another job is already running on an NE, the first job takes priority. The log records the details of the simultaneous backup attempt.

The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.

1. Click the **Current NE Status** tab and search for the required NEs to be backed up. For details on how to search, see [“Search for NEs to view their backup status and details” on page 36](#).
2. From the Available NE List in the search results, select one or more NEs to be backed up.
3. Click **Run Immediate Backup**.

The system displays the Immediate Backup Information screen with the fields already populated.

Immediate Backup Information

Immediate Backup Information —

Backup Job Name *

Backup Root Directory

Number of Backups per-NE, per-job *

Maximum Concurrent Backups *

Maximum Concurrent Backups per GNE *

Description

User ID bcarty

File Server —

Server Name *

IP Address 10.5.0.11

Port Number 21

User Name nakcs

Rows per page: 10

NE Name	Last Successful Backup Time	Last Backup Result	Current Backup State
OM3500-1-SP		Failed	Idle
OM3500-3-SP		Failed	Idle

Run Now Close

4. If required, you can modify the backup information fields as described in table “[Backup configuration parameters](#)” on page 19. Fields marked with a red asterisk are mandatory.
5. To perform the backup, click **Run Now**.
The system prompts for confirmation.
6. Click **OK** to confirm the action and run the backup.
7. To view the job details, click the **Jobs** tab and then click the name of the backup job in the **Name** column.
8. From the job details screen, you can “[Re-run a backup job for one or more failed NEs](#)” on page 27.

3.2.5 Re-run a backup job for one or more failed NEs

Use this procedure from any job details screen to re-run the backup on only the failed NEs. If desired, you can also select successfully backed up NEs, but the default list of NEs contains only the failed NEs.

1. Make sure that you are on the job details screen from either an immediate backup of a scheduled backup. To update the displayed status, click the **Refresh Now** button.

Backup Job Status Details

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Backup Job Status Details

Job Name: Nortel OM
 Schedule: Once, 2008.02.29 06:00:50 AM GMT
 File Server: lucy
 Last Successful Backup Time:
 Last Backup Time: 2008.03.12 02:41:51 PM GMT
 Current State: Failed
 Passed: 2
 Fail: 2
 In Progress: 0
 Pending: 0

Any Status Search Reset Rows per page: 10

NE Name	Vendor	Model	State
VERIZON1	Adtran	OPTI-6100	Success
OM3500-3-NP	Nortel	OPTera Metro 3000 MSP Series NP	Success
OM3500-3-SP	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-SP	Nortel	OPTera Metro 3500 MSP	Failed

Run immediate backup on failed NEs Close

2. To re-run the backup on the failed NEs, click **Run immediate backup on failed NEs**.

The system displays the first step of the Create Immediate Backup wizard with the fields already populated.

Create Immediate Backup

Step 1: General Information

Backup Job Name: Backup_2008.02.11 03:31:32 PM EST
 Backup Root Directory: backups
 Number of Backups per-NE, per-job: 10
 Maximum Concurrent Backups: 3
 Maximum Concurrent Backups per GNE: 3
 Description:
 User ID: sysadmin

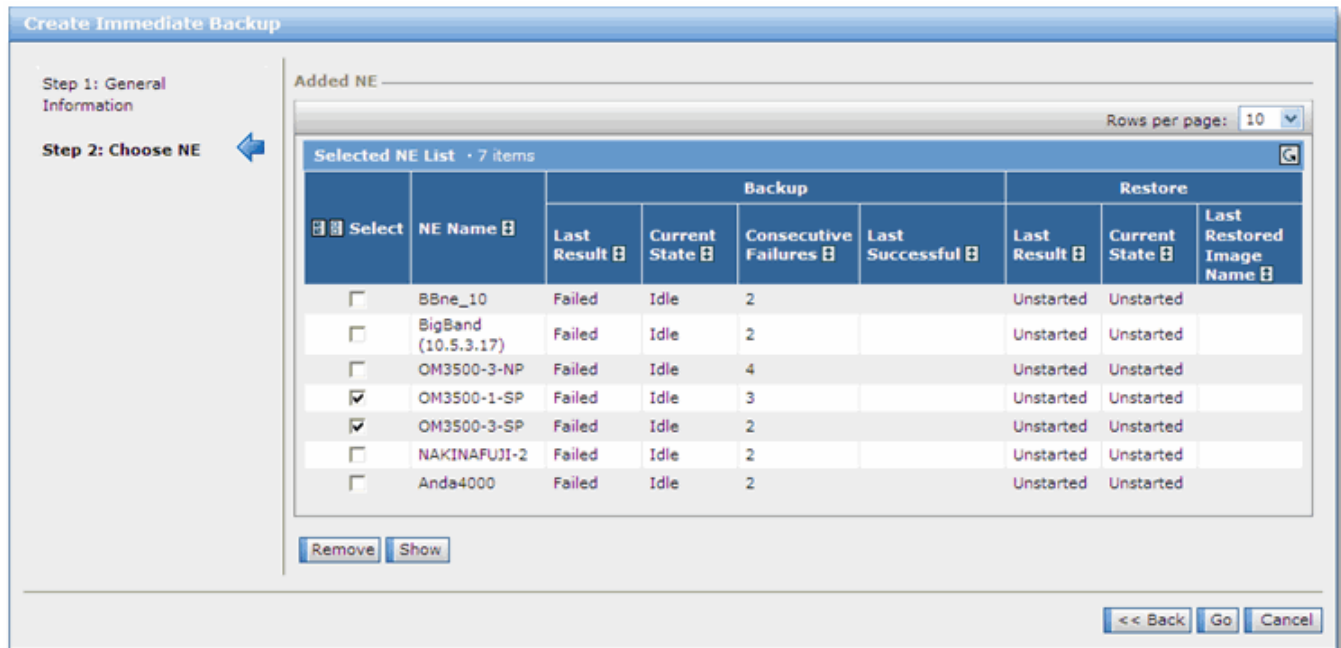
File Server

Server Name: MyServer
 IP Address: 172.16.1.58
 Port Number: 21
 User Name: temp

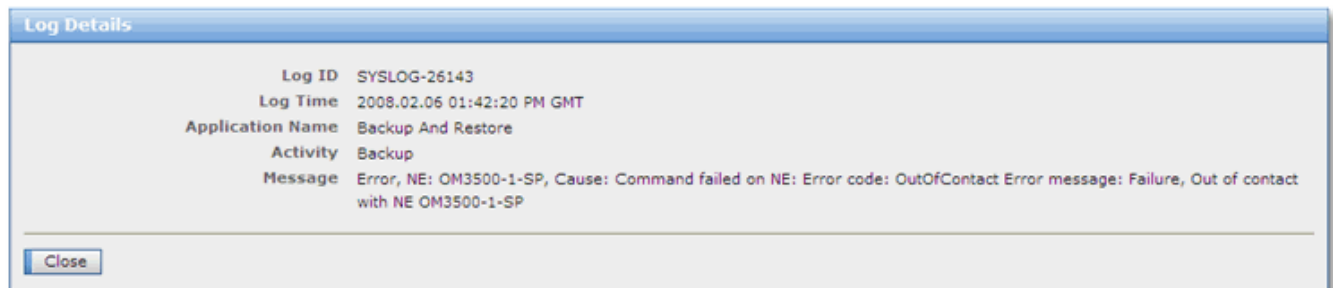
Next >> Cancel

3. If required, make changes to the general information and file server fields as described in table "Backup configuration parameters" on page 19.
4. Click **Next** to continue.

The system displays the next step of the Create Immediate Backup wizard where you select the failed NEs on which to re-run the failed backup.



5. Select the desired NEs on which to re-run the failed backup. If you want to display all NEs including the successful ones, click **Show Available**. Select the desired NEs in the Available NE List, then click **Add** to move the NEs to the Selected NE List.
6. When the desired NEs have been selected, click **Go**.
The system displays the job details as shown in [Step 1](#).
7. To troubleshoot a failed NE and view the log, click the **Failed** link in the **State** column.



8. To return to the previous screen, click **Close**.
9. If the backup fails again for a specific NE, you can re-run the backup, or select the desired NE and obtain a local copy of the backup image for further troubleshooting. See ["Copy a backup image from the file server to your PC" on page 30](#).
10. The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the

consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.

Matching Alarms - 5 items						
Select	Severity	Time	Application	Service Affecting	Condition	Description
	Warning	2008.02.06 07:09:02 PM GMT	Backup And Restore	NSA	Consecutive backup failure threshold exceeded	At least one NE has exceeded the consecutive backup failure threshold OM3500-3-SP Consecutive backup failures: 4 System threshold: 3

3.2.6 Copy a backup image from the file server to your PC

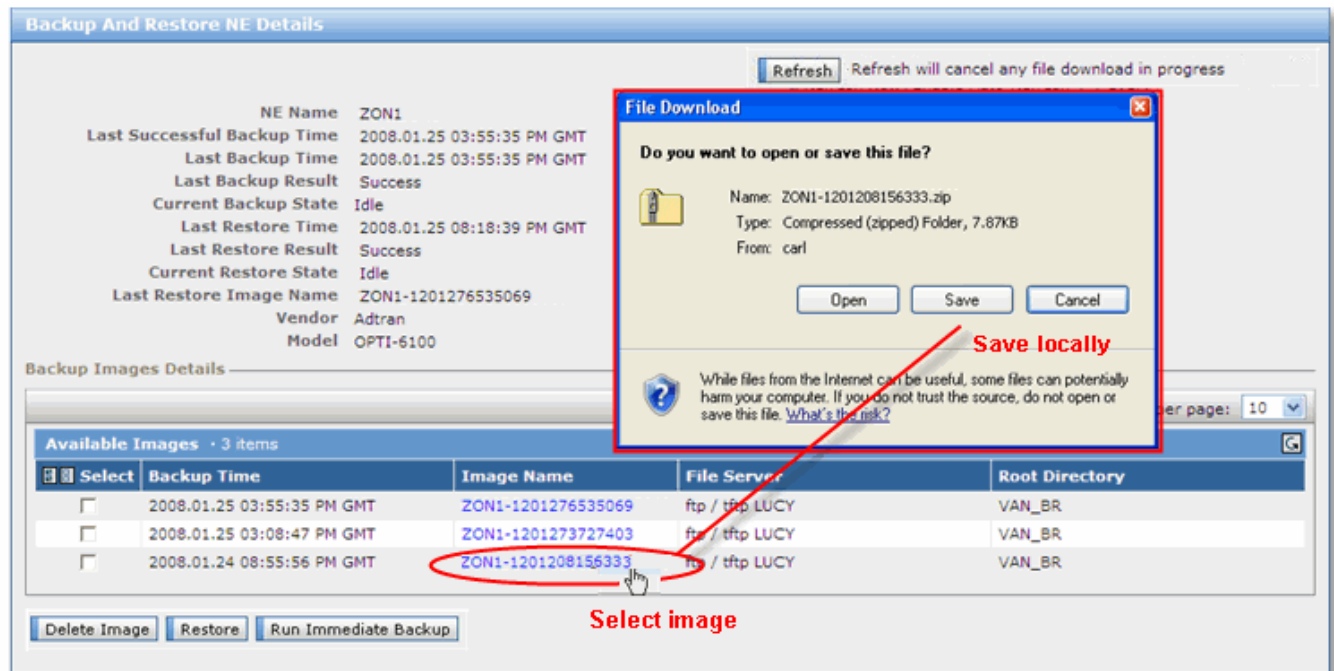
Use this procedure to find an NE and download a copy of a backup image from the file server to your local PC.

1. Click the **Current NE Status** tab and search for the desired NE for which you want to obtain a local copy of the backup image. For details on how to search, see [“Search for NEs to view their backup status and details” on page 36](#).
2. In the **NE Name** column, click the name of the NE.
The system displays the Backup and Restore NE Details.
3. In the **Image Name** column, click the desired image, which has the NE Name as the prefix followed by a numeric identifier.

Note: After clicking on the desired image, do not click the Refresh button. Clicking Refresh cancels the image download.

The screen that is displayed depends on your operating system. Typically, you are prompted to either Open or Save the file. If your system is configured with a ZIP file

association to launch a ZIP application, such as WinZIP, the corresponding ZIP application is launched automatically.



4. Select the appropriate action for the ZIP file based on how your system is configured.

A copy of the image is now on your PC.

3.3 Managing scheduled backups

From the **Scheduled Backups** tab of the Backup and Restore application, you can view and manage scheduled backups that have already been configured. The following procedures are available from the Scheduled Backups tab:

- “List the scheduled backups and view or modify details” on page 32
- “Enable a backup schedule for one or more NEs” on page 34
- “Disable a scheduled backup” on page 34
- “Delete a scheduled backup from the database” on page 35



Note: If you want to backup a network element to two file servers simultaneously, it is recommended that you stagger the data backups by five minutes. This is a precaution in the event that one of the file servers should crash.

Prerequisites

To manage scheduled backups, your user account must be assigned to the Backup and Restore Administration Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.

3.3.1 List the scheduled backups and view or modify details

Use this procedure to view a list of the scheduled backups that are configured. The list provides the following information for each scheduled backup:

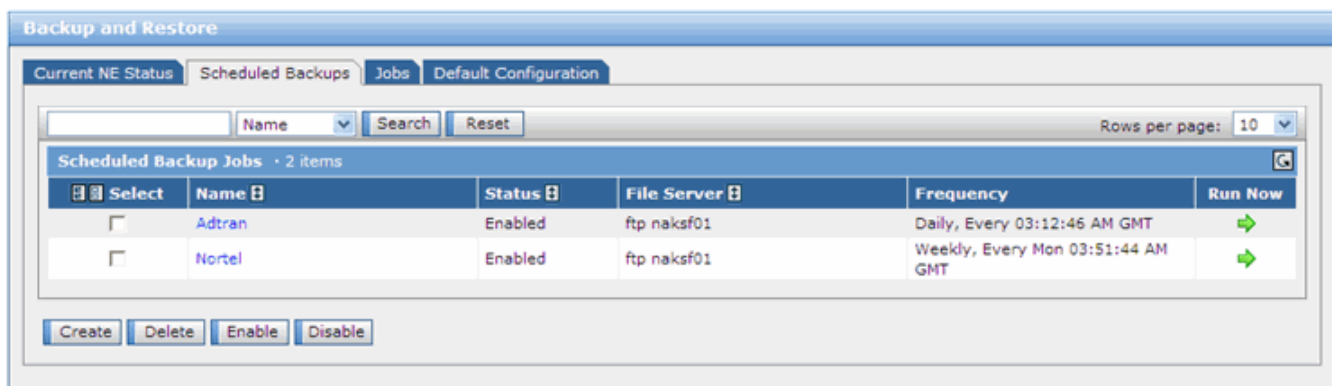
- **Name:** a unique name that identifies the scheduled backup job
- **Status:** indicates whether the scheduled backup job is disabled, or enabled to run at the specified time
- **File Server:** the name of the file server being used to store the backup data
- **Frequency:** indicates when the job is scheduled to run
- **Run Now:** a link that allows to you bypass the schedule and run the backup immediately

For each scheduled backup job in the list you can select it to view or modify the following information which is described in detail in table “Backup configuration parameters” on page 19 and table “Backup schedule and status” on page 23:

- Modify the general information about the job including:
- Modify the File Server used for the backup job.
- Add or remove NE groups associated with the backup job
- Modify the schedule and frequency.
- Change the status of a job: Enabled or Disabled.

1. Launch **Backup And Restore**.
2. If not already selected, click the **Scheduled Backups** tab.

The system displays the list of scheduled backups.



3. From this screen you can:
 - “Enable a backup schedule for one or more NEs” on page 34
 - “Disable a scheduled backup” on page 34

- “Delete a scheduled backup from the database” on page 35
 - “Run a scheduled backup job immediately” on page 24
4. You can filter the list of backups that are displayed by selecting the criteria; **File Server**, **Name** or **Status**; typing the filter term in the text field; and then clicking **Search**. You can use wildcards as described in “Using wildcards in search criteria” on page 199.
 5. To view or update details about the backup, click the name.
The system displays the Backup Job Details screen.

6. Select the tab representing the backup parameters to be modified:

To	Then
modify the general information and file server for the job	click the General Information tab and make the required changes as described in table “Backup configuration parameters” on page 19
modify the NE Groups being backed up	click the NE Groups tab and add or remove the NEs to be backed up. If the list contains a large number of NE Groups, you can filter the list to view a subset of NE Groups. Select the criteria, type the filter term in the text field, and then click Search . Wildcards can be used in the filter field. For information about wildcards, see “Using wildcards in search criteria” on page 199.
modify the schedule and frequency for a job	click the Schedule tab and make the required changes as described in table “Backup schedule and status” on page 23:

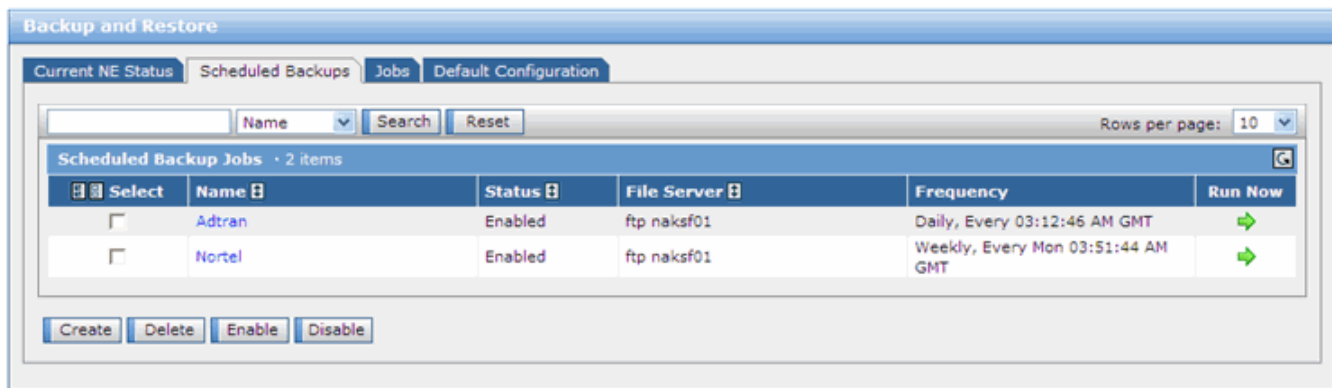
7. When you have finished making the required changes, click **OK**.
The system returns to the list of backups.

3.3.2 Enable a backup schedule for one or more NEs

Use this procedure to enable a backup schedule that was previously disabled. When a backup scheduled is enabled, it runs at the scheduled time and frequency, or it can be run manually.

To run a scheduled backup manually, see [“Run a scheduled backup job immediately” on page 24](#).

1. Launch **Backup And Restore**.
2. If not already selected, click the **Scheduled Backups** tab.
The system displays the Scheduled Backup Jobs list.



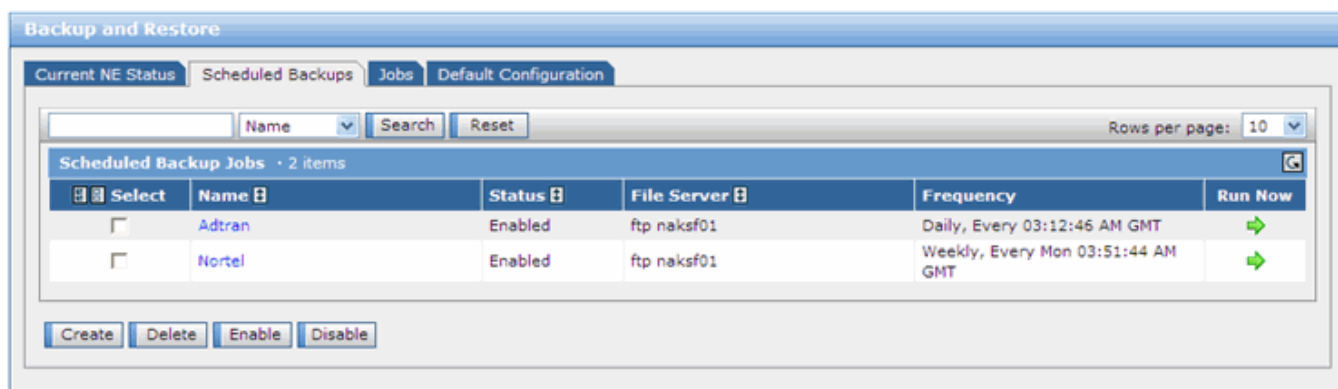
3. In the **Scheduled Backup Jobs** list, select one or more jobs to be enabled.
4. Click **Enable**.
The job status changes to Enabled. The selected jobs run at the scheduled time and frequency.

3.3.3 Disable a scheduled backup

Use this procedure to disable a scheduled backup that was previously enabled. When a scheduled backup is disabled, it cannot be run manually, and it does not run at the scheduled time and frequency.

1. Launch **Backup And Restore**.
2. If not already selected, click the **Scheduled Backups** tab.

The system displays the Scheduled Backup Jobs list.



3. In the Scheduled Backup Jobs list, select one or more enabled backups to be disabled.

4. Click **Disable**.

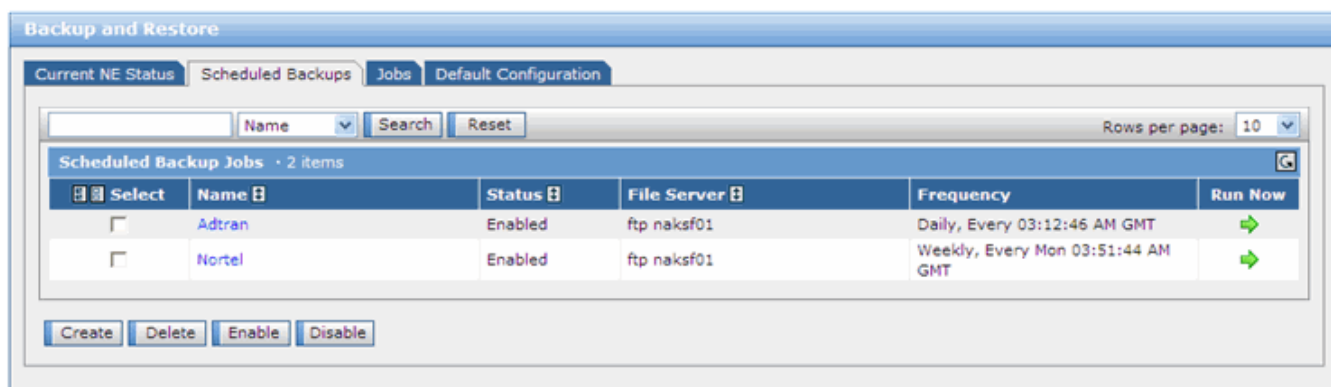
The backup status changes to Disabled. The disabled backup no longer runs at the scheduled time and frequency, and it can not be run manually.

3.3.4 Delete a scheduled backup from the database

Use this procedure to delete a scheduled backup from the database.

1. Launch **Backup And Restore**.
2. If not already selected, click the **Scheduled Backups** tab.

The system displays the list of scheduled backups.



3. In the Scheduled Backup Jobs list, select one or more scheduled backups to be deleted.

4. Click **Delete**.

The system prompts for confirmation.

5. Click **OK** to confirm the operation.

The system removes the backup schedule from the database.

3.4 Managing immediate NE backups

From the **Current NE Status** tab of the Backup and Restore application, you can search for NEs to check their backup status and to obtain a local copy of a backup image. For each NE you can view the details about the backup images and delete backup images that are no longer required.

This section includes the following procedures:

- [“Search for NEs to view their backup status and details” on page 36](#)
- [“Delete an NE backup image” on page 40](#)

Prerequisites

To manage immediate NE backups, your user account must be assigned to the Backup and Restore Administration Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

3.4.1 Search for NEs to view their backup status and details

Use this procedure to search for one or more NEs so that you can view and compare the backup and restore information side-by-side, as described in the [Current NE status fields](#) table. From the list of NEs in the search results, you can drill-down to view the Backup and Restore details for a specific NE.

Table 3–4: Current NE status fields

Field	Meaning
NE Name	The network element identifier. Can be clicked to display the job details.
Backups	
Last Result	the status of the last backup: <ul style="list-style-type: none">• Unstarted: backup jobs that have not started• Success: backup jobs that have completed successfully• Failed: backup jobs that failed
Current State	the status of the current backup: <ul style="list-style-type: none">• Unstarted: backup jobs that have not started on the NE• Success: backup jobs that have completed successfully• Failed: backup jobs failed on the NE• InProgress: backup jobs are currently in progress on the NE• Pending: backup jobs are waiting to run on the NE• Idle: no backup action currently being performed on the NE
Consecutive failures	the number of consecutive backup failures on this NE
Last Successful	the date and time of the last successful backup on this NE
Restore	

Field	Meaning
Last Result	the status of the last restore: <ul style="list-style-type: none"> Unstarted: last restore job did not started on the NE Success: last restore job completed successfully Failed: last restore job failed on the NE
Current State	the status of the current restore: <ul style="list-style-type: none"> Unstarted: restore job has not started Success: restore job has completed successfully Failed: restore job failed InProgress: restore job is currently in progress Pending: restore job is waiting to run Idle: no restore action being performed on the NE
Last Restored Image Name	the name of the image that was last restored successfully

1. Launch **Backup And Restore**.
2. If not already selected, click the **Current NE Status** tab.
The system displays the NE search screen.

Backup and Restore

Current NE Status | Scheduled Backups | Jobs | Default Configuration

Backup Search Criteria

Last Backup Result: Any

Current Backup State: Any

Last Restore Result: Any

Current Restore State: Any

NE Search Criteria

NE Name: [] Equals: [] [] []

Vendor/Model/Version: [] Equals: [] Nortel [] [] [] [] [] []

Load Search | Save Search | ☐ Case Sensitive

Search

Search Result

Rows per page: 10

Available NE List - no entries

Select	NE Name	Backup				Restore		
		Last Result	Current State	Consecutive Failures	Last Successful	Last Result	Current State	Last Restored Image Name
No items in list!								

Run Immediate Backup

3. Enter the desired search criteria to find the NEs for which you want to check the status. If you have an existing search query, you can use the **Load Search** button to load the query. For a complete description of searches, see [“Understanding searches” on page 188](#).

The Backup And Restore search filter allows you to find specific Network Elements based on the following search criteria:

- **Last Backup Result:** search results can be filtered on the status of the last backup: Any, Unstarted, Success, or Failed
 - **Current Backup State:** - search results can be filtered on the status of the current backup: Any, Unstarted, InProgress, Idle, Stopped, Success, Failed, or Pending
 - **Last Restore Result:** search results can be filtered on the status of the last restore: Any, Unstarted, Success, or Failed
 - **Current Restore State:** search results can be filtered on the status of the current restore: Any, Unstarted, InProgress, Idle, Stopped, Success, Failed, or Pending
4. Click **Search** to display the results.

The system displays all the NEs that match the search criteria. The following example shows a search for all Nortel NEs for which the last backup status was Failed.

Backup and Restore

Current NE Status | **Scheduled Backups** | Jobs | Default Configuration

Backup Search Criteria

Last Backup Result: **Failed** (dropdown)
 Current Backup State: Any (dropdown)
 Last Restore Result: Any (dropdown)
 Current Restore State: Any (dropdown)

NE Search Criteria

Vendor/Model/Version: **Equals** **Nortel** (dropdowns)

Load Search | Save Search | ☐ Case Sensitive

Search

Search Result

Rows per page: 10

Available NE List - 2 items

Select	NE Name	Backup				Restore		
		Last Result	Current State	Consecutive Failures	Last Successful	Last Result	Current State	Last Restored Image Name
<input type="checkbox"/>	OM3500-3-NP	Failed	Idle	1		Unstarted	Unstarted	
<input type="checkbox"/>	OM3500-1-SP	Failed	Idle	1		Unstarted	Unstarted	

Run Immediate Backup

- From the search results, you can [“Perform an immediate backup of one or more NEs” on page 26](#), or to view the details for an NE, click the name in the **NE Name** column.

The system displays the Backup and Restore NE Details.

Backup And Restore NE Details

Refresh

Refresh will cancel any file download in progress

NE Name

ZON1

Last Successful Backup Time

2008.02.06 04:23:03 PM GMT

Last Backup Time

2008.02.06 04:23:03 PM GMT

Last Backup Result

Success

Current Backup State

Idle

Last Restore Time

2008.01.25 08:18:39 PM GMT

Last Restore Result

Success

Current Restore State

Idle

Last Restore Image Name

ZON1-1201276535069

Vendor

Adtran

Model

OPTI-6100

Backup Images Details

Rows per page: 10

Available Images - 9 items

Select	Backup Time	Image Name	File Server	Root Directory
<input type="checkbox"/>	2008.02.06 04:23:03 PM GMT	ZON1-1202314983580	ftp naksf01	ADback
<input type="checkbox"/>	2008.02.06 01:51:03 PM GMT	ZON1-1202305863251	ftp naksf01	ADback
<input type="checkbox"/>	2008.02.06 01:48:25 PM GMT	ZON1-1202305705915	ftp naksf01	ADback
<input type="checkbox"/>	2008.02.06 01:42:05 PM GMT	ZON1-1202305325977	ftp naksf01	Nbacks
<input type="checkbox"/>	2008.02.06 01:28:52 PM GMT	ZON1-1202304532824	ftp naksf01	Nbacks
<input type="checkbox"/>	2008.02.06 03:12:50 AM GMT	ZON1-1202267570558	ftp naksf01	ADback
<input type="checkbox"/>	2008.01.25 03:55:35 PM GMT	ZON1-1201276535069	ftp / tftp LUCY	VAN_BR
<input type="checkbox"/>	2008.01.25 03:08:47 PM GMT	ZON1-1201273727403	ftp / tftp LUCY	VAN_BR
<input type="checkbox"/>	2008.01.24 08:55:56 PM GMT	ZON1-1201208156333	ftp / tftp LUCY	VAN_BR

Delete Image

Restore

Run Immediate Backup

6. From the details, you can perform the following tasks:
 - a. “Copy a backup image from the file server to your PC” on page 30.
 - b. “Delete an NE backup image” on page 40.
 - c. “Restore NE configuration data” on page 44.

3.4.2 Delete an NE backup image

Use this procedure to delete any backup images that are no longer required for an NE.

There is no limit to the number of backup images for an NE other than the space limitations on the server.



Note: You cannot delete an image for an NE that is actively undergoing a backup or restore operation. You must wait until the backup or restore operation has completed before deleting an image.

1. Search for the NE whose image is to be deleted. See “[Search for NEs to view their backup status and details](#)” on page 36.
2. From the Available NE List in the search results, click the name of the desired NE whose backup image you would like to delete.

3. From the list of available images, select one or more images to be deleted.
4. Click **Delete Image**.
The system prompts for confirmation.
5. Click **OK** to confirm the operation.
The system deletes the image.

3.5 Managing backup jobs

From the **Jobs** tab, you can view the status for each scheduled backup and for all immediate backup jobs, and if required, delete the job status information.

This includes the following procedures:

- [“List all backup jobs and view job details” on page 41](#)
- [“Delete an immediate backup job” on page 43](#)



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

Prerequisites

To manage the status of backup jobs, your user account must be assigned to the Backup and Restore Administration Role and have the correct permissions set. Without the correct permissions, you can not access some or all of the features.

3.5.1 List all backup jobs and view job details

Use this procedure to view the status for each scheduled backup and for all immediate backup jobs that are in progress or have already run. For each job that is displayed, you can run the job and view details, which include a link to the log files.

The list of backup jobs provides the following information about each job, as described in the [Backup job list information](#) table.

Table 3–5: Backup job list information

Parameter	Description
Name	the name of the backup job
Last Run Time	the date and time that the last backup was run
Passed	the number of NEs that were successfully backed up
Fail	the number of NEs that failed to be backed up
InProgress	the number of NEs that are in the process of being backed up
Pending	the number of NEs that are remaining to be backed up
Status	the overall status of the job



Note: You cannot drill down and obtain details about a job if the current job status is “Unstarted”.

1. Launch **Backup And Restore**.
2. If not already selected, click the **Jobs** tab.
The system displays the list of backup jobs.

Backup and Restore

Current NE Status

Scheduled Backups

Jobs

Default Configuration


Name


Search

Reset

Rows per page: 10

Backup Jobs Status · 1 to 10 of 15



 Select	Name	Last Run Time	Passed	Fail	InProgress	Pending	Status
<input type="checkbox"/>	Adtran	2008.02.07 03:15:26 AM GMT	1	0	0	0	Success
<input type="checkbox"/>	Backup_2008.02.05 07:45:11 PM GMT	2008.02.05 07:43:20 PM GMT	0	2	0	0	Failed
<input type="checkbox"/>	Backup_2008.02.06 01:49:25 PM GMT	2008.02.06 01:47:08 PM GMT	0	1	0	0	Failed
<input type="checkbox"/>	Backup_2008.02.06 06:07:25 PM GMT	2008.02.06 06:19:49 PM GMT	0	7	0	0	Failed
<input type="checkbox"/>	Backup_2008.02.06 07:09:43 PM GMT	2008.02.06 07:09:03 PM GMT	0	2	0	0	Failed
<input type="checkbox"/>	Backup_2008.02.07 02:09:33 PM GMT	2008.02.07 02:07:58 PM GMT	1	0	0	0	Success
<input type="checkbox"/>	Backup_2008.02.07 02:10:44 PM GMT	2008.02.07 02:08:46 PM GMT	1	0	0	0	Success
<input type="checkbox"/>	Nortel	2008.02.06 01:43:04 PM GMT	2	7	0	0	Failed
<input type="checkbox"/>	Test	2008.02.07 03:57:27 AM GMT	1	0	0	0	Success

You can filter the list of jobs by Name. You can use wildcards as described in “Using wildcards in search criteria” on page 199.

3. To view details, click the name of the desired backup job.

The system displays the details about the job. For each NE, the current backup status is displayed.

Backup Job Status Details

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Backup Job Status Details

Job Name: Nortel
 Schedule: Weekly, Every Mon 03:51:44 AM GMT
 File Server: MyServer
 Last Successful Backup Time:
 Last Backup Time: 2008.02.06 01:43:04 PM GMT
 Current State: Failed
 Passed: 2
 Fail: 7
 In Progress: 0
 Pending: 0

Any Status Search Reset Rows per page: 10

NE Name	Vendor	Model	State
OM3500-133SP	Nortel	OPTera Metro 3500 MSP	Success
OM3500-3-10.3	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-22 SP	Nortel	OPTera Metro 3500 MSP	Success
OM3500-13-17	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-SP	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-3-17	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-3-SP	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-3-10	Nortel	OPTera Metro 3500 MSP	Failed
OM3500-1-SP2	Nortel	OPTera Metro 3500 MSP	Failed

Run immediate backup on failed NEs Close

- To view the log file, click status in the **State** column.
The system displays the log record for the backup.

Log Details

Log ID: SYSLOG-26143
 Log Time: 2008.02.06 01:42:20 PM GMT
 Application Name: Backup And Restore
 Activity: Backup
 Message: Error, NE: OM3500-1-SP, Cause: Command failed on NE: Error code: OutOfContact Error message: Failure, Out of contact with NE OM3500-1-SP

Close

The threshold for the maximum number of consecutive NE backup failures is set to three. If one of the NEs in a scheduled or immediate backup job exceeds the consecutive failure threshold, a Backup and Restore application alarm is raised and can be viewed with the Fault Manager.

- To return to the previous screen, click **Close**.

3.5.2 Delete an immediate backup job

Use this procedure to delete an immediate backup job.

(To delete an image, see “Delete an NE backup image” on page 40.)



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

1. Launch **Backup And Restore**.
2. If not already selected, click the **Jobs** tab.
The system displays the list of backup jobs.

Select	Name	Last Run Time	Passed	Fail	InProgress	Pending	Status
<input type="checkbox"/>	Adtran	2008.02.07 03:15:26 AM GMT	1	0	0	0	Success
<input checked="" type="checkbox"/>	Backup_2008.02.05 07:45:11 PM GMT	2008.02.05 07:43:20 PM GMT	0	2	0	0	Failed
<input checked="" type="checkbox"/>	Backup_2008.02.06 01:49:25 PM GMT	2008.02.06 01:47:08 PM GMT	0	1	0	0	Failed
<input checked="" type="checkbox"/>	Backup_2008.02.06 06:07:25 PM GMT	2008.02.06 06:19:49 PM GMT	0	7	0	0	Failed
<input checked="" type="checkbox"/>	Backup_2008.02.06 07:09:43 PM GMT	2008.02.06 07:09:03 PM GMT	0	2	0	0	Failed
<input checked="" type="checkbox"/>	Backup_2008.02.07 02:09:33 PM GMT	2008.02.07 02:07:58 PM GMT	1	0	0	0	Success
<input checked="" type="checkbox"/>	Backup_2008.02.07 02:10:44 PM GMT	2008.02.07 02:08:46 PM GMT	1	0	0	0	Success
<input type="checkbox"/>	Nortel	2008.02.06 01:43:04 PM GMT	2	7	0	0	Failed
<input type="checkbox"/>	Test	2008.02.07 03:57:27 AM GMT	1	0	0	0	Success

3. Select one or more immediate jobs to be deleted. The system does not allow you to select scheduled backups.
4. Click **Delete**.
The system prompts for confirmation.
5. Click **OK** to confirm the operation.
The system deletes the immediate backup jobs from the database.

3.6 Restore NE configuration data

From the **Current NE Status** tab of the Backup and Restore application, you can search for an NE to restore, and then restore the configuration from the list of backup images. When the NE data is restored, it overwrites the existing Network Element configuration data.

Data restores use a file transfer protocol to securely transfer and maintain network element configuration data. If a network element experiences a system crash or if data becomes corrupted, the network administrator can authorize the restoration to a previously backed up view. It is only possible to restore a single NE at any given time.

The Backup And Restore searches allow you to find a specific Network Element based on the search criteria you specify. For a complete description of searches, see [“Understanding searches” on page 188](#).



CAUTION: Restoring an NE configuration can result in a loss of service to the NE. Consult your NE documentation for details.



Note: Before an NE can be restored, a compatible backup image must be available on the backup server.

Prerequisites

To perform a restoration, your user account must be assigned to the Backup and Restore Administration Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

1. Click the **Current NE Status** tab and search for the NE to be backed up. For details on how to search, see [“Search for NEs to view their backup status and details” on page 36](#).
2. From the Available NE List in the search results, click the name of the NE to be restored.

The system displays the Backup and Restore NE Details.

Backup And Restore NE Details

Refresh will cancel any file download in progress

NE Name: ZON1
 Last Successful Backup Time: 2008.02.06 04:23:03 PM GMT
 Last Backup Time: 2008.02.06 04:23:03 PM GMT
 Last Backup Result: Success
 Current Backup State: Idle
 Last Restore Time: 2008.01.25 08:18:39 PM GMT
 Last Restore Result: Success
 Current Restore State: Idle
 Last Restore Image Name: ZON1-1201276535069
 Vendor: Adtran
 Model: OPTI-6100

Backup Images Details

Rows per page: 10

Select	Backup Time	Image Name	File Server	Root Directory
<input type="checkbox"/>	2008.02.06 04:23:03 PM GMT	ZON1-1202314983580	ftp naksf01	ADback
<input checked="" type="checkbox"/>	2008.02.06 01:51:03 PM GMT	ZON1-1202305863251	ftp naksf01	ADback
<input type="checkbox"/>	2008.02.06 01:48:25 PM GMT	ZON1-1202305705915	ftp naksf01	ADback
<input type="checkbox"/>	2008.02.06 01:42:05 PM GMT	ZON1-1202305325977	ftp naksf01	Nbacks
<input type="checkbox"/>	2008.02.06 01:28:52 PM GMT	ZON1-1202304532824	ftp naksf01	Nbacks
<input type="checkbox"/>	2008.02.06 03:12:50 AM GMT	ZON1-1202267570558	ftp naksf01	ADback
<input type="checkbox"/>	2008.01.25 03:55:35 PM GMT	ZON1-1201276535069	ftp / tftp LUCY	VAN_BR
<input type="checkbox"/>	2008.01.25 03:08:47 PM GMT	ZON1-1201273727403	ftp / tftp LUCY	VAN_BR
<input type="checkbox"/>	2008.01.24 08:55:56 PM GMT	ZON1-1201208156333	ftp / tftp LUCY	VAN_BR

3. Select the desired image name to be used to restore the NE.
4. Click **Restore**.
The system prompts for confirmation of the restoration.
5. Click **OK** to confirm the restore operation and begin the restoration.
The system displays the details of the restoration job.

The screenshot shows a window titled "Backup And Restore NE Details". In the top right corner, there is a "Refresh Now" button, a checkbox for "Enable Auto-Refresh", and a dropdown menu set to "every 05:00 (mm:ss)". The main area contains a list of backup and restore details for NE Name VERN1.

