Upgrading the CS 2000 Management Tools

Upgrade strategy

Upgrading CS 2000 Management Tools software occurs when a new load is delivered to the customer site. Upgrade loads are delivered on a CD-Rom. The CS 2000 Management Tools are upgraded after the CS 2000 Core Manager.

ATTENTION
Once you begin an upgrade of the CS2000 Management Tools applications, continue until you have upgraded each application to SN06.2. Failing to upgrade an application to the SN06.2 release will result in operational difficulties.

ATTENTION
The CS 2000 Core Manager must be upgraded prior to upgrading the CS 2000 Management Tools.

ATTENTION
Once the CS 2000 Core Manager (SDM) is upgraded, you cannot provision Gateway Controllers (GWCs) until the CS 2000 Management (CS2M) software package on the CS 2000 Management Tools server is upgraded to the same release.

Tools and utilities

Upgrades are performed at the CS 2000 Management Tools server. Some procedures are also performed at the CS 2000 Core Manager.

System requirements

Before you perform the CS 2000 Management Tools upgrade, ensure the Netra T1400 is at the SN06.2 Solaris platform configuration as specified below.

Component	Quantity
Base enclosure	1
Processors	2 Sparc II (440 MHz)
Memory	2 GB
Disks	4 x 36 GB
DVD-ROM (10x)	1
DAT (DDS-3)	1
Ethernet	1 x 100BaseT (on motherboard)
Quad Fast Ethernet (QFE)	1card with 4 Ethernet I/Fs

Note: Only fresh installs are supported on the Netra 240, therefore, the upgrade procedures do not apply to the Netra 240.

ATTENTION
The SSPFS must be at the latest maintenance release (MNCL) for the release you are currently running, prior to performing the upgrade procedures.

Upgrading the CS 2000 Management Tools software

You can upgrade the CS 2000 Management Tools software from the SN05, SN06, or SN06.1 release to the SN06.2 release. Refer to one of the following sections according to the release you are upgrading from:

- Upgrading from SN05 to SN06.2
- Upgrading from SN06 or SN06.1 to SN06.2

ATTENTION
Any devices put on hold using the NPM prior to the upgrade, will no longer be on hold after the upgrade. Therefore, if you want those devices to remain on hold, you need to put them back on hold after the upgrade (see procedure “Setting field values using the NPM” in document *Upgrading the Succession Network*, NN10261-450 to put devices on hold).

Upgrading from SN05 to SN06.2

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

ATTENTION

If you are upgrading from SN05 and you have the Audio Provisioning Server (APS) on a separate server from the CS 2000 Management Tools, you need to combine the servers prior to upgrading the office to the SN06.2 release. This procedure assumes that APS is on the same server as the CS 2000 Management Tools for an SN05 to an SN06.2 upgrade.

Use this table as a checklist during the upgrade. Place a check (√) in the √column as you complete each procedure.

SN05 to SN06.2 checklist

	Activities	√	Procedures
1	Back up the Oracle data on the server.		Perform procedure Performing a full backup of Oracle data on a Sun server in this document.
2	Back up the file systems on the server.		Perform procedure Performing a full backup of file systems in this document.
3	Back up the Network Patch Manager (NPM) data.		Perform procedure Saving user-defined NPM data using the NPM in this document.
			Perform procedure Saving the NPM patch files in this document.
4	Back up the Audio Provisioning Server (APS) data		Perform procedure Performing a backup of APS application files in this document.
5	Prepare for the CS 2000 SAM21 Manager data migration. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Preparing for the CS 2000 SAM21 Manager data migration in this document.