NE Name	VERN1
Last Successful Backup Time	2008.02.07 02:06:56 PM GMT
Last Backup Time	2008.02.07 02:06:56 PM GMT
Last Backup Result	Success
Current Backup State	Idle
Last Restore Time	2008.01.25 08:18:39 PM GMT
Last Restore Result	Success
Current Restore State	Idle
Last Restore Image Name	VERIZON1-1201276535069
Vendor	Adtran
Model	OPTI-6100

At the bottom left, there is a "Close" button.

6. To refresh the details, click **Refresh Now**.
7. To close the details and return to the Current NE Status screen, click **Close**.

4 Network Audit: Auditing the network before a software delivery

The NI-Director **Network Audit** application allows network administrators to prepare for a network software delivery by checking hardware and alarm conditions before the delivery is performed. Audits are not required, but are highly recommended to help ensure a successful software delivery.



Note: If an application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they know what to expect when managing network elements from the Network Integrity client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

This section includes the following procedures for configuring and managing Network Audits:

“About hardware and alarm audits” on page 49

Provides an introduction to hardware and alarm audits.

“Configuring and running hardware and alarm audits” on page 50

This section contains the following procedures to configure and run hardware and alarm audits:

- [“Create a hardware component XML file” on page 50](#)
- [“Create a hardware audit profile” on page 52](#)
- [“Create an alarm audit XML file” on page 57](#)
- [“Create an alarm audit profile” on page 58](#)
- [“Perform an audit” on page 62](#)

“Managing audit specifications and jobs” on page 66

This section contains the following procedures for managing hardware and alarm audits that have already been configured:

- [“View the list of audit specifications” on page 66](#)
- [“Modify an existing hardware audit specification” on page 67](#)
- [“Modify an existing alarm audit specification” on page 71](#)

- [“View a list of audit jobs and job details” on page 74](#)
- [“Delete an audit job from the database” on page 76](#)
- [“Delete an audit specification from the database” on page 77](#)

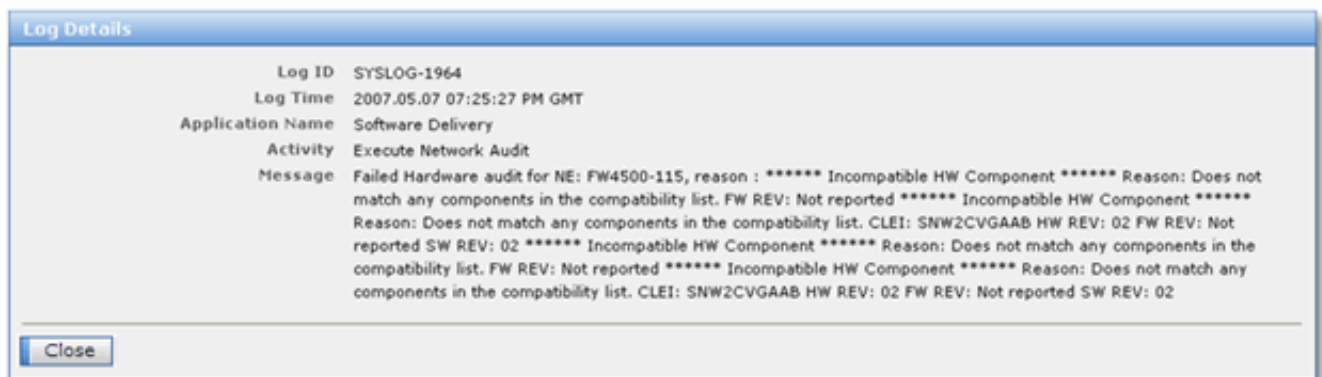
Prerequisites

To use the Software Delivery application, your user account must be assigned to the Software Delivery Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

4.1 About hardware and alarm audits

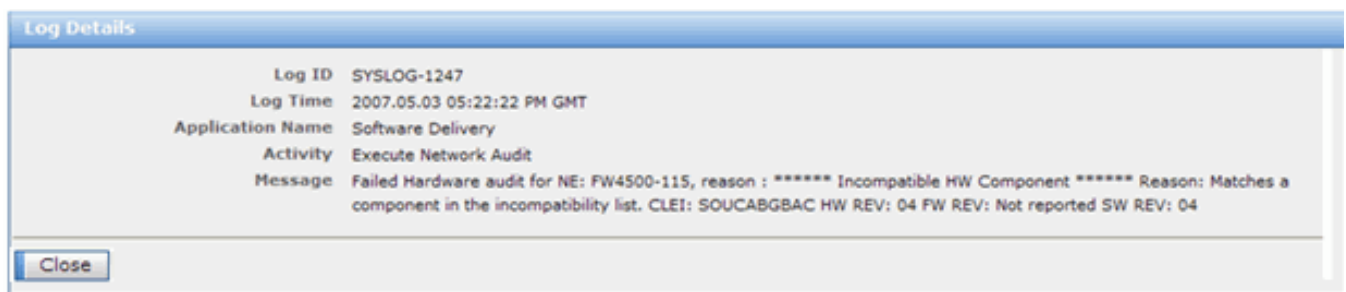
Based on audit criteria entered by the administrator, the Network Audit application conducts an automated, network-wide audit to ensure that all NEs meet the appropriate hardware or alarm conditions before a software delivery is performed with the Software Delivery application. The following types of audit profiles can be defined to ensure the success of a software delivery before it is performed:

- **hardware audit:** checks each NE to ensure that the installed hardware meets the audit criteria before a software delivery is performed. You can create audits that check for “compatible” hardware or “incompatible” hardware, as follows:
 - **Compatible:** For a "Compatible" hardware audit, the user defines a COMPLETE list of hardware components (Circuit Packs) that are considered compatible with the new software load being deployed. In order to pass the compatible hardware audit, every circuit pack found on the NE must be defined in the hardware component list. If a circuit pack is found on the NE that is not defined in the hardware component list, the audit fails indicating the circuit pack that caused the failure.



Note: You must make sure to enter a complete and accurate list of all CLEIs or Vendor Codes for all circuit packs on the network element. If the audit detects any missing or mismatched circuit packs on the NE that do not match the hardware component list, the audit fails.

- **Incompatible:** An "Incompatible" audit is looking for hardware exceptions. The user defines a list of one or more hardware components (Circuit Packs) that are considered incompatible with the new software load being deployed. If a circuit pack from the list is found on the NE, the audit fails indicating the incompatible circuit pack.



If the audit does not detect any incompatible circuit packs on the NE, the audit passes and a software delivery can be performed. For example, you could define the criteria for a Controller card that is known to be incompatible with a new software load. The audit fails if the incompatible Controller card is found on an NE. This allows the operator to replace the incompatible card before performing the software delivery.



Note: In general an “incompatible” audit is easier to define than a “compatible” audit, because a compatibility audit requires a complete and accurate list of hardware on the NE, whereas an “incompatible” audit requires only a list of hardware exceptions.

- **alarm audit:** checks for any alarm conditions on an NE before a software delivery is performed. If an alarm audit fails, the alarm conditions exist, which means the equipment is not ready for a software delivery. If an alarm audit passes, it means the equipment is ready for a software delivery.

Audits can run as part of a software delivery to ensure that all network elements have the appropriate conditions for performing a software delivery, or they can be run independently.

For vendor-specific NE issues that may affect software delivery, see the Adapter Notes that came with your network element adapter.

4.2 Configuring and running hardware and alarm audits

This section contains the following procedures to configure and run hardware and alarm audits:

- [“Create a hardware component XML file” on page 50](#)
- [“Create a hardware audit profile” on page 52](#)
- [“Create an alarm audit XML file” on page 57](#)
- [“Create an alarm audit profile” on page 58](#)
- [“Perform an audit” on page 62](#)

4.2.1 Create a hardware component XML file

Use this procedure to create a hardware component XML file that can be imported when you [“Create a hardware audit profile” on page 52](#). For a description of audit types, see [“About hardware and alarm audits” on page 49](#).

The hardware component file can be created with any XML or text editor and must have **.xml** as the file extension. Table [“Hardware audit XML criteria” on page 51](#) describes the mandatory and optional tags in the XML file.

Store the hardware component XML file on a server that can be accessed from the Network Integrity Framework client interface while configuring a hardware audit.

Sample hardware component XML file

The format for the hardware component XML file is shown in the following example:

```

<?xml version="1.0" encoding="UTF-8"?>
<network-audit xmlns="http://www.nakinasystems.com/nadl"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.nakinasystems.com/nadl com/nakina/swdl/
model/nadl/nadl.xsd">
  <description>Nortel OPTera Metro 3500 MSP</description>
  <hwc-matrix>
    <hardware-model>
      <model>OPTera Metro 3500 MSP</model>
      <compatible-component-list>
        <component>
          <clei>SNC3MB06AB</clei>
          <hw-version>11</hw-version>
          <fw-version>2.4.3(07)</fw-version>
          <sw-version>3.01</sw-version>
        </component>
        <component>
          <clei>SNC3RP06AA</clei>
          <hw-version>012</hw-version>
          <fw-version>Not reported</fw-version>
          <sw-version>Not reported</sw-version>
        </component>
      </compatible-component-list>
    </hardware-model>
  </hwc-matrix>
</network-audit>

```

Table 4–1: Hardware audit XML criteria

Tag	Content
<description>	Provides a description for the hardware audit.
<hwc-matrix>	Parent tag for the hardware audit.
<hardware-model>	Defines the hardware model for the audit.
<model>	The specific model of the compatible or incompatible hardware.
<compatible-component-list>	Parent tag to identify each of the <component> entries that are compatible with the audit.
<incompatible-component-list>	Parent tag to identify each of the <component> entries that are incompatible with the audit.
<component>	Identifies each component in the audit by <clei>, <hw-version>, <fw-version>, and <sw-version>.
<clei>	Identifies the CLEI of the compatible hardware component, by its 10-character code used to precisely identify telecommunications equipment, such as SNPQCPR5AA. Do not type a space character in the string. Note: when performing a “compatibility” audit, the audit fails if any circuit pack is found whose CLEI is not in the specification, so you must make sure to enter a complete list of all CLEIs.

Tag	Content
<hw-version>	Identifies the version of the compatible or incompatible hardware component, for example, 06 or Not Reported.
<fw-version>	Identifies the version of the compatible or incompatible firmware, for example, 12.11 or Not Reported.
<sw-version>	Identifies the version of the compatible or incompatible software component, for example, 7.1 or Not Reported.

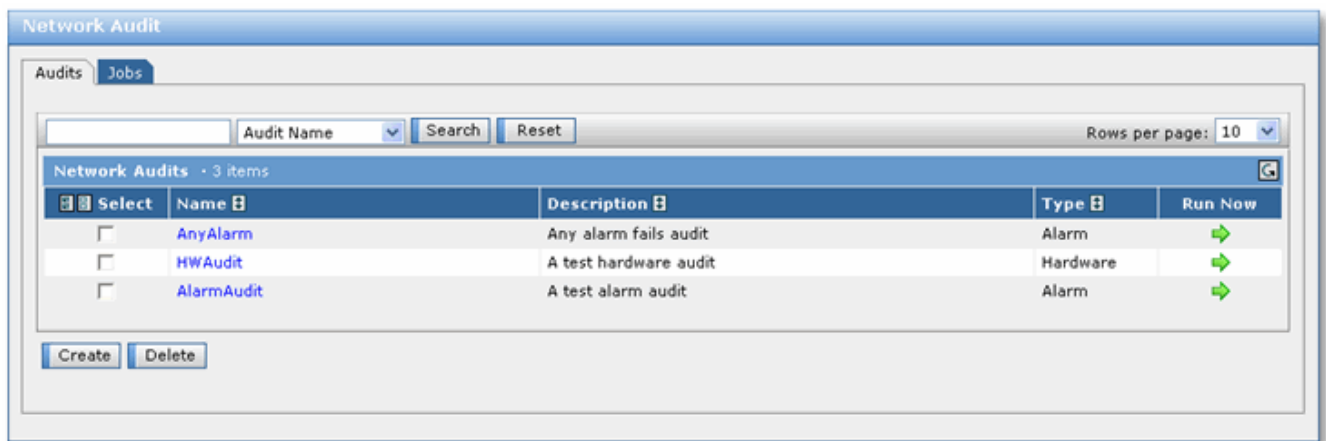
4.2.2 Create a hardware audit profile

Use this procedure to create a profile for a hardware audit that checks the compatibility or incompatibility of the hardware on NEs in the network. For an explanation of these types of audits, see [“About hardware and alarm audits” on page 49](#). The hardware audit profile can be run independently or as part of a software delivery.

As part of the configuration of a hardware audit, specify the hardware components that either permit or prevent a software release. For a description of compatibility and incompatibility audits, see [“About hardware and alarm audits” on page 49](#).

As part of this process, you can manually enter data about the hardware that is compatible/incompatible with the specific software release to be delivered, or you can import the data from a file. If you want to import the hardware component data from a file, create the file before creating the hardware audit. See [“Create a hardware component XML file” on page 50](#).

1. Launch **Network Audit**.
2. If not already selected, click the **Audits** tab.
The system displays the audit screen.



3. Click **Create**.

The system displays Step1 of the Create Audit wizard.

4. In the **Audit Name** field, type a name to describe the audit, such as “NE hardware incompatibility”.
5. In the **Audit Description** field, type a brief description of the audit, such as “Check for all incompatible Controller cards”.
6. In the **Audit Type** list, select **Hardware**.
7. Click **Go**.

The system displays the hardware audit details. At this point you must configure the details of the hardware components for the audit.

8. Click **Create**.

The system displays the hardware audit creation screen.

Hardware Audit - Test

Vendor

--- Select Vendor ---

Model

--- Select Model ---

Component List Type

--- Select Type ---

Rows per page: 10

Hardware Component List

no entries

Select

CLEI

Vendor Codes

Hardware Version

Firmware Version

Software Version

Message Upon Found

No items in list!

Create

Delete

Load Hardware Component List From File

Browse

Load & Merge

Load & Overwrite

Save

Close

9.

From the **Vendor** list, select the vendor of the hardware to be audited.
10.

From the **Model** list, select the model of the hardware to be audited.
11.

In the **Component List Type** field, select either **Compatible** or **Incompatible**.
Note: (Make sure you understand the difference between the requirements for a “Compatible” vs “Incompatible” audit by reading [“About hardware and alarm audits” on page 49.](#))
12.

Manually create the list of hardware components, or import the data from an existing file.

To	Then
import the hardware component list from an existing file	go to Step 13 .
manually create the hardware component list	go to Step 16 .

13.

Click **Browse** to locate the hardware component XML file.
14.

Determine how you want the data to be added:

If	Then
you want the data in the file to merge with existing data	click Load & Merge
you want the data to overwrite and replace any existing data	click Load & Overwrite

15. Determine how you want to proceed:

If	Then
you have more data to import	repeat from step Step 13 .
you want to manually add more hardware data	go to Step 16 .
you are finished adding hardware data	go to Step 19 .

16. Click **Create**.

The system displays a blank entry in the hardware component list.

Hardware Component List - 1 item

Select	CLEI	Vendor Codes	Hardware Version	Firmware Version	Software Version	Message Upon Found
<input type="checkbox"/>						

Create Delete

17. Specify the details for the hardware as described in table “[Hardware component list attributes](#)” on page 56.



Note: At minimum, you must define either the **CLEI** or one **Vendor Code** plus the version information.

Hardware Audit - Corestream audit

Vendor: Nortel
Model: OPTera Metro 3500 MSP
Component List Type: Incompatible

Rows per page: 10

Hardware Component List - 2 items

Select	CLEI	Vendor Codes	Hardware Version	Firmware Version	Software Version	Message Upon Found
<input type="checkbox"/>	SNC3MB06AB			2.0.7	3.1	Older version
<input type="checkbox"/>		SER=644051		3.22(4)	12.0.1	

Create Delete

Load Hardware Component List From File: Browse... Load & Merge Load & Overwrite

Save Close

Table 4–2: Hardware component list attributes

Field	Description
CLEI	<p>(required if there is no Vendor Code defined) If the equipment has a CLEI code, it is best to use it for the audit, because the code contains a complete description of the card. The CLEI can be obtained from the vendor documentation, or if reported by the card, it can be obtained by using the Inventory application and drilling down to the circuit pack details. The CLEI is also available from the NOC shelf level graphics card details.</p> <p>Type the 10-character CLEI code of the hardware component, such as SNPQCPR5AA. Do not use space characters in the string.</p> <p>Note: when performing a “compatibility” audit, the audit fails if any circuit pack is found whose CLEI is not in the audit specification, so you must make sure to enter a complete list of all CLEIs for the network element.</p>
Vendor Codes	<p>(required if there is no CLEI defined) If the equipment does not have a CLEI, identify the hardware by entering one or more vendor codes, which is a comma separated list of attribute value pairs. You can specify one or more of the Vendor Codes, such as AGE, CTYPE, partNum, entityID, SER, etc. The Vendor Codes can be obtained from the vendor documentation, or by using the NOC and drilling down to the circuit pack details, and then displaying the Attributes, which contain the value pairs.</p> <p>Type the vendor code for the equipment that is either compatible or incompatible. For example, enter something like entityID=AMP-1-01 or partNum=130-4203-930 or SER=644051, or enter a combination separated by commas, such as entityID=AMP-1-01, SER=644051. Do not put a space before or after the equal sign, and do not use quotes.</p> <p>Do not enter the hardware, firmware, or software version (hwVer, fwVer, swVer) as part of the vendor code. If used, these values must be entered in the fields labelled “Hardware Version”, “Firmware Version”, or “Software Version”.</p>
Hardware Version	Type the hardware version of the equipment, such as 11
Firmware Version	Type the version of firmware associated with the hardware, such as 2.5.4(07)
Software Version	Type the version of software associated with the hardware, such as 3.01
Message Upon Found	<p>optional - type the message to be displayed if the audit fails.</p> <p>Note: The message does not appear if a standalone audit is performed. This message appears only if the HW audit is defined within the details of a Software Release specification and performed within a Software Delivery workflow.</p>

18. Manually enter more data, or complete the procedure:

To	Then
enter additional criteria in the Hardware Component List,	repeat from Step 16 .
complete the procedure	go to Step 19 .

19. Click **Save**.

The system adds the hardware specification to the list of Network Audits.

20. [“Perform an audit” on page 62.](#)

4.2.3 Create an alarm audit XML file

Use this procedure to create an alarm audit XML file that can be imported when you configure an alarm audit. The file can be created with any XML or text editor and must have **.xml** as the file extension.

Table [“Alarm audit XML criteria” on page 58](#) describes the mandatory and optional fields in the XML file.

Store the alarm checking criteria XML file on a server that can be accessed from the Network Integrity Framework client interface while configuring an alarm audit.



Note: You can obtain the details for the XML file by creating an Inventory report for the desired equipment and copying the values from the report into the XML file. See [“Saving search results to a file” on page 202.](#)

Sample alarm audit XML file

The format for the alarm checking criteria file is shown in the following example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<network-audit xmlns="http://www.nakinasystems.com/nadl"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.nakinasystems.com/nadl com/nakina/swdl/
model/nadl/nadl.xsd">
  <description>Sample alarm audit criteria definition</description>
  <alarm-audit>
    <alarm-list>
      <t11-alarm>
        <description>Loss</description>
        <comparison>contain</comparison>
      </t11-alarm>
      <t11-alarm>
        <aid-type>EQPT</aid-type>
        <notification-code>CR</notification-code>
        <condition-type>SNPQADE5AD-FLT</condition-type>
        <service-effect>NSA</service-effect>
        <description>Equipment failure</description>
        <comparison>exact</comparison>
      </t11-alarm>
      <t11-alarm>
        <aid-type>EQPT</aid-type>
        <notification-code>MJ</notification-code>
        <condition-type>RMVD</condition-type>
        <service-effect>SA</service-effect>
        <description>Unit is removed</description>
        <comparison>contain</comparison>
      </t11-alarm>
    </alarm-list>
  </alarm-audit>
```

```
</network-audit>
```

Table 4–3: Alarm audit XML criteria

XML Element	Description and values
<alarm-audit>	Parent element used to define all alarm audit criteria.
<alarm-list>	Defines the list of TL1 alarms to check for in the audit. Sub element to <alarm-audit>. Parent element to one or more <tl1-alarm> elements.
<tl1-alarm>	Defines the details of the TL1 alarm.
<aid-type>	An alphanumeric string to identify the type of the component that originates the alarm, such as EQPT
<notification-code>	Identifies the severity of the alarm: CR (critical), MJ (major), MN (minor).
<condition-type>	An alphanumeric string to identify the error code for the alarm, for example RMVD
<service-effect>	The service affecting status for the alarm, where “code” is: SA or sa (service-affecting), or NSA or nsa (non service-affecting).
<comparison>	The comparison logic for the alarm audit: exact (must match all criteria exactly) or (contain) match any of the criteria
<description>	Provides a long description for the alarm.

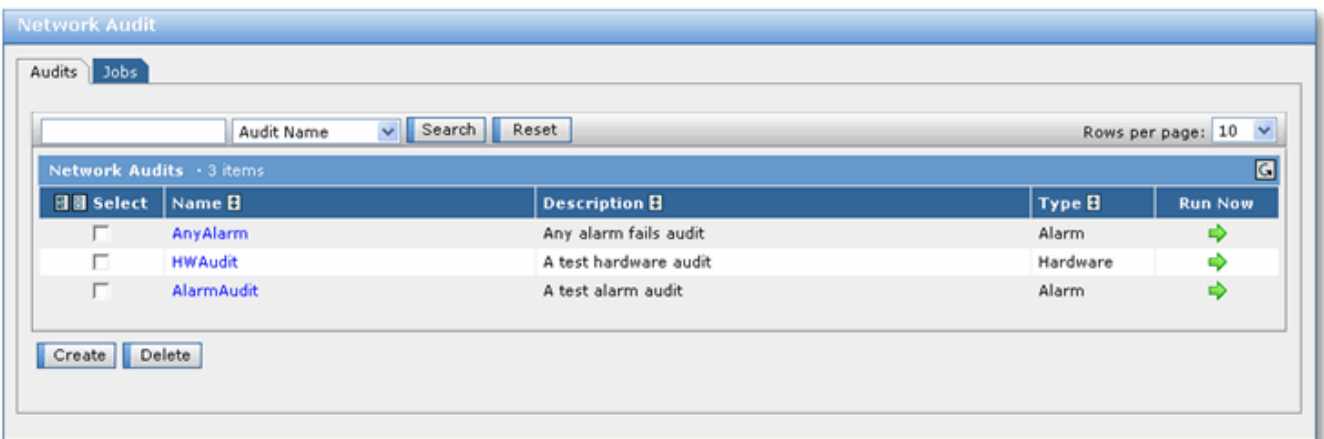
4.2.4 Create an alarm audit profile

Use this procedure to create an alarm audit profile that checks for specific alarm conditions or for any alarm condition on NEs.

As part of the alarm audit configuration you can specify which alarms cause the audit to fail. This alarm specification can be done manually, or the alarms can be imported from an XML file. If you want to import a list of alarms from a file, create the file before using this procedure. To create the alarm file, see [“Create an alarm audit XML file” on page 57](#).

1. Launch **Network Audit**.
2. If not already selected, click the **Audits** tab.

The system displays the Network Audit screen.

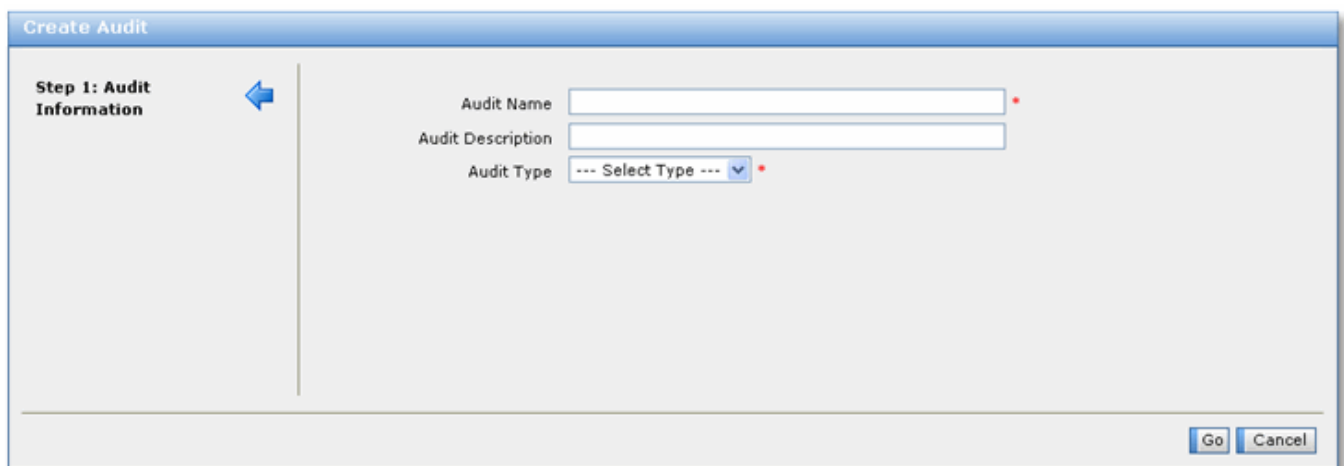


The screenshot shows the 'Network Audit' window with two tabs: 'Audits' and 'Jobs'. The 'Audits' tab is active. At the top, there is a search bar with a text input field, a dropdown for 'Audit Name', and buttons for 'Search' and 'Reset'. To the right, it says 'Rows per page: 10'. Below this is a table titled 'Network Audits - 3 items'. The table has five columns: 'Select', 'Name', 'Description', 'Type', and 'Run Now'. There are three rows of audit data. At the bottom, there are 'Create' and 'Delete' buttons.

Select	Name	Description	Type	Run Now
<input type="checkbox"/>	AnyAlarm	Any alarm fails audit	Alarm	
<input type="checkbox"/>	HWAudit	A test hardware audit	Hardware	
<input type="checkbox"/>	AlarmAudit	A test alarm audit	Alarm	

3. Click **Create**.

The system displays Step 1 of the Create Audit wizard.



The screenshot shows the 'Create Audit' wizard, Step 1: Audit Information. On the left, there is a sidebar with 'Step 1: Audit Information' and a blue arrow pointing left. The main area contains three fields: 'Audit Name' (text input), 'Audit Description' (text input), and 'Audit Type' (dropdown menu with '--- Select Type ---' selected). There are red asterisks next to the 'Audit Name' and 'Audit Type' fields. At the bottom right, there are 'Go' and 'Cancel' buttons.

4. In the **Audit Name** field, type a name to describe the alarm audit.
5. In the **Audit Description** field, type a brief description of the alarm audit.
6. In the **Audit Type** list, select **Alarm**.
7. Click **Go**.

The system displays the alarm audit configuration screen. At this point you must configure the details of the alarm audit.

Alarm Audit

Audit NameCiena Critical

Audit DescriptionAudit for critical Ciena alarms

Any alarm fails audit

Specified alarms fail audit

Rows per page: 10

Alarm Checking Criteria - no entries

Select

Alarm/Condition Type

Severity

Service Effect

AID Type

Comparison Logic

Description

No items in list!

Create

Delete

Load Alarm Checking Criteria From File

Browse...

Load & Merge

Load & Overwrite

Save

Close

8. Select the alarm condition that causes the audit to fail:

To	Then
have one or more specific alarm conditions cause the audit to fail	go to Step 9 .
have any alarm condition cause the audit to fail	go to Step 17 .

9. Select **Specified alarms fail audit**.

10. Manually create the list of alarms or import the data from an existing file:

To	Then
import the list of alarms from an existing file	go to Step 11 .
manually create the list of alarms	go to Step 14 .

11. Click **Browse** to locate the alarm XML file.

12. Determine how you want the data to be added:

If	Then
you want the alarm data in the file to merge with existing data	click Load & Merge
you want the alarm data to overwrite and replace any existing data	click Load & Overwrite

13. Determine how you want to proceed:

If	Then
you have more data to import	repeat from step Step 11 .
you want to manually add more alarm data	go to Step 14 .
you are finished adding alarm data	go to Step 18 .

14. Click **Create**.

The system displays a blank entry in the Alarm Checking Criteria list.

Alarm Checking Criteria - 1 item

Select	Alarm/Condition Type	Severity	Service Effect	AID Type	Comparison Logic	Description
<input type="checkbox"/>		All	All		Exact	

Create Delete

15. Specify the details for the alarm condition as described in the [Alarm checking criteria attributes](#) table.

Table 4–4: Alarm checking criteria attributes

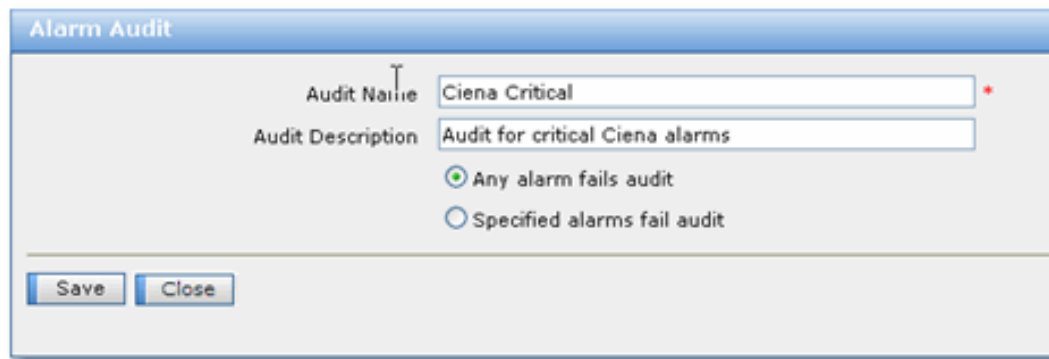
Field	Description
Alarm/Condition Type	Enter the alarm condition type, for example, EQPT
Severity	Enter the alarm severity: <ul style="list-style-type: none"> Intermediate Cleared Warning Minor Major Critical
Service Effect	Enter the effect that the alarm has on service: NSA (non service-affecting) or SA (service-affecting)
AID Type	Enter the alarm AID type, for example, OC192
Comparison Logic	Enter the comparison logic for the alarm: <ul style="list-style-type: none"> Exact: match all of the alarm audit criteria Contain: match any of the alarm audit criteria
Description	Enter a brief description of the alarm condition

16. Determine how you want to proceed:

To	Then
manually create more alarm entries	repeat from Step 14 .
complete the procedure	Step 18 .

17. Select **Any Alarm Fails Audit**.

The system hides the list of Alarm Checking Criteria.



The 'Alarm Audit' dialog box contains the following fields and options:

- Audit Name:** Ciena Critical
- Audit Description:** Audit for critical Ciena alarms
- Options:**
 - ☒ Any alarm fails audit
 - ☐ Specified alarms fail audit
- Buttons:** Save, Close

- Click **Save** to save the audit specification.

The system adds the alarm audit to the list of Network Audits.

- [“Perform an audit” on page 62.](#)

4.2.5 Perform an audit

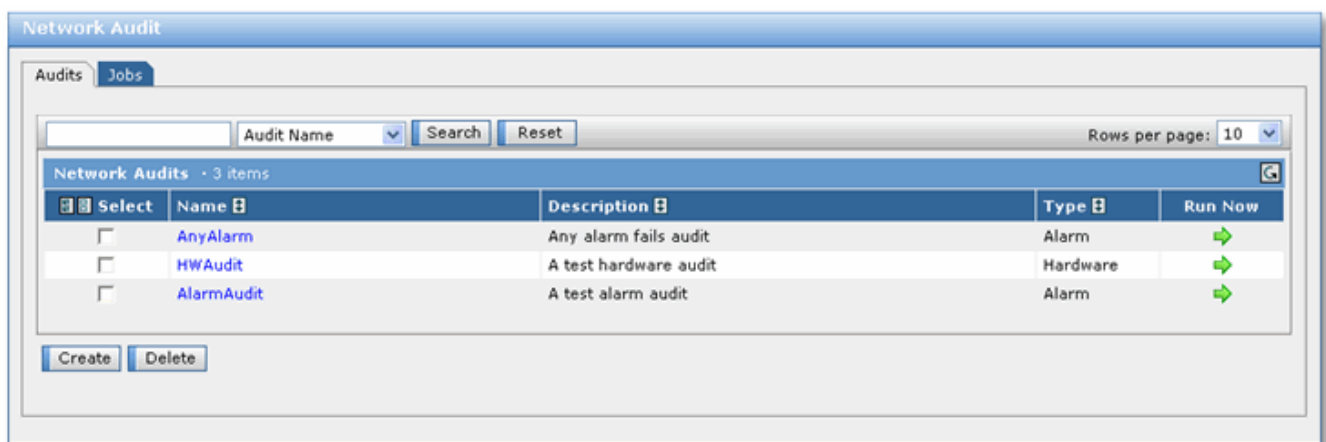
Use this procedure to run a hardware or alarm audit on selected NE Groups or on selected NEs. When an audit runs, it creates an audit job which is identified by a Job ID. To view the jobs, see [“View a list of audit jobs and job details” on page 74.](#)

- Launch **Network Audit**.

The system displays the Network Audit screen.

- If not already selected, click the **Audits** tab.

The system displays the list of existing audits. Each audit is named and identified by type as either a Hardware or Alarm audit.



The 'Network Audit' screen shows the 'Audits' tab selected. It includes a search bar with 'Audit Name' and 'Search' buttons, and a 'Reset' button. The table below lists the existing audits:

Select	Name	Description	Type	Run Now
<input type="checkbox"/>	AnyAlarm	Any alarm fails audit	Alarm	
<input type="checkbox"/>	HWAudit	A test hardware audit	Hardware	
<input type="checkbox"/>	AlarmAudit	A test alarm audit	Alarm	

Buttons: Create, Delete

- Click the green arrow in the Run Now column beside the audit to be run.

The system displays Step 1 of the Run Audit wizard.

Run Audit - AnyAlarm

Step 1: Target Type

☒ Run audit on select NE Groups
☐ Run audit on select NEs

Next >> Cancel

4. Select the scope of the audit.

To	Then
run the audit on specific NE groups	go to Step 5 .
run the audit on specific NEs	go to Step 8 .

5. Select **Run audit on select NE Groups**.

The system displays Step 2 of the Run Audit wizard.

Run Audit - AnyAlarm

Step 1: Target Type

Step 2: Select NE Groups

Available NE Groups

Rows per page: 10

Available NE Groups - 1 item

Select NE Group Name

All NEs

Add Hide

Selected NE Groups

Rows per page: 10

Selected NE Groups - no entries

Select NE Group Name

No items in list!

Remove

<< Back Go Cancel

For Hardware audits only, there is an option called **Run audit only on NEs with matching Vendor and Model**. If you select this, the audit runs only on NEs within the NE Groups that match the Vendor and Model criteria defined in the hardware audit.

6. Select the NE Groups on which to run the audit, and then click **Add**. This moves the NEs from the **Available NE Groups** list to the **Selected NE Groups** list. Repeat this as many time as required to select the necessary groups.
7. To continue with NE Group selection, skip to [Step 11](#).
8. Select **Run audit on select NEs**.
The system displays the NE selection screen.

Run Audit - rrrr

Step 1: Target Type

Step 2: Select NEs

Available NEs

View: All NEs

NE Name:

Vendor: Custom...

Model: Custom...

Software Version:

NE Group Name:

Rows per page: 10

Select	NE Name	Vendor	Model	SW Version	Active GNE
<input type="checkbox"/>	Anda4000	Anda	EtherEdge 4000	2.5.5(35)	Anda4000
<input type="checkbox"/>	FW45001-7001	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7002	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7003	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7004	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7005	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7006	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7007	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7008	Fujitsu	Flashwave4500	8.1	FW45001-7001
<input type="checkbox"/>	FW45001-7009	Fujitsu	Flashwave4500	8.1	FW45001-7001

Selected NEs

Rows per page: 10

Selected NEs - no entries

Select	NE Name	Vendor	Model	SW Version	Active GNE
No items in list!					

<< Back Go Cancel

9. You can filter the list of displayed NEs by performing a search. For complete information on how to perform a search, see [“Understanding searches”](#) on page 188.

10. From the search results, select the NEs on which to run the audit, and then click **Add**. This moves the NEs from the **Available NEs** list to the **Selected NEs** list. Repeat this as many times as required to select the necessary NEs for the audit.
11. Click **Go** to run the audit.
The system runs the audit, creates an audit job, and displays the Network Audit Job screen.



The screenshot shows a web application window titled "Network Audit Job". At the top right, there is a "Refresh Now" button, a checkbox for "Enable Auto-Refresh", and a dropdown menu set to "every 05:00 (mm:ss)". Below this is a "Job Summary" section containing the following information:

Job ID:	3
Audit Name:	AnyAlarm
Originator:	sysadmin
Status:	In Progress
Total NEs:	6
In Progress:	6
Passed:	0
Failed:	0

At the bottom left of the summary section is a "Show Details >>" button, and at the bottom center is a "Close" button.

The Network Audit Job screen provides the following information about the audit:

- **Job ID:** a numeric identifier for the audit job
- **Audit Name:** the name assigned to the audit job when it was created
- **Originator:** the user ID of the person who created the audit job
- **Status:** the current status of the audit job.
- **Total NEs:** the total number of NEs being audited
- **In Progress:** the number of NEs that are currently in the process of being audited
- **Passed:** the number of NEs that passed the audit
- **Failed:** the number of NEs that failed the audit

12. To view more details about the NEs being audited, click **Show Details**.

The system displays the details of the audit job, which lists the status of each NE being audited. The status is one of Unstarted, Failed, Passed, or In Progress.

Network Audit Job

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Job Summary

Job ID: 3
 Audit Name: AnyAlarm
 Originator: sysadmin
 Status: In Progress
 Total NEs: 6
 In Progress: 6
 Passed: 0
 Failed: 0

<< Hide Details

NE Status

All Status Search Reset Rows per page: 10

Network Element Job Status - 6 items

NE Identifier	Vendor	Model	Status
CORESTREAM-10008-0	Ciena	Corestream	In Progress
CORESTREAM-10017-0	Ciena	Corestream	In Progress
CORESTREAM-10009-0	Ciena	Corestream	Failed
CORESTREAM-10016-0	Ciena	Corestream	Failed
CORESTREAM-10007-0	Ciena	Corestream	In Progress
CORESTREAM-10018-0	Ciena	Corestream	In Progress

Close

13. To refresh the screen with the latest status information, click **Refresh Now** or select **Auto-Refresh** and specify a frequency.

14. To return to the list of audit profiles, click **Close**.

4.3 Managing audit specifications and jobs

This section contains the following procedures for managing hardware and alarm audit specifications and jobs that have already been created:

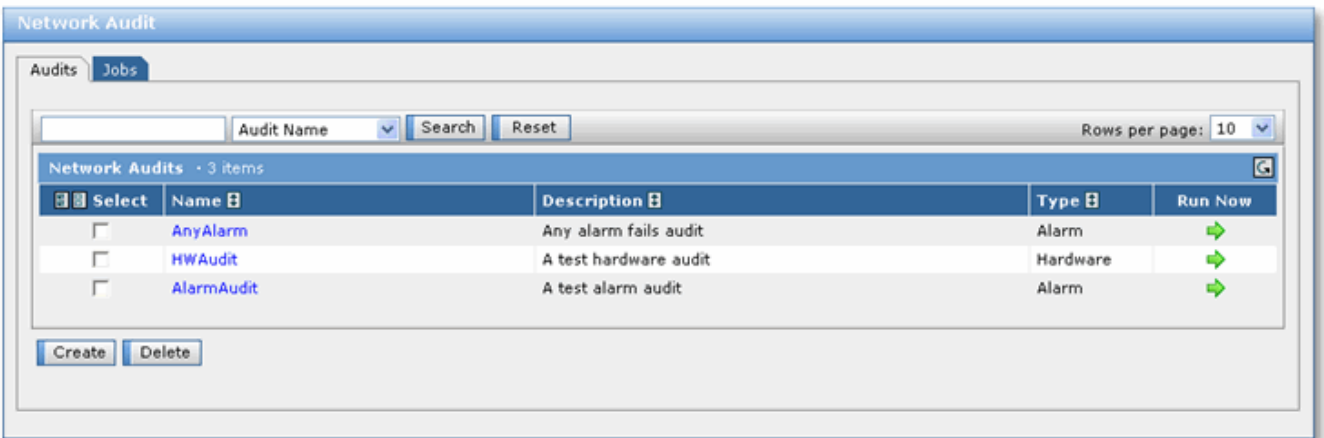
- “View the list of audit specifications” on page 66
- “Modify an existing hardware audit specification” on page 67
- “Modify an existing alarm audit specification” on page 71
- “View a list of audit jobs and job details” on page 74
- “Delete an audit job from the database” on page 76
- “Delete an audit specification from the database” on page 77

4.3.1 View the list of audit specifications

Use this procedure to view the list of existing hardware and alarm audit specifications. The list of network audits provides the following information for each audit specification:

- the audit name

- the audit type: hardware or alarm
 - a link that allows you to run the audit
1. Launch **Network Audit**.
The system displays the audit screen.
 2. If not already selected, click the **Audits** tab.



The system displays the list of existing audits. Each audit is named and identified as either a Hardware or Alarm audit type.

3. You can filter the list of network audits that are displayed by selecting the search criteria: **Audit Type**, **Audit Name** or **Audit Description**; typing the search term in the text field; and then clicking **Search**.
You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#).
4. From the list of network audits, you can perform the following tasks:

To	See
create a hardware audit specification	“Create a hardware audit profile” on page 52
configure an alarm audit specification	“Create an alarm audit profile” on page 58.
modify a hardware audit specification	“Modify an existing hardware audit specification” on page 67
run an audit	“Perform an audit” on page 62
remove an audit job	“Delete an audit job from the database” on page 76
delete an audit specification	“Delete an audit specification from the database” on page 77
view an audit job	“View a list of audit jobs and job details” on page 74

4.3.2 Modify an existing hardware audit specification

Use this procedure to modify an existing specification for a hardware audit that checks the compatibility or incompatibility of the hardware in the network. For a description of audit types, see [“About hardware and alarm audits” on page 49](#).

As part of the modification you can specify the hardware component list, which either permits or prevents a download of a software release to a network element based on whether the software release is compatible or incompatible with the installed hardware of the network element. As part of this process, you must enter all the hardware that is compatible with the specific software release to be delivered, or you can import the information from a file. If you want to import the hardware component data from a file, create the file before using this procedure. To create the hardware component file, see [“Create a hardware component XML file” on page 50](#).

1. Launch **Network Audit**.
2. If not already selected, click the **Audits** tab.
The system displays the audit screen.

The screenshot shows the 'Network Audit' window with the 'Audits' tab selected. It features a search bar with 'Audit Name' and 'Search' buttons, and a 'Reset' button. A 'Rows per page' dropdown is set to 10. Below is a table titled 'Network Audits - 3 items'.

Select	Name	Description	Type	Run Now
<input type="checkbox"/>	AnyAlarm	Any alarm fails audit	Alarm	
<input type="checkbox"/>	HWAudit	A test hardware audit	Hardware	
<input type="checkbox"/>	AlarmAudit	A test alarm audit	Alarm	

At the bottom are 'Create' and 'Delete' buttons.

3. Click the name of the hardware audit to be modified.
The system displays the hardware audit details.

The screenshot shows the 'Hardware Audit' window. It has fields for 'Audit Name' (HWAudit) and 'Audit Description' (A test hardware audit). Below these is a search bar with 'Model' and 'Search' buttons, and a 'Reset' button. A 'Rows per page' dropdown is set to 10. Below is a table titled 'Hardware Matrix - 1 item'.

Select	Model	Vendor	Component List Type
<input type="checkbox"/>	Corestream	Ciena	Compatible

At the bottom are 'Create', 'Delete', 'Save', and 'Close' buttons.

4. If required, in the **Audit Name** field, change the name that describes the audit.
5. If required, in the **Audit Description** field, change the description of the audit.
6. To add hardware information to the audit, click **Create**.

The system displays the hardware audit creation screen.

7. From the **Vendor** list, select the vendor of the hardware to be audited.
8. From the **Model** list, select the model of the hardware to be audited.
9. In the **Component List Type** field, select either **Compatible** or **Incompatible**. When set to Compatible, the audit checks for hardware that conforms to the criteria. When set to Incompatible, the audit checks for hardware that conflicts with the criteria.
10. Manually create the hardware component list or import the data from an existing file:

To	Then
import the hardware components from an existing file	go to Step 11 .
manually create the hardware component list	go to Step 16 .

11. Click **Browse** to locate the hardware compatibility XML file.
12. Determine how you want the data to be added:

If	Then
you want the alarm data in the file to merge with existing data	click Load & Merge
you want the alarm data to overwrite and replace any existing data	click Load & Overwrite

13. Determine how you want to proceed:

If	Then
you have more data to import	repeat from step Step 11 .
you want to manually add more hardware data	go to Step 14 .
you are finished adding hardware data	go to Step 17 .

14. Click **Create**.

The system displays a blank entry in the hardware component list.

The screenshot shows a web-based interface titled "Hardware Component List - 1 item". It features a table with the following columns: "Select", "CLEI", "Vendor Codes", "Hardware Version", "Firmware Version", "Software Version", and "Message Upon Found". Below the table, there are "Create" and "Delete" buttons. The table currently contains one blank row for data entry.

15. Specify the details for the hardware as described in the [Hardware component list attributes](#) table.

Table 4–5: Hardware component list attributes

Field	Description
CLEI	type the CLEI for the equipment that is either compatible or incompatible. Whether the equipment is compatible or incompatible is based on the setting of the “Component List Type” field. Note: when performing a compatibility audit, the audit fails if any circuit pack is found whose CLEI is not in the specification, so you must make sure to enter a complete list of all CLEIs.
Vendor Codes	type the vendor code for the equipment that is either compatible or incompatible. For example, enter something like entityID=AMP-1-01 or partNum=130-4203-930 or swVer=6.1.4 . Vendor codes can be found in the vendor documentation or by viewing the equipment details with the NI-Director Operations Console.
Hardware Version	type the hardware version of the equipment that is either compatible or incompatible
Firmware Version	type the version of firmware that is either compatible or incompatible
Software Version	type the version of software that is either compatible or incompatible
Message Upon Found	type the message that is to be displayed when hardware is found to be either compatible or incompatible. For example, enter something like Bad Part Number .

16. Determine how you want to proceed:

To	Then
manually create the list of hardware components	repeat from Step 14 .
complete the procedure	go to Step 17 .

17. Click **Save** to save the changes.

The system modifies the hardware specification and displays the list of Network Audits.

4.3.3 Modify an existing alarm audit specification

Use this procedure to modify an existing alarm audit specification that checks for specific alarm conditions or for any alarm condition on NEs.

As part of the alarm audit modification you can specify which alarms cause the audit to fail. This alarm specification can be done manually, or the alarms can be imported from an XML file. If you want to import a list of alarms from a file, create the file before using this procedure. To create the alarm file, see [“Create an alarm audit XML file” on page 57](#).

1. Launch **Network Audit**.
2. If not already selected, click the **Audits** tab.
The system displays the Network Audit screen.



3. Click the name of the alarm audit to be modified.

The system displays the alarm audit details.

Alarm Audit

Audit Name

AnyAlarm

Audit Description

Any alarm fails audit

Any alarm fails audit

Specified alarms fail audit

Alarm Checking Criteria · no entries

Select

Alarm/Condition Type

Severity

Service Effect

AID Type

Comparison Logic

Description

No items in list!

Create

Delete

Load Alarm Checking Criteria From File

Browse...

Load & Merge

Load & Overwrite

Save

Close

Rows per page: 10

4.

If required, in the **Audit Name** field, change the name to describe the audit.
5.

If required, in the **Audit Description** field, change the description of the audit.
6.

Select appropriate action for the audit to take when alarms are detected:

To	Then
have any alarm cause the audit to fail	go to Step 15 .
have one or more specific alarm conditions cause the audit to fail	go to Step 7 .

7.

Select **Specified alarms fail audit**.
8.

Determine how you want to proceed:

To	Then
import the list of alarms from an existing file	go to Step 9 .
manually create the list of alarms	go to Step 12 .

9.

Click **Browse** to locate the alarm XML file.
10.

Determine how you want the data to be added:

To	Then
you want the alarm data in the file to merge with existing data	click Load & Merge
you want the alarm data to overwrite and replace any existing data	click Load & Overwrite

11. Determine how you want to proceed:

If	Then
you have more data to import	repeat from step Step 9 .
you want to manually add more alarm data	go to Step 12 .
you are finished adding alarm data	go to Step 16 .

12. Click **Create**.

The system displays a blank entry in the Alarm Checking Criteria list.

The screenshot shows a web interface titled "Alarm Checking Criteria" with a sub-header "1 item". Below this is a table with the following columns: "Select" (with a checkbox), "Alarm/Condition Type" (text input), "Severity" (dropdown menu showing "All"), "Service Effect" (dropdown menu showing "All"), "AID Type" (text input), "Comparison Logic" (dropdown menu showing "Exact"), and "Description" (text input). Below the table are two buttons: "Create" and "Delete".

13. Specify the details for the alarm condition as described in the [Alarm checking criteria attributes](#) table.

Table 4–6: Alarm checking criteria attributes

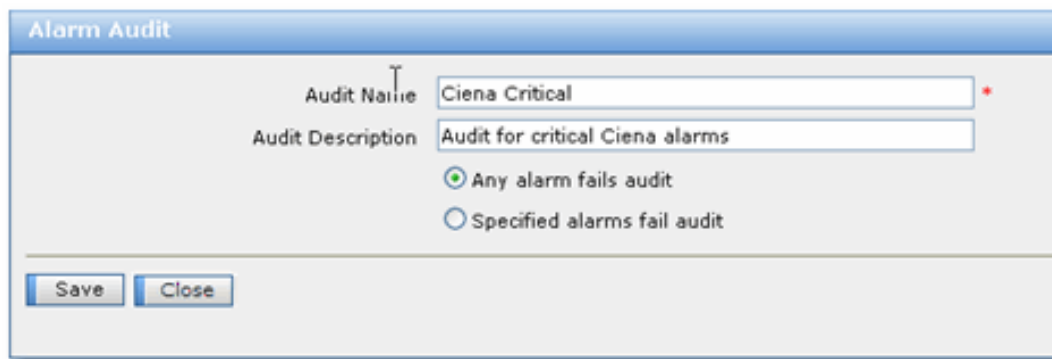
Field	Description
Alarm Condition Type	Enter the alarm condition type, for example, EQPT
Severity	Enter the alarm severity: <ul style="list-style-type: none"> • Intermediate • Cleared • Warning • Minor • Major • Critical
Service Effect	Enter the effect that the alarm has on service: NSA (non service-affecting) or SA (service-affecting)
AID Type	Enter the alarm AID type, for example, OC192
Comparison Logic	Enter the comparison logic for the alarm: <ul style="list-style-type: none"> • Exact: matches all of the alarm audit criteria • Contain: matches any of the alarm audit criteria
Description	The long description of the alarm condition

14. Determine how you want to proceed:

To	Then
manually create more alarm entries	repeat from Step 12 .
complete the procedure	Step 16 .

15. Select **Any Alarm Fails Audit**.

The system hides the list of Alarm Checking Criteria.



The 'Alarm Audit' dialog box contains the following fields and options:

- Audit Name:** Ciena Critical
- Audit Description:** Audit for critical Ciena alarms
- Options:**
 - ☒ Any alarm fails audit
 - ☐ Specified alarms fail audit
- Buttons:** Save, Close

- Click **Save** to save the changes.

The system adds the alarm audit to the list of Network Audits.

4.3.4 View a list of audit jobs and job details

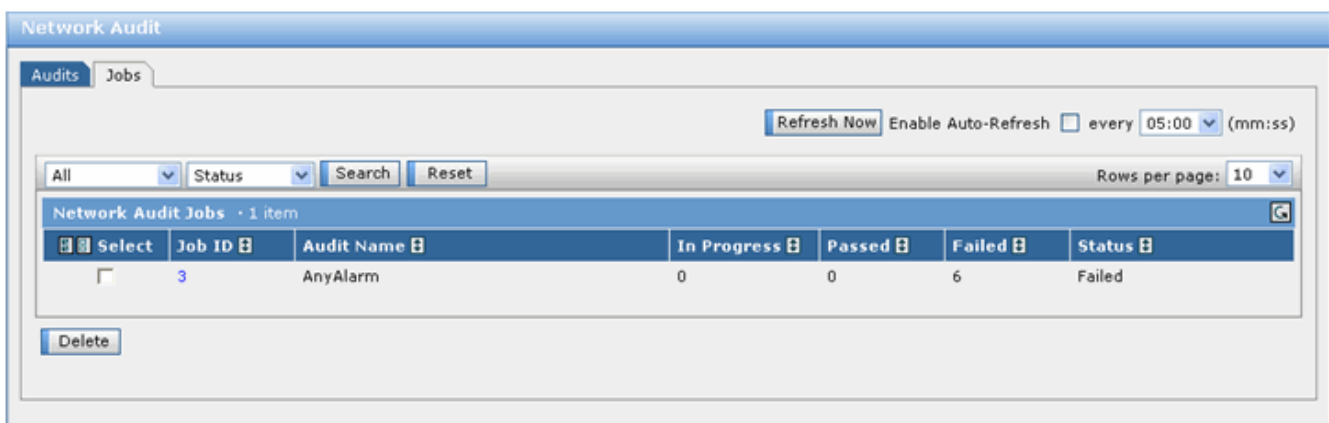
Use this procedure to view the list of existing audit jobs, which provides the following information:

- **Job ID:** a numeric identifier for the audit job
- **Audit Name:** the name assigned to audit when it was created
- **Originator:** the user ID of the person who created the audit
- **Status:** the current status of the audit job.
- **Total NEs:** the total number of NEs being audited
- **In Progress:** the number of NEs that are currently in the process of being audited
- **Passed:** the number of NEs that passed the audit
- **Failed:** the number of NEs that failed the audit

- Launch **Network Audit**.

The system displays the Network Audit screen.

- If not already selected, click the **Jobs** tab.



The 'Network Audit' screen shows the 'Jobs' tab. It includes a 'Refresh Now' button, an 'Enable Auto-Refresh' checkbox, and a time interval dropdown set to '05:00 (mm:ss)'. Below these are filters for 'All' (selected), 'Status', 'Search', and 'Reset'. A 'Rows per page' dropdown is set to '10'. The main table, titled 'Network Audit Jobs - 1 item', displays the following data:

Select	Job ID	Audit Name	In Progress	Passed	Failed	Status
<input type="checkbox"/>	3	AnyAlarm	0	0	6	Failed

A 'Delete' button is located at the bottom left of the table.

3. You can filter the list of network audits that are displayed by selecting the criteria (**Status** or **Audit Name**), typing the filter term in the text field, and then clicking **Search**.

You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#).

4. To drill down and view the details of a job, click the **Job ID** number.
The system displays the details of the audit job.



5. To view more details about the NEs being audited, click **Show Details**.

The system displays the details of the job, which lists the status of each NE being audited. The status is one of Unstarted, Failed, Passed, or In Progress.

The screenshot shows a 'Network Audit Job' window. At the top right, there is a 'Refresh Now' button and an 'Enable Auto-Refresh' checkbox with a frequency dropdown set to '05:00 (mm:ss)'. Below this is the 'Job Summary' section, which displays the following information:

- Job ID: 3
- Audit Name: AnyAlarm
- Originator: sysadmin
- Status: In Progress
- Total NEs: 6
- In Progress: 6
- Passed: 0
- Failed: 0

Below the summary is a '<< Hide Details' button. The 'NE Status' section features a filter bar with 'All' and 'Status' dropdowns, 'Search' and 'Reset' buttons, and a 'Rows per page: 10' dropdown. The main area displays a table titled 'Network Element Job Status - 6 items'.

NE Identifier	Vendor	Model	Status
CORESTREAM-10008-0	Ciena	Corestream	In Progress
CORESTREAM-10017-0	Ciena	Corestream	In Progress
CORESTREAM-10009-0	Ciena	Corestream	Failed
CORESTREAM-10016-0	Ciena	Corestream	Failed
CORESTREAM-10007-0	Ciena	Corestream	In Progress
CORESTREAM-10018-0	Ciena	Corestream	In Progress

At the bottom left of the window is a 'Close' button.

- To refresh the screen with the latest status information, click **Refresh Now** or select **Auto-Refresh** and specify a frequency.
- To return to the list of audit profiles, click **Close**.

4.3.5 Delete an audit job from the database

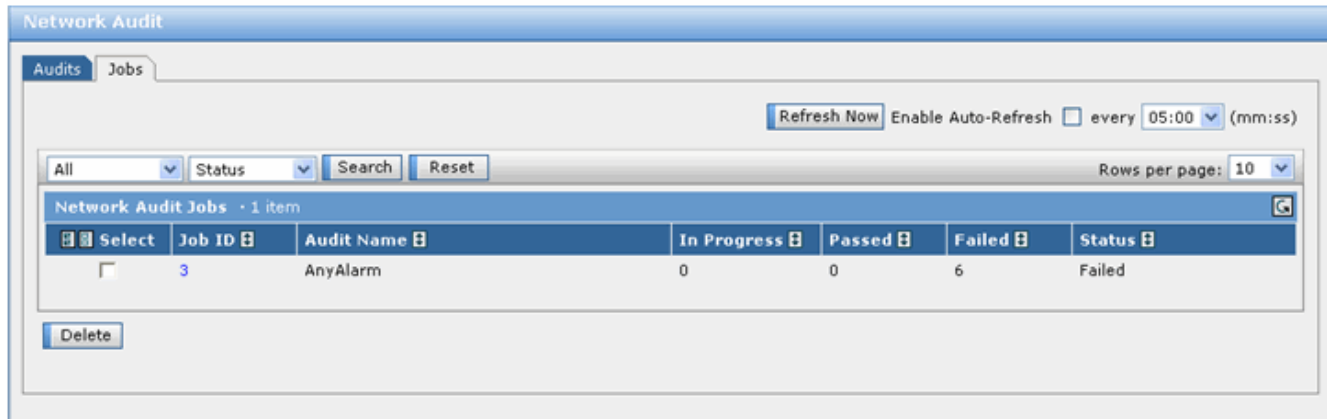
Use this procedure to delete an audit job from the database.



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

- Launch **Network Audit**.
- If not already selected, click the **Jobs** tab.

The system displays the list of audit jobs.

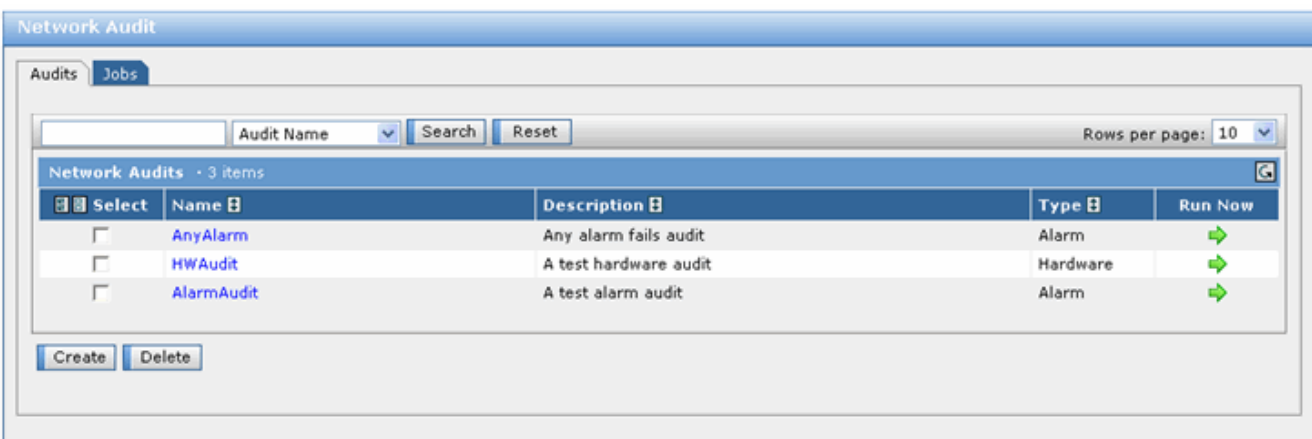


3. From the list of audit jobs, select one or more audit jobs to be deleted.
4. Click **Delete**.
The system prompts for confirmation.
5. Click **OK** confirm the operation.
The system removes the audit job from the list.
To re-run the audit, see [“Perform an audit” on page 62](#).

4.3.6 Delete an audit specification from the database

Use this procedure to delete a hardware or alarm audit specification.

1. Launch **Network Audit**.
2. If not already selected, click the **Audits** tab.
The system displays the list of existing audits. Each audit is named and identified as either a hardware or alarm audit.



3. From the list of Network Audits, select one or more audit specifications to be deleted.
4. Click **Delete**.
The system prompts for confirmation.
5. Click **OK** to confirm the operation.
The system removes the audits from the database.

5 Software Delivery: Performing NE software delivery

The NI-Director **Software Delivery** application allows network administrators to quickly and easily perform parallel software upgrades on a large number of network elements all at the same time, and from a single interface.

When preparing for a network software upgrade, the Software Delivery application can conduct an automated, network-wide audit of network element readiness to ensure that all network elements meet the appropriate conditions before the upgrade is performed. (Network audits are configured and managed with the Network Audit application. See [“Network Audit: Auditing the network before a software delivery” on page 47.](#))

Once all relevant network elements are deemed ready, the application automates delivery of the software upgrades to the network elements over the network itself, eliminating the need for manual intervention.

The Software Delivery application is divided into two functional areas:

- [Software Releases](#)
- [Workflows](#)

Software Releases: A software release identifies the software load, its location on a managed file server, the hardware and software compatibility details, the audit requirements, and it specifies the behavior during the different phases of the network element software delivery process.

Workflows: A workflow associates a single software release with a group of network elements. After a workflow is created, you create targets, which represent smaller units of work within the workflow. Targets identify specific NEs from within the NE Groups that are defined in a workflow. The actual network software delivery process is executed and controlled at the Target level. In order for the software release to be delivered, all of the NEs in a target must be compatible with the vendor’s software release.



Note: If an application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they know what to expect when managing network elements from the Network Integrity client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

This section includes the following procedures for configuring and managing Software Delivery:

“Configuring and performing a software delivery” on page 80

This section contains the following procedures for configuring and running a software delivery:

- [“Create and run hardware and alarm audits” on page 81](#)
- [“Copy software releases to the managed file server” on page 81](#)
- [“Create a software image configuration file” on page 82](#)
- [“Create a software release specification” on page 83](#)
- [“Create a software delivery workflow” on page 93](#)
- [“Create targets in a workflow” on page 98](#)
- [“Perform a software delivery on workflow targets” on page 101](#)
- [“Monitor the software release process” on page 109](#)

“Managing software releases” on page 111

This section contains the following procedures for managing software releases that have already been configured:

- [“List of software releases and view or modify details I” on page 112](#)
- [“Delete a software release from the database” on page 118](#)

“Managing software delivery workflows” on page 119

This section contains the following procedures for managing workflows that have already been configured:

- [“List workflows and view or modify details” on page 119](#)
- [“Delete a workflow from the database” on page 124](#)

“Managing software delivery targets” on page 125

This section contains the following procedures for managing targets that have already been configured:

- [“List targets within a workflow and view or modify target details” on page 125](#)
- [“Delete targets from a workflow” on page 130](#)



Note: For NEs that use TFTP, you must configure the TFTP server on a Unix system so that the Software Delivery features function properly. This is done by editing the `inetd.conf` file. See the Network Integrity Installation and Administration Guide for Details.

5.1 Configuring and performing a software delivery

This section contains the following procedures for configuring and performing a software delivery:

- [“Create and run hardware and alarm audits” on page 81](#)
- [“Copy software releases to the managed file server” on page 81](#)
- [“Create a software image configuration file” on page 82](#)
- [“Create a software release specification” on page 83](#)
- [“Create a software delivery workflow” on page 93](#)
- [“Create targets in a workflow” on page 98](#)
- [“Perform a software delivery on workflow targets” on page 101](#)
- [“Monitor the software release process” on page 109](#)

5.1.1 Create and run hardware and alarm audits

Use the Network Audit application to create audits that check for hardware compatibility and alarms on NEs in the network. Audits can be run as part of a software delivery, or they can be run independently. If you are going to run audits as part of a software release, the audits must be created before the software release specification is created so that the audits are available when you configure the details of the software release. If you are going to be running audits manually, use the Network Audit application to create audits. See [“Create a hardware audit profile” on page 52](#) or [“Create an alarm audit profile” on page 58](#).



Note: As part of the configuration of a hardware audit, you must specify the hardware compatibility matrix, which either permits or prevents the download of a software release to a network element based on whether the software release is compatible or incompatible with the network element’s installed hardware. As part of this process, you can manually enter data about the hardware that is compatible with the specific software release to be delivered, or you can import the data from a file. If you want to import the hardware compatibility matrix data from a file, create the file before creating the hardware audit. See [“Create a hardware component XML file” on page 50](#).



Note: Hardware compatibility matrix naming must exactly match adapter naming or an “adapter not-found” error message appears.



Note: As part of the configuration of an alarm audit, you can specify which alarms cause the audit to fail. This alarm specification can be done manually, or the alarms can be imported from an XML file. If you want to import a list of alarms from a file, create the file before creating the alarm audit. To create the alarm file, see [“Create an alarm audit XML file” on page 57](#).

5.1.2 Copy software releases to the managed file server

Before a software delivery can occur, follow the procedure in the NI-Framework Configuration Guide to “Configure file servers for your products” and add a remote server for NI-Director.

After the file server has been added to the database, copy the vendor's NE software release load to the server following the recommended procedures for the server.

5.1.3 Create a software image configuration file

When you create the software release specification, you can manually configure the release, or you can import the release information from a Software Image Configuration File. If you want to import the data from a file, use this procedure to create a Software Image Configuration file that can be imported when you create a software release. The file can be a CSV, TXT or XML file format.

Store the Software Image Configuration file on a server that can be accessed from the Network Integrity Framework client interface while creating a software release. See [“Create a software release specification” on page 83](#).

A TXT configuration file lists the software image information each on a separate line of the file as shown in the following example:

10.10.39.0_release.catalog

10.10.39.0_releaseSPE.catalog

CertInstall.jar

HWRUL101.DAT

OPTeraSM.info

OPTeraSM.jar

smi.bat

smitps.info

smitps.jar

Zone_apbe_release.bin

Zone_gsrn_release.bin

Zone_motr_release.bin

Zone_mtr2_release.bin

Zone_oci_release.bin

Zone_ocld_release.bin

Zone_ocm_release.bin

Zone_ola_release.bin

Zone_osc_release.bin

Zone_otr_release.bin

Zone_sp_release.bin

Zone_sp2_release.bin

Zone_srm_release.bin

A CSV lists the software image information separated by commas.

5.2 Create a software release specification

Use this procedure to create a software release specification, which adds a network element software release to the database and configures the actions that occur when the release is delivered. After the release is created with this procedure, it becomes available for use in Workflows.



Note: When you create the software release specification, you can manually configure the release, or you can import the release information from a Software Image Configuration File. If you want to import the data from a file, create the file before creating the software release specification. See [“Create a software image configuration file” on page 82](#).

The Software Delivery application uses the Software Release Creation Wizard to guide you through the following process of creating a software release specification:

- identify the software release by naming it and specifying the vendor and version.



Note: The version that you specify must be supported by the adapter, and you must enter the new release version in its complete form, exactly as specified by the vendor, such as 14.0.7. Do not enter an abbreviated version, such as 14.0. To obtain the exact version number, consult the vendor documentation or the Adapter Release notes.

- specify and validate the location of the vendor software loads that were placed on a server
 - specify the current software versions that are compatible with the release specification being created
 - specify the hardware that is compatible with the release specification being created
 - specify whether to perform a hardware or alarm audit as part of the distribution phase of the software release. Note that the audit must be created before performing this procedure.
 - specify whether to perform a hardware and alarm audit during each phase of the software release process. Note that the audit must be created before using this procedure.
1. Launch **Software Delivery**.
 2. If not already selected, click the **Software Release** tab.

The system displays the Software Release screen.

3. Click **Create**.

The system displays Step 1 of the Create Software Release wizard where you identify the software release being added.

4. In the **New Software Release Name** field, type a descriptive name to identify the software release.
5. From the **Vendor** list, select the NE vendor to which the release applies.
6. In the **New Version** field, type the software release version.
 Note: The version number that you type in the “Version” field must exactly match the software version that is supported by the network adapter. For example, if the version is 4.1.1, do not enter 4.1.
7. In the **Description** field, type a description for the software release load.
8. Click **Next**.

The system displays Step 2 of the software creation wizard where you specify and validate the location of the vendor software load that was placed on a server.

9. From the **File Server** list, select the file server that contains the software image for the release you are creating.

Note: The File Server list displays only the servers that were added to the database.

10. Determine how you want to proceed:

To	Then
import the software configuration from an existing file	go to Step 11 .
manually create the software configuration	go to Step 14 .

11. Click **Browse** to locate the software configuration file.

12. Determine how you want to add data:

If	Then
you want the data in the file to merge with existing data	click Load & Merge
you want the data to overwrite and replace any existing data	click Load & Overwrite

13. Determine how to proceed:

If	Then
you have more configuration data to import	repeat from Step 11 .
you want to manually add a configuration file	go to Step 14 .
you are finished adding data to the matrix	go to Step 16 .

14. Click **Add**.

The system displays a blank entry in the files list.

Create Software Release - Ciena

Step 1: General Profile
Step 2: File Location

File Server: MVEM files Create
Relative Path: aload

Rows per page: 10

Select	File Name
<input type="checkbox"/>	ConfigFile.CON

Add Delete Test File Presence

Load software image file names from a configuration file
File Browse...
Load & Merge Load & Overwrite

<< Back Next >> Cancel

15. In the blank field in the File Name column, type the name of the software image exactly as it would appear on the file server where the software load is stored.
16. To validate the presence of a software load file, select one or more files in the list and click **Test File Presence**.

The system displays the status of the validation:

- **Yes:** the file location was present
- **No:** the file was not present
- **Untested:** a validation was requested, but the file presence has not been validated yet

17. Click **Next**.

The system displays Step 3 of the software creation wizard. The status that is displayed in the "Adapter Deployed For Specified Version" column must say "Yes".

If the status is “No,” there is no network adapter to support the software version you entered in the “Version” field in [Step 6](#).

Create Software Release - Ciena

Step 1: General Profile
Step 2: File Location
Step 3: Hardware Compatibility

Rows per page: 10

Compatible	Name	Adapter Deployed For Specified Version
<input type="checkbox"/>	Core	Yes

<< Back Next >> Cancel

18. Select the hardware that is compatible with the release specification you are creating.

19. Click **Next**.

The system displays Step 4 of the software creation wizard where you identify and add software versions that are compatible with the release being created.

Create Software Release - NewLoad

Step 1: General Profile
Step 2: File Location
Step 3: Hardware Compatibility
Step 4: Software Compatibility

Rows per page: 10

Select	Previous Versions
No items in list!	

Add Delete

<< Back Next >> Cancel

20. To add an entry to the compatible software list, click **Add**