SN05 to SN06.2 checklist

	Activities	√	Procedures
6	Stop the applications on the CS 2000 Management Tools server.		Perform procedure Stopping the SESM server application in this document.
			Perform procedure Stopping the NPM server application in this document.
7	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software in this document.
8	Install any SSPFS MNCLs. ***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to.		Refer to the instructions provided with the MNCL.
9	Configure the Patching Server Element (PSE).		Perform procedure Configuring the Patching Server Element on a Sun server in this document.
10	Set up the BootP file. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Setting up the BootP file on SSPFS in this document.
11	Re-configure DCE (Distributed Computing Environment). ***Note:*** Only perform this activity if DCE is used as an authentication mechanism.		Perform procedure Unconfiguring DCE on a Sun server in this document.
			Perform procedure Configuring DCE on a Sun server in this document.

SN05 to SN06.2 checklist

	Activities	√	Procedures
12	Install an HTTPS certificate. ***Note:*** Only perform this activity if you want to use HTTPS. Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the CS 2000 Management Tools Configuration Management document, NN10106-511, if required).		Perform procedure Installing an HTTPS certificate on a Sun server in this document.
13	Configure the Apache Server ***Note:*** Only perform this activity if STORage Management (STORM) units are configured in your network.		Perform procedure Configuring the Apache Web Server for HTTPS proxy in this document.
14	Install the CS 2000 Management Components (CS2M) software package.		Perform procedure Installing or upgrading the CS2M software in this document
15	Initialize the NPM database.		Perform procedure Initializing the NPM database in this document.
16	Set up users with user group access.		Perform procedure Setting up users on a Sun server in this document.
17	Start the applications on the CS 2000 Management Tools server.		Perform procedure Starting the SESM server application in this document.
			Perform procedure Starting the NPM server application in this document.

SN05 to SN06.2 checklist

	Activities	√	Procedures
18	Configure the NPM for automatic patch file delivery. ***Note:*** Only perform this activity if you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS).		Perform procedure Configuring NPM for automatic patch file delivery in this document.
19	Restore NPM data.		Perform procedure Restoring NPM data in this document.
20	Configure QCA.		Perform procedure Modifying the QoS Collector Application in this document.
21	Install the QCA software package on a separate server. ***Note:*** This activity is optional if you want redundancy. You must have another server that is running the SN06.2 release of SSPFS.		Perform procedure Installing the QCA software package on a separate server
22	Upgrade the Audio Provisioning Server (APS) software.		Perform procedure Upgrading APS software in this document.
23	Configure the APS SNMP agent.		Perform procedure Configuring the SNMP agent in this document.
24	Migrate the SAM21 Manager data from the CS 2000 Core Manager to the CS 2000 Management Tools server. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Migrating the CS 2000 SAM21 Manager data in this document.

SN05 to SN06.2 checklist

	Activities	√	Procedures
25	Install the SAM21 platform fileset on the CS 2000 Core Manager. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Installing SAM21 fileset in this document.
26	Start the SAM21 Manager server application that resides on the CS 2000 Management Tools server. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Starting the SAM21 Manager server application in this document.
27	Apply all of the released patches that are available for the following OAM devices: PSE, SESM, SAM21 Manager, and NPM. Apply all patches to all devices, then restart each device, one at a time, starting with the PSE. ***Note:*** You must restart each OAM device after applying the patches to that device. The restart takes the application out of service temporarily, then returns the application to service.		Perform procedure Transferring patches to the NPM database manually in this document.
			Perform procedure Applying patches using the NPM in this document.
			Perform procedure Restarting a device using the NPM in this document.

SN05 to SN06.2 checklist

	Activities	√	Procedures
28	Launch the CS 2000 SAM21 Manager client application that resides on the CS 2000 Management Tools server. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Launching CS 2000 Management Tools client applications in this document. ***Note:*** Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 must be installed. The "Client Software Install Guide" link on the launch page, provides instructions on how to verify the version, and provides the installation packages and instructions, if required. The user who installs JWS and JRE must have admin privileges on the client workstation.
29	Upgrade the shelf controllers to SN06.2 for all shelves using the CS 2000 SAM21 Manager client that resides on the CS 2000 Core Manager. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Upgrading software on the shelf controller in this document.
30	Migrate all the SAM21 shelves to the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server in this document.
31	Complete the SAM21Manager migration, which includes removing the SAM21 Manager fileset from the CS 2000 Core Manager. ***Note:*** Only perform this activity if the CS 2000 SAM21 Manager is in your network.		Perform procedure Completing the CS 2000 SAM21 Manager migration in this document.