The system displays a blank entry in the list of compatible software.

The screenshot shows the 'Create Software Release - NewLoad' window. On the left, a sidebar lists five steps: Step 1: General Profile, Step 2: File Location, Step 3: Hardware Compatibility, Step 4: Software Compatibility (highlighted with a blue arrow), and Step 5: General Profile. The main area displays a table titled 'Compatible Software' with 1 item. The table has two columns: 'Select' and 'Previous Versions'. Below the table are 'Add' and 'Delete' buttons. At the bottom right, there are '<< Back', 'Next >>', and 'Cancel' buttons.

21. In the blank field in the Previous Versions column, type the software version that is compatible with the software release being created. To remove an entry, select it and click **Delete**.

Note: If you are in a situation, such as testing, where you are not actually upgrading, but re-installing the same version of software, you must enter the value of the “Version” being installed as a “Previous Version” in the Compatible Software list. For example, if you are re-installing version 7.2, 7.2 must also appear as a Previous Version in the Compatible Software list.

22. Repeat from [Step 20](#). until all the compatible software has been entered.
23. Click **Next**.

The system displays Step 5 of the software creation wizard where you create a General Profile that can be used for the different phases of the software release.

The screenshot shows the 'Create Software Release - NewLoad' window. On the left, a sidebar lists five steps: Step 1: General Profile, Step 2: File Location, Step 3: Hardware Compatibility, Step 4: Software Compatibility, and Step 5: General Profile (highlighted with a blue arrow). The main area contains two radio button options: 'No Hardware Audit' (selected) and 'Select Hardware Audit'. Below these are two more radio button options: 'No Alarm Audit' (selected) and 'Select Alarm Audit'. At the bottom right, there are '<< Back', 'Next >>', and 'Cancel' buttons.

24. Determine whether you want to add hardware audits to the General Profile, which can be used by the different phases of the software release process:

To	Then
have specific hardware audits added to the General Profile	select Select Hardware Audit and then go to Step 25 .
not have hardware audits in the General Profile	select No Hardware Audit and then go to Step 26 .

25. In the Choose column of the list of hardware audits, select the required hardware audits to perform as part of the General Profile.

The screenshot shows the 'Create Software Release - NewLoad' application window. On the left, a sidebar lists steps: Step 1: General Profile, Step 2: File Location, Step 3: Hardware Compatibility, Step 4: Software Compatibility, and Step 5: General Profile (which is highlighted with a blue arrow). The main area is divided into two sections. The top section is for 'Hardware Audits' and has two radio buttons: 'No Hardware Audit' and 'Select Hardware Audit' (which is selected). Below these is a search bar with a 'Name' dropdown, 'Search', and 'Reset' buttons. A table titled 'Hardware Audits - 2 items' is shown with columns 'Choose' and 'Name'. The table contains two rows: 'HWAudit' and 'Test', both with checkboxes in the 'Choose' column. The bottom section is for 'Alarm Audits' and has two radio buttons: 'No Alarm Audit' (which is selected) and 'Select Alarm Audit'. At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

26. Determine whether you want to add alarm audits to the General Profile, which can be used by the different phases of the software release process.

To	Then
have specific alarm audits added to the General Profile	select Select Alarm Audit and then go to Step 27 .
not have hardware audits in the General Profile	select No Alarm Audit and then go to Step 28 .

27. In the Choose column of the list of alarm audits, select the required alarm audits to perform.

Create Software Release - NewLoad

Step 1: General Profile
Step 2: File Location
Step 3: Hardware Compatibility
Step 4: Software Compatibility
Step 5: General Profile

☒ No Hardware Audit
☐ Select Hardware Audit

☐ No Alarm Audit
☒ Select Alarm Audit

Search: [Name] [Search] [Reset] Rows per page: 10

Choose	Name
<input type="checkbox"/>	AnyAlarm
<input type="checkbox"/>	AlarmAudit
<input type="checkbox"/>	Critical

<< Back Next >> Cancel

28. Click **Next**.
- The system displays Step 6 of the software creation wizard where you specify whether to use the General Profile during the Distribution phase of the software release, or to use a customized profile during the Distribution phase.

Create Software Release - NewLoad

Step 1: General Profile
Step 2: File Location
Step 3: Hardware Compatibility
Step 4: Software Compatibility
Step 5: General Profile
Step 6: Distribution Profile

☒ Use general profile during Distribution
☐ Use following profile during Distribution

<< Back Next >> Cancel

29. Determine which profile is to be used during the Distribution phase of the software release:

To	Then
use a custom profile	select Use Following Profile During Distribution and then go to step Step 30 .
use the General Profile. Note that the General Profile was created in Step 5 of the wizard.	select Use General Profile During Distribution and then go to Step 34 .

30. Determine whether a hardware audit is to be performed during the Distribution phase of the software release:

To	Then
have a hardware audit performed as part of the Distribution phase	select Select Hardware Audit and then go to step Step 31 .
not have a hardware audit performed as part of the Distribution phase	select No Hardware Audit and then go to Step 32 .

31. In the Choose column of the list of hardware audits, select the required hardware audits to perform as part of the Distribution phase.

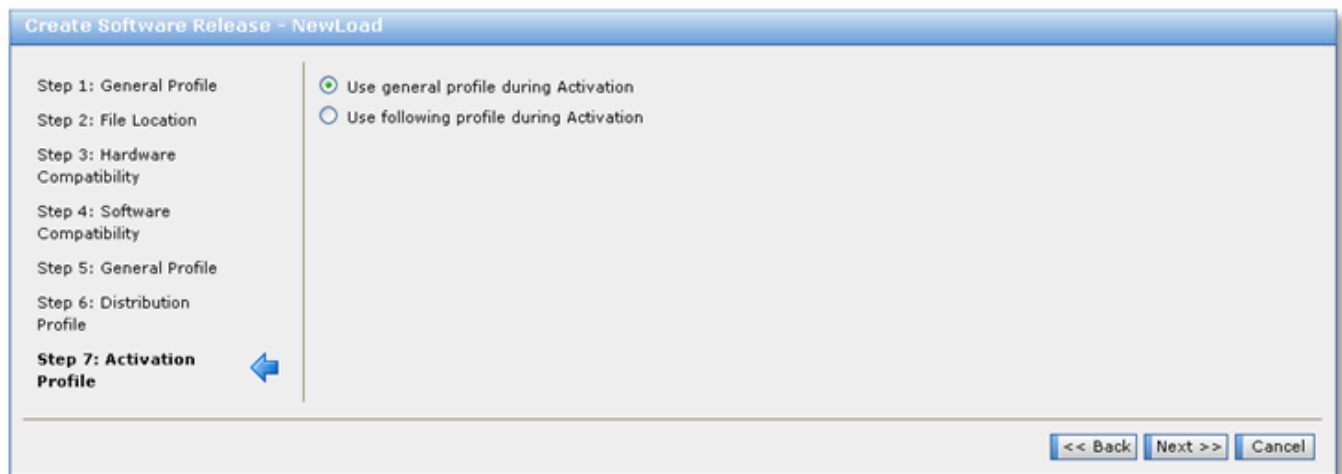
32. Determine whether an alarm audit is to be performed during the Distribution phase of the software release:

To	Then
have an alarm audit performed as part of the Distribution phase	select Select Hardware Audit and then go to step Step 33 .
not have an alarm audit performed as part of the Distribution phase	select No Alarm Audit and then go to Step 34 .

33. In the Choose column of the list of alarm audits, select the required alarm audits to perform as part of the Distribution phase.

34. Click **Next**.

The system displays Step 7 of the software creation wizard where you specify whether to use the General Profile during the Activation phase of the software release, or to use a customized profile during the Activation phase.



35. Determine whether a hardware audit is to be performed during the Activation phase of the software release:

To	Then
have a hardware audit performed as part of the Activation phase	select Select Hardware Audit and then go to step Step 36 .
not have a hardware audit performed as part of the Activation phase	select No Hardware Audit and then go to Step 37 .

36. In the Choose column of the list of hardware audits, select the required hardware audits to perform as part of the Activation phase.

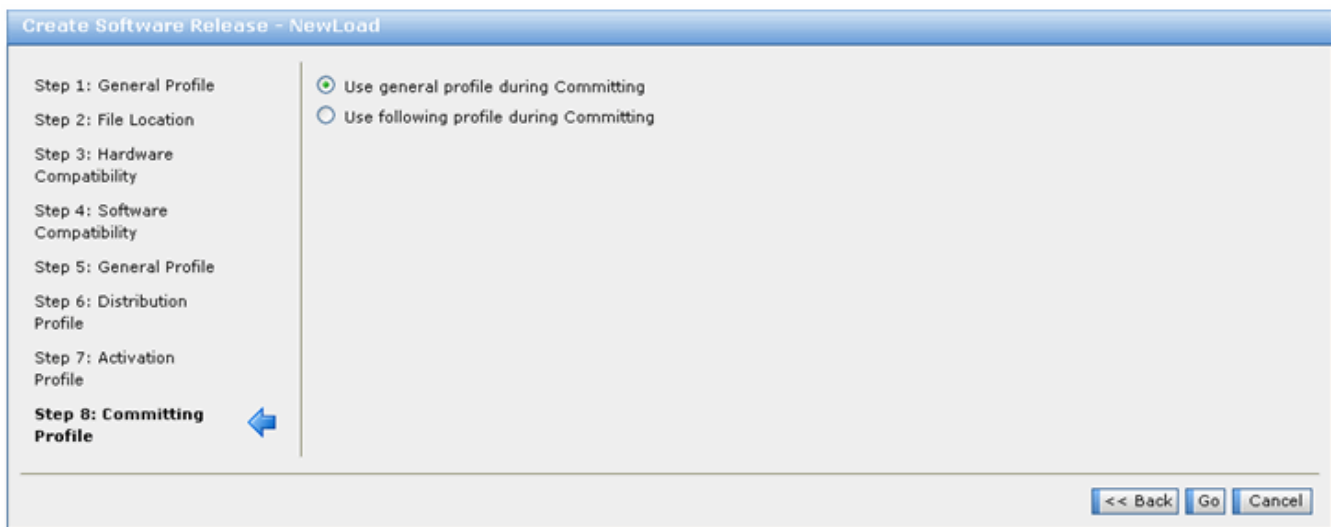
37. Determine whether an alarm audit is to be performed during the Activation phase of the software release:

To	Then
have an alarm audit performed as part of the Activation phase	select Select Hardware Audit and then go to step Step 38 .
not have an alarm audit performed as part of the Activation phase	select No Alarm Audit and then go to Step 39 .

38. In the Choose column of the list of alarm audits, select the required alarm audits to perform as part of the Distribution phase.

39. Click **Next**.

The system displays Step 8 of the software creation wizard where you specify whether to use the General Profile during the Committing phase of the software release, or to use a customized profile during the Committing phase.



40. Determine whether a hardware audit is to be performed during the Committing phase of the software release:

To	Then
have a hardware audit performed as part of the Committing phase	select Select Hardware Audit and then go to step Step 41 .
not have a hardware audit performed as part of the Committing phase	select No Hardware Audit and then go to Step 42 .

41. In the Choose column of the list of hardware audits, select the required hardware audits to perform as part of the Committing phase.
42. Determine whether an alarm audit is to be performed during the Committing phase of the software release:

To	Then
have an alarm audit performed as part of the Committing phase	select Select Hardware Audit and then go to step Step 43 .
not have an alarm audit performed as part of the Committing phase	select No Alarm Audit and then go to Step 44 .

43. In the Choose column of the list of alarm audits, select the required alarm audits to perform as part of the Committing phase.
44. Click **Next**.
45. Click **Go** to create the software release.

The new software release is added to the software release list.

5.2.1 Create a software delivery workflow

Use this procedure to create a software delivery workflow, which associates a single software release with a group of network elements. For example, you could create a Workflow to upgrade all of a specific vendor/model of network element that are installed in California.

The [Procedure Policy parameters for each phase](#) table describes the parameters for each phase of the workflow procedure policy.

Table 5–1: Procedure Policy parameters for each phase

Parameter	Description
GNE Sequence Policy	Specifies when to perform the corresponding phase on the Primary gateway network element (GNE): First , Last , or at Any time
Run Audits Before (per NE)	Audits the network elements before each phase of the upgrade procedure

Parameter	Description
On Audit Error (per NE)	Directs the upgrade process to stop or continue if the audit fails on a network element
Concurrent Policy (per target)	Specifies how many NEs on which to execute the policy concurrently: Specify , Min , or Max . If you select Specify , a dialogue window opens next to the box where you can type in the number of NEs.
On Operation Error (per target)	Directs the process to either Stop or Continue with NEs in a target that are in the “pending” state after one or more NEs in the target fail

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.
The system displays the list of existing workflows.

The screenshot shows the 'Software Delivery' application window with the 'Workflow' tab selected. At the top right, there are buttons for 'Refresh Now' and 'Enable Auto-Refresh' with a dropdown set to '05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main area displays a table titled 'Workflows - 1 item' with columns: 'Select', 'Workflow', 'Prime', 'Status', 'Number of Targeted NEs', and 'Completed'. A single workflow is listed: 'Eastern Seaboard Workflow' with Prime 'Martin', Status 'Unstarted', 0 targeted NEs, and 0 completed. At the bottom left are 'Create' and 'Delete' buttons.

3. Click **Create**.
The system displays Step 1 of the Create Workflow wizard.

The screenshot shows the 'Create Workflow' wizard, Step 1: Information. On the left is a sidebar with 'Step 1: Information' and a blue arrow pointing left. The main area contains four input fields: 'Workflow Name:', 'Prime:', 'Description:', and 'First Comment:'. The 'Description' and 'First Comment' fields have expandable arrows on their right sides. At the bottom right are 'Next >>' and 'Cancel' buttons.

4. In the **Workflow Name** field, type a descriptive name for the workflow.

5. In the **Prime** field, type the name of the person who is the prime contact for this workflow.
6. In the **Description** field, type a description for the workflow.
7. In the **First Comment** field, type any comments that you want to associate with the workflow.
8. Click **Next**.

The system displays Step 2 of the Create Workflow wizard, which lists available software releases.

Create Workflow - Upgrade Workflow

Step 1: Information

Step 2: Software Release Selection

Software Release Search Reset Rows per page: 10

Choose	Software Release	Vendor	Version
<input type="checkbox"/>	NewLoad	C...	ReleaseZZ

<< Back Next >> Cancel

9. You can filter the list by selecting the criteria (**Software Release**, **Vendor** or **Version**), typing the filter term in the text field, and then clicking **Search**.
You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#).
10. From the list, select one software release for the workflow. Note that only one software release can be selected.
11. Click **Next**.

The system displays Step 3 of the Create Workflow wizard, which is where you select the NE Groups for the workflow.

Create Workflow - Upgrade Workflow

Step 1: Information

Step 2: Software Release Selection

Step 3: NE Groups Selection

Available NE Groups · 1 item

Select NE Group Name

All NEs

Add

Selected NE Groups · no entries

Select NE Group Name

No items in list!

Remove

<< Back Next >> Cancel

12. You can filter the list of displayed NE groups by selecting **NE Group Name**, typing the criteria in the text field, and then clicking **Search**. You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#).
13. Select the NE Groups to assign to the workflow, and then click **Add**. This moves the NEs from the **Available NE Groups** list to the **Selected NE Groups** list. Repeat this as many time as required to select the necessary NE groups.
14. Click **Next**.

The system displays Step 4 of the Create Workflow wizard, which is where you specify the policies to use.

Create Workflow - Upgrade Workflow

Step 1: Information

Step 2: Software Release Selection

Step 3: NE Groups Selection

Step 4: Procedure Policy

Use Default Procedure Policy

Specify Procedure Policy

<< Back Go Cancel

The procedure policy enables you to define the sequence of an upgrade and how an upgrade behaves if errors occur during the upgrade process. This policy can be defined for each phase of the workflow: **Distribute**, **Activate**, and **Commit**.

15. You can use the Default Procedure Policy for these phases or you can customize each phase of the policy. Select the type of procedure policy you want to use:

To	Then
specify the parameters of procedure policy	select Specify Procedure Policy and then go to Step 16 .
use the default procedure policy	select Use Default Procedure Policy and then go to Step 17 .

16. Set the required parameter for each phase of the workflow as described in table “[Procedure Policy parameters for each phase](#)” on page 93.

Create Workflow - Upgrade Workflow

Step 1: Information
Step 2: Software Release Selection
Step 3: NE Groups Selection
Step 4: Procedure Policy

☐ Use Default Procedure Policy
☒ Specify Procedure Policy

Procedure Policy	Distribute	Activate	Commit
GNE Sequence Policy	Any	Any	Any
Run Audits Before (per NE)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
On Audit Error (per NE)	Stop	Stop	Stop
Concurrency Policy (per Target)	Min	Min	Min
On Operation Error (per Target)	Continue	Stop	Stop

[Reset to Defaults](#)

[<< Back](#) [Go](#) [Cancel](#)

17. Click **Go**.

The system displays the Workflow Details, which is where you can create the targets.

Workflow Details

Name: Upgrade Workflow
Prime: Martin
Upgrade To: **NewLoad**
Vendor: Acme
Description:

Targets | Comments | NE Groups | Procedure Policy

[Refresh Now](#) Enable ☐ Auto-Refresh ☐ every 05:00 (mm:ss)

Rows per page: 10

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
No items in list!									

[Create](#) [Delete](#)

[Save](#) [Close](#)

18. Proceed according to when you specify the targets as follows:

If you want to	Then
specify the targets now	follow the instructions in “Create targets in a workflow” on page 98 beginning at Step 5 .
specify the targets later	click Save and do not continue with this procedure. To create the targets later, see “Create targets in a workflow” on page 98 .

5.2.2 Create targets in a workflow

The actual software delivery is executed on a targets, which identify specific NEs from within the workflow on which to perform the delivery.



Note: In order for the software release to be compatible, all of the NEs defined in a target must be compatible with the vendor's software release.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.

The system displays the list of workflows.



3. Click the name of the workflow to which you want to add a target.
The system displays the Workflow details screen.
4. If not already selected, click the **Targets** tab.

The system displays a list of existing targets that have been configured for the workflow.

The 'Workflow Details' window displays configuration for a target named 'Eastern Seaboard'. The 'Prime' is 'Martin', 'Upgrade To' is 'NewLoad', and 'Vendor' is 'C'. The 'Description' field is empty. Below the configuration fields are tabs for 'Targets', 'Comments', 'NE Groups', and 'Procedure Policy'. The 'Targets' tab is active, showing a table with one item: 'Vermont'. The table columns are: Select, Target, Prime, Status, Number of NEs, Distributed, Activated, Committed, Available Operations, and Run. The 'Run' column has a green arrow icon. Below the table are 'Create' and 'Delete' buttons. At the bottom are 'Save' and 'Close' buttons.

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	

- Click **Create**.

The system displays Step 1 of the Create Target wizard.

The 'Create Target' wizard is shown at Step 1: Information. The fields are: Target Name, Prime, Description, and First Comment. The 'Next >>' and 'Cancel' buttons are at the bottom right.

- In the **Target Name** field, type a descriptive name to identify the target.
- In the **Prime** field, type the name of the person responsible for the target.
- In the **Description** field, type a description of the target.
- In the **First Comment** field, type any comments to associate with the target. Note that additional comments can be added to the target later from the Comments tab of the target details screen.
- Click **Next**.

The system displays Step 2 of the Create Target wizard where you select the subset of NEs for the target from the NE groups that were assigned to the workflow.

Create Target - Ciena

Step 1: Information
Step 2: NE Selection

Search Available NEs

Compatibility: All

View: All NEs

NE Name:

Vendor: Custom...

Model: Custom...

Software Version:

NE Group Name:

Load Search Save Search

Search

Rows per page: 10

Available NEs - 1 to 10 of 24

Select	NE Identifier	Vendor	Model	Software Version	Compatible
<input type="checkbox"/>	CNRL01TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL12TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL09TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL10TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL08TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL07TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL11TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL06TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL04TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL02TX-0001	Ciena	Corestream	6.3.0	Yes

Add

Rows per page: 10

Target NEs - no entries

Select	NE Identifier	Vendor	Model	Software Version
No items in list!				

Remove

<< Back Next >> Cancel

11. Enter the desired search criteria to find a subset of NEs from which to select the targets. If you have an existing search query, you can use the **Load Search** button to load the query. For a complete description of searches, see [“Understanding searches” on page 188](#). You can also search based on the **Compatibility**: Compatible or Incompatible.
12. Select the NEs to assign to the target, and then click **Add**. This moves the NEs from the **Available NEs** list to the **Target NEs** list. Repeat this as many time as required to select the necessary NEs for the target.

13. Click **Next**.

The system displays Step 3 of the Create Target wizard.

Create Target - Upgrade Workflow - NEast

Step 1: Information
Step 2: NE Selection
Step 3: Procedure Policy

☐ Use Workflow Procedure Policy
☒ Specify Procedure Policy

Procedure Policy	Distribute	Activate	Commit
GNE Sequence Policy	Any	Any	Any
Run Audits Before (per NE)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
On Audit Error (per NE)	Stop	Stop	Stop
Concurrency Policy (per Target)	Min	Min	Min
On Operation Error (per Target)	Continue	Stop	Stop

Reset to Workflow Procedure Policy

<< Back Go Cancel

14. Assign a procedure policy for the target:

To	Then
use the procedure policy that was defined in the workflow	select Use The Workflow Procedure Policy , and then go to Step 15 .
customize the procedure policy for the target	select Specify Procedure Policy and set the required parameter for each phase of the workflow as described in table “Procedure Policy parameters for each phase” on page 93.

15. Click **Go**.

The system adds the target to the workflow.

5.2.3 Perform a software delivery on workflow targets

The actual network software delivery process is executed and controlled at the Target level. You can perform a software delivery on all or some of the Targets within a Workflow, all the network elements within the Target, or on selected network elements within the Target. There are three phases to the software delivery process:

- [“Distribute the software release”](#) on page 101
- [“Activate the software”](#) on page 105
- [“Commit the software”](#) on page 107

Distribute the software release

Use this procedure to start the distribution phase of a software release. Distribution places the software load on each of the NEs specified in the workflow target.

During the distribution phase, software is downloaded from one of the following locations:

- for GNEs that support staging, the software is staged on the GNE before it is distributed to each network element in its span of control.
- for GNEs that do not support staging, the software is downloaded from the managed server directly to the NE.

Depending on how the policy is defined, the process can be stopped if a failure occurs.



Note: If during the audit the Software Delivery application discovers incompatible hardware components in a network element, the audit log for that network element indicates this. The log may also display “Null” values for non-affecting fields. These fields should be ignored.

While the distribution phase is running, you can terminate the process, which ends the process on the managed server for any NEs that are still pending an update.



Note: If terminate is issued against an NE that is in the “pending” state, the NE reverts back to “unstarted”. If terminate is issued against an NE that is in the “in progress” state, the process is terminated on the server, but the operation may continue on the NE itself. In this case, the termination may lead to a mismatch between the state of the NE and the state that is displayed by the Software Delivery application.

After the distribution phase has run, you can restart the phase, undo the phase, or force the status to indicate unstarted or successful.



Note: Some vendor NEs do not support the Distribute:Undo command. On some NEs, after performing a Distribute:Undo action the software load is not rolled back or removed from the NE. The Distribute:Undo action simply resets the software delivery state.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.

The system displays the list of workflows.

The screenshot shows the 'Software Delivery' window with the 'Workflow' tab selected. At the top right, there are buttons for 'Refresh Now' and 'Enable Auto-Refresh' with a dropdown set to 'every 05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main table, titled 'Workflows - 1 item', has columns: 'Select', 'Workflow', 'Prime', 'Status', 'Number of Targeted NEs', and 'Completed'. One row is visible for 'Eastern Seaboard Workflow' with Prime 'Martin' and Status 'Unstarted'. At the bottom are 'Create' and 'Delete' buttons.

Select	Workflow	Prime	Status	Number of Targeted NEs	Completed
<input type="checkbox"/>	Eastern Seaboard Workflow	Martin	Unstarted	0	0

3. Click the Workflow for which you want to perform the software distribution phase.
The system displays the workflow details.
4. If not already selected, click the **Targets** tab.
The system displays the list of targets defined for the workflow.

The screenshot shows the 'Workflow Details' window with the 'Targets' tab selected. At the top, there are input fields for 'Name' (Eastern Seaboard), 'Prime' (Martin), 'Upgrade To' (NewLoad), 'Vendor' (C), and 'Description'. Below the tabs, there are buttons for 'Refresh Now' and 'Enable Auto-Refresh' with a dropdown set to 'every 05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main table, titled 'Targets - 1 item', has columns: 'Select', 'Target', 'Prime', 'Status', 'Number of NEs', 'Distributed', 'Activated', 'Committed', 'Available Operations', and 'Run'. One row is visible for 'Vermont' with Prime 'Martin' and Status 'Unstarted'. The 'Available Operations' column shows 'Distribute:Run' and the 'Run' column has a green arrow button. At the bottom are 'Create', 'Delete', 'Save', and 'Close' buttons.

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	

5. Select one or more targets on which to distribute the software release.
6. From the **Available Operations** list, select **Distribute:Run**.
7. For each of the selected targets, click **Run**.

The software distribution process begins.

Note: If a process is just underway and you select that same process again from the **Available Operations** list, the system displays an error. The original

process is unaffected and any subsequent request for same process are ignored.

The system displays the status of the distribution for each NE in the target.

Target Details

Target Name

Vermont

Prime

Martin

Upgrade To:

NewLoad

Vendor:

C

Description

NEs

Comments

Procedure Policy

Refresh Now

Enable Auto-Refresh

☐

every

05:00

(mm:ss)

Rows per page:

10

Target NEs

no entries

NE Identifier	Model	Current Release	Stage	Status	Duration	End Time	Available Operations	Run
No items in list!								

Add/Remove Target NEs

Save

Close

8. While the distribution phase is running, you can perform the following tasks:

To	Then
terminate the distribution phase	select Distribute:Terminate and then click the green run arrow. When prompted with: Warning: Terminating an operation does not necessarily end all activity associated with the operation. Terminate merely sets the administrative state of the operation to failed. If there are background tasks running in support of the operation, either on the NE or in Network Integrity, they continue to completion. Click OK to confirm the operation.

9. After the distribution phase has run, you can perform the following tasks:

To	Then
restart the distribution phase if it fails,	select Distribute:Run and then click the green run arrow
force the distribution phase back to unstarted	select Distribute:ForceUnstarted and then click the green run arrow. When prompted, confirm the operation.
force the distribution phase to a successful status	select Distribute:ForceSuccess and then click the green run arrow. When prompted, confirm the operation.

To	Then
undo the distribution phase	<p>select Distribute:Undo and then click the green run arrow. When prompted, confirm the operation.</p> <p>Note: If you perform an Undo of the Distribution phase and the software load in the bank does not roll back to the previous release, the action may not be supported by the NE.</p>

Activate the software

Use this procedure after the distribution phase is successful to activate the software on the NEs in the target. If Network Integrity can not find an adapter that is compatible with the new software, the activate step fails with an error message: "Could not refingerprint and change adapter".

While the activation phase is running, you can terminate the process.



Note: If terminate is issued against an NE that is in the "pending" state, the NE reverts back to "unstarted". If terminate is issued against an NE that is in the "in progress" state, the process is terminated, but the operation may continue on the NE itself. In this case, the termination may lead to a mismatch between the state of the NE and the state that is displayed by the Software Delivery application.

After the activation phase has run, you can restart the phase, undo the phase, or force the status to indicate unstarted or successful.



Note: During the activation phase of an upgrade, the current network adapter (for example version 5.1) attempts to find a matching adapter for the new load by trying to match the version pattern with the new load (for example 8.*). If there is a match, it switches to the new load. However, this does not work in cases where the old and new software loads have the same version pattern match. For example, if upgrading from version 9.1 to 9.4, the current adapter has a version pattern of 9.* and the new adapter has a pattern of 9.4.*. In this case there is potential that the current adapter will be selected because version 9.4 matches pattern 9.*. If this is the case, after the upgrade has completed, you must use the NE Manager to change to the correct adapter.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.

The system displays the list of workflows.

The screenshot shows the 'Software Delivery' application window with the 'Workflow' tab selected. At the top right, there is a 'Refresh Now' button and an 'Enable Auto-Refresh' checkbox with a dropdown set to '05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main area displays a table titled 'Workflows · 1 item'.

Select	Workflow	Prime	Status	Number of Targeted NEs	Completed
<input type="checkbox"/>	Eastern Seaboard Workflow	Martin	Unstarted	0	0

At the bottom left, there are 'Create' and 'Delete' buttons.

- Click the Workflow for which you want to perform the activation phase.
The system displays the workflow details.
- If not already selected, click the **Targets** tab.
The system displays the list of targets defined for the workflow.

The screenshot shows the 'Workflow Details' application window. The top section contains form fields for 'Name' (Eastern Seaboard), 'Prime' (Martin), 'Upgrade To' (NewLoad), 'Vendor' (C), and 'Description'. Below this are tabs for 'Targets', 'Comments', 'NE Groups', and 'Procedure Policy', with 'Targets' selected. At the top right, there is a 'Refresh Now' button and an 'Enable Auto-Refresh' checkbox with a dropdown set to '05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main area displays a table titled 'Targets · 1 item'.

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	

At the bottom left, there are 'Create' and 'Delete' buttons. At the bottom right, there are 'Save' and 'Close' buttons.

- Select one or more targets on which to activate the software release.
- From the **Available Operations** list, select **Activate:Run**.
- For each of the selected targets, click **Run**.
- Confirm the prompt.
The software activation process begins.

9. While the activation phase is running, you can perform the following tasks:

To	Then
terminate the activation phase	select Activate:terminate and then click the green run arrow. When prompted with: Warning: Terminating an operation does not necessarily end all activity associated with the operation. Terminate merely sets the administrative state of the operation to failed. If there are background tasks running in support of the operation, either on the NE or in Network Integrity, they continue to completion. Click OK to confirm the operation.

10. After the activation phase has run, you can perform the following tasks:

To	Then
restart the activation phase if it fails	select Activate:Run and then click the green run arrow.
force the activation phase back to unstarted	select Activate:ForceUnstarted and then click the green run arrow. When prompted, confirm the operation.
force the activation phase to a successful status,	select Activate:ForceSuccess and then click the green run arrow. When prompted, confirm the operation.
undo the activation phase,	select Activate:Undo and then click the green run arrow. When prompted, confirm the operation.

Commit the software

Use this procedure after the activation phase is successful to commit the software release for each network element.

While the committing phase is running, you can terminate the process.



Note: If terminate is issued against an NE that is in the “pending” state, the NE reverts back to “unstarted”. If terminate is issued against an NE that is in the “in progress” state, the process is terminated, but the operation may continue on the NE itself. In this case, the termination may lead to a mismatch between the state of the NE and the state that is displayed by the Software Delivery application.

After the committing phase has completed, no other actions can be performed other than to delete the target. See [“Delete targets from a workflow” on page 130](#).

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.

The system displays the list of workflows.

The screenshot shows the 'Software Delivery' application window with the 'Workflow' tab selected. At the top right, there are buttons for 'Refresh Now' and 'Enable Auto-Refresh' with a dropdown set to '05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main area displays a table titled 'Workflows · 1 item'.

Select	Workflow	Prime	Status	Number of Targeted NEs	Completed
<input type="checkbox"/>	Eastern Seaboard Workflow	Martin	Unstarted	0	0

At the bottom left, there are 'Create' and 'Delete' buttons.

3. Click the Workflow for which you want to perform the committing phase.
The system displays the workflow details.
4. If not already selected, click the **Targets** tab.
The system displays the list of targets defined for the workflow.

The screenshot shows the 'Workflow Details' window for the 'Eastern Seaboard' workflow. The 'Targets' tab is selected. At the top, there are input fields for 'Name' (Eastern Seaboard), 'Prime' (Martin), 'Upgrade To' (NewLoad), 'Vendor' (C), and a 'Description' field. Below these are tabs for 'Targets', 'Comments', 'NE Groups', and 'Procedure Policy'. At the top right, there are buttons for 'Refresh Now' and 'Enable Auto-Refresh' with a dropdown set to '05:00 (mm:ss)'. Below this is a 'Rows per page' dropdown set to '10'. The main area displays a table titled 'Targets · 1 item'.

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	

At the bottom left, there are 'Create' and 'Delete' buttons. At the bottom right, there are 'Save' and 'Close' buttons.

5. Select one or more targets on which to commit the software release.
6. From the **Available Operations** list, select **Commit:Run**.
7. For each of the selected targets, click **Run**.
8. Confirm the prompt.
The software committing process begins.

9. While the committing phase is running, you can perform the following task:

To	Then
terminate the committing phase	select Commit::terminate and then click the green run arrow. When prompted with: Warning: Terminating an operation does not necessarily end all activity associated with the operation. Terminate merely sets the administrative state of the operation to failed. If there are background tasks running in support of the operation, either on the NE or in Network Integrity, they continue to completion. Click OK to confirm the operation.

10. After the committing phase has run, you cannot perform any additional tasks.

5.2.4 Monitor the software release process

Use this procedure to monitor the progress of the different phases of the software delivery process at the Workflow, Target, and Network Element level. The phases of the software delivery process are distribute, activate, and commit.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.
The system displays the list of workflows.



The Completed column indicates the number of NEs from all targets that have completed an operation.

3. To drill down into the workflow to obtain details about the targets, click the required Workflow.
The system displays the workflow details.
4. If not already selected, click the **Targets** tab.

The system displays the list of targets defined for the workflow.

The screenshot shows a 'Workflow Details' window. At the top, there are input fields for 'Name' (Eastern Seaboard), 'Prime' (Martin), 'Upgrade To' (NewLoad), 'Vendor' (C), and 'Description'. Below these are tabs for 'Targets', 'Comments', 'NE Groups', and 'Procedure Policy'. The 'Targets' tab is active, showing a 'Refresh Now' button and an 'Enable Auto-Refresh' checkbox with a dropdown set to '05:00 (mm:ss)'. Below this is a table of targets. The table has columns: Select, Target, Prime, Status, Number of NEs, Distributed, Activated, Committed, Available Operations, and Run. There is one target listed: 'Vermont' with Prime 'Martin', Status 'Unstarted', and all other counts at 0. The 'Available Operations' column shows 'Distribute:Run' and the 'Run' column has a green arrow icon. At the bottom are 'Create', 'Delete', 'Save', and 'Close' buttons.

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	

- To view details for each NE in the target, click the name of the desired target.
The system displays the Target NE details and the status for each phase. In the following example, the first NE has successfully completed all three phases of the software delivery and there are no other available options that can be performed. The second NE has failed the distribution phase. The only available option is to run

the distribution again. For each phase, the system indicates how long the phase took to complete, and when the phase was completed.

Target Details

Target Name: *

Prime:

Upgrade To: **Ciena Corestream 6.4.0**

Vendor: **Ciena**

Description:

NEs | Comments | Procedure Policy

Enable Auto-Refresh ☐ every (mm:ss)

Rows per page:

NE Identifier	Model	Current Release	Stage	Status	Duration	End Time	Available Operations	Run
CNRL13TX-0001	Corestream	6.3.0	Distribute	Unstarted	00:00:00		Distribute:Run	<input type="button" value="Run"/>
			Activate	Unstarted	00:00:00			
			Commit	Unstarted	00:00:00			

5.3 Managing software releases

The Software Delivery application manages your network element software releases by controlling the actions that occur during each phase of the network element upgrade process. This is done by creating a software release specification that can be configured to audit each network element in the Workflow and validate the hardware compatibility, or the software release can be configured to audit alarms and define which actions the system should take if an alarm condition is present.

This section contains the following procedures for managing software releases that have already been configured:

- [“Copy software releases to a managed file server” on page 112](#)
- [“List of software releases and view or modify details I” on page 112](#)
- [“Delete a software release from the database” on page 118](#)

Prerequisites

To use the Software Delivery application, your user account must be assigned to the Software Delivery Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

5.3.1 Copy software releases to a managed file server



Note: Before using any of the software delivery procedures in this section to add or modify a software release, you must copy the vendor's software release loads to the designated file server.

5.3.2 List of software releases and view or modify details I

Use this procedure to see which software releases have been loaded into the database and view or modify details about the release.

1. Launch **Software Delivery**.
2. If not already selected, click the **Software Release** tab.
The system displays the list of existing software releases.

Select	Release Name	Vendor	Version
<input type="checkbox"/>	NewLoad	C	ReleaseZZ

3. You can filter the list of software releases that are displayed by selecting the criteria (**Name**, **Vendor**, or **Version**), typing the filter term in the text field, and then clicking **Search**.
You can use wildcards as described in [“Using wildcards in search criteria”](#) on page 199.
4. Click the name of the software release being modified.

The system displays the software release details window. Each tab can be selected to modify different aspects of the software release

Software Release Details

Name:

Vendor:

Version:

Description:

File Server:

Relative Path:

Files - 4 items

Select	File Name
<input type="checkbox"/>	CONFIGFILE.CON
<input type="checkbox"/>	LOADFILEA.PGM
<input type="checkbox"/>	LOADFILEB.PGM
<input type="checkbox"/>	LOADFILEC.PGM

Load software image file names from a configuration file

- To modify basic information about the software release, make any of the following changes in the corresponding field:

Field	Description
Name	type a descriptive name to identify the software release
Vendor	select the vendor of the software release
Version	type the software version. The Software Delivery application does not validate the version of the software release located on the server. It is important that care be exercised at the time that the software release data is entered into the database otherwise any upgrade using that release fails.
Description	type a description for the software load

- If you have no more changes to make, click **Save** to return to the list of software releases.

7. To modify the software load file details, click the **Files** tab.

Software Release Details

Name:

Vendor:

Version:

Description:

Files | Hardware Compatibility | Software Compatibility | Profiles

File Server:

Relative Path:

Rows per page: 10

Select	File Name
<input type="checkbox"/>	CONFIGFILE.CON
<input type="checkbox"/>	LOADFILEA.PGM
<input type="checkbox"/>	LOADFILEB.PGM
<input type="checkbox"/>	LOADFILEC.PGM

Load software image file names from a configuration file:

8. Make any of the following changes:
- **File Server:** select the file server that contains the software image file
 - **Relative Path:** type the path to the software image file relative to the home directory for the file server user.
 - **File:** click **Browse** and navigate to the software load file on the server.
 - a. To merge the selected load with the existing loads, click **Load & Merge**.
 - b. To overwrite the existing loads with the selected load, click **Load & Overwrite**.
 - c. To validate the location of a software load file select one or more files in the list and click **Validate Location**.

The system displays the status of the validation.

- **Yes:** the file location was validated
 - **No:** the file location failed validation
 - **Untested:** the file location has not been validated yet
9. If you have no more changes to make, click **Save** to return to the list of software releases.

10. To modify the software compatibility details, click the **Software Compatibility** tab.

Software Release Details

Name: ONS_15454 R7.20

Vendor: C

Version: 7.20

Description:

Files | Hardware Compatibility | **Software Compatibility** | Profiles

Compatible Software - 2 items

Select	Previous Versions
<input type="checkbox"/>	04.60.50
<input type="checkbox"/>	7.02.00

Add Delete

Save Close

11. Make any of the following changes.
- To add an entry to the software compatibility, click **Add**, or to remove an entry, click **Delete**.
 - In the list of Compatible Software, select the acceptable Previous Versions.
- Note: If you are in a situation, such as testing, where you are not actually upgrading, but re-installing the same version of software, you must enter the value of the “Version” being installed as a “Previous Version” in the Compatible Software list. For example, if you are re-installing version 7.2, 7.2 must also appear as a Previous Version in the Compatible Software list.
12. If you have no more changes to make, click **Save** to return to the list of software releases.

13. To modify the hardware compatibility details, click the **Hardware Compatibility** tab.

Software Release Details

Name:
 Vendor:
 Version:
 Description:

Files Hardware Compatibility Software Compatibility Profiles

Rows per page: 10

Hardware Models - 1 item

Compatible	Name	Adapter Deployed For Specified Version
<input checked="" type="checkbox"/>	Corestream	No

Save Close

14. Select the hardware that the software release is compatible with.
15. If you have no more changes to make, click **Save** to return to the list of software releases.
16. To make changes to the audit profiles, click the **Profiles** tab.

Software Release Details

Name:
 Vendor:
 Version:
 Description:

Files Hardware Compatibility Software Compatibility Profiles

General Profile - 1 item

Profile	Hardware Audit	Alarm Audit
General	None	AnyAlarm

Stage Profiles - 3 items

Profile	Uses General Profile	Hardware Audit	Alarm Audit
Distribution	Yes	None	AnyAlarm
Activation	Yes	None	AnyAlarm
Committing	Yes	None	AnyAlarm

Save Close

17. Click the name of the profile to be modified and make the required changes in the profile details screen.

Software Release Details

☒ No Hardware Audit
☐ Select Hardware Audit

☐ No Alarm Audit
☒ Select Alarm Audit

Search: Name Rows per page: 10

Choose	Name
<input checked="" type="checkbox"/>	AnyAlarm
<input type="checkbox"/>	AlarmAudit
<input type="checkbox"/>	Critical

18. Determine whether you want to add alarm audits to the selected Profile:

To	Then
have specific hardware audits added to the selected Profile	select Select Hardware Audit and then go to Step 19 .
not have hardware audits in the selected Profile	select No Hardware Audit and then go to Step 20 .

19. In the “Choose” column of the list of hardware audits, select the required hardware audits to perform.

Software Release Details

☐ No Hardware Audit
☒ Select Hardware Audit

☐ No Alarm Audit
☒ Select Alarm Audit

Search: Name Rows per page: 10

Choose	Name
<input type="checkbox"/>	HWAudit
<input type="checkbox"/>	Test

20. Determine if you want to add alarm audits to the selected Profile:

To	Then
have specific alarm audits added to the selected Profile	select Select Alarm Audit and then go to Step 21 .
not have hardware audits in the General Profile	select No Alarm Audit and then go to Step 22 .

21. In the Choose column of the list of alarm audits, select the required alarm audits to perform.

Software Release Details

☒ No Hardware Audit
☐ Select Hardware Audit

☐ No Alarm Audit
☒ Select Alarm Audit

Name Rows per page: 10

Alarm Audits - 3 items

Choose	Name
<input checked="" type="checkbox"/>	AnyAlarm
<input type="checkbox"/>	AlarmAudit
<input type="checkbox"/>	Critical

22. If you have no more changes to make, click **OK** to return to the Software Release Details window.

The system updates the software release specification with your changes.

5.3.3 Delete a software release from the database

Use this procedure to delete network element software releases from the database.



Note: If a software release is being used by a workflow, you can not select or delete the software release until you remove any workflows associated with the software release.

1. Launch **Software Delivery**.
2. If not already selected, click the **Software Release** tab.

The system displays the list of software releases.



3. Select one or more software releases to be deleted.
4. Click **Delete**.
The system prompts for confirmation.
5. Click **OK** to confirm the operation.
The software release is removed from the database.

5.4 Managing software delivery workflows

A software delivery workflow associates a single software release with a group of network elements. For example, you could create a Workflow to upgrade all of a specific vendor/model or network element in your network that are installed in California. After the workflows are created, you create targets, which represent smaller units of work within the workflow. Targets identify specific NEs from within the NE Groups that are defined in a workflow. Targets identify the NEs you wish to upgrade as a single operation, or at the same time. For more information about creating targets, see [“Managing software delivery targets” on page 125](#).

This section contains the following software delivery workflow procedures:

- [“List workflows and view or modify details” on page 119](#)
- [“Delete a workflow from the database” on page 124](#)

Prerequisites

To use the Software Delivery application, your user account must be assigned to the Software Delivery Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

5.4.1 List workflows and view or modify details

Use this procedure to view all the workflows that have been created and view or modify the details of a workflow.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.

The system displays the Workflow window, which lists all the existing workflows.

Select	Workflow	Prime	Status	Number of Targeted NEs	Completed
<input type="checkbox"/>	Eastern Seaboard Workflow	Martin	Unstarted	0	0

- To refresh the screen with the latest status information, click **Refresh Now** or select **Enable Auto-Refresh** and specify a frequency.
- To view the details of a workflow, click the name in the workflow column.
The system displays the workflow details.

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	➔

- Click the workflow name that you want to view or modify.

The system displays the workflow details.

Workflow Details

Name: *

Prime:

Upgrade To: **NewLoad**

Vendor: Acme

Description:

Targets | Comments | NE Groups | Procedure Policy

Enable Auto-Refresh ☐ every (mm:ss)

Rows per page:

Targets - 2 items

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	
<input type="checkbox"/>	Maine	Martin	Unstarted	0	0	0	0	Distribute:Run	

6. If required, modify any of the following general parameters in the corresponding field:
 - **Name:** type a descriptive name for the workflow
 - **Prime:** type the name of the person who is the prime contact for this workflow
 - **Description:** type a description for the workflow
7. To modify the targets, click the **Targets** tab.

Workflow Details

Name: *

Prime:

Upgrade To: **NewLoad**

Vendor:

Description:

Targets | Comments | NE Groups | Procedure Policy

Enable Auto-Refresh ☐ every (mm:ss)

Rows per page:

Targets - 1 item

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	

8. Modify the target details as required:

To	Then
create a target	see “Create targets in a workflow” on page 98 for a detailed procedure
delete a target	select one or more targets, and then click Delete . When the system prompts for confirmation, click OK .

9. If you have no more changes to make, click **Save** to return to the list of workflows.

10. To add comments to the workflow, click the **Comments** tab.

The screenshot shows the 'Workflow Details' window with the 'Comments' tab selected. The 'Name' field is 'Eastern Seaboard', 'Prime' is 'Martin', 'Upgrade To' is 'NewLoad', 'Vendor' is 'C', and 'Description' is 'Upgrade for June'. Below the tabs, there is a 'New Comment' text area. At the bottom, there is a 'Comments' table with columns 'Time' and 'Comment', and a 'Save' button.

Workflow Details	
Name:	Eastern Seaboard
Prime:	Martin
Upgrade To:	NewLoad
Vendor:	C
Description:	Upgrade for June

Targets | **Comments** | NE Groups | Procedure Policy

New Comment:

Rows per page: 10

Comments - no entries	
Time	Comment
No items in list	

Save Close

11. To add a comment, type the desired text in the New Comment field.

12. If you have no more changes to make, click **Save** to return to the list of workflows.

13. To modify the NE Groups in a workflow, click the **NE Groups** tab.

Workflow Details

Name: Eastern Seaboard
 Prime: Martin
 Upgrade To: NewLoad
 Vendor: C
 Description: Upgrade for June

Targets **Comments** **NE Groups** **Procedure Policy**

NE Group Name Search Reset Rows per page: 10

Available NE Groups - 1 item

Select	NE Group Name
<input type="checkbox"/>	All NEs

Add

Rows per page: 10

Selected NE Groups - no entries

Select	NE Group Name
No items in list!	

Remove

Save Close

14. Modify the NE Groups as required:

To	Then
add NE Groups	select the NE Groups to assign to the workflow, and then click Add . This moves the NEs from the Available NE Groups list to the Selected NE Groups list.
delete NE Groups from the workflow	select the NE Groups to remove from the workflow, and then click Remove

15. If you have no more changes to make, click **Save** to return to the list of workflows.

16. To modify the workflow procedure policies, click the **Procedure Policy** tab.

Workflow Details

Name: Eastern Seaboard

Prime: Martin

Upgrade To: NewLoad

Vendor: C

Description: Upgrade for June

Targets

Comments

NE Groups

Procedure Policy

Procedure Policy

	Distribute	Activate	Commit
GNE Sequence Policy	Any	Any	Any
Run Audits Before (per NE)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
On Audit Error (per NE)	Stop	Stop	Stop
Concurrency Policy (per Target)	Min	Min	Min
On Operation Error (per Target)	Continue	Stop	Stop

Reset to Defaults

Save

Cancel

17. Modify the procedure policy as required:

To	Then
use the default procedure policy for each phase	select Reset to Defaults , and then go to Step 18 .
customize the procedure policy for each phase	select Specify Procedure Policy and set the required parameter for each phase of the workflow as described in table “Procedure Policy parameters for each phase” on page 93.

18. Click **Save** to return to the list of workflows.

5.4.2 Delete a workflow from the database

Use this procedure to delete a workflow from the database.



Note: You can delete a workflow as long as no targets associated with the workflow are in the process of being upgraded.

- 1. Launch **Software Delivery**.
- 2. If not already selected, click the **Workflow** tab.

The system displays the list of workflows.



3. Select one or more workflows to be deleted.
4. Click **Delete**.
The system prompts for confirmation.
5. Click **OK** to confirm the operation.
The system deletes the workflow.

5.5 Managing software delivery targets

While workflows associate one or more software releases with one or more network element groups, a target represents a smaller unit of work within the workflow. The target identifies specific NEs from within the NE Groups that are defined in a workflow. The actual software delivery is executed on a target by target basis. In order for the software release to be delivered, all of the NEs in a target must be compatible with the vendor's software release.

This section contains the following procedures for managing targets:

- [“List targets within a workflow and view or modify target details” on page 125](#)
- [“Delete targets from a workflow” on page 130](#)

Prerequisites

To use the Software Delivery application, your user account must be assigned to the Software Delivery Role and have the correct permissions and NE Groups set. Without the correct permissions, you can not access some or all of the features or NEs.

5.5.1 List targets within a workflow and view or modify target details

Use this procedure to list targets that have been defined within a workflow and view or modify target details. For each target, the system displays the following information:

- **Target:** the name assigned to the target when it was added to the workflow
- **Prime:** the person responsible for the target work
- **Status:** the current status

- **Number of NEs:** the number of NEs in the target
- **Distributed:** the number of NEs in the distribution phase of the software delivery
- **Activated:** the number of NEs in the activation phase of the software delivery
- **Committed:** the number of NEs in the committing phase of the software delivery
- **Available Operations:** a list of the phases that you can manually select and run on the target
- **Run:** a link that allows you to run the selected operation from the Available Operations column.

For each target in the list, you can obtain detailed information about the NEs in the target and details about the procedure policy.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.
The system displays the list of workflows.



3. Click the workflow that contains the targets you want to view.
The system displays the Workflow details screen.
4. If not already selected, click the **Targets** tab.

The system displays all the targets that are configured for the selected workflow.

Workflow Details

Name: *

Prime:

Upgrade To: **NewLoad**

Vendor: **C**

Description:

Targets | Comments | NE Groups | Procedure Policy

Enable Auto-Refresh ☐ every (mm:ss)

Rows per page:

Targets - 1 item

Select	Target	Prime	Status	Number of NEs	Distributed	Activated	Committed	Available Operations	Run
<input type="checkbox"/>	Vermont	Martin	Unstarted	0	0	0	0	Distribute:Run	<input type="button" value="Run"/>

5. Click the name of the Target to be viewed or modified.
The system displays the target details with the NEs tab selected.

Target Details

Target Name: *

Prime:

Upgrade To: **Ciena Corestream 6.4.0**

Vendor: **Ciena**

Description:

NEs | Comments | Procedure Policy

Enable Auto-Refresh ☐ every (mm:ss)

Rows per page:

Target NEs - 1 item

NE Identifier	Model	Current Release	Stage	Status	Duration	End Time	Available Operations	Run
CNRL13TX-0001	Corestream	6.3.0	Distribute	Unstarted	00:00:00		Distribute:Run	<input type="button" value="Run"/>
			Activate	Unstarted	00:00:00			
			Commit	Unstarted	00:00:00			

6. To view or modify the general information about a target, make the required changes in the corresponding fields:
 - a. If required, in the **Target Name** field change the name to identify the target.

- b. If required, in the **Prime** field type the name of the person responsible for the target.
 - c. If required, in the **Description** field type a description of the target.
7. To add or remove NE targets, click **Add/Remove Target NEs**.
The system displays the network element selection screen.

Add Remove NEs from Target - All NEs

Search Available NEs

Compatibility:

View:

NE Name:

Vendor:

Model:

Software Version:

NE Group Name:

Rows per page: 10

Available NEs - 1 to 10 of 24

Select	NE Identifier	Vendor	Model	Software Version	Compatible
<input type="checkbox"/>	CNRL01TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL12TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL09TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL10TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL08TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL07TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL11TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL06TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL04TX-0001	Ciena	Corestream	6.3.0	Yes
<input type="checkbox"/>	CNRL02TX-0001	Ciena	Corestream	6.3.0	Yes

Rows per page: 10

Target NEs - 1 item

Select	NE Identifier	Vendor	Model	Software Version
<input type="checkbox"/>	CNRL13TX-0001	Ciena	Corestream	6.3.0

8. Enter the desired search criteria to find a subset of NEs from which to select the targets. If you have an existing search query, you can use the **Load Search** button to load the query. For a complete description of searches, see [“Understanding searches” on page 188](#). You can also search based on the **Compatibility**: Compatible or Incompatible.

9. To add target NEs, select one or more NEs, and then click **Add**. This moves the NEs from the **Available NEs** list to the **Target NEs** list. Repeat this as many time as required to select the desired target NEs.
10. To remove target NEs, select one or more NEs to be removed and then click **Remove**.

Note: You can only remove network elements from a Target under the following conditions:

 - no operations have been performed on the network element (except audit)
 - all operations have been undone
 - the commit operation has completed
11. If you have no more changes to make, click **Save** to return to the list of targets.
12. To change the procedure policy for the target, click the **Procedure Policy** tab. The system displays the target procedure policy screen.

Target Details

Target Name: Vermont
 Prime: Martin
 Upgrade To: NewLoad
 Vendor: C
 Description:

NEs | **Comments** | **Procedure Policy**

☐ Use Default Procedure Policy
☒ Specify Procedure Policy

	Distribute	Activate	Commit
GNE Sequence Policy	Any	Any	Any
Run Audits Before (per NE)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
On Audit Error (per NE)	Stop	Stop	Stop
Concurrency Policy (per Target)	Min	Min	Min
On Operation Error (per Target)	Continue	Stop	Stop

Reset to Workflow Procedure Policy

Save Close

13. If required, modify the procedure policy for the target:

To	Then
use the procedure policy that was defined in the workflow	select Use The Workflow Procedure Policy , and then go to Step 14 .
customize the procedure policy for the target	select Specify Procedure Policy and set the required parameter for each phase of the workflow as described in table “Procedure Policy parameters for each phase” on page 93.

14. If you have no more changes to make, click **Save** to return to the list of targets.

15. To add a comment to the target, click the **Comments** tab.
The system displays the comment screen.
16. Type the required comment in the comment field.
17. Click **Save** to apply the changes and return to the list of targets.

5.5.2 Delete targets from a workflow

Use this procedure to delete a Target from a workflow.



Note: You can not delete a Target that has started the distribution phase.

1. Launch **Software Delivery**.
2. If not already selected, click the **Workflow** tab.
The system displays the list of workflows.
3. Click the workflow name from which you would like to delete a target.
4. Select one or more targets to be deleted.
5. Click **Delete**.
The system prompts for confirmation.
6. Click **OK** to confirm the operation.
The system deletes the targets from the workflow.

6 Fault Manager: Configuring NE fault collection and reporting

The **Fault Manager** application collects and reports active and historical network element faults, and reports alarms associated with Network Integrity security and application activity. To view and troubleshoot alarms for managed NEs, the NI-Director Operations Console provides a graphical view of the network. For detailed procedures, see the NI-Director Operations Console User Guide or online help.

This section contains the procedures to configure active and historical fault collection for network elements and to configure the reporting parameters:

- [“Configure fault collection for each network element” on page 131](#)
- [“Configure the automatic fault reporting parameters” on page 134](#)
- [“View archived historical events” on page 135](#)



Note: In order for Network Integrity to collect fault data, fault monitoring **must be enabled on the NE**. The procedures in this section are used only to configure collection of the data; they do not control the reporting and monitoring settings on the NEs.

6.1 Configure fault collection for each network element

The default configuration for all types of fault collection is OFF as follows:

- **Active Alarms:** default configuration is collection **OFF**
- **Historic Alarms:** default configuration is collection **OFF**
- **Historic TCA:** default configuration is collection **OFF**
- **Historic Other Events:** default configuration is collection **OFF**

Use this procedure to change the default settings and enable fault monitoring collection as required for the network elements in your network. If you have previously enabled fault monitoring collection, you can use this procedure to disable fault monitoring for the NEs in your network.



Note: When alarm monitoring is turned on or off for one or more NEs, it affects the alarm display on the NI-Director Operations Console. When reporting is off/disabled, the letters “NR” appear on the network element icon in the NOC topology view, which indicates “Not Reported”.

If the Active Alarm monitoring status is changed from off/disabled to on/enabled, the system performs an alarm reconciliation and automatically updates the alarms displayed in the NI-Director Operations Console.



Note: For SNMP NEs, you must configure each NE with SNMP trap destinations, which are the IP Address and port for each agent. Consult the NE vendor documentation for the procedure to do this.



Note: To compensate for the UDP protocol used for SNMP, which lacks an acknowledgment and retransmission mechanism for its traps, Network Integrity performs an audit every 6 hours (default) to check for active alarms on SNMP NEs that are connected and that have alarms enabled. If required, the default audit value can be disabled, or it can be adjusted between 6 and 1 hour. Contact customer support for assistance.

1. Launch **Fault Manager**.
2. If not already selected, click the **Network Element** tab.
3. Click the **Configuration** tab.
The system displays the network element search screen. This is where you search for the NEs on which to configure fault collection.
4. Enter the desired search criteria to find the NEs to be configured. If you have an existing search query, you can use the **Load Search** button to load the query.
5. When you have entered the required search criteria, click **Search** to display the NEs to be configured.
The system displays the NEs that match the criteria and shows the current monitoring status for each NE, for Active Alarms, Historic Alarms, Historic TCA,

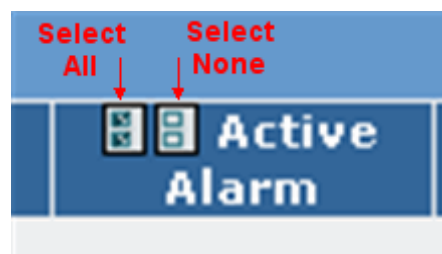
and Historic Other Events. If a sector box is grayed out, it means that the fault collection is not supported by the adapter, which may be from a previous release.

The screenshot shows the 'Network Element' configuration page with tabs for 'Application' and 'Security'. Under 'Configuration', there is a 'Reports' tab. A search bar is present with fields for 'NE Name' and 'Vendor/Model/Version', both set to 'Equals'. Below the search bar are buttons for 'Load Search', 'Save Search', and 'Search'. A 'Case Sensitive' checkbox is also visible. The search results show 'Matching NEs - 6 items'. The table below has columns for 'NE Details' (Name, Vendor, Model) and 'Monitoring Status' (Active Alarm, Historic Alarm, Historic TCA, Historic Other Event). A red circle highlights the 'Monitoring Status' columns.

NE Details			Monitoring Status			
Name	Vendor	Model	Active Alarm	Historic Alarm	Historic TCA	Historic Other Event
CNRL01TX-0001	Ciena	Corestream	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNRL02TX-0001	Ciena	Corestream	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CNRL03TX-0001	Ciena	Corestream	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OMMSP0001	Nortel	OPTera Metro 3500 MSP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OMMSP0002	Nortel	OPTera Metro 3500 MSP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OMMSP0003	Nortel	OPTera Metro 3500 MSP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- For each NE, select or deselect the required configuration for **Active Alarm**, **Historic Alarm**, **Historic TCA**, and **Historic Other Event**. When an item is selected, fault collection is On/enabled. When it is deselected, it is Off/disabled.

Note: If you want to select or deselect all items, use the selection icons at the top of the column to **Select All** or **Select None**. Note that "Select All" only selects all of the NEs on the currently displayed page. If there are multiple pages of NEs, page through the NEs and repeat the selection.



- When the desired fault collection selections have been made, click **Save**. The system starts or stops collecting fault data as determined by the selections.

6.2 Configure the automatic fault reporting parameters

Use this procedure to configure the file server, directory and start time for the automatic daily fault reporting. The generated report file is a Tab Separated Value (TSV) ASCII file in a compressed ZIP format that is sent to a managed file server.

Reporting produces one file for each network element containing all faults that occurred for the day prior to the configured reporting time. Each report contains, the following information: Type (one of Alarm, TCA, Other), System Time, NE Time, NE ID, Source ID (SID), Vendor, Model, and NE Message. If a report fails, use the Log Manager to view the System Logs for details of the failure.

The report configuration screen contains the following fields:

- **Frequency:** Daily (fixed value) - If you want to change the reporting frequency, contact your customer service representative.
- **File Server Name:** the managed file server where the reports are sent
- **File Server Directory:** the directory on the server where reports are stored. Note: If a managed file server is to be shared between multiple Network Integrity systems, be sure to define different directories for each system or else “View Event Reports” may contain reports for both systems.
- **Start Time:** the daily starting time for the report generation

The data cleanup policy is fixed at the following default values and runs daily at midnight GMT:

- Historical alarm data is deleted every 30 days
- Historical TCA data is deleted every 2 days
- Historical other events data is deleted every 2 days

If a cleanup fails because of a server failure or any other reason, Network Integrity attempts the cleanup at the next midnight interval.



Note: If you want to change the data cleanup policy values, contact your customer service representative.

1. Launch **Fault Manager**.
2. If not already selected, click the **Network Elements** tab.
3. Click the **Reports** tab.

The system displays the Automatic File Reporting Setup screen.

Fault Manager

Network Element Application Security

Configuration Reports

Automatic File Reporting Setup

Data cleanup policy

Historical Alarm Data 30 days
TCA Data 2 days
Others Data 2 days

Report monitored data

Frequency Daily
File Server Name Report *
File Server Directory faults/daily
Start Time 07 00 AM GMT/UTC

Save View Event Reports

4. From the **File Server Name** list, select the file server where the reports are sent.
5. In the **File Server Directory** field type the path to where the reports are to be stored on the server, such as **faults/daily**. Do not begin the path with a slash /.
6. From the **Start Time** lists, specify the time and time zone when the daily reports are to be generated.
7. When the parameters have been set, click **Save**.

6.3 View archived historical events

Use this procedure to view historical event reports that have been archived. These reports are Tab Separated Value (TSV) files.

1. Launch the **Fault Manager**.
2. If not already selected, click the **Network Element** tab followed by the **Reports** tab.
3. Click the **View Event Reports** button.
The system displays the Event Reports search screen.
4. From the **Year**, **Month** and **Day** menus, select the desired range for the reports you want to view.
5. Click **Search** to display the matching reports.
6. To view details about an archived report, click the **File Name**.

The screen that is displayed depends on your operating system. Typically, you will be prompted to either Open or Save the file. If your system is configured with a ZIP file association to launch a ZIP application, such as WinZIP, the corresponding ZIP application will be launched automatically.

7. Perform the desired action to Open or Save the file on your PC.

7 Performance Monitoring: Configuring and managing performance monitoring

For NEs and adapters that support performance monitoring, the NI-Director Performance Monitoring (PM) application allows you to:

- configure NEs or NE Groups with the PM Groups to be collected
- configure the PM data export parameters and data cleanup policy
- view the data in the CSV files for each collected bin
- modify the PM group collection on individual NEs, or modify the PM group collection for multiple NEs or NE Groups



Note: When enabled on the NI-Director Operations Console, the Performance Monitoring (PM) Viewer plugin provides a snapshot of the most current PM counts and the last completed bin counts for the interfaces on a network element (NE). PM data counts are retrieved directly from an NE and presented in the PM Viewer. For details, see the NI-Director Operations Console online help or user guide.

This section is divided into the following topics:

[“About Performance Monitoring” on page 138](#)

This section provides a general description of performance monitoring.

- [“Adapter support for PM data collection” on page 138](#)
- [“About PM collection configuration” on page 139](#)
- [“About PM export collection and configuration” on page 139](#)
- [“About PM jobs” on page 140](#)
- [“About PM data removal configuration” on page 141](#)
- [“PM report viewing and format” on page 141](#)
- [“Performance Monitoring search attributes” on page 142](#)

[“Configuring performance monitoring collection” on page 142](#)

This section provides all the procedures to view and modify performance monitoring data.

- [“Configure the PM groups to be collected for NEs or NE Groups” on page 142](#)
- [“Configure a data cleanup policy and a data export server” on page 146](#)
- [“Modify the PM Groups that are collected for an individual NE” on page 147](#)
- [“Modify the PM groups to be collected for multiple NEs or NE Groups” on page 150](#)

[“View or modify NE performance monitoring details” on page 153](#)

[“Managing performance monitoring jobs” on page 159](#)

This section provides all the procedures to manage PM jobs:

- [“View PM jobs and job details” on page 159](#)
- [“Delete a job from the database” on page 160](#)
- [“Re-run a failed “PM Collection Configuration” job” on page 161](#)

Prerequisites

To configure Performance Monitoring, your user account must be assigned to the Performance Monitoring Role and have the correct permissions set. Without the correct permissions, you can not access some or all of the features. If you do not see a tab or menu item, your user account is not authorized.



Note: If an application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they know what to expect when managing network elements from the Network Integrity client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

7.1 About Performance Monitoring

This section has the following information about the Performance Monitoring application, which is used to collect PM Groups from NEs that support performance monitoring and that have an adapter that supports PMs:

- [“Adapter support for PM data collection” on page 138](#)
- [“About PM collection configuration” on page 139](#)
- [“About PM export collection and configuration” on page 139](#)
- [“About PM jobs” on page 140](#)
- [“About PM data removal configuration” on page 141](#)
- [“PM report viewing and format” on page 141](#)

7.1.1 Adapter support for PM data collection

The Performance Monitoring (PM) application supports the collection of statistics as described in Telcordia GR0253, and only if the NE and its adapter support the collection of the data. The PM application also supports the collection of proprietary, non-standard counts, such as power levels, if supported by the NE and its adapter.

Any PM groups that are supported by an adapter are automatically loaded into the database when an adapter is installed, but the administrator must use the PM application to configure which PM Groups are collected for that model of NE. To configure the PM groups to be collected, see [“Configure the PM groups to be collected for NEs or NE Groups” on page 142.](#)

7.1.2 About PM collection configuration

In order to collect PM data, you must configure the PM groups that you want collected for each model of NE. The PM groups that can be configured for collection are determined by the NE and its installed adapter.



Note: By default, no PM groups are configured for collection for any given model of NE. You must use the configuration wizard to configure the PM groups to be collected for NEs or NE groups.

The supported PM groups are obtained from the installed adapters and are presented in the wizard for selection. The configuration wizard steps you through the configuration of PM Groups for each model of NE, but you can also configure customized PM Group collection for individual NEs. For details, see [“Configure the PM groups to be collected for NEs or NE Groups” on page 142](#) and [“Modify the PM Groups that are collected for an individual NE” on page 147.](#)



Note: If you configure PM collection for a group of NEs, and then after configuration is complete an NE is added to the group, it does not automatically get configured for PM collection. You must configure collection for the newly added NE. See [“Modify the PM Groups that are collected for an individual NE” on page 147.](#)

7.1.3 About PM export collection and configuration

Before you can export PM data files, follow the procedure in the NI-Framework Configuration Guide to [“Configure file servers for your products”](#) and add a local server for NI-Director.

The export process begins as soon as [“Configure a data cleanup policy and a data export server” on page 146.](#)

Network Integrity obtains the PM bin counts from the NE based on the maximum storage interval defined in the NE adapter. For example, if an NE can store a maximum of 32, 15-minute bins (which is eight hours of bin storage), Network Integrity obtains the PM data some time within the eight-hour period. As soon as Network Integrity obtains the PM bin counts, they are written to the database, placed in compressed CSV files, and exported immediately to the configured file server and directory.

Network Integrity also runs an hourly background task that checks for PM data that did not get exported. The logs reflect the overall status of export activity on an hourly basis. If the FTP server is unavailable after 4 hourly attempts, an Application alarm is raised to indicate the problem. As soon as FTP connectivity is restored, the transfer of PM data resumes and the Application alarm is cleared.



Note: Changing the PM collection for an NE reschedules all the PM groups for that NE.

The Network Integrity Northbound Interface can be used to make PM data available to third-party systems for analysis.

7.1.4 About PM jobs

Performance monitoring actions are tracked in jobs which indicate the status of the following types of PM job types:

- **PM Data Export:** the status of the hourly exports. Note: When an hourly PM export job runs and there is no data to be exported, the job is automatically deleted after it has finished. Successful exports are not listed in the jobs.
- **PM Data Removal:** the status of PM data removal jobs. Successful removals are not listed in the jobs.
- **PM Collection Configuration:** the status of PM configuration on one or more NEs. In order for the status of a “PM Collection Configuration” to be **Success**, all NEs in the job must pass the configuration task.

The table [PM job details](#) explains the information on the PM Job Details screen.

Table 7–1: PM job details

Parameter	Description
Job ID	the ID that the system assigned to the job when it was run.
Job Type	the type of job: PM Data Export, PM Collection Configuration, or PM Data Removal
Job Name	the name of the job: “PM Collection Configuration”, “PM Data Export” or “PM Data Removal”.
In Progress	the number of NEs in the job that are currently having the task performed. If the job type is “PM Data Export” or “PM Data Removal”, the number for “In Progress”, “Passed”, and “Failed” appears as N/A.
Passed	the number of NEs in the job that have passed the task.
Failed	the number of NEs in the job that have failed the task.
Status	the overall status of the job. If one NE fails the task, the status is “Failed”. The status is a clickable link to display the Job Details. From the job details, the status link can be clicked to view log details.

For PM Collection Configuration jobs, the details show the name of the user who originated the job (Originator).

For job details, see [“Managing performance monitoring jobs” on page 159](#).

7.1.5 About PM data removal configuration

Network Integrity allows administrators to configure the frequency for removing old PM data. PM data cleanup executes every day at the time specified in the “Start Time” field. When executed, the PM data cleanup removes all PM data that is older than the number of days entered in the “Remove all counts older than” field (which defaults to 7).

7.1.6 PM report viewing and format

The PM data files can be viewed by performing a search for the desired NE or count, and simply clicking on the required bin data file. The system downloads the file and prompts you to open or save the .CSV file.

The format of the PM report File Name is “**NE Name**”_”**PM Group Name**”_”**Unique PM Group Identifier**”_”**Latest End Time in report**”_”**Bin size**”.csv.zip.

If you open a .CSV PM data file in a spread sheet, the data is displayed in columns.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Inventory ID	StartTime	EndTime	BinSize	SES	SES_Stat	SEFS	SEFS_Sta	ES	ES_Status	CV	CV_Status
2	Anda4000::TTP::SECT::10066	6/17/2009 17:45	6/17/2009 18:00	15						0 invalid		
3	Anda4000::TTP::SECT::10066	6/17/2009 17:45	6/17/2009 18:00	15				0 invalid				
4	Anda4000::TTP::SECT::13421	6/17/2009 17:45	6/17/2009 18:00	15		0 invalid						
5	Anda4000::TTP::SECT::13421	6/17/2009 17:45	6/17/2009 18:00	15							0 invalid	
6	Anda4000::TTP::SECT::10066	6/17/2009 18:00	6/17/2009 18:15	15				0 invalid				
7	Anda4000::TTP::SECT::10066	6/17/2009 18:00	6/17/2009 18:15	15				0 invalid				
8	Anda4000::TTP::SECT::13421	6/17/2009 18:00	6/17/2009 18:15	15							0 invalid	
9	Anda4000::TTP::SECT::13421	6/17/2009 18:00	6/17/2009 18:15	15						0 invalid		
10	Anda4000::TTP::SECT::10066	6/17/2009 18:15	6/17/2009 18:30	15		0 invalid						
11	Anda4000::TTP::SECT::10066	6/17/2009 18:15	6/17/2009 18:30	15				0 invalid				
12	Anda4000::TTP::SECT::13421	6/17/2009 18:15	6/17/2009 18:30	15							0 invalid	
13	Anda4000::TTP::SECT::13421	6/17/2009 18:15	6/17/2009 18:30	15						0 invalid		
14	Anda4000::TTP::SECT::10066	6/17/2009 18:30	6/17/2009 18:45	15				0 invalid				

The first four columns (**Inventory ID**, **StartTime**, **EndTime**, **BinSize**) appear in every PM report file, but the remaining columns are specific to the PM Group.

The **Inventory ID** is a Network Integrity identifier that is used to associate PM reports with Inventory reports, in the form of NE-SH-CP-PT-IF (Network Element- Circuit Pack- Port-Interface), such as NE-872.SH-1.SL-11.CP-1.PT-1.DS3-1.

The **StartTime** and **EndTime** for a bin is in the form of mm/dd/yyyy hh:mm. If the **Start Time** or **End Time** data appears as “#####”, expand the width of the column to display the data in the correct format.

The **BinSize** indicates the number of minutes of data in the bin, such as 15 or 1440 (for 24 hours).

The PM counts are in pairs with the “CountName” and “CountName_Status”, such as “UAS_R” and “UAS_R_Status”. The status indicates if the count is valid, invalid or partial.

To view PM reports, see [“View or modify NE performance monitoring details” on page 153](#).

7.1.7 Performance Monitoring search attributes

The [Performance Monitoring search attributes](#) allow you to search for all attributes associated with Performance Monitoring.

Table 7–2: Performance Monitoring search attributes

Attribute	Searches for
PM Group	The specified PM group: Any, Ethernet, OCH, OTS, SONET Line, SONET Path, SONET Section, T1andDS1, T3andDS3, or Unknown.
Collection Status	Performance monitoring data based on the status of the collection: Any: search for any data (enabled, disabled, or enabled and not collected) Enabled: search only for enabled PM data Enabled and Not Collected: search for PM data that is enabled for collection, but has not been collected Disabled: search for PM data that is currently disabled
Last Collected Time Start	The start of a collection interval that corresponds to a specific date and time. To search back to the first PM collection, select Time Zero.
Last Collected Time End	The end of a collection interval that corresponds to a specific date and time. To search up to the most recent PM collection, select No End Time.

7.2 Configuring performance monitoring collection

This section contains the following procedures to configure and modify performance monitoring:

- “Configure the PM groups to be collected for NEs or NE Groups” on page 142
- “Configure a data cleanup policy and a data export server” on page 146
- “Modify the PM Groups that are collected for an individual NE” on page 147
- “Modify the PM groups to be collected for multiple NEs or NE Groups” on page 150

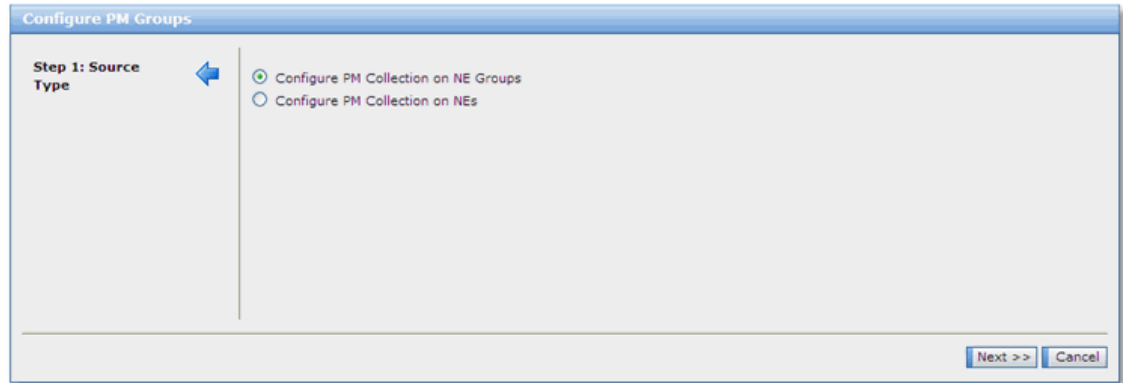
7.2.1 Configure the PM groups to be collected for NEs or NE Groups

Use this procedure to launch the “Configure PM Groups” wizard and configure the PM Groups and bin sizes to be collected for supported NEs or NE Groups.



Note: The PM groups and bins that can be collected are determined by the capabilities of the NE and by the installed NE adapter. Any performance monitoring groups that are supported by an adapter are automatically loaded when the adapter gets installed, but must be configured for the desired NEs or NE Groups using this procedure.

1. Launch **Performance Monitoring**.
2. If not already selected, click the **NE Status** tab.
3. Click **Configure Collection on NEs/NE Groups**.
The System displays step 1 of the Configure PM Groups wizard.



4. Select either NEs or NE Groups to configure:

To configure PM Groups	Then select
by specifying individual NEs,	Configure PM Collection on NEs
by specifying NE Groups,	Configure PM Collection on NE Groups

The system displays Step 2 of the wizard, which is where you select NEs or NE Groups.

5. From the list of **Available NEs** or **NE Groups**, select one or more NEs or NE Groups to configure for PM Group collection. For NE Groups, you can Search for the desired groups.
6. Click **Add** to move the NEs or NE Groups from the **Available List** to the **Selected List**.

Note: You can select NEs or NE Groups that support different PM Groups because the wizard displays only the PM groups supported by any given model of NE. For example, you can select a mix of vendor NEs and the wizard provides separate steps to select the PM groups for each NE model.

7. When the desired NEs or NE Groups are selected for configuration, click **Next**.
The system displays a list of available PM Groups that can be configured for the first model of NE. The NE model is displayed beside the "Step". As shown in this example, the PM Groups that are displayed are specifically for the "F FLM600" 15.0 NEs. If multiple NE models have been selected, additional PM Group steps appear

as you click Next. When PM Groups have been configured for all NE models, the Next button is replaced by Go.