SN05 to SN06.2 checklist

	Activities	√	Procedures
32	Back up the SN06.2 CS 2000 Management Tools server.		Perform procedure Performing a full backup of Oracle data on a Sun server in this document.
			Perform procedure Performing a full backup of file systems in this document.
			Perform procedure Performing a backup of APS application files in this document.
33	Verify the upgrade was successful.		Perform procedure Verifying the upgrade was successful in this document.

Upgrading from SN06 or SN06.1 to SN06.2

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use this table as a checklist during the upgrade. Place a check (√) in the √column as you complete each procedure.

SN06 or SN06.1 to SN06.2 checklist

	Activities	√	Procedures
1	Back up the Oracle data on the server.		Perform procedure Performing a full backup of Oracle data on a Sun server in this document.
2	Back up the file systems on the server.		Perform procedure Performing a full backup of file systems in this document.
3	Back up the Network Patch Manager (NPM) data.		Perform procedure Saving user-defined NPM data using the NPM in this document.
			Perform procedure Saving the NPM patch files in this document.
4	Back up the Audio Provisioning Server (APS) data		Perform procedure Performing a backup of APS application files in this document.

SN06 or SN06.1 to SN06.2 checklist

	Activities	√	Procedures
5	Stop the applications on the CS 2000 Management Tools server.		Perform procedure Stopping the SESM server application in this document.
			Perform procedure Stopping the NPM server application in this document.
6	Upgrade the Succession Server Platform Foundation Software (SSPFS).		Perform procedure Upgrading SSPFS software in this document.
7	Install any SSPFS MNCLs. ***Note:*** Only perform this activity if you received a notification bulletin that an SSPFS MNCL is available for the release you just upgraded to.		Refer to the instructions provided with the MNCL.
8	Configure the Patching Server Element (PSE).		Perform procedure Configuring the Patching Server Element on a Sun server in this document.
9	Re-configure DCE (Distributed Computing Environment). ***Note:*** Only perform this activity if DCE is used as an authentication mechanism.		Perform procedure Unconfiguring DCE on a Sun server in this document.
			Perform procedure Configuring DCE on a Sun server in this document.

SN06 or SN06.1 to SN06.2 checklist

	Activities	√	Procedures
10	Install an HTTPS certificate. ***Note:*** Only perform this activity if HTTPS was not previously installed. An existing HTTPS certificate is maintained over the upgrade. Installing an HTTPS certificate requires that Domain Name Service (DNS) be turned on (refer to procedure "Configuring Domain Name Service" in the CS 2000 Management Tools Configuration Management document, NN10106-511, if required).		Perform procedure Installing an HTTPS certificate on a Sun server in this document.
11	Configure the Apache Server ***Note:*** Only perform this activity if STORage Management (STORM) units are configured in your network.		Perform procedure Configuring the Apache Web Server for HTTPS proxy in this document.
12	Upgrade the CS 2000 Management Components (CS2M) software package.		Perform procedure Installing or upgrading the CS2M software in this document
13	Initialize the NPM database.		Perform procedure Initializing the NPM database in this document.
14	Set up users with user group access. ***Note:*** Only perform this activity if you are adding new users. Existing users are maintained over the upgrade.		Perform procedure Setting up users on a Sun server in this document.