Step 1: Source Type
Step 2: Select NEs
Step 3: Select PM Groups - F FLM600 15.0

Available PM Groups - 12 items

Select	PM Group	Bin Size
<input checked="" type="checkbox"/>	T3Line	15 min
<input checked="" type="checkbox"/>	T3Line	1 day
<input checked="" type="checkbox"/>	SONETPath	15 min
<input checked="" type="checkbox"/>	SONETPath	1 day
<input checked="" type="checkbox"/>	SONETSection	15 min
<input checked="" type="checkbox"/>	SONETSection	1 day
<input type="checkbox"/>	SONETLine	15 min
<input type="checkbox"/>	SONETLine	1 day
<input type="checkbox"/>	SONETPhysical	15 min
<input type="checkbox"/>	SONETPhysical	1 day
<input type="checkbox"/>	T3Path	15 min
<input type="checkbox"/>	T3Path	1 day

Add

Collected PM Groups - no entries

Select	PM Group	Bin Size
No items in list!		

Remove

<< Back Go Cancel

8. From the list of **Available PM Groups**, select the PM groups that you want to collect.
9. Click **Add** to move the select PM groups to the **Collected PM Groups** list.
10. To view the details of a PM group, click the name of the group in the PM Group column.

The system displays the PM groups details.

PM Group Details - T3Line

Description : T3 Line

PM Count Definitions - 3 items

Name	Description
SES	Line Severely Errored Seconds
ES	Line Errored Seconds
CV	Line Code Violations

OK

11. To close the details, click **OK**.

12. When you have finished selecting the desired PM Groups for collection, the wizard allows you to click **Go** or **Next** depending on the NEs or NE groups that were previously selected:

If you previously selected

Then

a variety of NE models, or you selected NE Groups that contained a variety of NE models

click the **Next** button and repeat from [Step 8](#). until all NE models have been configured and the Go button appears at the bottom right of the wizard. Then go to [Step 13](#).

one model of NE, or an NE Group that contained only one NE model,

go to [Step 13](#).

13. When the desired PM Groups have been selected for each NE model, click **Go**. The system creates and runs a job, which shows the status of the PM Group collection configuration for each model of NE.

Job Details

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Job Summary

Job ID 6765516
 Job Name PM Collection Configuration
 Originator Bill
 Total NEs 5
 Job Status InProgress
 Success 0
 Pending 0
 In Progress 0
 Failed 0

NE Name	Vendor	Model	SW Version	Status
CORESTREAM-30113-1003	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1004	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1001	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1002	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1000	Ciena	Corestream	7.1.1t3	Unstarted

Close Re-run Job Stop Job

14. When the Status is successful, the system begins collecting the configured PM Groups.

The screenshot shows the 'Job Details' window. At the top, there's a 'Job Summary' section with the following information:

- Job ID: 6765516
- Job Name: PM Collection Configuration
- Originator: Bill
- Total NEs: 5
- Job Status: Success
- Success: 5
- Pending: 0
- In Progress: 0
- Failed: 0

Below the summary is a table titled 'NE List - 5 items'. The table has five columns: NE Name, Vendor, Model, SW Version, and Status. The Status column is circled in red. All five entries show a 'Success' status.

NE Name	Vendor	Model	SW Version	Status
CORESTREAM-30113-1003	Ciena	Corestream	7.1.1t3	Success
CORESTREAM-30113-1004	Ciena	Corestream	7.1.1t3	Success
CORESTREAM-30113-1001	Ciena	Corestream	7.1.1t3	Success
CORESTREAM-30113-1002	Ciena	Corestream	7.1.1t3	Success
CORESTREAM-30113-1000	Ciena	Corestream	7.1.1t3	Success

At the bottom of the window, there are three buttons: 'Close', 'Re-run Job', and 'Stop Job'.

The Re-run Job button appears only when the job status is Stopped or Failed, and the Stop button appears only when job status is InProgress or Pending.

15. To view the logs, click the status.
16. To return to the Collection Configuration screen, click **Close**.
17. To view collected PM group counts, see [“View or modify NE performance monitoring details” on page 153](#).

7.2.2 Configure a data cleanup policy and a data export server

Use this procedure to configure the following:

- **Data Cleanup policy:** configure the age of PM reports to be deleted and when to perform the deletion.
- **Data Export:** configure the managed file server and directory where PM data is to be exported.

Prerequisite

Follow the procedure in the NI-Framework Configuration Guide to “Configure file servers for your products” and add a local server for NI-Director.

1. Launch **Performance Monitoring**.
2. If not already selected, click the **Export Configuration** tab.

The system displays the Automatic Clean and Export Setup screen.

To configure the data cleanup policy

3. In the **Remove all counts older than** field, specify the age of the PM report files to be deleted. For example, if you specify 7 days, PM data count files more than 7 days old are deleted at the specified time.
4. From the **Start Time** lists, specify the time and time zone at which the cleanup occurs.

When the specified start time arrives, the system performs the cleanup action.

To configure a data export server

5. From the **File Server** list, select the managed file server to be used for exporting PM data.
6. In the file server **File Server Directory** field, type the path to where the PM data is to be stored on the server, such as **pm/reports**. Do not begin the path with a slash /.
7. When the desired configuration is complete, click **Save**.

7.2.3 Modify the PM Groups that are collected for an individual NE

Use this procedure to modify or remove the PM Groups that are collected for an individual NE. You can select an NE and add or remove the collected PM Groups without affecting the collection on other NEs. Changing the PM collection for an NE reschedules all the PM groups for that NE.

(If you want to modify the PM collection for multiple NEs or NE Groups at the same time, use the procedure [“Modify the PM groups to be collected for multiple NEs or NE Groups”](#) on page 150.)



Note: The PM groups and bins that can be collected are determined by the capabilities of the NE and by the installed NE adapter.

1. Launch **Performance Monitoring**.
2. If not already selected, click the **NE Status** tab.
The system displays the search screen.
3. Perform a search to find the NE whose PM Groups are to be modified.
4. In the search results, click the **Edit** icon beside the name of the desired NE.
The system displays the PM Group Collection screen. The following example shows all PM Groups being collected.

PM Group Collection - FLM600-20000-2

Available PM Groups

Available PM Groups - no entries

Select	PM Group	Bin Size
No items in list!		

Add

Collected PM Groups

Collected PM Groups - 12 items

Select	PM Group	Bin Size
<input type="checkbox"/>	SONETPhysical	1 day
<input type="checkbox"/>	SONETSection	15 min
<input type="checkbox"/>	T3Path	15 min
<input type="checkbox"/>	SONETLine	15 min
<input type="checkbox"/>	T3Path	1 day
<input type="checkbox"/>	T3Line	15 min
<input type="checkbox"/>	SONETSection	1 day
<input type="checkbox"/>	SONETPath	1 day
<input type="checkbox"/>	SONETPath	15 min
<input type="checkbox"/>	T3Line	1 day
<input type="checkbox"/>	SONETPhysical	15 min
<input type="checkbox"/>	SONETLine	1 day

Remove

Save Close

5. To remove PM Groups, select one or more groups from the **Selected PM Groups** list and then click **Remove**.
The system moves the selected PM Groups to the **Available PM Groups** list.
6. To add PM Groups for collection, select one or more groups from the **Available PM Groups** list and then click **Add**.
The system moves the selected PM Groups to the **Selected PM Groups** list.
7. To view the details of a PM group, click the name of the group in the PM Group column.

The system displays the PM groups details.

PM Group Details - T3Line

Description : T3 Line

PM Count Definitions - 3 items

Name	Description
SES	Line Severely Errored Seconds
ES	Line Errored Seconds
CV	Line Code Violations

OK

8. To close the details, click **OK**.
9. When the desired PM Groups have been added or removed, click **Save**.
The system creates and runs a job, which shows the status of the PM Group collection configuration for the NE.

Job Details

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Job Summary

Job ID 6765892
 Job Name PM Collection Configuration
 Originator Bill
 Total NEs 1
 Job Status InProgress
 Success 0
 Pending 0
 In Progress 0
 Failed 0

NE List - 1 item

NE Name	Vendor	Model	SW Version	Status
CORESTREAM-30113-1004	Ciena	Corestream	7.1.1t3	In Progress

Close Re-run Job Stop Job

To stop the currently running job, you can click **Stop Job**. If the job fails, it can be re-run by clicking **Re-run Job**.

10. When the Status is successful, the system begins collecting the PMs for the selected Groups. Click the status to view the logs.
The system displays the details of the failure. To view the log, click the **Log ID**.

Job Details Logs - CORESTREAM-30113-1004

Rows per page: 10

Job Logs - 1 item

Log ID	Log Time	Details	Status
SYSLOG-6765902	2007.04.25 02:39:39 PM GMT	Changed PM collection on CORESTREAM-30113-1004; Job: TASK-06765892	Success

Close

11. To return to the Collection Configuration screen, click **Close**.
12. To view collected PM group counts, see [“View or modify NE performance monitoring details” on page 153](#).

7.2.4 Modify the PM groups to be collected for multiple NEs or NE Groups

Use this procedure to modify or remove the PM Groups and bin sizes to be collected for multiple NEs or NE Groups. Using the Configure PM Groups wizard, you can select multiple NEs or NE Groups and add or remove the collected PM Groups.

(If you want to modify the PM collection for an individual NE, use the procedure [“Modify the PM Groups that are collected for an individual NE” on page 147](#).)



Note: The PM groups and bins that can be collected are determined by the capabilities of the NE and by the installed NE adapter. Any performance monitoring groups that are supported by an adapter are automatically loaded when the adapter gets installed, but must be configured for the desired NEs or NE Groups using this procedure.

1. Launch **Performance Monitoring**.
2. If not already selected, click the **NE Status** tab.
3. Click **Configure Collection on NEs/NE Group**.
The System displays step 1 of the Configure PM Groups wizard.



4. Select either NEs or NE Groups to configure:

To configure PM Groups	Then select
by specifying individual NEs,	Configure PM Collection on NEs
by specifying NE Groups,	Configure PM Collection on NE Groups

5. From the list of **Available NEs** or **NE Groups**, select one or more NEs or NE Groups on which to modify PM Group collection.

6. Click **Add** to move the NEs or NE Groups from the **Available List** to the **Selected List**.

Note: You can select NEs or NE Groups that support different PM Groups because the wizard displays only the steps for the PM groups supported by any given model of NE. For example, you can select a mix of vendor NEs and the wizard provides separate steps to select the PM groups for each NE model.

7. When the desired NEs or NE Groups are selected for modification, click **Next**.
The system displays a list of available PM Groups that can be configured for the first model of NE. The NE model is displayed beside the “Step”. If multiple NE models have been selected, additional steps PM Group steps appear as you click Next.

Step 1: Source Type
Step 2: Select NEs
Step 3: Select PM Groups - F FLM600 15.0

Available PM Groups — 12 items

Select	PM Group	Bin Size
<input checked="" type="checkbox"/>	T3Line	15 min
<input checked="" type="checkbox"/>	T3Line	1 day
<input checked="" type="checkbox"/>	SONETPath	15 min
<input checked="" type="checkbox"/>	SONETPath	1 day
<input checked="" type="checkbox"/>	SONETSection	15 min
<input checked="" type="checkbox"/>	SONETSection	1 day
<input type="checkbox"/>	SONETLine	15 min
<input type="checkbox"/>	SONETLine	1 day
<input type="checkbox"/>	SONETPhysical	15 min
<input type="checkbox"/>	SONETPhysical	1 day
<input type="checkbox"/>	T3Path	15 min
<input type="checkbox"/>	T3Path	1 day

Add

Collected PM Groups — no entries

Select	PM Group	Bin Size
No items in list		

Remove

<< Back Go Cancel

8. Make the desired PM group selections as follows:
 - a. If you want to remove all PM Groups from being collected, leave the **Collected PM Groups** list empty and go to [Step 10](#).
 - b. If you want to modify the groups that are collected, move the desired groups from the **Available PM Groups** list to the **Collected PM Groups** list. To view the details of a PM group, click the name of the group in the PM Group column.

9. When you have finished modifying the PM Groups for collection, the wizard allows you to click **Go** or **Next** depending on the NEs or NE groups that were previously selected:

If you previously selected**Then**

a variety of NE models, or you selected NE Groups that contained a variety of NE models

click the **Next** button and repeat from [Step 8](#). until all NE models have been modified and the Go button appears at the bottom right of the wizard. Then go to [Step 10](#).

one model of NE, or an NE Group that contained only one NE model,

go to [Step 13](#).

10. When the desired PM Groups have been selected for each NE model, click **Go**.
The system creates and runs a job, which shows the status of the PM Group collection modification for each NE model.

The screenshot shows a 'Job Details' window with a 'Job Summary' section and a table of NEs.

Job Summary:

- Job ID: 6765516
- Job Name: PM Collection Configuration
- Originator: Bill
- Total NEs: 5
- Job Status: InProgress
- Success: 0
- Pending: 0
- In Progress: 0
- Failed: 0

NE List - 5 items:

NE Name	Vendor	Model	SW Version	Status
CORESTREAM-30113-1003	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1004	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1001	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1002	Ciena	Corestream	7.1.1t3	Unstarted
CORESTREAM-30113-1000	Ciena	Corestream	7.1.1t3	Unstarted

Buttons at the bottom: Close, Re-run Job, Stop Job.

11. When the Status is successful, the system begins collecting the selected PM Groups, or stop collecting any groups that were removed from the configuration.
12. When the job has finished, click the status to view the logs.
13. To return to the Collection Configuration screen, click **Close**.
14. To view collected PM group counts, see [“View or modify NE performance monitoring details” on page 153](#).

7.3 View or modify NE performance monitoring details

Use this procedure from the **NE Status** tab of the Performance Monitoring application, to search for specific NEs, NE Groups, or PM criteria, and drill down to view or modify the following details:

- **NE Name:** the name of the NE that matches the search criteria.
 - You can click on the NE name in this column to drill down and display the matching files of compressed PM data.
 - You can click on a PM data file name to open or save the file. The data for each PM Group bin is in a compressed CSV file that can be saved and imported to a spread sheet application, such as Excel or imported into various third-party applications, such as HP OpenView.
- **Enabled PM Groups:** the number of PM groups that are enabled for collection on the corresponding NE.
 - You can click on the number in this column to drill down to display which PM groups are enabled for collection, the bin size, and the next collection time.
 - You can click the PM group name to drill down to display the PM count definitions for the group.
- **Supported PM Groups:** the number of PM groups that are available for collection on the corresponding NE.
 - You can click on the number in this column to drill down to display the names of the PM groups that are supported for collection.
 - You can click the PM group name to drill down to display the PM count definitions for the group.
- **edit icon:** You can click the edit icon to display the Available PM Groups that can be enabled, and the Enabled PM Groups that can be removed from collection for the corresponding NE.



Note: When a PM count is invalid or contains only partial information, the number is displayed with a '?' behind it to indicate this condition.



Note: Performance monitoring (PM) is also available through a NI-Director Operations Console plug-in that provides a browser for viewing current PM counts and historical bins on an NE. For details, see the NI-Director Operations Console online help or user guide.

Prerequisites

To view PM data, your user account must be assigned to the Performance Monitoring Role and have the permission set to Browse PM Counts. Without the correct permission, you can not access PM counts. If you do not see a tab or menu item, your user account is not authorized.

1. Launch **Performance Monitoring**.
2. If not already selected, click the **NE Status** tab.

The system displays the search criteria screen.

Search for the desired NEs using any combination of search criteria. In addition to standard NE search criteria (see [“Understanding searches” on page 188](#)) you can search for any combination of the performance monitoring criteria.

3.

The system displays the list of NEs that match the search criteria. For each NE in the search results, the system displays the name of the NE, the number of enabled PM groups, the number of PM groups that are supported, the time of the last collection, and an edit icon that can be clicked to modify the collection for the corresponding NE.

Search Results

Rows per page: 10

NE Name	Enabled PM Groups	Supported PM Groups	Last Collected Time	Edit
OM3500-3-SP	16	16	2009.11.10 05:15:00 AM GMT	
OM3500-11754-9	16	16	N/A	
NAKINAFUJI-3	8	8	2009.11.10 10:15:00 AM GMT	
NAKINAFUJI-1	8	8	2009.11.10 01:15:00 PM GMT	
FW4500-10004-9	14	14	2009.11.10 05:15:00 AM GMT	
FLM600-11744-9	8	8	2009.11.10 06:45:00 AM GMT	
CORESTREAM-11734-9	2	2	2009.11.11 12:00:00 AM GMT	

Configure Collection on NEs/NE Groups

From this screen you can click the desired link to drill down:

- [To view the list of PM data files associated with an NE](#)

- To see which groups have been enabled for the corresponding NE (including bin size and next collection time)
- To see which groups are available for collection for the corresponding NE
- To enable or remove PM groups for the corresponding NE

To view the list of PM data files associated with an NE

4. Click the name of the NE in the **NE Name** column. If there are many matching files, you can refine the results by searching for File Name, PM Group, Start Time and End Time.

The system displays the list of matching PM data files.

NE Name - Anda4000

Search Criteria

File Name

PM Group Any

Start Time June 22 2009 03 30 PM ☒ Time Zero

End Time June 23 2009 03 30 PM ☒ No End Time

Search Results

Rows per page: 10

Matching Files - 3 items

File Name	PM Group	Start Time	End Time	Exported
Anda4000_SONETSection_254_2009-06-19_13.00.00_15.csv.zip	SONETSection	2009.06.18 12:00:00 AM EDT	2009.06.19 12:00:00 AM EDT	false
Anda4000_SONETSection_254_2009-06-18_13.15.00_15.csv.zip	SONETSection	2009.06.17 12:00:00 AM EDT	2009.06.18 12:00:00 AM EDT	false
Anda4000_SONETSection_254_2009-06-17_17.45.00_15.csv.zip	SONETSection	2009.06.16 12:00:00 AM EDT	2009.06.17 12:00:00 AM EDT	false

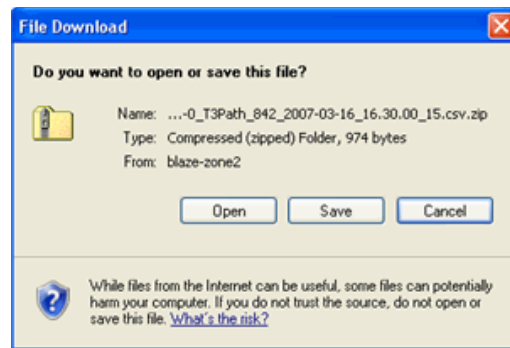


Note: If the Matching Files list is empty, the data may have already been removed, which is based on the setting of the Data cleanup policy.

To open or save the file locally

- a. Click the desired file name in the **File Name** column. The format of the file name is “**NE Name**”_”**PM Group Name**”_”**Unique PM Group Identifier**”_”**Latest End Time in report**”_”**Bin size**”.csv.zip. See “[PM report viewing and format](#)” on page 141 for more details.

- b. Depending on how your PC is configured, you are prompted to Open or Save the file to a location on your PC. Use any standard application to unzip the file.



If you open the file in a spread sheet, the data is displayed in columns.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Inventory ID	StartTime	EndTime	BinSize	SES	SES_Stat	SEFS	SEFS_Stat	ES	ES_Status	CV	CV_Status
2	Anda4000::TTP::SECT::10066	6/17/2009 17:45	6/17/2009 18:00	15						0 invalid		
3	Anda4000::TTP::SECT::10066	6/17/2009 17:45	6/17/2009 18:00	15				0 invalid				
4	Anda4000::TTP::SECT::13421	6/17/2009 17:45	6/17/2009 18:00	15		0 invalid						
5	Anda4000::TTP::SECT::13421	6/17/2009 17:45	6/17/2009 18:00	15							0 invalid	
6	Anda4000::TTP::SECT::10066	6/17/2009 18:00	6/17/2009 18:15	15				0 invalid				
7	Anda4000::TTP::SECT::10066	6/17/2009 18:00	6/17/2009 18:15	15				0 invalid				
8	Anda4000::TTP::SECT::13421	6/17/2009 18:00	6/17/2009 18:15	15							0 invalid	
9	Anda4000::TTP::SECT::13421	6/17/2009 18:00	6/17/2009 18:15	15					0 invalid			
10	Anda4000::TTP::SECT::10066	6/17/2009 18:15	6/17/2009 18:30	15		0 invalid						
11	Anda4000::TTP::SECT::10066	6/17/2009 18:15	6/17/2009 18:30	15				0 invalid				
12	Anda4000::TTP::SECT::13421	6/17/2009 18:15	6/17/2009 18:30	15							0 invalid	
13	Anda4000::TTP::SECT::13421	6/17/2009 18:15	6/17/2009 18:30	15					0 invalid			
14	Anda4000::TTP::SECT::10066	6/17/2009 18:30	6/17/2009 18:45	15				0 invalid				

For an explanation of the PM report data, see “PM report viewing and format” on page 141.

To see which groups have been enabled for the corresponding NE

- Click the number in the **Enabled PM Group** column to see a list of enabled PM groups, the bin size and the date and time of the next collection. To return to the previous screens, click Close.

PM Group Collection - FW4500-10004-9

Enabled PM Groups

Enabled PM Groups · 1 to 10 of 14

PM Group	Bin Size	Next Collection Time
FujitsuEportWAN	1 day	2009.11.10 06:36:00 AM GMT
SONETLine	1 day	2009.11.10 06:36:00 AM GMT
SONETSection	1 day	2009.11.10 06:36:00 AM GMT
FujitsuOpticalSnapshot	1 day	2009.11.10 06:36:00 AM GMT
FujitsuOCH107_OC192S4	1 day	2009.11.10 06:36:00 AM GMT
FujitsuEportLAN	1 day	2009.11.10 06:36:00 AM GMT
FujitsuOCH107_OC192S5	1 day	2009.11.10 06:36:00 AM GMT
SONETLine	15 min	2009.11.09 10:20:00 PM GMT
FujitsuOCH107_OC192S4	15 min	2009.11.09 10:20:00 PM GMT
FujitsuOCH107_OC192S5	15 min	2009.11.09 10:20:00 PM GMT

Click to drill down for details

Close

Click the name of a PM group to drill down and see the PM count definitions. To return to the previous screens, click Close.

PM Group Details - EthernetCount

Description : Ethernet

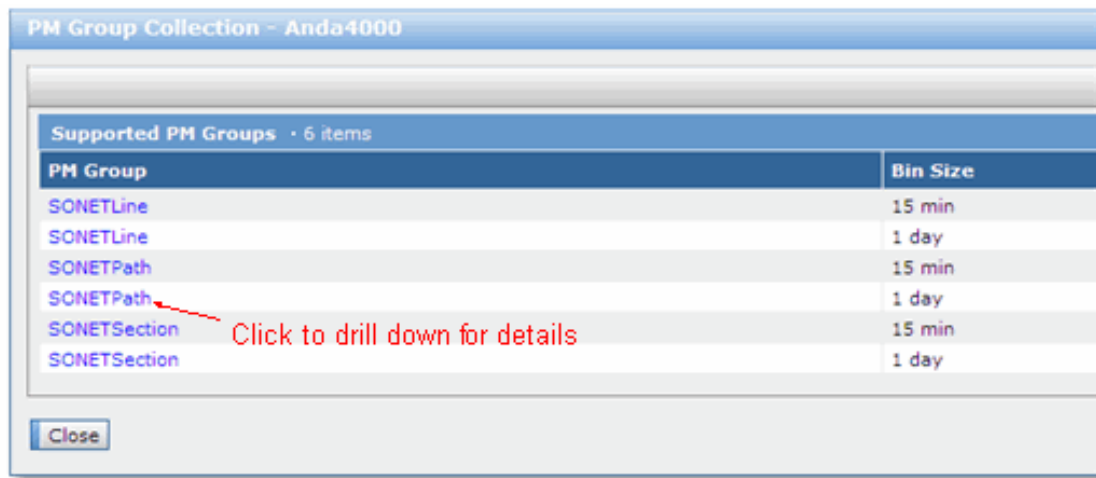
PM Count Definitions · 6 items

Name	Description
ES	Errored Seconds
INFRAMES	In frames
INFRAMESDISC	In discarded frames
INFRAMESERR	In errored frames
SES	Severely Errored Seconds
UAS	Unavailable Seconds

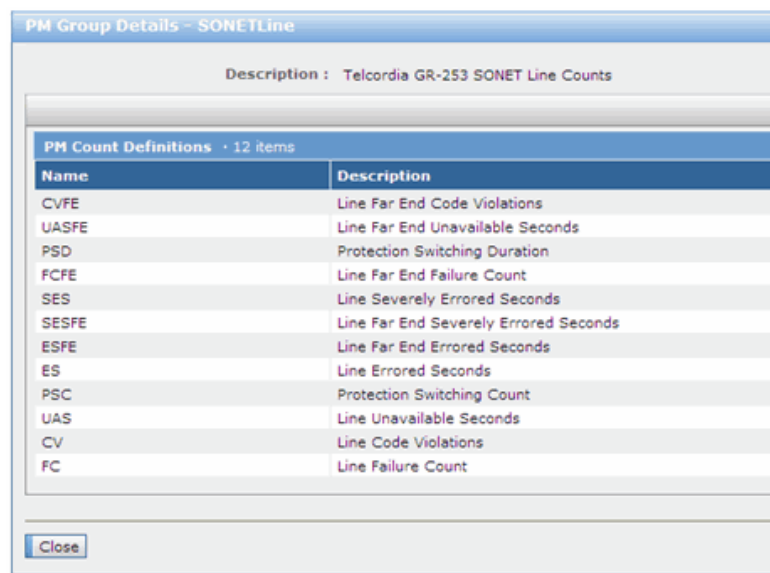
Close

To see which groups are available for collection for the corresponding NE

- Click the number in the **Supported PM Group** column to see the PM groups that are supported. Click the name of a group to drill down and see the PM count definitions.



You can click the name of a PM Group to drill down and view the PM count definitions.

**To enable or remove PM groups for the corresponding NE**

- Click the edit icon. The following example shows the groups that are available and the groups that are currently enabled. To add PM groups, select them in the Available PM Groups list and click Add to move them to the Enabled PM Groups

list. To remove PM groups, select them in the Enabled PM Groups list and click Remove to move them to the Available PM Groups list.

The screenshot shows a window titled "PM Group Collection - Anda4000". It contains two main sections: "Available PM Groups" and "Enabled PM Groups".

Available PM Groups (3 items):

Select	PM Group	Bin Size
<input type="checkbox"/>	SONETLine	1 day
<input type="checkbox"/>	SONETPath	1 day
<input type="checkbox"/>	SONETSection	1 day

Below this table is an "Add" button.

Enabled PM Groups (3 items):

Select	PM Group	Bin Size
<input type="checkbox"/>	SONETLine	15 min
<input type="checkbox"/>	SONETPath	15 min
<input type="checkbox"/>	SONETSection	15 min

Below this table is a "Remove" button. At the bottom of the window are "Save" and "Close" buttons.

8. To store any changes, click **Save**. To close a window without saving, click **Close**.

7.4 Managing performance monitoring jobs

This section contains the following procedures for viewing and managing PM jobs:

- [“View PM jobs and job details” on page 159](#)
- [“Delete a job from the database” on page 160](#)
- [“Re-run a failed “PM Collection Configuration” job” on page 161](#)



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

7.4.1 View PM jobs and job details

Use this procedure to view a list of the three types of PM jobs: Collection Configuration, PM Data Export, or PM Data Removal.

From the list of jobs, you can see the information described in the table [“PM job details” on page 140](#).

1. Launch **Performance Monitoring**.
2. If not already selected, click the **Jobs** tab.

The system displays the list of jobs. You can filter the list by **Job Status** or **Job Types**.

The screenshot shows the 'Performance Monitoring' application window with the 'Jobs' tab selected. At the top, there are tabs for 'NE Status', 'Export Configuration', and 'Jobs'. Below the tabs, there is a 'Refresh Now' button and a checkbox for 'Enable Auto-Refresh' set to 'every 05:00 (mm:ss)'. A 'Search Criteria' section contains dropdown menus for 'Job Status' and 'Job Types', both set to 'Any'. A 'Search' button is located below the search criteria. The main area displays a table of jobs with 6 items. The table has columns: 'Select', 'Job ID', 'Job Type', 'Time', 'In Progress', 'Passed', 'Failed', and 'Status'. All jobs are marked as 'Failed' in the 'Status' column. Below the table is a 'Delete' button.

Select	Job ID	Job Type	Time	In Progress	Passed	Failed	Status
<input type="checkbox"/>	107990	PM Data Removal	Thu, 12 Nov 2009 02:00:47 GMT-05:00	N/A	N/A	N/A	Failed
<input type="checkbox"/>	110898	PM Data Removal	Fri, 13 Nov 2009 02:01:06 GMT-05:00	N/A	N/A	N/A	Failed
<input type="checkbox"/>	2314	PM Data Removal	Mon, 9 Nov 2009 02:00:54 GMT-05:00	N/A	N/A	N/A	Failed
<input type="checkbox"/>	104164	PM Data Removal	Wed, 11 Nov 2009 02:00:59 GMT-05:00	N/A	N/A	N/A	Failed
<input type="checkbox"/>	101576	PM Data Removal	Tue, 10 Nov 2009 02:01:15 GMT-05:00	N/A	N/A	N/A	Failed
<input type="checkbox"/>	1666	PM Data Removal	Sun, 8 Nov 2009 02:01:01 GMT-05:00	N/A	N/A	N/A	Failed

- To view the job details, click the link in the **Status** column.
The system displays the PM Logs.
- To return to the previous screen, click **Close**.
- To delete a job that is no longer required, see [“Delete a job from the database” on page 160](#).

7.4.2 Delete a job from the database

Use this procedure to delete a job that is no longer required.



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

- Launch **Performance Monitoring**.
- If not already selected, click the **Jobs** tab.
The system displays the list of jobs. You can filter the list by **Job Status** or **Job Types**.
- Select one or more jobs to be deleted.
The system prompts for confirmation to delete the selected jobs.
- Click **OK** to confirm the operation.
The system removes the selected jobs from the database.

7.4.3 Re-run a failed “PM Collection Configuration” job

Use this procedure to re-run a Failed “PM Collection Configuration” job.



Note: You cannot re-run a successful job.

1. Launch **Performance Monitoring**.
2. If not already selected, click the **Jobs** tab.

The system displays the list of jobs. You can filter the list by **Job Status** or **Job Types** to locate the failed job.

Performance Monitoring

NE Status | Export Configuration | **Jobs**

Refresh Now | Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Search Criteria

Job Status: Any
Job Types: Any

Search

Rows per page: 10

Select	Job ID	Job Type	Time	In Progress	Passed	Failed	Status
<input type="checkbox"/>	107990	PM Data Removal	Thu, 12 Nov 2009 02:00:47 GMT-05:00	N/A	N/A	N/A	Success
<input type="checkbox"/>	110898	PM Data Removal	Fri, 13 Nov 2009 02:01:06 GMT-05:00	N/A	N/A	N/A	Success
<input type="checkbox"/>	2314	PM Data Removal	Mon, 9 Nov 2009 02:00:54 GMT-05:00	N/A	N/A	N/A	Success
<input type="checkbox"/>	104164	PM Data Removal	Wed, 11 Nov 2009 02:00:59 GMT-05:00	N/A	N/A	N/A	Success
<input type="checkbox"/>	101576	PM Data Removal	Tue, 10 Nov 2009 02:01:15 GMT-05:00	N/A	N/A	N/A	Success
<input type="checkbox"/>	1666	PM Data Removal	Sun, 8 Nov 2009 02:01:01 GMT-05:00	N/A	N/A	N/A	Success
<input type="checkbox"/>	113991	PM Collection Configuration	Fri, 13 Nov 2009 14:40:25 GMT-05:00	0	0	1	Failed

Delete

3. Click the Failed link in the **Status** column for the “PM Collection Configuration” job to be re-run.
The system displays the Job Details.
4. To re-run the job, click the **Re-run Job** button.
5. To close the job details and return to the previous screen, click **Close**.

8 NE Security: Managing network element credentials



Note: Depending on your permissions or product configuration, some Network Integrity Framework tools may not be available or applicable.

NE Security allows administrators to create change and delete NE credentials and password policy settings on managed NEs.



Note: The information that gets displayed in the NE Security user interface will vary according to the NE and its installed adapter. This is because control over password policy parameters, such as user classes, inactive session timeout, and credential expiry parameters are determined by the features supported by the network element and its network adapter.

This chapter contains the following NE Security procedures:

“NE Security prerequisites and considerations” on page 164

“Creating credentials on network elements” on page 165

The section contains procedures that allow you to create NE credentials on one or more NEs in your network in a variety of ways:

- “Create a credential on a single network element” on page 167
- “Create a credential on multiple NEs” on page 171

“Deleting or changing credentials” on page 178

This section contains the procedures to modify credentials on NEs in your network. If supported by the NE and adapter, changes can be made to the password, protocol and security parameters.

- “Change or delete one or more credentials on a specific network element” on page 179
- “Change or delete a specific credential on all NEs” on page 181

“About searching for credentials” on page 182

This section contains information about performing credential and NE searches.

“Managing NE security jobs” on page 184

This section contains the following procedures for managing security jobs that are created when credentials are created, modified or deleted:

- “View NE Security job details” on page 184
- “Delete unwanted NE security jobs” on page 186

8.1 NE Security prerequisites and considerations

This section describes prerequisites and special considerations that apply to the NE Security application, which allows administrators to create and manage NE credentials (user accounts and security settings) on all NEs in the managed network. Administrators can create, change and delete NE credentials and password policy settings on individual NEs, or on multiple NEs at the same time.



Note: The information that gets displayed in the NE Security user interface will vary according to the NE and its installed adapter. This is because control over password policy parameters, such as user classes, inactive session timeout, and credential expiry parameters are determined by the features supported by the network element and its network adapter.

8.1.1 NE Security Role and permission prerequisite

To use the NE Security application, a user account must be assigned to the “NE Security Role” and have the correct permissions and NE Groups set. Without the correct permissions, a user will not be able to access some or all of the features or NEs.

8.1.2 NE Security adapter considerations



Note: Network Integrity uses the information from the installed network adapters to determine which credential parameters are supported. For example, some NEs may not support password aging, so the system will not display it as an option for the NE credential being created. If a parameter is not supported by an adapter or an NE, it will not be available in the user interface. If a Network Integrity feature is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they will know what to expect when managing network elements from the client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.



Note: Some adapters, especially ones from previous releases, may not support new Network Integrity release functionality. If an adapter does not support a new feature, the user may be prevented from performing certain actions.

8.1.3 NE Security and password rule considerations



Note: Before using NE security to create credentials, **you must not provision password rule settings on NEs that support this capability; and for NEs that have already had password rules set, these settings must be returned to their default values before credentials are created.** This is necessary because Network Integrity does not support the retrieval of password rule settings from an NE, and therefore the default values are hard-coded within a network adapter. This allows Network Integrity to validate user-entered passwords and automatically-generated passwords before they are updated on these NEs.



Note: **Data mining does not retrieve passwords from NEs.** Passwords are only stored in the database for credentials that were created on NEs using the NE Security application. Passwords that are stored in the database are in an encrypted format using the symmetric-key algorithm recommended by the ANS T1.276-2003 AES specification.

8.2 Creating credentials on network elements

The NE Security application allows you to create NE credentials on one or more NEs in your network in a variety of ways:

- [“Create a credential on a single network element” on page 167](#)
- [“Create a credential on multiple NEs” on page 171](#)



Note: A “credential” is any account on the network element, while a “management credential” is an account on the network element that is being used by Network Integrity as a Session Credential or Connection Credential to login and manage the device.

The [NE credential parameters](#) table lists all of the parameters associated with NE credentials and is referenced by the procedures in this section.

Table 8–1: NE credential parameters

Parameter	Description
Credential Database Name	Network elements can have one or more credential databases. The “Credential Database Name” parameter is defined in the adapter and can be selected to define which database is to be used for any given management credential. The available choices depend on what is defined in the adapter, such as Account (for TL1 and CLI), SNMP, or possibly LDAP for credentials associated with a directory server.

Parameter	Description
Management Credential	<p>(For SNMP, this field only appears when the SNMP Type is set to snmp_write). Specify whether or not the credential will be a Management Credential which is used by Network Integrity to login and manage the NEs:</p> <ul style="list-style-type: none"> If the credential will be used to manage the NEs, select Yes. Selecting Yes will display the Name and Protocol lists, which can be used to select existing credentials that were created with the Manage Credentials tool in the NE Manager, or to use the Create button to create a credential. Selecting Yes will disable the NE Login ID field and Password field because the Manage Credentials tool manages the passwords for these credentials. <p>Note: if you select Yes, you should ensure that password settings, such as Inactive Session Timeout, Password Aging and Account Expiry are disabled so that the credential used for managing the NEs never expires or times out. Also ensure that the User Class is set to a level high enough to allow Credential changes on the NE.</p> <ul style="list-style-type: none"> If the credential will not be used by Network Integrity to manage the NEs, select No. This will enable the option to Manage Passwords and enable the NE Login ID field and Password field.
Manage Password	<p>(Appears only when Management Credential is set to No and the NE adapter requires a login reset of the password.) This selection is to accommodate devices that force a password change on first login. When selected, the credential can be created with an initial password, and when the device forces a password change, the new password entered by the user will be captured and stored in the database.</p> <p>Passwords are stored in an encrypted format using the symmetric-key algorithm recommended by the ANS T1.276-2003 AES specification.</p>
Name	<p>(Appears only when Management Credential is set to Yes.) From the list, select the name for the credential that will be used to manage the devices. The credentials in this list come from the Manage Credentials tool in the NE Manager. If the credential you require is not in the list, click the Create button and create the desired credential. After the credential has been created, you will be returned to this screen where you can select the credential from the list.</p>
Interface	<p>(Appears only when Management Credential is set to Yes.) From the list, select the interface name to associate with the management credential that will be used to manage the devices. For example, if more than one TL1 interface exists on the NE, such as "TL1 Admin" and "TL1 Events", two interfaces would be present in the Interface list.</p>
NE Login ID	<p>(Appears only for TL1, CLI and SOAP. For SNMP, Community String appears.) If Management Credential is set to Yes, the system populates this field with the NE login ID selected in the "Name" list, and this field is not accessible. If Management Credential is set to No, type the ID for the NE login account to be created on the NEs. For SNMP, type the Community String.</p> <p>Note: when modifying a credential, you can not change the NE Login ID.</p> <p>Note: For CLI, do not use the dollar sign character (\$) in the NE Login ID.</p>

Parameter	Description
Password	If Management Credential is set to Yes, the system uses the password from the management credential that was selected in the Name list. The Password field will be blank and not accessible. If Management Credential is set to No, type a password for the NE Login ID . Note: when modifying an NE credential that is being used as a management credential, you can not change the password.
Confirm Password	(Available only if Management Credential is set to No.) Re-type the password for the NE Login ID to confirm it.
User Class	(Varies by NE). Specify the user security class for the NE credential being created. Not all NE vendors use the same security class, so this selection will vary for each type of NE. Consult the vendor documentation for an explanation of their user classes.
Custom	(Varies by NE). If you selected Custom as the User Class , use this field to type the name of the custom user class.
Inactive Session Timeout	(If supported by NE) Specify the number of minutes after which an inactive session will timeout and be terminated by the system, or select never for no timeout. If the network adapter has specific timeout restrictions, they will be displayed under the field.
Password Aging	(If supported by NE) Select the number of days after which a password must be changed, or select never for no aging. If the network adapter has specific aging restrictions, they will be displayed under the field. (Not supported by all adapters.)
Expiry Date	(Not supported by all NEs or adapters) Select the date on which the NE credential will expire, or select Never for no expiration.
SNMP Type	Appears only for SNMP protocols. Select the type of community string: snmp_read, snmp_write, or snmp_trap.
Trap Destination IP Address	Appears only when SNMP Type is set to snmp_trap Community String. Type the IP address of the host that receives the trap messages.
Trap Port	Appears only when SNMP Type is set to snmp_trap Community String. Type the destination trap port for the trap community string.
Community String	Appears only when SNMP Type is set to snmp_trap Community String or snmp_write Community String. Type the required community string. Note: Do not use the dollar sign character (\$) in an SNMPv2c write community string.

8.2.1 Create a credential on a single network element

Use this procedure to search for an NE and create a credential on it.

1. Launch **NE Security**.
2. If not already selected, click the **NEs** tab.

The system displays the NE Security search screen that you use to search for the NE on which to create the NE credential.

NE Security

NEs Credentials Jobs

Credential Search Criteria

Credential Name

Credential Database Name

NE Search Criteria

NE Name Equals

Vendor/Model/Version Equals Nortel

Load Search Save Search Case Sensitive

Search

Search Result

Rows per page: 10

Select	NE Name	Vendor	Model	SW Version	Assigned Template
No items in list!					

Use the **NE Search Criteria** fields and menus in any combination to specify the search criteria for the desired NEs. In addition to the standard NE Search Criteria, you can use the Credential Search Criteria to search for a specific **Credential Name** or **Credential Database Name** that is on the NE you want to locate. You can also load a previously saved search by clicking the **Load Search** button. You can use wildcards as described in the Inventory application.

3. Click **Search** to display the list of matching NEs.
4. When the search results contain the NE on which you want to create the credential, click the name of the NE in the **NE Name** column.

The system displays the NE Details, which lists the credentials already on the NE (if any).

NE Details

NE Name: OM3500-3-SP
 Vendor: Nortel
 Model: OPTera Metro 3500 MSP
 Software Version: REL1210X.AG
 Assigned Template Name:

Credential List - 1 to 10 of 29

Select	Credential Name	Credential DB Name	Management Credential	Credential Type	Trap IP Address	Trap Port
<input type="checkbox"/>	LCHENG3	TL1	false	account		
<input type="checkbox"/>	JWANG2	TL1	false	account		
<input type="checkbox"/>	RK1	TL1	false	account		
<input type="checkbox"/>	JWANG	TL1	false	account		
<input type="checkbox"/>	JWANG1	TL1	false	account		
<input type="checkbox"/>	ADMIN	TL1	true	account		
<input type="checkbox"/>	SURVEIL	TL1	false	account		
<input type="checkbox"/>	NADIR	TL1	false	account		
<input type="checkbox"/>	TFARROW	TL1	false	account		
<input type="checkbox"/>	LCHENG	TL1	false	account		

Create Delete Close

5. Click **Create**.

The system displays the Credential Information screen. The information that is displayed will vary according to the adapter.

6. Define the credential parameters as described in table “NE credential parameters” on page 165. The parameters, such as timeout and aging will vary depending on what is supported by the adapter and the NE.

The following example shows the screen for a typical TL1 credential.

Credential Information

Credential Database Name: TL1 *

Management Credential: ☐ Yes ☒ No

☒ Manage Password

NE Login ID: *

Password: *

Confirm Password: *

User Class: --Select-- *

Inactive Session Timeout: Minutes

The Inactivity Timeout value must be within range: 1-99

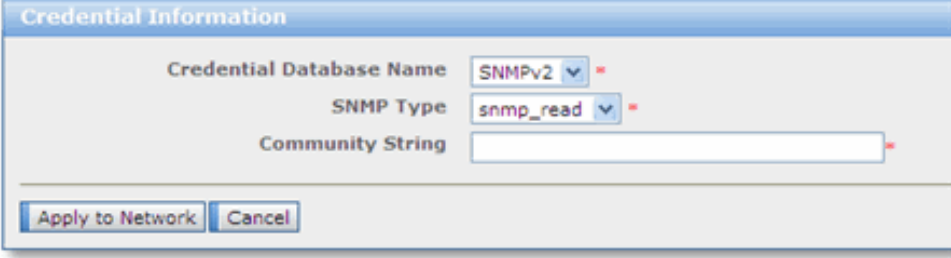
Password Aging: Days

The Password Aging value must be within range: 0-999

Expiry Date: Aug 13 2012

Apply to Network Close

The following example shows the screen for a typical SNMP credential.




The 'Credential Information' dialog box contains the following fields and controls:

- Credential Database Name:** A dropdown menu with 'SNMPv2' selected.
- SNMP Type:** A dropdown menu with 'snmp_read' selected.
- Community String:** An empty text input field.
- Buttons:** 'Apply to Network' and 'Cancel' at the bottom.

- When the credential parameters have been configured, click **Apply to Network**. The system prompts for confirmation.

- Click **OK** to create the credential on the selected NE.

The system starts an NE Security job and displays the NE Security Job screen. The system attempts to create the credential on the selected NE, and displays the status of the credential creation process: Unstarted, Success or Failed. If successful, the credential settings are created on the NE.



The 'NE Security Job' screen displays the following information:

- Job Summary:**
 - Job ID: 47473
 - Job Description: Create TL1 credential maintc
 - Originator: sysadmin
 - Total NEs: 1
 - Job Status: InProgress
 - Success: 0
 - Pending: 0
 - In Progress: 0
 - Failed: 0
- Refresh Now** button and **Enable Auto-Refresh** checkbox with a dropdown set to '05:00 (mm:ss)'.
- NE List** table with 1 item:

NE Name	Vendor	Model	SW Version	Status
OM3500MIX-1001	Nortel	OPTera Metro 3500 MSP	REL1210X.AG	Unstarted

Buttons: **Close**

- To manually refresh the screen, click **Refresh Now**, or set the Auto-Refresh feature for the desired interval.

10. To view details about the status of a Failed job, click the status in the **Status** column.



11. To return to the previous screen, click **Close**; to view the log details, click the log name in the **Log ID** column.
The system displays the log details.
12. To return to the previous screen, click **Close** twice.

8.2.2 Create a credential on multiple NEs

Use this procedure to create one credential on multiple NEs or NE Groups using the NE Security wizard.

1. Launch **NE Security**.
2. If not already selected, click the **Credentials** tab.

The system displays the credential search screen.

NEs

Credentials

Jobs

Credential Search Criteria

Credential Name

Credential Type

Management Credential

NE Search Criteria

NE Name

Equals

Vendor/Model/Version

Equals

Load Search

Save Search

Case Sensitive

Search

Search Result

Rows per page: 10

Credential List

No items in list!

Create

Delete

3. Click **Create**.
- The system displays Step 1 of the Create Credential wizard.

Create Credential Wizard

Step 1: Source Type.

Choose NEs.

Choose NE Groups.

Next >>

Cancel


4. Select the devices on which to create the credential.

To create the credential on	Then select
one or more network elements	Choose NEs
one or more network element groups	Choose NE Groups

The system displays Step 2 of the Create Credential wizard. The screen that is displayed will depend on your device selection in the previous step, but the procedure is similar for both NEs or NE Groups. The following screen shows Step 2 if "Choose NEs" was selected.

Create Credential Wizard

Step 1: Source Type.

Step 2: Choose NEs. 

Available NEs

View:

NE Name:

Vendor:

Model:

Software Version:

NE Group Name:

Rows per page: 10

Available NE List - 7 items

Select	NE Name	Vendor	Model	SW Version
<input type="checkbox"/>	VERIZON1	Adtran	OPTI-6100	3.3
<input type="checkbox"/>	OM3500-3-NP	Nortel	OPTera Metro 3000 MSP Series NP	REL1210.AG
<input type="checkbox"/>	OM3500-1-SP	Nortel	OPTera Metro 3500 MSP	REL1210X.AG
<input type="checkbox"/>	OM3500-3-SP	Nortel	OPTera Metro 3500 MSP	REL1210X.AG
<input type="checkbox"/>	NAKINAFUJI-2	Fujitsu	FLM600	15.0
<input type="checkbox"/>	anda2108	Anda	EtherReach 2108	2.0
<input type="checkbox"/>	anda2200	Anda	EtherReach 2200	2.1

Selected NEs

Rows per page: 10

Selected NE List - no entries

Select	NE Name	Vendor	Model	SW Version
No items in list!				

The following screen shows Step 2 if “Choose NE Groups” was selected.

Step 1: Source Type.

Step 2: Select NE Groups

Available NE Groups

NE Group Name Search Reset Rows per page: 10

Available NE Groups · 6 items

Select	NE Group Name
<input type="checkbox"/>	Alberta
<input type="checkbox"/>	All NEs
<input type="checkbox"/>	Ontario
<input type="checkbox"/>	Quebec
<input type="checkbox"/>	New Brunswick
<input type="checkbox"/>	Nova Scotia

Add

Added NE Groups

Rows per page: 10

Added NE Groups · no entries

No items in list!

Remove

<< Back Next >> Cancel

5. Search for the NEs or NE Groups on which the credential will be created.

Note: The NEs or groups that you search for and select must have similar protocols and credential parameters. For example, you cannot mix TL1 and SNMP NEs, because the credential criteria is different.

6. Select one or more NEs or NE Groups and then click **Add** to move the selected items from the **Available** list to the **Selected** list.

Search

Rows per page: 10

Available NE List • 2 items

Select	NE Name	Vendor	Model	SW Version
<input type="checkbox"/>	CNRL01TX-0001	Ciena	Corestream	
<input checked="" type="checkbox"/>	CNRL02TX-0001	Ciena	Corestream	

Add

Selected NEs

Rows per page: 10

Selected NE List • 1 item

Select	NE Name	Vendor	Model	SW Version
<input type="checkbox"/>	CNRL02TX-0001	Ciena	Corestream	

Remove

7. After the required NEs or NE Groups are in the **Selected NE List**, click **Next**.
The system displays Step 3 of the Create Credential wizard, which will vary according to the NE and adapter. Note: If you selected NEs or Groups with different operational characteristics, the system displays the message: **"Selected NEs are not compatible."** If this happens, select the incompatible NEs, and use the **Remove** button to remove them from the list of Selected NEs.

This example shows typical credential information for TL1.

Create Credential Wizard

Step 1: Source Type.
Step 2: Choose NEs.
Step 3: Credential Information. ←

Credential Database Name TL1 *

Management Credential ☐ Yes ☒ No

☐ Manage Password

NE Login ID *

Password: *

Confirm Password: *

User Class: --Select-- *

Inactive Session Timeout: ☒ Disable ☐ Enable [] Minutes

The Inactivity Timeout value must be within range: 1-99

Password Aging: ☒ Disable ☐ Enable [] Days

The Password Aging value must be within range: 0-999

Parameters depend on adapter

<< Back Go Cancel

This example shows typical credential information for CLI.

Create Credential Wizard

Step 1: Source Type.
Step 2: Choose NEs.
Step 3: Credential Information. ←

Credential Database Name CLI *

Management Credential ☐ Yes ☒ No

☐ Manage Password

NE Login ID *

Password: *

Confirm Password: *

User Class: --Select-- *

Inactive Session Timeout: ☒ Disable ☐ Enable [] Minutes

The Inactivity Timeout value must be within range: 5-30

Parameters depend on adapter

<< Back Go Cancel

This example shows typical credential information for SNMP.

Create Credential Wizard

Step 1: Source Type.
Step 2: Choose NEs.
Step 3: Credential Information.

Credential Database Name: SNMPv2
SNMP Type: Write Community String
Management Credential: ☒ Yes ☐ No
Name: write on Anda 4000
Interface: SNMPv2
Community String: write

<< Back Go Cancel

8. Define the credential parameters as described in table “NE credential parameters” on page 165.
9. When you have entered all the credential parameters, click **Go**.
The system starts an NE Security job and displays the NE Security Job screen. The system attempts to create the credential on the selected NEs, and displays the status of the credential creation process for each NE: Unstarted, Success or Failed. If successful, the credential is created on the NEs.

NE Security Job

Refresh Now Enable Auto-Refresh ☐ every 05:00 (mm:ss)

Job Summary

Job ID 47430
Job Description Create TL1 credential adminis
Originator sysadmin
Total NEs 5
Job Status Success
Success 5
Pending 0
In Progress 0
Failed 0

Rows per page: 10

NE Name	Vendor	Model	SW Version	Status
OM3500MIX-1001	Nortel	OPTera Metro 3500 MSP	REL1210X.AG	Success
OM3500MIX-1002	Nortel	OPTera Metro 3500 MSP	REL1210X.AG	Success
OM3500MIX-1003	Nortel	OPTera Metro 3500 MSP	REL1210X.AG	Success
OM3500MIX-1004	Nortel	OPTera Metro 3500 MSP	REL1210X.AG	Success
OM3500MIX-1005	Nortel	OPTera Metro 3500 MSP	REL1210X.AG	Success

Close

10. To manually refresh the screen, click **Refresh Now**, or set the Auto-Refresh feature for the desired interval.

11. To view details about the status of a Failed job, click the status in the Status column. The system displays the log details.



12. To return to the previous screen, click **Close**; to view the log details, click the log name in the **Log ID** column.

The system displays the log details.



13. To return to the previous screen, click **Close** twice.

8.3 Deleting or changing credentials

The NE Security application allows you to change existing credentials on the NEs in your network, or delete credentials that are no longer required. It can be useful to perform this on a regular basis to meet corporate security policies. The NE Security application provides a number of ways to change or delete credentials:

- [“Change or delete one or more credentials on a specific network element” on page 179](#)
- [“Change or delete a specific credential on all NEs” on page 181](#)

As part of this credential modification process, Network Integrity uses the information from the installed network adapters to determine which credential parameters are supported. For example, some NEs may not support password aging, so the system will not display it as an option for the credential being changed.

About changing the password for a credential

To change the password for an NE credential that is not being used as a Management Credential, use the procedure in this section to change the password and apply the change to the NEs:

- “Change or delete one or more credentials on a specific network element” on page 179



Note: To change the password for an NE credential that is being used as a management credential, you must create a new Management Credential and associate it with the NE credential. This is required because other NEs may be using the same Management Credential, and by changing the Management Credential password you may affect connectivity to the other NEs.

8.3.1 Change or delete one or more credentials on a specific network element

Use this procedure to search for a specific NE and change one or more credentials on the NE, or delete one or more credentials from the NE.

1. Launch **NE Security**.

The system displays the NE Security screen.

2. If not already selected, click the **NEs** tab.

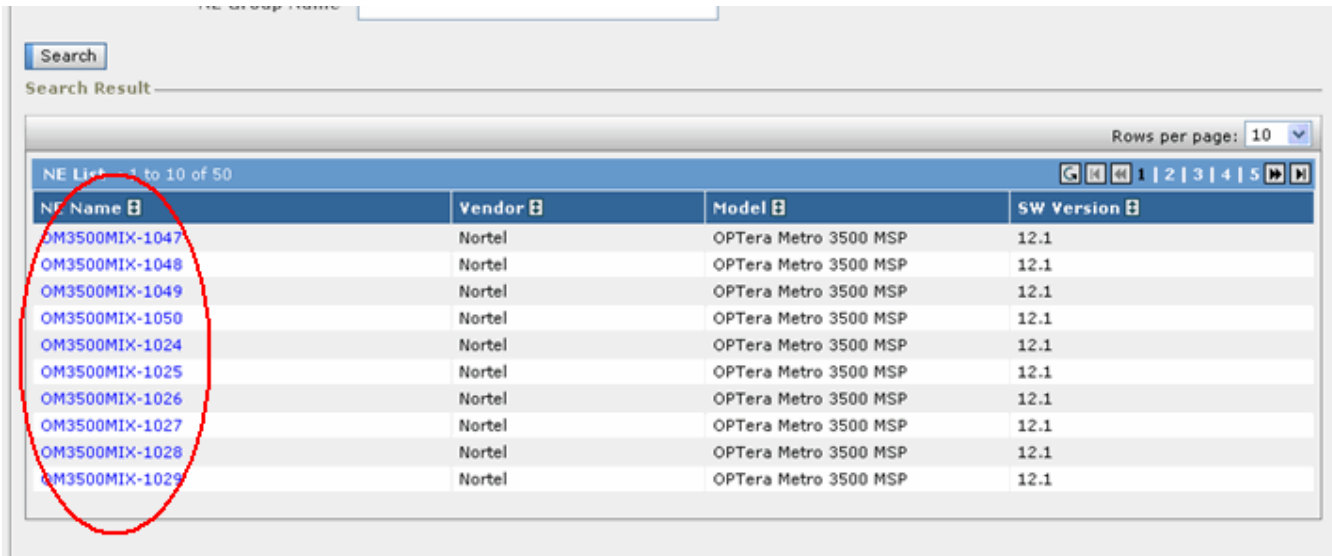
The system displays the NE Security search screen.

Use the **NE Search Criteria** fields and menus in any combination to specify the search criteria for the desired NEs. In addition to the standard NE Search

Criteria, you can search for a specific **Credential Name** or **Protocol** that is on the NE you want to locate. You can also load a previously saved search by clicking the **Load Search** button. You can use wildcards as described in the Inventory application.

3. Click **Search** to display the matching NEs for which you want to view the NE credentials.

The system displays the NEs that match the search criteria.



Search Result

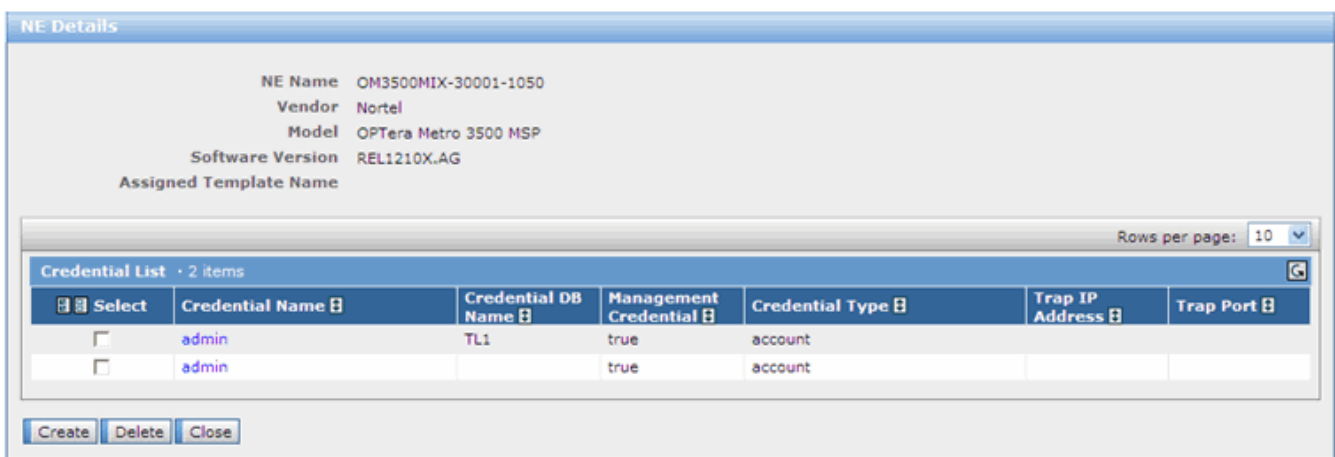
Rows per page: 10

NE List 1 to 10 of 50

NE Name	Vendor	Model	SW Version
OM3500MIX-1047	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1048	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1049	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1050	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1024	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1025	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1026	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1027	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1028	Nortel	OPTera Metro 3500 MSP	12.1
OM3500MIX-1029	Nortel	OPTera Metro 3500 MSP	12.1

4. To see the list of credentials on an NE, click the name of the NE in the **NE Name** column.

The system displays the list of credentials on the selected NE.



NE Details

NE Name OM3500MIX-30001-1050
Vendor Nortel
Model OPTera Metro 3500 MSP
Software Version REL1210X.AG
Assigned Template Name

Rows per page: 10

Credential List - 2 items

Select	Credential Name	Credential DB Name	Management Credential	Credential Type	Trap IP Address	Trap Port
<input type="checkbox"/>	admin	TL1	true	account		
<input type="checkbox"/>	admin		true	account		

Create Delete Close

5. To delete credentials from the selected NE:
 - a. In the Credential List, select one or more credentials to be deleted.
 - b. Click **Delete**.

The system prompts for confirmation.

- c. Click **Delete** to confirm the removal of the selected credentials from the NE.
The system starts an NE Security job, which shows the status of the deletion process on the NE. If successful, the system removes the credentials from the NE.
6. To modify credential parameters on the selected NE:
 - a. In the **Credential Name** column, click the name of the credential you want to change.
The system displays the credential details.
 - b. Configure the credential parameters.
 - c. When the desired credentials changes have been made, click **Apply to Network**.
The system prompts for confirmation.
 - d. Click **OK** to create an NE Security job, which applies the changes to the NE.
7. To create a credential on an NE, click Create and follow the wizard.

8.3.2 Change or delete a specific credential on all NEs

Use this procedure to search for a specific credential, and if required, make changes or delete it from all NEs that contain it.

If a credential is used as a management credential, it can not be deleted.

1. Launch **NE Security**.
The system displays the NE Security screen.
2. If not already selected, click the **Credentials** tab.
The system displays the Credential Search screen.
3. In the corresponding fields, specify the criteria to perform a search for the credentials you want to view.
For a description on how to perform credential searches, see [“About searching for credentials” on page 182](#).
4. After entering the required search criteria, click **Search**.

The system displays the list of matching credentials, as shown in the following example:

Search Result

Credential List · 41 to 50 of 80

Rows per page: 10

Select	Credential Name	Credential DB Name	Credential Type	Trap IP Address	Trap Port	Management Credential	NE Name	Vendor	Model	SW Version
<input type="checkbox"/>	johnTest41	CLI	account			false	Anda4000			
<input type="checkbox"/>	public	SNMPv2	snmp_read			false	Anda4000			
<input type="checkbox"/>	private	SNMPv2	snmp_write			true	Anda4000			
<input type="checkbox"/>	no Credential ID	SNMPv2	snmp_trap	10.11.49.50	162	false	Anda4000			
<input type="checkbox"/>	johnTest1	SNMPv2	snmp_trap	1.1.1.1	162	false	Anda4000			
<input type="checkbox"/>	trap3	SNMPv2	snmp_trap	10.11.12.13	162	false	Anda4000			
<input type="checkbox"/>	johnTest1	SNMPv2	snmp_trap	1.1.1.2	162	false	Anda4000			
<input type="checkbox"/>)(*^%\$#@!\$37afim	SNMPv2	snmp_trap	10.55.33.88	162	false	Anda4000			
<input type="checkbox"/>	ADMIN	TL1	account			true	OM3500-3-NP			
<input type="checkbox"/>	SURVEIL	TL1	account			false	OM3500-3-NP			

Create Delete

5. To modify a credential:
 - a. Click the name of the credential in the **Credential Name** column.
The system displays the credential details.
 - b. Make the desired changes.
 - c. Click **Apply to Network**.
The system prompts for confirmation.
 - d. Click **OK** to create the NE Security job, which will apply the changes.
6. To delete credentials:
 - a. Select one or more credentials in the list.
 - b. Click **Delete**.
The system prompts for confirmation.
 - c. Click **OK** to create the NE Security job, which will delete the credentials for all NEs that contain it.

8.4 About searching for credentials

The NE Security application provides a powerful search engine that allows you to search for credentials that have been retrieved through NE Manager data mining, or created with the NE Security application.



Note: The data mining process does not retrieve passwords from NEs. Passwords are only stored in the database for credentials that were created or modified on NEs using the NE Security application. Passwords that are stored in the database are in an encrypted format using the symmetric-key algorithm recommended by the ANS T1.276-2003 AES specification.

- Credential searches show you where specific credentials are being used: you can search for credentials and see which network elements contain them.

- NE searches show you the credentials on specific NEs: You can search for network elements and see which credentials are on them.

If you know the credential and want to view or modify it

Use the **Credentials** tab of the NE Security application to search for a specific credential and see where it is being used in the system. The search results contain a list of credentials and a summary. See [“Change or delete a specific credential on all NEs” on page 181](#).

If you know the NE or group and want to view or modify the credentials:

Use the **NEs** tab of the NE Security application to search for a specific NE and see which credentials it has installed on it. See [“Change or delete one or more credentials on a specific network element” on page 179](#).

Credential search criteria

The Network Integrity search engine allows you to perform searches to find credentials in a variety of ways. In addition to the standard NE search fields for vendor/model/version, credential searches allow you to specify the following search criteria that are specific to credentials.

Table 8–2: Credential-specific search criteria

Attribute	Searches for
Credential Name	All or part of a specific credential name.
Credential Database Name	NEs based on the name of the credential database. The available choices depend on what is defined in the adapter, such as Account (for TL1 and CLI), SNMP, or possibly LDAP for credentials associated with a directory server., which is defined in the adapter.
Credential Type	Specific type of credential: account, snmp_read, snmp_write, or snmp_trap
Management Credential	Credentials based on whether or not they are used to connect and establish a session with an NE: True, False or All.

For a complete details on how to use searches, see the Inventory application.

Credential search results

If data mining has been performed, the database will contain credential information obtained directly from the NEs. If an unauthorized credential is found, it can be deleted. To change or delete a credential, see [“Change or delete one or more credentials on a specific network element” on page 179](#).

If data mining has not been performed, the database will only contain information about credentials that were created with the NE Security application.



Note: Network Integrity does not retrieve passwords from NEs. Passwords are only stored in the database when the NE Security application has been used to create or modify the credentials on the NEs. Passwords are stored in an encrypted format using the symmetric-key algorithm recommended by the ANS T1.276-2003 AES specification.

8.5 Managing NE security jobs

From the **Jobs** tab of the NE Security application, you can monitor all security jobs that are in progress or completed. This includes jobs to create, modify and delete credentials on network elements. Security jobs that are completed and no longer relevant can also be removed.

This section contains the following procedures:

- [“View NE Security job details” on page 184](#)
- [“Delete unwanted NE security jobs” on page 186](#)



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

Prerequisites

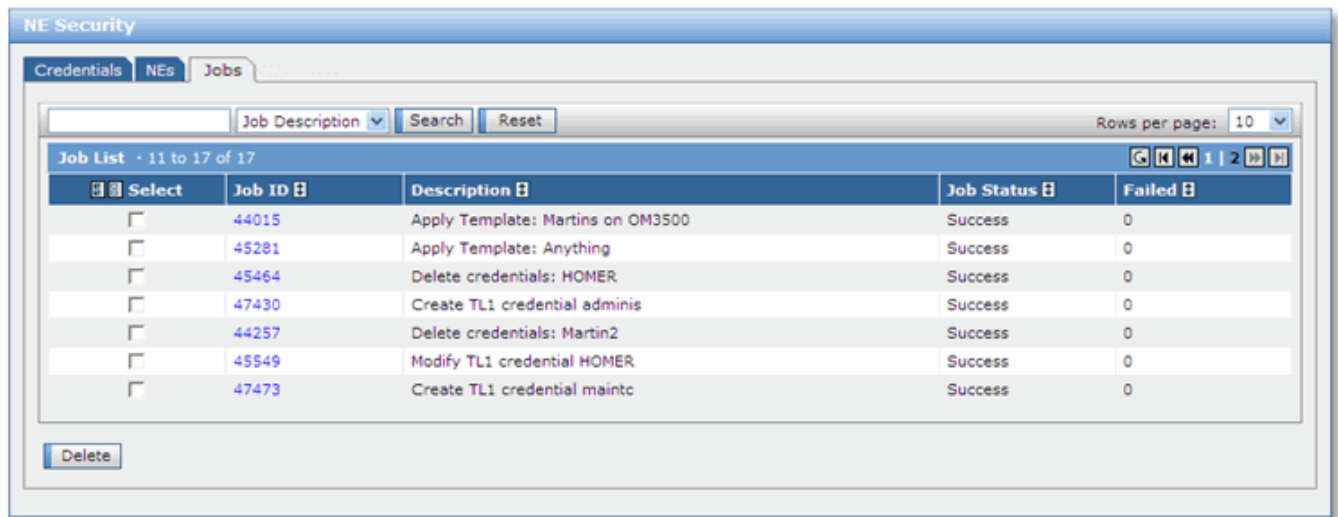
To manage NE security jobs, your user account must be assigned to the NE Security Role and have the correct permissions and NE Groups set. Without the correct permissions, you will not be able to access some or all of the features or NEs.

8.5.1 View NE Security job details

Use this procedure to view the details and status of an NE Security job. The job details show the number of NEs in progress, the number of successful credential creations or changes, and the number of failed NEs.

1. Launch **NE Security**.
2. If not already selected, click the **Jobs** tab.

The system displays the list of jobs.



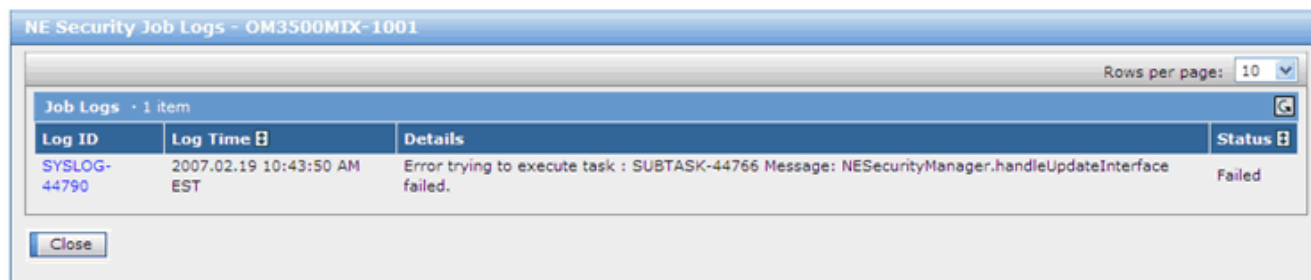
- Click the **Job ID** of the job whose details you want to view.
The system displays the NE Security Job Details screen.



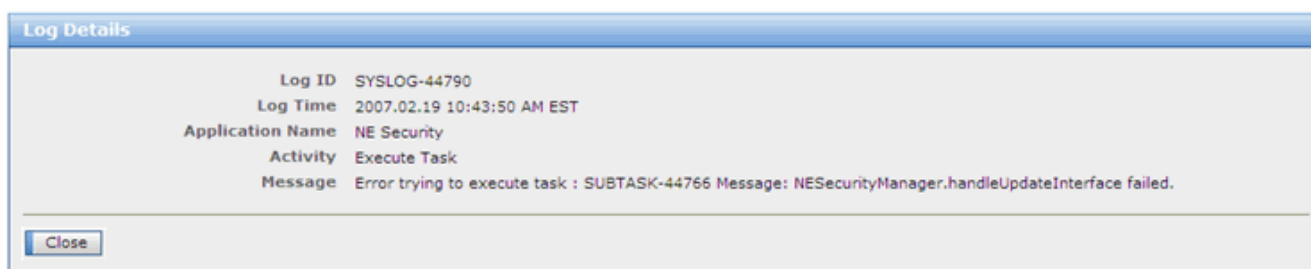
The system displays information for the selected job.

- To view additional details for a job, click the status in the Status column.

The system displays additional details.



- To display the log, click the name of the log in the Log ID column.
The system displays the log details.



- To return to the main screen, click **Close** twice.

8.5.2 Delete unwanted NE security jobs

Use this procedure to delete NE security jobs that are no longer required.



Note: The default setting automatically performs an audit every day at 2:02 AM, which deletes successful and failed jobs that are more than 30-days old. The audit does not delete Stopped or Unstarted jobs.

- Launch **NE Security**.
- If not already selected, click the **Jobs** tab.
The system displays the list of jobs.
- Select one or more jobs to be deleted, and then click **Delete**.
The system prompts for confirmation.
- Click **Delete** to confirm the operation.
The system removes the job from the list of jobs.

9 Inventory: Performing and managing searches



Note: Depending on your permissions or product configuration, some Network Integrity Framework tools may not be available or applicable.

The **Inventory** application allows you to perform searches for the following types of equipment and connection inventory that has been obtained through the NI-Framework Data Mining process:

- Physical inventory is the actual equipment resources in the managed network including the managed Network Elements, Equipment Holders (bays and shelves), Circuit Packs, Ports, Pluggable Transceiver Modules, and Interfaces.
- Logical inventory represents infrastructure resources that can be provisioned on network elements and that Network Integrity can retrieve, such as facilities, trail termination points and protection groups.
- Service inventory represents specific functionality or services that can be provisioned or configured on network elements, such as cross-connects and circuit termination points.



Note: The search procedures and techniques described in this section apply to all Network Integrity applications that provide search capabilities.

This section contains the following Inventory procedures:

“Understanding searches” on page 188

This section contains the following information about the Network Integrity search engine:

- [“About the search screens” on page 188](#)
- [“AND versus OR searches” on page 190](#)
- [“Complete list of search attributes” on page 191](#)
- [“Using wildcards in search criteria” on page 199](#)
- [“Working with table data” on page 199](#)

“Performing a search” on page 201

“Loading, saving and deleting search criteria” on page 201

“Saving search results to a file” on page 202

Prerequisites

To use the Inventory application, your user account must be assigned to the Inventory Management Role and/or the Inventory Filter Management Role and have the correct

permissions set. Without the correct permissions, you will not be able to access some or all of the features.



Note: If a Network Integrity feature is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they will know what to expect when managing network elements from the client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

9.1 Understanding searches

This section contains the following information about how to perform searches and to use wildcards in a search query.

- [“About the search screens” on page 188](#)
- [“AND versus OR searches” on page 190](#)
- [“Complete list of search attributes” on page 191](#)
- [“Using wildcards in search criteria” on page 199](#)
- [“Working with table data” on page 199](#)



Note: The search concepts and examples that are described in this section apply to all NI-Framework client applications. The search criteria may differ slightly between applications, but the selection method and use of wildcards is the same. For example, the Backup and Restore application includes general search criteria for network elements, but it also includes search criteria that applies only to backups, such as “Last Backup Result” or “Current Backup State”.

9.1.1 About the search screens

Users can search the database for physical and logical inventory data that has been obtained through the data mining process.

Figure [“Sample search criteria” on page 190](#) shows the layout of the search screen in the Inventory application, which has the following components:

- **Search Category:** displays a predefined set of common Search Attributes for Network Elements, Bays, Circuit Packs, Ports, Pluggable Transceiver Modules and Interfaces. Search attributes can be added to or removed from the predefined set by clicking the “plus” (+) or “minus” (-) icon. The Search Category appears only in the Inventory application.

- **Condition:** Specifies whether or not the search engine displays results that “Equals” or “Doesn’t Equal” the Search Value.
Note: the search Condition is not exclusive. For multiple values, such as multiple interface names on an NE, the search may return an excluded value in the results. This can occur if you perform a “doesn’t equal” search for an interface name, but the NE has multiple interfaces, such as CLI and TL1. For example, if you search for all NEs where Interface Name “doesn’t equal” CLI, the search would return an NE with the Interfaces CLI and TL1 because the NE contains at least one interface (TL1) that doesn’t equal CLI.
- **Search Value:** Defines the actual value of the attribute to be searched for using either text fields with or without wildcards, or menu selections. For more on wildcards, see [“Using wildcards in search criteria” on page 199](#).
- **Search Attributes:** (not displayed on all search screens) Specify the type of data to be searched for, such as NE Name or Channel. The Search Value provides the detail for the attribute. The initial Search Category determines which search attributes are available. The following tables explain all possible search attributes that can be selected in the Inventory application and other applications and wizards that allow searches:
 - [“Network element search attributes” on page 192](#)
 - [“Bay search attributes” on page 193](#)
 - [“Shelves search attributes” on page 194](#)
 - [“Circuit pack search attributes” on page 195](#)
 - [“Port search attributes” on page 196](#)
 - [“Pluggable transceiver modules” on page 196](#)
 - [“Interfaces search attributes” on page 198](#)
- **Add/Remove attributes:** Allows you to add or remove search attributes. Clicking the “plus” (+) icon adds another of the same attribute below the current attribute. Clicking the “minus” (-) icon removes the attribute from the search.
- **Show/Hide:** Displays or hides the search area to provide more room for the search results. Alternatively, you can click anywhere on the search bar to toggle the display.

Figure 9–1: Sample search criteria

The screenshot shows the 'Search Criteria' dialog box. It has a title bar 'Search Criteria' and a close button. Below the title bar is a dropdown menu set to 'Interfaces'. The main area contains a table with columns: 'Search Category', 'Condition', 'Search Value - field or menu', and 'Show/Hide'. The table has five rows of search criteria for 'Interfaces': 'NE Name (Network Elements)', 'Vendor/Model/Version (Network Element)', 'User Label (Interfaces)', 'Network Layer (Interfaces)', and 'Network Layer Rate (Interfaces)'. Each row has a dropdown for the search category, a dropdown for the condition (all set to 'Equals'), and a text input for the search value. To the right of each row are two buttons: a green '+' and a red '-'. At the bottom of the dialog are buttons for 'Search', 'Load Search', and 'Case Sensitive'. Annotations with arrows point to: 'Search Category' (pointing to the dropdown), 'Condition' (pointing to the 'Equals' dropdown), 'Search Value - field or menu' (pointing to the text input), 'Show/Hide' (pointing to the '+' and '-' buttons), 'Search Attributes' (pointing to the 'Interfaces' dropdown), and 'Add/Remove attributes' (pointing to the '+' and '-' buttons).

When the Search button is clicked, the system returns all search results that match the query.



Note: Searches are not case sensitive. A search does not differentiate between upper-case and lower-case letters in search values. For example “ACME” will yield the same search results as “acme”. If you require the search to be case sensitive, select the “Case Sensitive” option.

9.1.2 AND versus OR searches

For a search attribute that has multiple values, such as Vendor/Model/Version, the search engine performs an AND operation on the values. For example, the search results will contain all entries that contain vendor “Acme”, AND model “WonderNode”, AND version “8.1”, but will not include other attribute values.

The screenshot shows the 'Search Criteria' dialog box with the 'Vendor/Model/Version (Network Element)' search category selected. The search value field is divided into three sections: 'Ame', 'WonderNode', and '8.1', separated by red '+' signs. A red oval highlights these three sections, and the text 'AND operation' is written in red below the oval. The dialog also shows the 'Search', 'Load Search', and 'Case Sensitive' buttons at the bottom.

For multiple entries of different attributes, the search engine performs an AND operation. For example, if you enter NE Name: “Acme”, Agent Group: “Group1”, with

Location: “East”, the search results will contain all entries that contain “Acme” AND “Group1” AND “East”, but will not include other attribute values.

The screenshot shows the 'Search Criteria' dialog box with the 'Network Elements' dropdown selected. Three search criteria are listed, each with a dropdown menu, a comparison operator, and a value. The criteria are: 'NE Name (Network Elements)' with 'Equals' and 'Acme'; 'Agent Group Name (Network Elements)' with 'Equals' and 'Group1'; and 'Location (Network Elements)' with 'Equals' and 'East'. A red oval highlights the three criteria, and the text 'AND operation' is written in red to the right of the oval.

For multiple entries of the same search attribute, the search engine performs an OR operation. The following example shows two entries for the Commissioning State attribute, so search results will contain all entries that have a Commissioning State of “Commissioned” OR “Uncommissioned”.

The screenshot shows the 'Search Criteria' dialog box with the 'Network Elements' dropdown selected. Two search criteria are listed, each with a dropdown menu, a comparison operator, and a value. The criteria are: 'Commissioning State (Network Elements)' with 'Equals' and 'Commissioned'; and 'Commissioning State (Network Elements)' with 'Equals' and 'Uncommissioned'. A red oval highlights the two criteria, and the text 'OR operation' is written in red below the oval.

9.1.3 Complete list of search attributes

All Network Integrity applications and wizards that support searching have similar search attributes. The following sections explain all possible search attributes that can be selected in the Inventory application: NEs, Bays, Circuit Packs, Pluggable Transceiver Modules, Ports and Interfaces:

- [Inventory network element search attributes](#)
- [Inventory Bay search attributes](#)
- [Inventory Shelves search attributes](#)
- [Inventory Circuit Pack search attributes](#)
- [Inventory Port search attributes](#)
- [Inventory Pluggable Transceiver Module search attributes](#)
- [Inventory interfaces search attributes](#)

Inventory network element search attributes

The [Network element search attributes](#) table lists all search attributes that are associated with network elements.

Table 9–1: Network element search attributes

Attribute	Searches for
Adapter Name	NEs that match the adapter name that “Equals” or “Doesn’t Equal” the selection from the menu of installed adapters.
Agent Group Name	NEs that match an agent group name that “Equals” or “Doesn’t Equal” the value you type in the field.
Agent Name	NEs that match an agent name that “Equals” or “Doesn’t Equal” the value you type in the field.
Alias	NEs that match an alias that “Equals” or “Doesn’t Equal” the string you type in the field.
CLLI	NEs that match a Common Language Location Identifier (CLLI) that “Equals” or “Doesn’t Equal” the string you type in the field.
Configuration State	Equipment with a specific commissioning state that “Equals” or “Doesn’t Equal” the value you select from the menu, such as Commissioned, Uncommissioned, etc. The commissioning states that appear in the menu will depend on the states that have been created.
Gateway IP Address	Searches for a gateway network element based on the IP address of the access point that “Equals” or “Doesn’t Equal” the address you type in the field.
Location	NEs that match a location identifier that “Equals” or “Doesn’t Equal” the value you type in the field.
Management State	NEs that are in a management state that “Equals” or “Doesn’t Equal” the state you select from the menu: Managed, Under Test, or Unmanaged.
Manufacture Date	NEs that match a manufacturing date that “Equals” or “Doesn’t Equal” the value you type in the field. You will need to know the convention used by the manufacturer, such as yyyy/mm/dd or Month, Day, Year.
Model	NEs that match a model that “Equals” or “Doesn’t Equal” the string you type in the field.
NE Group Name	NEs that match a network element group that “Equals” or “Doesn’t Equal” the string you type in the field.
NE Name	NEs that match a network element name that “Equals” or “Doesn’t Equal” the string you type in the field, such as the TID.
NE Type	NEs that match a network element type that “Equals” or “Doesn’t Equal” the string you type in the field.
Native Name	NEs that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Software Version	NEs that match a software version that “Equals” or “Doesn’t Equal” the string you type in the field.
Vendor	NEs that match a vendor that “Equals” or “Doesn’t Equal” the string you type in the field.

Attribute	Searches for
Vendor/Model/Version	NEs that match the vendor and model and version that “Equals” or “Doesn’t Equal” the values selected from the menus.
X Coordinate	NEs that match one coordinate (X) of the physical location of an NE that “Equals” or “Doesn’t Equal” the value you type in the field, such as a longitude.
Y Coordinate	NEs that match one coordinate (Y) of the physical location of an NE that “Equals” or “Doesn’t Equal” the value you type in the field, such as such a latitude.

Inventory Bay search attributes

The Bay search attributes include many of the attributes listed in the [Network element search attributes](#) table plus the attributes listed in the [Bay search attributes](#) table.

Table 9–2: Bay search attributes

Attribute	Searches for
Administrative State	Bays with an administrative state that “Equals” or “Doesn’t Equal” the value you select from the menu: Locked, Shutting Down, Unlocked, or Unknown.
CLEI	Bays that match a Common Language Equipment Identifier (CLEI) that “Equals” or “Doesn’t Equal” the string you type in the field.
Firmware Version	Bays with a specific version of firmware that “Equals” or “Doesn’t Equal” the value you type in the field.
Hardware Version	Bays with a specific version of hardware that “Equals” or “Doesn’t Equal” the value you type in the field.
Holder State	Bays with a holder state that “Equals” or “Doesn’t Equal” the value you select from the menu: Empty, Expected and not installed, Installed and Expected, Installed and Not Expected, Mismatched, N/A, Unavailable, Unknown.
Location	Bays that match a location identifier that “Equals” or “Doesn’t Equal” the value you type in the field.
Manufacture Date	Bays that match a manufacturing date that “Equals” or “Doesn’t Equal” the value you type in the field. You will need to know the convention used by the manufacturer, such as yyyy/mm/dd or Month, Day, Year.
Native Name	Bays that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Operational State	Bays that are in an operational state that “Equals” or “Doesn’t Equal” the state you select from the menu: Disabled, Enabled or Unknown.
Part Number	Bays that match the part number that “Equals” or “Doesn’t Equal” the value typed in the field.
Resource Type	Bays that match the resource type that “Equals” or “Doesn’t Equal” the value typed in the field.

Attribute	Searches for
Serial Number	Bays that match the serial number that “Equals” or “Doesn’t Equal” the value typed in the field.
User Label	Bays with a label assigned by a user, that “Equals” or “Doesn’t Equal” the value you type in the field.
Vendor	Bays that match the vendor that “Equals” or “Doesn’t Equal” the value typed in the field.

Inventory Shelves search attributes

The Shelves search attributes include many of the attributes listed in the [Network element search attributes](#) table plus the attributes listed in the [Shelves search attributes](#) table.

Table 9–3: Shelves search attributes

Attribute	Searches for
Administrative State	Shelves with an administrative state that “Equals” or “Doesn’t Equal” the value you select from the menu: Locked, Shutting Down, Unlocked, or Unknown.
CLEI	Shelves that match a Common Language Equipment Identifier (CLEI) that “Equals” or “Doesn’t Equal” the string you type in the field.
Firmware Version	Shelves with a firmware version that “Equals” or “Doesn’t Equal” the string you type in the field.
Hardware Version	Shelves with a hardware version that “Equals” or “Doesn’t Equal” the string you type in the field.
Location	Shelves that match a location identifier that “Equals” or “Doesn’t Equal” the value you type in the field.
Manufacture Date	Shelves that match a manufacturing date that “Equals” or “Doesn’t Equal” the value you type in the field. You will need to know the convention used by the manufacturer, such as yyyy/mm/dd or Month, Day, Year.
Native Name	Shelves that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Operational State	Shelves that are in an operational state that “Equals” or “Doesn’t Equal” the state you select from the menu: Disabled, Enabled or Unknown.
Part Number	Shelves that match a part number that “Equals” or “Doesn’t Equal” the value you type in the field.
Resource Type	Shelves that match the resource type that “Equals” or “Doesn’t Equal” the value typed in the field.

Attribute	Searches for
Serial Number	Shelves with a serial number that “Equals” or “Doesn’t Equal” the value you type in the field.
User Label	Shelves with a label assigned by a user, that “Equals” or “Doesn’t Equal” the value you type in the field.
Vendor	Shelves that match the vendor that “Equals” or “Doesn’t Equal” the value typed in the field.

Inventory Circuit Pack search attributes

The Circuit Pack search attributes include many of the attributes listed in the [Network element search attributes](#) table plus the attributes listed in the [Circuit pack search attributes](#) table.

Table 9–4: Circuit pack search attributes

Attribute	Searches for
Administrative State	Circuit packs that have an administrative state that “Equals” or “Doesn’t Equal” the value you select from the menu: Unknown, Locked, Unlocked or Shutting Down.
CLEI	Circuit packs that have a Common Language Equipment Identifier (CLEI) that “Equals” or “Doesn’t Equal” the string you type in the field.
Expected Circuit Pack Type	Circuit packs that match an expected type that “Equals” or “Doesn’t Equal” the string you type in the field, such as OC48S or LANGSD3.
Firmware Version	Circuit packs with a firmware version that “Equals” or “Doesn’t Equal” the string you type in the field.
Hardware Version	Circuit packs with a hardware version that “Equals” or “Doesn’t Equal” the string you type in the field.
Installed Circuit Pack Type	Circuit packs that match an installed type that “Equals” or “Doesn’t Equal” the string you type in the field, such as OC48S or LANGSD3.
Manufacture Date	Circuit packs that match a manufacturing date that “Equals” or “Doesn’t Equal” the value you type in the field. You will need to know the convention used by the manufacturer, such as yyyy/mm/dd or Month, Day, Year.
Native Name	Circuit Packs that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Operational State	Circuit packs in an operational state that “Equals” or “Doesn’t Equal” the state you select from the menu: Disabled, Enabled or Unknown.
Part Number	Circuit packs that match a part number that “Equals” or “Doesn’t Equal” the value you type in the field.
Serial Number	Circuit packs with a serial number that “Equals” or “Doesn’t Equal” the value you type in the field.

Attribute	Searches for
Software Version	Circuit packs with a software version that “Equals” or “Doesn’t Equal” the value you type in the field.
User Label	Circuit packs with a label assigned by a user, that “Equals” or “Doesn’t Equal” the value you type in the field.
Vendor	Circuit packs that match the vendor that “Equals” or “Doesn’t Equal” the value typed in the field.

Inventory Port search attributes

The Port search attributes include many of the attributes listed in the [Network element search attributes](#) table plus the attributes listed in the [Port search attributes](#) table.

Table 9–5: Port search attributes

Attribute	Searches for
Administrative State	Ports that have an administrative state that “Equals” or “Doesn’t Equal” the value you select from the menu: Unknown, Locked, Unlocked or Shutting Down.
Holder State	Ports that have a holder state that “Equals” or “Doesn’t Equal” the value you select from the menu: Empty, Expected and Not Installed, Installed and Expected, Installed and Not Expected, Mismatch, N/A, Unavailable, or Unknown.
Native Name	Ports that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Operational State	Ports in an operational state that “Equals” or “Doesn’t Equal” the state you select from the menu: Disabled, Enabled or Unknown.
Port Type	Ports that match a port type that “Equals” or “Doesn’t Equal” the value you type in the field.
User Label	Ports with a label assigned by a user, that “Equals” or “Doesn’t Equal” the value you type in the field.

Inventory Pluggable Transceiver Module search attributes

The Pluggable Transceiver Module search attributes include many of the attributes listed in the [Network element search attributes](#) table plus the attributes listed in the [Pluggable transceiver modules](#) table.

Table 9–6: Pluggable transceiver modules

Attribute	Searches for