SN06 or SN06.1 to SN06.2 checklist

	Activities	√	Procedures
15	Start the applications on the CS 2000 Management Tools server.		Perform procedure Starting the SESM server application in this document.
			Perform procedure Starting the NPM server application in this document.
			Perform procedure Starting the SAM21 Manager server application in this document.
16	Configure the NPM for automatic patch file delivery. ***Note:*** Only perform this activity if you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS).		Perform procedure Configuring NPM for automatic patch file delivery in this document.
17	Restore NPM data.		Perform procedure Restoring NPM data in this document.
18	Intall the QCA software package on a separate server. ***Note:*** This activity is optional if you want redundancy. You must have another server that is running the SN06.2 release of SSPFS.		Perform procedure Installing the QCA software package on a separate server
19	Upgrade the Audio Provisioning Server (APS) software.		Perform procedure Upgrading APS software in this document.
20	Configure the APS SNMP agent.		Perform procedure Configuring the SNMP agent in this document.

SN06 or SN06.1 to SN06.2 checklist

	Activities	√	Procedures
21	Apply all of the released patches that are available for the following OAM devices: PSE, SESM, SAM21 Manager, and NPM. Apply all patches to all devices, then restart each device, one at a time, starting with the PSE. ***Note:*** You must restart each OAM device after applying the patches to that device. The restart takes the application out of service temporarily, then returns the application to service.		Perform procedure Transferring patches to the NPM database manually in this document.
			Perform procedure Applying patches using the NPM in this document.
			Perform procedure Restarting a device using the NPM in this document.
22	Back up the SN06.2 CS 2000 Management Tools server.		Perform procedure Performing a full backup of Oracle data on a Sun server in this document.
			Perform procedure Performing a full backup of file systems in this document.
			Perform procedure Performing a backup of APS application files in this document.
23	Verify the upgrade was successful.		Perform procedure Verifying the upgrade was successful in this document.

SN06 or SN06.1 to SN06.2 checklist

	Activities	√	Procedures
24	Stop and start the Patching Server Element (PSE) on each of the Media Gateway 9000 (MG 9000) manager servers (t1400). That is on the MG 9000 manager server, MG 9000 manager midtier, and MG 9000 manager OMCollector. ***Note:*** Only perform this activity if you have MG 9000 network elements in your network.		Perform procedure Stopping the PSE server application on a Sun server in this document.
			Perform procedure Starting the PSE server application on a Sun server in this document.

Patching and patch management procedures

Patching and patch management activities for the CS 2000 Management Tools are performed using the Network Patch Manager (NPM).

The CS 2000 Management Tools components that support the patching capability using the NPM, are listed below:

- Patch Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element and Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Network Patch Manager (NPM)

ATTENTION

Once patches have been applied to the PSE, CS 2000 SAM21 Manager, SESM, QCA and NPM devices, a restart of each device is required. The restart takes the application out of service temporarily, then returns the application to service.

The table titled Patching procedures, lists the procedures associated with patching activities, and the table titled Patch management procedures, lists the procedures associated with patch management activities.

Patching procedures

Procedure	Page
Transferring patches to the NPM database manually	181
Accessing the Network Patch Manager CLUI	187
Performing a device audit using the NPM	189
Applying patches using the NPM	195
Removing patches using the NPM	203
Restarting a device using the NPM	223

Patch management procedures

Procedure	Page
Defining sets using the NPM	231
Saving a task using the NPM	237
Setting field values using the NPM	243
Defining reports using the NPM	249
Defining a plan using the NPM	255
Modifying a plan using the NPM	263
Deleting a plan using the NPM	271
Prioritizing a patching maintenance request using the NPM	275

Rollback procedures

The sections that follow list the activities and associated procedures to rollback the CS 2000 SAM21 Manager to SN05, and the SSPFS and CS 2000 Management Tools software to SN05 or SN06.

Rollback of the CS 2000 SAM21 Manager to SN05

Use the table titled CS 2000 SAM21 Manager rollback to SN05 as a checklist during the rollback of the CS 2000 SAM21 Manager to SN05. Place a check (√) in the √column as you complete each procedure.

Note: Only perform these activities if you are performing a roll back of the CS 2000 SAM21 Manager to the SN05 release. If you are performing a rollback of the CS 2000 Manager to SN06, proceed to Rollback of the SSPFS and CS 2000 Management Tools software.