Administrative State	Modules that have an administrative state that “Equals” or “Doesn’t Equal” the value you select from the menu: Unknown, Locked, Unlocked or Shutting Down.
CLEI	Modules that have a Common Language Equipment Identifier (CLEI) that “Equals” or “Doesn’t Equal” the string you type in the field.

Attribute	Searches for
Expected Module Type	Modules that match an expected type that “Equals” or “Doesn’t Equal” the string you type in the field.
Firmware Version	Modules with a firmware version that “Equals” or “Doesn’t Equal” the string you type in the field.
Hardware Version	Modules with a hardware version that “Equals” or “Doesn’t Equal” the string you type in the field.
Installed Module Type	Modules that match an installed type that “Equals” or “Doesn’t Equal” the string you type in the field.
Manufacture Date	Modules that match a manufacturing date that “Equals” or “Doesn’t Equal” the value you type in the field. You will need to know the convention used by the manufacturer, such as yyyy/mm/dd or Month, Day, Year.
Native Name	Modules that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Operational State	Modules in an operational state that “Equals” or “Doesn’t Equal” the state you select from the menu: Disabled, Enabled or Unknown.
Part Number	Modules that match a part number that “Equals” or “Doesn’t Equal” the value you type in the field.
Serial Number	Modules with a serial number that “Equals” or “Doesn’t Equal” the value you type in the field.
User Label	Modules with a label assigned by a user, that “Equals” or “Doesn’t Equal” the value you type in the field.
Vendor	Modules that match the vendor that “Equals” or “Doesn’t Equal” the value typed in the field.

Inventory interfaces search attributes

The Interface search attributes include many of the attributes listed in the [Network element search attributes](#) table plus the attributes listed in the [Interfaces search attributes](#) table.

Table 9–7: Interfaces search attributes

Attribute	Searches for
Administrative State	Interfaces that have an administrative state that “Equals” or “Doesn’t Equal” the value you select from the menu: Unknown, Locked, Unlocked or Shutting Down.
Channel	Interfaces that match a channel number that “Equals” or “Doesn’t Equal” the value you type in the field.
Expected Trace	Interfaces that have an expected trace message in the control channel that “Equals” or “Doesn’t Equal” the string you type in the field. (Some network layers allow a trace message to be transmitted in the control channel. The 'Expected Trace' contains the message that is expected to be received by this interface. Values for the trace fields are defined only if they are applicable for the layer.)
Far-End Source	Interfaces that match the source of the far-end that “Equals” or “Doesn’t Equal” the value, such as Network or user, as set through the NI-Director Operations Console).
Far-End Source Details	Interfaces that match the far-end source detail that “Equals” or “Doesn’t Equal” the string typed in the field, such as: "Matched trace: transmitted and received trace" for a network source.
Far-End Update Time	Interfaces that match the time that “Equals” or “Doesn’t Equal” the far-end information that was last set either by discovery or the user.
Inward Facing	Interfaces that are or are not inward facing. This attribute “Equals” or “Doesn’t Equal” Yes (are inward) or No (are not).
Monitor Only	Interfaces that are not actually terminating the transmission path, but providing the capability of monitoring some characteristics of the path (PM, trace, etc.). An example is an NE that may monitor SONET section overhead on the signals it receives, but doesn't actually terminate the SONET section. This attribute “Equals” or “Doesn’t Equal” true or false.
Native Name	Interfaces that match a native name that “Equals” or “Doesn’t Equal” the string you type in the field. The native name is the name data-mined from the NE.
Network Layer	Interfaces that match the layer that “Equals” or “Doesn’t Equal” the value, such as Ethernet, SONET Section, VCAT, etc.
Network Layer Rate	Interfaces that match the rate that “Equals” or “Doesn’t Equal” the value, such as 10 Gig Ethernet, OC-192, T3, etc.
Received Trace	Interfaces that have a received trace message in the control channel that “Equals” or “Doesn’t Equal” the string you type in the field.

Attribute	Searches for
Traffic Direction	Interfaces that match the direction of traffic that “Equals” or “Doesn’t Equal” the value, such as Unidirectional, Bidirectional, Sink or Source.
Transmitted Trace	Interfaces that have a transmitted trace message in the control channel that “Equals” or “Doesn’t Equal” the string you type in the field.
User Label	Interfaces with a label assigned by a user, that “Equals” or “Doesn’t Equal” the value you type in the field.

9.1.4 Using wildcards in search criteria

You can use the following wildcards when you type search criteria into text fields:

- An asterisk (*) wildcard matches any number of characters. This means that you can use it as a placeholder for any sequence of characters. For example, if you type Acme* as a search value, the search results will include AcmeABC and Acme123. If you searched for *Node, the search results will include SuperNode and WonderNode.
- The question mark (?) wildcard matches exactly one character. This means that you can use it as a placeholder for a single character. For example, if you type v?_1, the search results will include v6_1 and v5_1, but not v12_1.

9.1.5 Working with table data

In the table of search results, you can perform a number of tasks to organize and change the appearance and content of the table data. Columns can be sorted, added and removed, rearranged, and scrolled, as described in this section. Actions that can be performed on the Inventory search results table, can also be performed within other applications.

- [“Refresh” on page 199](#)
- [“Sort table data” on page 199](#)
- [“Add or remove columns in a table” on page 200](#)

Refresh

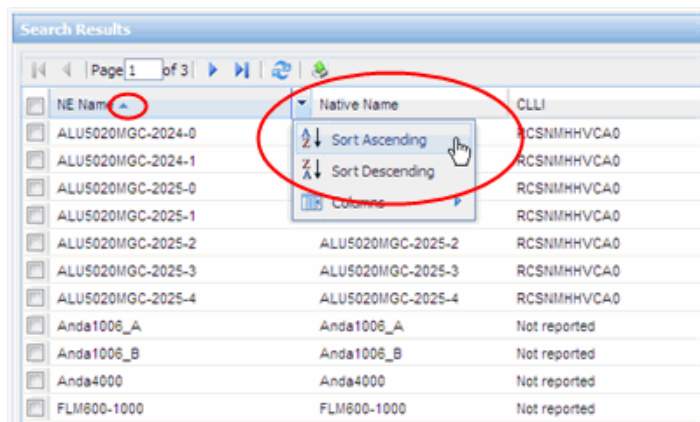
By default, the table data does not refresh automatically. If you want the table data to refresh, select the desired interval:

- Auto-Refresh Off (default)
- Every 30 seconds
- Every 1 minute
- Every 5 minutes

Sort table data

Data within a table column can be sorted in ascending order (A to Z) or descending order (Z to A). The system does not differentiate between upper-case and lower-case letters.

To sort a column of data, click on the column heading and select the desired sort order. An up-arrow or down-arrow also appears in the column header to indicate the current sort order (up=ascending, down=descending).



Rows are sorted according to the order that the columns are selected. For example, if a user wants to sort on Model first, then NE Name within Model, the user must first sort on the Model column, and then sort on the NE Name column.

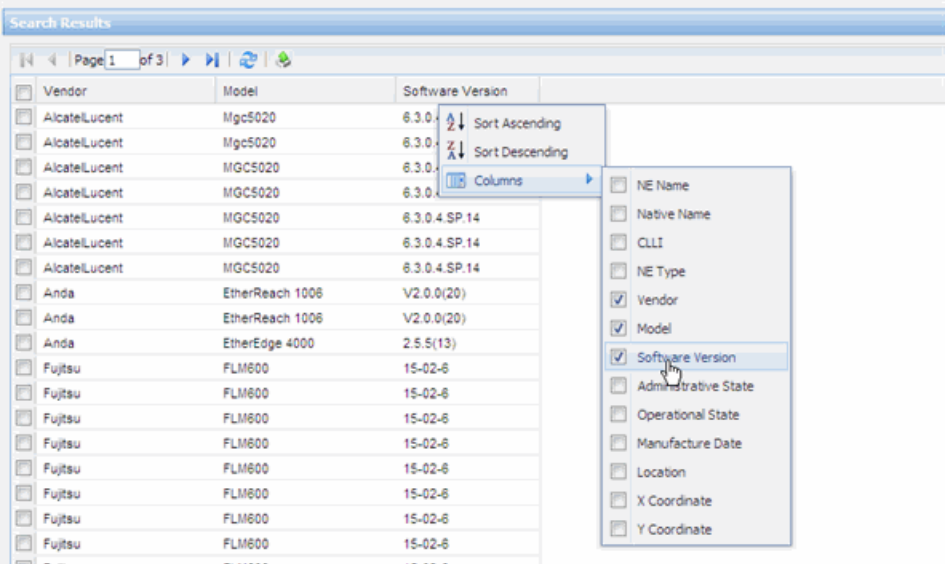
Add or remove columns in a table

Columns can be added or removed from the search results table to provide a customized view of the data.



Note: If you are going to save the table data to a file, only the information from the displayed columns will be saved.

To remove columns from the table, click any column heading and select **Columns** followed by the name of the columns to be added or removed. Remove the check mark to remove the column from the table. Place a check mark to add the column to the table.

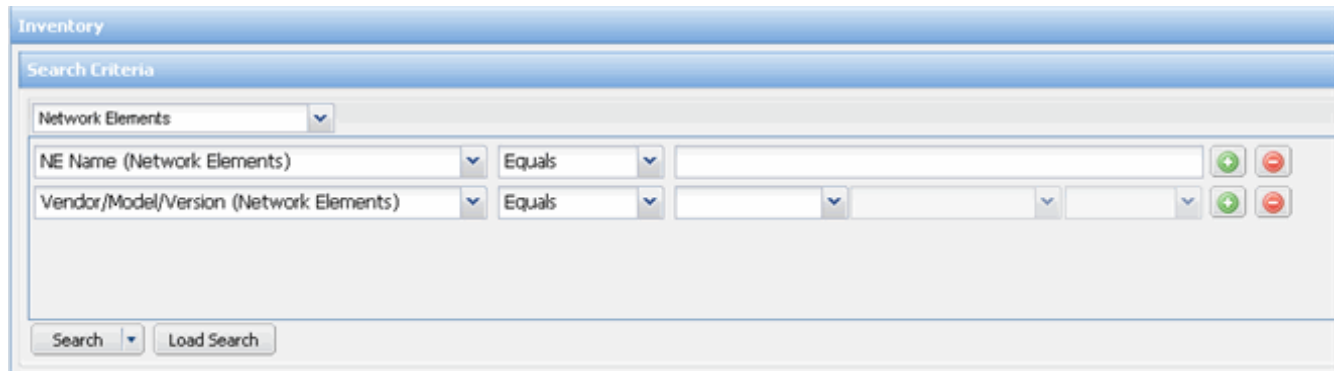


9.2 Performing a search

Use this procedure to locate one or more NEs based on the desired search criteria and display the search results.

1. Launch **Inventory**.

The system displays the default search screen.

The screenshot shows a software window titled "Inventory". Inside, there is a section labeled "Search Criteria". At the top of this section is a dropdown menu currently set to "Network Elements". Below this, there are two rows of search criteria. The first row has a dropdown for "NE Name (Network Elements)", followed by a dropdown for "Equals", and then a text input field. The second row has a dropdown for "Vendor/Model/Version (Network Elements)", followed by a dropdown for "Equals", and then a text input field. To the right of each text input field are two small circular buttons, one green with a plus sign and one red with a minus sign. At the bottom of the "Search Criteria" section, there are two buttons: "Search" and "Load Search".

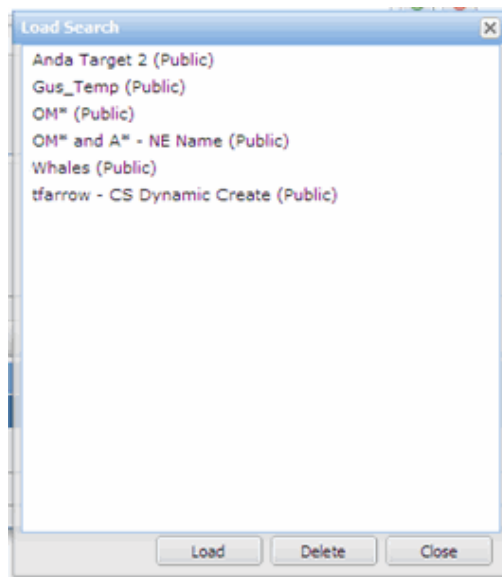
2. Define the search criteria to find the NEs associated with the deployed adapter. For more details about how to perform searches, see [“Understanding searches” on page 188](#).
3. To view the details of an NE, right-click and select **Show Details**.
The system displays the NE Details in a pop-up window.

9.3 Loading, saving and deleting search criteria

Each application that supports searches, such as the Fault Manager, provides authorized users with buttons to load previously defined search queries and to save search queries for future use.

- **Load Search:** This button, which is found on application search screens, allows authorized users to select from a list of searches that have been previously saved.

To load a search, select it in the Load Search window and then click the **Load** button.



- To delete a saved search, select it in the Load Search window and then click **Delete**. You can delete public searches or your own private searches, but not private searches created by other users.
- **Save Search:** This button, which is found on most application search screens, allows authorized users to save searches that are for Public or Private use:
 - **Public:** all users can load the search
 - **Private:** only the user who created the search can load it

9.4 Saving search results to a file

Use this procedure from any search results screen to export the search results data to one of the following file formats (depending on the data, some formats may not be available):

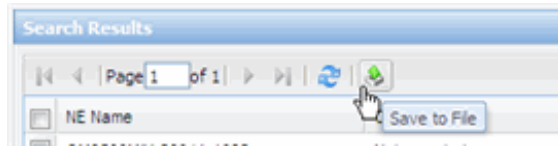
- Portable Document Format (.PDF)
- Comma Separated Values (.CSV)
- Tab Separated Values (.TSV)
- Single-Sheet Excel Spreadsheet (.XLS)
- Rich Text Format (.RTF)
- Hyper Text Markup Language (.HTML)

The columns in the saved file will correspond to the columns displayed in the search results. If you want to add or remove columns before saving, see [“Add or remove columns in a table” on page 200](#).

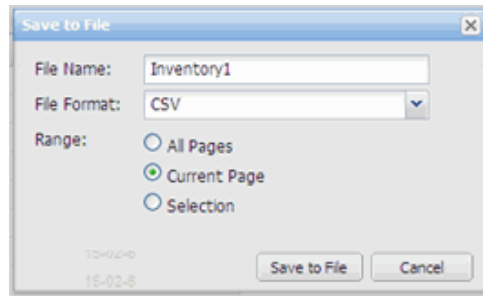
When saving you have the following options:

- **All Pages:** saves all data pages to a file
- **Current Page:** saves only the currently displayed page to a file
- **Selection:** saves results that are selected (with a check mark)

1. Launch **Inventory** and define the search criteria and perform the search.
2. At the top of the search results screen, click the **Save to File** icon.



The system displays Save to File screen.



3. In the **File Name** field, type a name to identify the file.
4. For the **File Format** menu, select either **CSV** or **TSV**.
5. Select the search results page range to be saved: **All Pages**, **Current Page**, or **Selection**.

The screen that is displayed depends on your operating system. Typically, you will be prompted to Save the file. If your system is configured for handling a CSV or TSV file association, you may have the option of launching the file in the corresponding application.

6. Select the appropriate action for the file based on how your system is configured.

10 Inventory Reports: Creating and managing inventory reporting



Note: Depending on your permissions or product configuration, some Network Integrity Framework tools may not be available or applicable.

The **Inventory Reports** application lets you can create and manage inventory reports that provide lists of Managed Elements, Equipment Holders, Circuit Packs, Ports, Pluggable Transceiver Modules, Interfaces, Equipment Protection Groups, Cross-Connections and Traffic Protection Groups in your network.

This section contains the following Inventory reporting procedures:

- [“Create an inventory reporting schedule” on page 204](#)
- [“Generate an inventory report immediately” on page 211](#)
- [“List report tasks and view or modify details” on page 213](#)
- [“Download an inventory report from the server” on page 216](#)
- [“Delete an inventory report task from the database” on page 217](#)

Prerequisites

To use the Inventory Reports application, your user account must be assigned to the Inventory Management Role and/or the Inventory Filter Management Role and have the correct permissions set. Without the correct permissions, you will not be able to access some or all of the features.



Note: If a Network Integrity feature is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of NE in question. The Adapter Notes provide important information about the applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports. You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the users so they will know what to expect when managing network elements from the client applications. Before raising a support issue against the product, be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

10.1 Create an inventory reporting schedule

Use this procedure to create an inventory reporting task, which is a schedule that defines the report criteria as shown in the table [“Inventory Report Criteria” on page 205](#).

Table 10–1: Inventory Report Criteria

Report Criteria	Description
Report Task Name	a name to identify the report
Report Format (under the Target tab in report task details)	the output format for the report: XML (Extensible Markup Language), CSV (Comma Separated Value) or TSV (Tab Separated Value)
File Server Name (under the Target tab in report task details)	the managed file server where the report will be sent
File Server Directory (under the Target tab in report task details)	the path to the directory where the report is to be stored on the file server, such as <i>inventory/reports</i> . If the directory does not exist on the server, it will be created by the system.
Report Recipients (under the Target tab in report task details)	a list of e-mail addresses that the report will be e-mailed to
Source Type (under the NEs or NE Groups tab in report task details)	the devices to include in the report
Report Content (under the Report Content tab in report task details)	the type of inventory data to include in the report: <ul style="list-style-type: none"> • Managed Element • Equipment Holder • Circuit Pack • Port • Pluggable Transceiver Module • Interface • Equipment Protection Group • Cross-Connection (When you select Cross-Connection, the system provides two reports: Cross-Connections and their associated Circuit Termination Points (CTPs)). • Traffic Protection Group (When you select Traffic Protection Group the system provides three reports: UPSR Config, PGs, and PG Members.)
Schedule (under the Schedule tab in report task details)	The frequency and schedule for the report. See the table “Inventory report schedule parameters” on page 205 .

Table 10–2: Inventory report schedule parameters

Criteria	Description
Start Date	the date on which reporting will begin.
Start Time	the start time and your time zone for the reporting.

Criteria	Description
Frequency	<p>the frequency for the reporting:</p> <ul style="list-style-type: none"> • Once: the reporting is performed only once at the specified Start Date and Start Time • Daily: the reporting is performed each day at the specified Start Time • Weekly on: the reporting is performed each week on the specified day (Sunday through Saturday) • Monthly on Day: the reporting is performed once a month on the specified day of the month. • Monthly on: the reporting is performed once a month on the (First, Second, Third or Fourth) specified day (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday or Sunday)
Status	<p>enable or disable the report</p> <ul style="list-style-type: none"> • Enable: the reporting schedule runs on the specified date and time • Disabled: the reporting schedule will not run



Note: Before using this procedure, you must follow the procedure in the NI-Framework Configuration Guide to “Configure file servers for your products” and add a local server for NI-Director.

1. Launch **Inventory Reports**.

The system displays the report search screen. (To display a list of existing reports, specify the search criteria and click **Search**).

2. Click **Create**.

The system displays Step 1 of the Create Report Task wizard.

Create Report Task

Step 1: Target Details

Report Task Name: Full Inventory *

Report Format: CSV *

File Server Name: MVEM files

File Server Directory: inventory

Rows per page: 10

Report Recipients - 1 item

Select	E-mail Address
<input type="checkbox"/>	person@telco.com

Delete Add

Next >> Cancel

3. In the corresponding fields specify the criteria listed in the table “Inventory Report Criteria” on page 205.
4. If you want the reports e-mailed, type the e-mail address of a recipient in the bottom field, and then click **Add**. To delete a recipient, select one or more from the list, and then click **Delete**.

The system adds the e-mail address to the list of Report Recipients.

Create Report Task

Step 1: Target Details

Report Task Name: Ciena NEa *

Report Format: CSV *

File Server Name: MVEM files

File Server Directory: inventory/reports

Rows per page: 10

Report Recipients - 1 item

Select	E-mail Address
<input type="checkbox"/>	person@telco.com

Delete Add

Next >> Cancel

5. Click **Next**.

The system displays Step 2 of the Create Report Task wizard, where you select the NEs or NE groups to include in the report.



6. Select the source for the report:

To	Then
specify NE Groups	select Run report on select NE Groups
specify individual NEs	select Run report on select NEs

7. Click **Next**.

If you selected	Then go to
Run report on select NE Groups	Step 8.
Run report on select NEs	Step 10.

8. From the list of Available NE Groups, select one or more groups to include in this report.

The screenshot shows the 'Create Report Task' dialog box, specifically Step 3: Select NE Groups. On the left, a navigation pane lists three steps: Step 1: Target Details, Step 2: Source Type, and Step 3: Select NE Groups. Step 3 is highlighted with a blue arrow pointing to it. The main area is divided into two sections: 'Available NE Groups' and 'Selected NE Groups'. The 'Available NE Groups' section has a 'Rows per page' dropdown set to 10 and a table with 3 items. The table has a 'Select' column with checkboxes and an 'NE Group Name' column. The items are 'Ciena 6.1', 'Ciena 6.3', and 'Rayexpress'. Below the table are 'Add' and 'Hide' buttons. The 'Selected NE Groups' section also has a 'Rows per page' dropdown set to 10 and a table with 1 item. The table has a 'Select' column with a checkbox and an 'NE Group Name' column. The item is 'All NEs'. Below the table is a 'Remove' button. At the bottom right of the dialog are '<< Back', 'Next >>', and 'Cancel' buttons.

Create Report Task

Step 1: Target Details
Step 2: Source Type
Step 3: Select NE Groups

Available NE Groups — Rows per page: 10

Available NE Groups · 3 items

Select	NE Group Name
<input type="checkbox"/>	Ciena 6.1
<input type="checkbox"/>	Ciena 6.3
<input type="checkbox"/>	Rayexpress

Add Hide

Selected NE Groups — Rows per page: 10

Selected NE Groups · 1 item

Select	NE Group Name
<input type="checkbox"/>	All NEs

Remove

<< Back Next >> Cancel

9. Click **Add** to move the groups to the Selected NE Groups list. Go to [Step 14](#).

10. Specify the search criteria to display the desired list of NEs to choose for the report.

Create Report Task

Step 1: Target Details
Step 2: Source Type
Step 3: Select NEs

Available NEs

NE Name Equals
Vendor/Model/Version Equals

☐ Case Sensitive

Rows per page: 10

Available NEs • 3 items

Select	NE Name	Vendor	Model	SW Version
<input type="checkbox"/>	OM3500-1-SP	Nortel	OPTera Metro 3500 MSP	REL1210X.AG
<input type="checkbox"/>	OM3500-3-NP	Nortel	OPTera Metro 3000 MSP Series NP	REL1210.AG
<input type="checkbox"/>	OM3500-3-SP	Nortel	OPTera Metro 3500 MSP	REL1210X.AG

Selected NEs

Rows per page: 10

Selected NEs • no entries

Select	NE Name	Vendor	Model	SW Version
No items in list!				

<< Back Next >> Cancel

11. Click **Search** to display the list of NEs.
12. From the list of **Available NEs**, select one or more NEs to include in this report.
13. Click **Add** to move the NEs to the **Selected NEs** list and repeat until the required NEs are selected.
14. Click **Next**.

The system displays the next step where you specify the report content.

15. Select one or more types of inventory data to include in the report.

16. Click **Next**.

The system displays Step 5 of the Create Report Task wizard.

17. Specify the reporting schedule as shown in the table [“Inventory report schedule parameters” on page 205](#)

18. Click **Go**.

If you created the report with the status Enabled, the report will be run automatically as scheduled.

If you created the report with the status disabled, you can [“Generate an inventory report immediately” on page 211](#) or [“List report tasks and view or modify details” on page 213](#) and change the status to Enabled so the report will run as scheduled.

10.2 Generate an inventory report immediately

Use this procedure to immediately generate a scheduled inventory report before the scheduled date and time.

1. Launch **Inventory Reports**.

The system displays the Inventory Report search and configuration screen.

To filter the list of available report tasks, type the required search criteria. You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#). If you do not enter search criteria, the system will display a list of all reports.

- **Report Task Name:** searches for reports by name
- **Frequency:** searches for reports of a certain frequency, that is one of Any, Once, Daily, Weekly, or Monthly
- **Report Format:** searches for reports of a certain format, that is one of Any, XML, TSV or CSV
- **File Server Name:** searches for reports on a specific server
- **E-mail Address:** searches for reports being sent to one or more e-mail addresses. Separate multiple entries with a semi-colon.
- **Status:** Enabled or Disabled

2. Click **Search** to display the list of available reports.

The system displays the list of reports that match the search criteria.

3. To generate a report, click the green arrow in the Run Now column for the desired report task.

The system prompts for confirmation.

4. Click **OK** to run the report.

The system will store the report on the server that was defined in the report, and if configured, will send the report to the defined e-mail recipients.

10.3 List report tasks and view or modify details

Use this procedure to display a list of all the inventory report tasks that are stored in the database. From the list of report tasks, you can select a report to view or modify the details listed in the table [“Inventory Report Criteria” on page 205](#) and [“Inventory report schedule parameters” on page 205](#).



Note: If you want inventory reports to be stored on a different file server than the one currently specified in the report, you must use the File Servers administration tool to add the new file server to the database so it is available for selection during this procedure.

1. Launch **Inventory Reports**.

The system displays the report search screen.

To filter the list of available report tasks, type the required search criteria. You can use wildcards as described in [“Using wildcards in search criteria” on page 199](#). If you do not enter search criteria, the system will display a list of all reports.

- **Report Task Name:** searches for reports by name
- **Frequency:** searches for reports of a certain frequency, that is one of Any, Once, Daily, Weekly, or Monthly
- **Report Format:** searches for reports of a certain format, that is one of Any, XML, TSV or CSV
- **File Server Name:** searches for reports on a specific server
- **E-mail Address:** searches for reports being sent to one or more e-mail addresses. Separate multiple entries with a semi-colon.
- **Status:** Enabled or Disabled

2. Click **Search** to display the list of available reports.

3. To view or modify the report details, click the name of the desired report.
- The system displays the Report Task Details screen. The following example shows the Target tab.

The screenshot shows the 'Report Task Details' window with the 'Target' tab selected. The 'Report Task Name' is 'Full Inventory'. The 'Report Format' is 'CSV', 'File Server Name' is 'MVEM files', and 'File Server Directory' is 'inventory'. The 'Report Recipients' section shows one item: 'person@telco.com'. The 'Rows per page' is set to 10. At the bottom are 'Save' and 'Cancel' buttons.

Select	E-mail Address
<input type="checkbox"/>	person@telco.com

The following example shows the NEs tab. If NE Groups had been configured for the report, the tab would be called NE Groups.

The screenshot shows the 'Report Task Details' window with the 'NEs' tab selected. The 'Report Task Name' is 'full inventory'. The 'Available NEs' section has search filters for 'NE Name' and 'Vendor/Model/Version'. The 'Selected NEs' section shows one item: 'FLM600-30097-1000' by 'Fujitsu' with model 'FLM600' and SW version '15-02-6'. The 'Rows per page' is set to 10. At the bottom are 'Save' and 'Close' buttons.

Select	NE Name	Vendor	Model	SW Version
<input type="checkbox"/>	FLM600-30097-1000	Fujitsu	FLM600	15-02-6

The following example shows the Report Content tab.

Report Task Details

Report Task Name: full inventory

Target | NEs | **Report Content** | Schedule

- ☒ Managed Element
- ☒ Equipment Holder
- ☒ Circuit Pack
- ☒ Port
- ☒ Pluggable Transceiver Module
- ☒ Interface
- ☒ Equipment Protection Group
- ☒ Cross-Connection
- ☒ Traffic Protection Group

Save Close

The following example shows the Schedule tab.

Report Task Details

Report Task Name: full inventory

Target | NEs | Report Content | **Schedule**

Start Date: June 7 2009

Start Time: 12:00 AM GMT

Frequency: ☐ Once

☐ Daily

☐ Weekly on Sunday

☒ Monthly on Day 7

☐ Monthly on Second Sunday

Status: ☒ Enabled

☐ Disabled

Save Close

4. Click the required tab to modify the report as described in the table [“Inventory Report Criteria”](#) on page 205 and [“Inventory report schedule parameters”](#) on page 205.:
5. When the desired changes have been made, click **Save** to save the changes.
If you modified the report so that the status is **Enabled**, the report will be run as scheduled.
If you created the report so that the status is **Disabled**, you can still [“Generate an inventory report immediately”](#) on page 211.

10.4 Download an inventory report from the server

Use this procedure to download an inventory report from the server. Reports are stored on the server as ZIP archives that contain individual files for each item select for the report content. These files can be opened or imported into various spreadsheet applications, such as Excel.

1. “List report tasks and view or modify details” on page 213 and search for the desired report to view.

The system displays the report.

Inventory Report

Search Criteria

Report Task Name: more*

Frequency: Any

Report Format: Any

File Server Name: Any

E-mail Address:

Status: Any

Search

Search Results

Rows per page: 10

Matching Report Tasks - 1 item

Select	Report Task Name	Frequency	Last Run	Current State	Format	Status	Run Now
<input type="checkbox"/>	more1000	Daily	2010.04.08 08:01 PM GMT	Completed	CSV	Disabled	➔

Create Delete

2. In the Current State column, click “Completed”.

The system displays the report status details.

Report Status Details

Report Name: more1000

Last Status: Completed

Format: CSV

Status: Disabled

Frequency: Daily

Total Time(minutes): 39.9863

Last Run: 2010.04.08 08:01:26 PM GMT

Last Success Run: 2010.04.08 08:41:26 PM GMT

Next Time: 2010.04.14 12:00:00 AM GMT

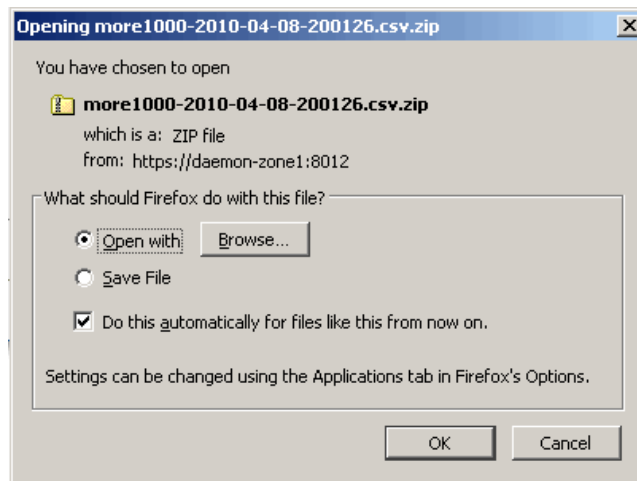
Download File

[more1000-2010-04-08-200126.csv.zip](#)

Close

3. Click the name of the desired report to be downloaded.

The system displays the file navigation screen for your computer.



4. Save or Open the file as prompted by your computer.
The ZIP archive contains files for each item.

10.5 Delete an inventory report task from the database

Use this procedure to delete an inventory report task from the database.

1. ["List report tasks and view or modify details" on page 213.](#)
2. From the list of reports, select one or more reports to be deleted.
3. Click **Delete**.
The system prompts for confirmation.
4. Click **OK** to confirm the action.
The system removes the selected reports from the database.

11 Command Broker: Configuring and managing TL1 command groups

The **Command Broker** application is used to configure TL1 Command Groups, which are lists of commands that can or can not be executed on a particular Vendor/Model/Version of network element through the NI-Director Operations Console.

This section provides the following procedures for configuring and managing the TL1 command groups:

[“About TL1 command groups” on page 220](#)

This section provides an overview of how TL1 command groups are applied when a user tries to execute a TL1 command from the NOC.

- [“How TL1 command groups are interpreted by the system” on page 220](#)
- [“About TL1 command formats” on page 223](#)
- [“About TL1 input command filtering” on page 223](#)

[“Create TL1 command groups” on page 224](#)

[“Managing TL1 command groups” on page 226](#)

This section provides the procedures for managing TL1 command groups that have already been configured.

- [“List TL1 command groups and view or modify details” on page 227](#)
- [“Copy and modify an existing TL1 command group” on page 228](#)
- [“Delete a TL1 command group” on page 229](#)

Prerequisites

To use the Command Broker application to configure TL1 command groups, your user account must be assigned to the Command Broker Administration Role and have the correct permissions set. Without the correct permissions, you will not be able to access some or all of the features.

11.1 About TL1 command groups

This section provides an overview of how TL1 command groups are applied when a user tries to execute a TL1 command from the NOC.

- [“How TL1 command groups are interpreted by the system” on page 220](#)
- [“About TL1 command formats” on page 223](#)
- [“About TL1 input command filtering” on page 223](#)

11.1.1 How TL1 command groups are interpreted by the system

TL1 Command Groups specify one or more TL1 commands that users can or can not execute through the NI-Director Operations Console. After TL1 Command Groups are defined, they are assigned to Command Broker User Roles. Users that are assigned to this role type will only be able to access the specified NEs and execute the commands that follow the rules of the assigned TL1 command groups.

The figure called [TL1 Command Groups](#) illustrates the TL1 Command Group application and filtering process. Each number in the flowchart corresponds to the text in this section that describes it in more detail.



Note: By default, the following three commands are Disallowed: "ACT-USER*", "CANC-USER*" and "*".

- 1) A NOC user selects a predefined TL1 command from a pop-up menu, or types a TL1 command in a command window. (For detailed information on how to enter TL1 commands from the NOC, see the NI-Director Operations Console User Guide or online help.)
- 2) The system checks if the NOC user has TL1 Command Groups assigned to the role. If the user's Command Broker User Role does not have TL1 Command Groups assigned to it, the three default command are Disallowed.
- 3) If the user's Command Broker User Role does have TL1 Command Groups assigned to it, the system filtering process finds the TL1 Command Group command that best matches the TL1 command using the following rules:
 - The system looks for the best match based on the number of non-asterisk characters: a matching command that has more non-asterisk "*" characters is considered a better match than a matching command with less non-asterisk "*" characters.
 - If two matching commands are identical, the one designated as "Allowed" is considered a better match. (This can occur if there are multiple TL1 Command Groups created and assigned to multiple Command Broker User Roles that are assigned to the user.)

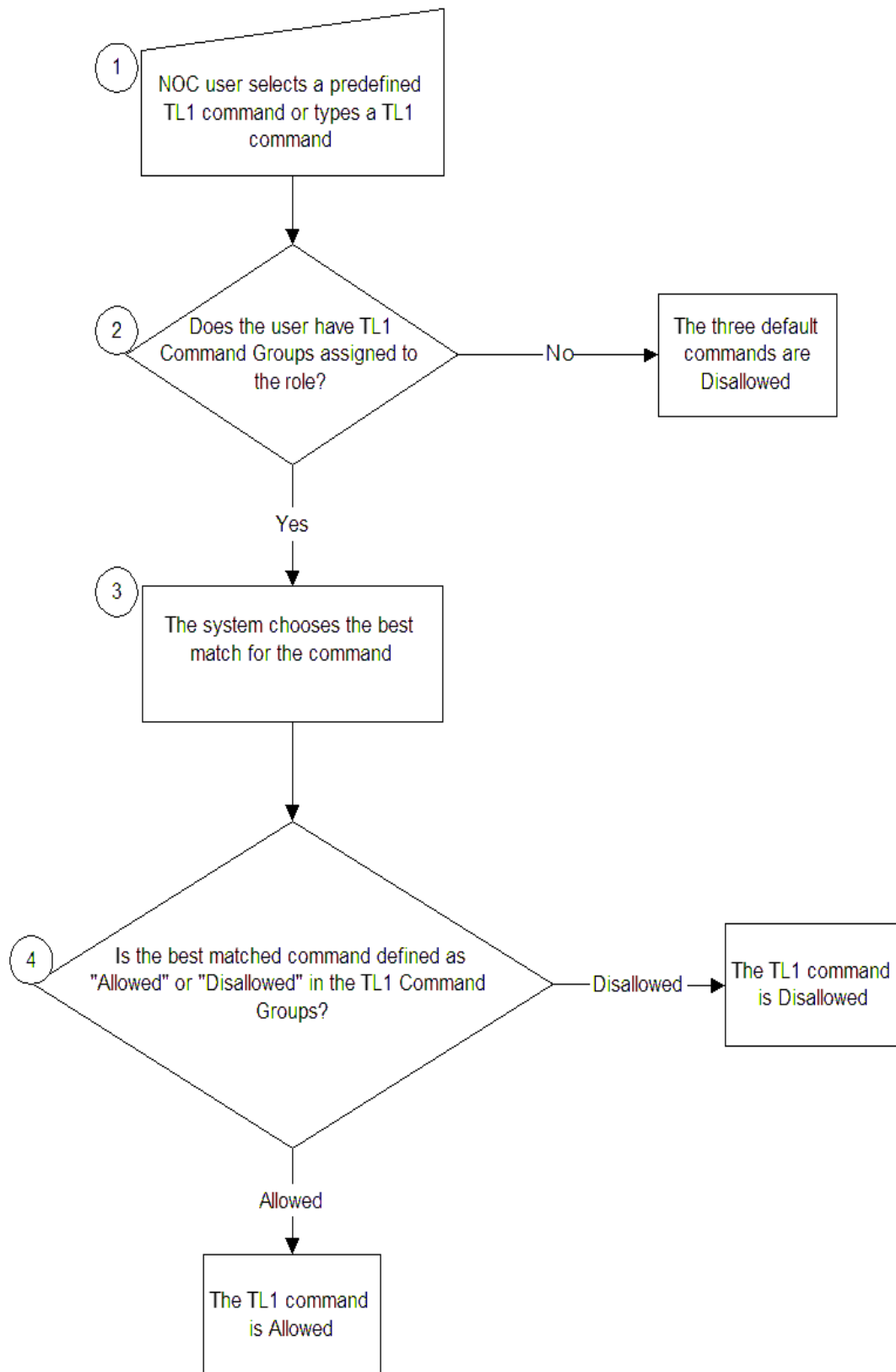


Note: To allow everything other than what is covered by more explicit commands, define the asterisk "*" command as "Allowed", which will be considered by the system to be a better match than the default "Disallowed" asterisk command "*".

4) After the system finds the best match for the command, it checks to see if it is "Allowed" or "Disallowed":

- If the best match for the command is defined as "Allowed" in the TL1 Command Group, the command is executed.
- If the best match for the command is defined as "Disallowed" in the TL1 Command Group, the command is disallowed.

Figure 11–1: TL1 Command Groups



11.1.2 About TL1 command formats

This section provides syntax information on filtering TL1 commands that can be added to TL1 Command Groups.

An asterisk “*” can be used as a wildcard at the beginning, middle, or at the end of a TL1 command string of a TL1 command group. The asterisk matches 0 or more characters within that portion of the TL1 command.

A command that is allowed overrides a command that is disallowed. For example, if ED-PID* is defined as allowed, but is also defined as disallowed, the command will be allowed.

An explicit command overrides a less specific command definition. For example, if all edit commands are allowed with ED-*, but ED-PID* is disallowed, then all commands starting with ED- will be allowed except any command starting with ED-PID. This is because ED-PID* is more explicit than ED-.*.

11.1.3 About TL1 input command filtering

The Command Broker only filters TL1 input commands on the Command Code, Staging Block and Optional General Block, but not the Payload Block. The following example explains the make-up of a TL1 command to show these filtered blocks.

A TL1 command is made up of the following four blocks:

<command code>:<staging block>:<optional general block>:<payload block>;

The following example shows a sample TL1 command:

INIT-REG-OC3:TID1:OC3-8:1234:1,09-03-17,11-22-40,Z,ID5:CVL,,NEND,RCV,ALL,ALL,ALL;

The table [Block filtering in the sample TL1 command](#) describes the filtering on the blocks in the example.

Table 11–1: Block filtering in the sample TL1 command

Block	Example	Description
command code	INIT-REG-OC3:	Filtered by Command Broker
staging block	TID1:OC3-8:1234:	In the staging block, TID1 is the TID, which is filtered by Command Broker OC3-8 is the AID, which is filtered by Command Broker 1234 is the CTAG, which is filtered by Command Broker

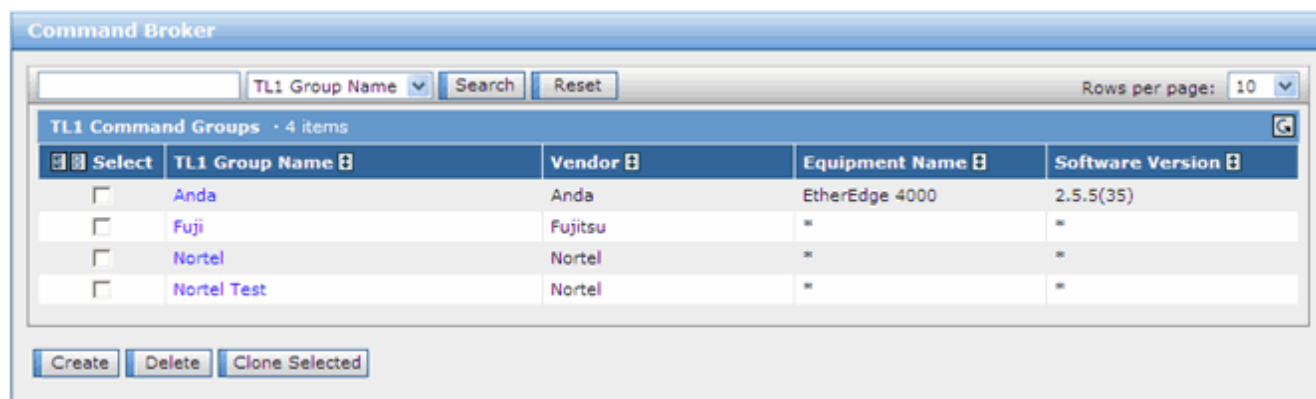
Block	Example	Description
optional general block	1,09-03-17,11-22-40,Z,ID5:	In the optional general block, 1 is the Delayed Activation Order Number, which is filtered by Command Broker 09-03-17 is the Delayed Activation Date, which is filtered by Command Broker 11-22-40 is the Delayed Activation Time, which is filtered by Command Broker Z is the Contingency Flag, which is filtered by Command Broker ID5 is the Indirect Data Retrieval Identifier, which is filtered by Command Broker
payload block	CVL,,NEND,RCV,ALL,ALL,ALL;	Not filtered by Command Broker

11.2 Create TL1 command groups

Use this procedure to create groups of TL1 commands that specify which commands users will be allowed or not allowed to enter while using the TL1 Command and Control feature of the NI-Director Operations Console.

1. Select **Applications > Command Broker**.

The system displays the Command Broker screen that lists the existing TL1 Command Groups.



2. Click **Create**.

The system displays Step 1 of the TL1 Command Group Creation wizard.

TL1 Command Group Creation Wizard

Step 1: TL1 Command Group Name

Name *

Vendor *

Equipment Model *

Software Version *

Next >> Cancel

3. In the corresponding fields, enter the Name, Vendor, Equipment Model, and Software Version of the NEs to which this TL1 Command Group will apply.
 - **Name** - the name of the NE
 - **Vendor** - NE vendor
 - **Equipment Model** - model of the NE
 - **Software Version** - software version running on the NE

The Vendor/Model/Version information that you type in the fields must exactly match the NE that is being managed. For example, if the Vendor is Acme, do not type acme. To check for the correct Vendor/Model/Version information, see [“View installed adapters, details and logs” on page 15](#) and copy the text from the Vendor/Model/Version columns. An asterisk “*” can be used as a wildcard at the beginning, middle, or at the end of a field value. The asterisk matches 0 or more characters within that portion of the field value. For example, you can type * in the Equipment Model field to represent all models of NE. You can add more than one value in a field by separating them with a comma character. For example, you can type "Acm*,Other Specific Vendor Name,a*b*c" in the Vendor field.

4. Click **Next**.

The system displays Step 2 of the TL1 Command Group Creation wizard.

TL1 Command Group Creation Wizard

Step 1: TL1 Command Group Name

Step 2: TL1 Command Group Commands

TL1 Commands - no entries

Select	Command	Allowed	Disallowed
No items in list!			

Add Delete

<< Back Go Cancel

5. Click **Add** to add a command.
6. In the **Command** field, type the name of a command that will either be allowed or disallowed on this equipment type.
For details about how TL1 commands are interpreted, see [“How TL1 command groups are interpreted by the system” on page 220](#).
7. Select either **Allowed** or **Disallowed**.
8. If you want to add more commands, repeat [Step 5](#). through [Step 7](#). for each command.
9. When you have finished entering all the commands to be allowed and disallowed on the equipment, click **Go**.

The system displays the TL1 Command Groups with the new command group added to the list.

Create or update the Command Broker User Roles

Use the User Security application to create or modify existing Command Broker User Roles and assign NE groups and TL1 Command Groups to the role. users assigned to a Command Broker User Role will only be able to access the devices in the NE groups assigned to the role, and will only be permitted to execute the commands as defined in the TL1 Command Groups assigned to the role.

11.3 Managing TL1 command groups

This section contains procedures for managing TL1 command groups that have already been configured.

- [“List TL1 command groups and view or modify details” on page 227](#)
- [“Copy and modify an existing TL1 command group” on page 228](#)
- [“Delete a TL1 command group” on page 229](#)

11.3.1 List TL1 command groups and view or modify details

Use this procedure to view a list of all TL1 Command Groups that have been created for a specific model of NE and view or modify the details.

1. Select **Applications > Command Broker**.

The system displays the Command Broker screen that lists the TL1 Command Groups.

Command Broker

TL1 Group Name Search Reset Rows per page: 10

TL1 Command Groups · no entries

Select	TL1 Group Name	Vendor	Equipment Name	Software Version
No items in list!				

Create Delete Clone Selected

2. You can filter the list by selecting the criteria **TL1 Group Name**, **Software Version**, **Equipment Name**, or **Vendor**; typing the filter term in the text field; and clicking **Search**.

3. Select the command group to be modified.

4. Click the name of the TL1 Command Group to be modified.

The system displays TL1 Command Group Details for the selected group.

TL1 Command Group Details

Name OM3000

Vendor Acme

Equipment Model Optical Metro 3000

Software Version 12.3

TL1 Commands · 4 items

Select	Command	Allowed	Disallowed
<input type="checkbox"/>	ACT-USER*	<input checked="" type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	CANC-USER*	<input checked="" type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	ED*	<input checked="" type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	ED-SECU-PID*	<input type="radio"/>	<input checked="" type="radio"/>

Add Delete

Save Close

5. In the **Name**, **Vendor**, **Equipment Model** and **Software Version** fields, modify the name and type of equipment to which this TL1 Command Group will apply.
6. In the **Command** field, type the name of a command that will either be allowed or disallowed on this equipment type.

For more information about how TL1 commands are interpreted, see [“About TL1 command formats” on page 223](#).

7. To remove allowed or disallowed commands from the group, select the command in the TL1 Commands List, and then click **Delete**.
8. When you have finished changing the desired parameters, click **Save**.
The system displays the TL1 Command Groups list.

11.3.2 Copy and modify an existing TL1 command group

Use this procedure to create a TL1 command group by copying and modifying an existing group that is similar to the group of commands you would like to create.

The TL1 command groups will be assigned to a Command Broker User role. Users that are assigned to the role will only be allowed to execute the commands specified in the assigned TL1 command groups.

You can also create a TL1 Command Group by creating the commands with the wizard. See [“Create TL1 command groups” on page 224](#).

For information about how TL1 commands are interpreted, see [“About TL1 command formats” on page 223](#) and [“About TL1 input command filtering” on page 223](#).

1. Select **Applications > Command Broker**.
The system displays the Command Broker screen that lists the TL1 Command Groups.
2. Select the command group that is the most similar to the one you would like to create.
3. Click **Clone Selected**.
The system adds a copy of the selected command group to the list of TL1 Command Groups with the prefix “Copy of”.
4. Click the name of the copied command group.
The system displays TL1 Command Group Details for the copied group.
5. In the **Name**, **Vendor**, **Equipment Model** and **Software Version** fields, modify the name and type of equipment to which this TL1 Command Group will apply.
6. In the **Command** field, type the name of a command that will either be allowed or disallowed on this equipment type.



Note: By default all commands are disallowed.

For details about how TL1 commands are interpreted, see [“About TL1 command formats” on page 223](#).

7. To remove allowed or disallowed commands from the group, select the command in the TL1 Commands List, and then click **Delete**.
8. When you have finished changing the desired parameters, click **Save** followed by **Close**.

The system displays the TL1 Command Groups with the new command group added to the list.

11.3.3 Delete a TL1 command group

Use this procedure to delete a TL1 command group from the database.

1. Select **Applications > Command Broker**.

The system displays the Command Broker screen that lists the TL1 Command Groups.

2. Select the command group to be deleted.

3. Click **Delete**.

The system prompts for confirmation.

4. Click **Ok** to confirm the operation.

The system removes the command group from the database.