CS 2000 SAM21 Manager rollback to SN05

	Activities	√	Procedures
1	Boot the CS 2000 Core Manager from the SN05 backup tape.		Refer to procedure “Performing a full restore of the software from S-tape” in the CS 2000 Core Manager Fault document, NN10082-911.
2	Migrate the SAM21 shelves back to the CS 2000 SAM21 Manager on the CS 2000 Core Manager.		Perform procedure Migrating the SAM21 network elements back to the CS 2000 SAM21 Manager on the CS 2000 Core Manager in this document.
3	Downgrade the shelf controllers to the SN05 release for all shelves.		Contact your next level of support if you already upgraded both SAM21 shelf controllers to SN06.2. or Perform procedure Rollback software on the shelf controller in this document if you only upgraded one SAM21 shelf controller to SN06.2.
4	Migrate the SAM21 Manager data back to the CS 2000 Core Manager.		Perform procedure Performing a rollback of the CS 2000 SAM21 Manager in this document.

Rollback of the SSPFS and CS 2000 Management Tools software

Use the table titled SSPFS and CS 2000 Management Tools software rollback as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software. Place a check (√) in the √column as you complete each procedure.

SSPFS and CS 2000 Management Tools software rollback

	Activities	√	Procedures
1	Install the previous version of SSPFS on the CS 2000 Management Tools server.		Perform procedure Reverting to the previous release of the SSPFS software in this document.
2	Restore the file systems from backup tapes.		Perform procedure Restoring root file systems in this document. and Perform procedure Restoring non-root file systems in this document.
3	Restore the Oracle data from backup tapes.		Perform procedure Restoring application data to the Oracle database in this document.
4	Clear the Java ™ Web Start (JWS) cache on the client workstation.		Perform procedure Clearing the JWS cache on a client workstation in this document.

Note: Installing the previous version of SSPFS and restoring the file systems and Oracle data from backup tape, restores your system as it was before the upgrade to SN06.2.

Performing a full backup of Oracle data on a Sun server

Application

Use this procedure to perform a full backup of application data in the Oracle database on a Sun server (t1400).

This procedure only applies to systems running SSPFS SN05, SN06, or SN06.1. For systems running SSPFS SN06.2 or greater, refer to procedure “Performing a data backup” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

ATTENTION
It is recommended that provisioning activities be put on hold during the time of the Oracle backup.

Prerequisites

This procedure has the following prerequisites:

- the Oracle database must be in-service
- you need a blank 4mm DDS-3 (Digital Data Storage) tape of 125m and 12GB to store the data

ATTENTION
The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have an image of both before you proceed. Performing a restore from the Oracle database alone may cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the blank tape into the tape drive.

At your workstation

2 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server on which you are performing a full backup of Oracle data

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

7 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

Note: You may be required to enter a password for the Oracle user.

8 Backup the Oracle data by typing

```
$ /opt/nortel/sspfs/bks/bkfullora
```

and pressing the Enter key.

9 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

10 List the content of the tape to ensure the backup was successful by typing

```
# tar tvf /dev/rmt/0
```

and pressing the Enter key.

Example response:

```
-rw-r--r-100/100 8296448 Jun 11 18:08 2003
/var/tmp/bkexpora_2003061118_co.dmp
```

11 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

12 You have completed this procedure.

Performing a full backup of file systems

Application

Use this procedure to perform a full backup of the file systems on the CS 2000 Management Tools server.

This procedure only applies to systems running SSPFS SN05, SN06, or SN06.1. For systems running SSPFS SN06.2 or greater, refer to procedure “Performing a full backup of system files” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Prerequisites

This procedure has the following prerequisites:

- the Oracle database must be in-service
- you need a blank 4mm DDS-3 (Digital Data Storage) tape of 125m and 12GB to store the data

Action

At the CS 2000 Management Tools server

1 Insert a blank tape into the tape drive.

At your workstation

2 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

7 Backup the file systems by typing

```
# /opt/nortel/sspfs/bks/bkfullsys
```

and pressing the Enter key.

8 List the content of the tape to ensure the backup was successful by typing

```
# ufsrestore tfs /dev/rmt/0 1 (for /)
# ufsrestore tfs /dev/rmt/0 2 (for /var)
# ufsrestore tfs /dev/rmt/0 3 (for /data)
# ufsrestore tfs /dev/rmt/0 4 (for /opt)
# ufsrestore tfs /dev/rmt/0 5 (for /opt/nortel)
```

and pressing the Enter key.

9 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

10 You have completed this procedure.

Saving user-defined NPM data using the NPM

Application

Before performing an upgrade of the Network Patch Manager (NPM) to a new release, it is recommended that you preserve any user-defined data in the current release. Examples would be user-defined sets, reports, alarms, tasks, etc. This does not include system defined data, which will be re-created during the NPM upgrade. All user-defined information will be removed during the NPM upgrade. This procedure contains the steps necessary to preserve this data so it will be available to the new NPM release once the upgrade is completed. You can save user-defined NPM data using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Prerequisites

The SSPFS software has not been upgraded yet.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Display all the set names present on the NPM by typing

```
npm> qsets
```

and pressing the Enter key.

3 Ignore all system-defined sets. These include the sets ALLDEVICES, ALLPATCHES, AUTOAPPLY, and NOSPAPP.

4 Display the definition details for any user-defined sets that should be propagated to the new release by typing

npm> **viewset SET <set_name>**

and pressing the Enter key.

where

set_name
is the name of the user-defined set.

5 Record the details of the set.

6 Repeat steps 4 and 5 for each user-defined set.

7 Display the list of all reports by typing

npm> **qreps**

and pressing the Enter key.

8 Ignore all system defined reports. These include ACTLIST, CALCLIST, DEVICE, DEVICELIST, DISABLEDAPPLIED, DISABLEDREMOVED, ENABLEDAPPLIED, ENABLEDREMOVED, FULLDEVICELIST, LOADLIST, PATCH, PATCHES_SINCE, PATCHINFO, and PATCHLIST.

9 View the details of the user-defined reports by typing

npm> **viewset REPORT <report_name>**

and pressing the Enter key.

where

report_name
is the name of a user-defined report

10 Record the details of the report.

11 Repeat steps 9 and 10 for each user-defined report.

12 Display all defined alarms by typing

npm> **alarminfo all**

and pressing the Enter key.

13 Ignore all system defined alarms. These include ACT_NOT_APP, ACT_NOT_ACT, DEVICE_ONHOLD, DISABLED_APPLIED, DNR_NOT_APP, OBE_NOT_REMOVED, ENABLED_REMOVED, OBS_NOT_REMOVED, DEBUG_APP, PATCH_ONHOLD, REMOVED_PATCHES, EMG_NOT_APP, GEN_NOT_APP, AND LTD_NOT_APP.

14 Display the details of the user-defined alarms by typing

```
npm> alarminfo <alarm_name>
```

and pressing the Enter key.

where

alarm_name
is the name of the user-defined alarm

15 Record the details of the alarm.

16 Repeat steps 14 and 15 for each user-defined alarm.

17 List all the task names by typing

```
npm> qtask all
```

and pressing the Enter key.

Note: Ignore all system-defined tasks. These include AUTOAPPLY, and AUDIT.

18 Display the details of the user-defined tasks by typing

```
npm> qtask <task_name>
```

and pressing the Enter key.

where

task_name
is the name of a user-defined task

19 Record the details of the task.

20 Repeat steps 18 and 19 for each user-defined task.

21 Display the System Plan by typing

```
npm> getplan
```

and pressing the Enter key.

22 If the System Plan has been modified from its original version, record the changes at this time.

Note: The original version should show [TASK:AUTOAPPLY].

23 Display the patchlist report by typing

```
npm> query PATCHLIST
```

and pressing the Enter key.

24 Save a copy of the PATCHLIST report for later reference.

25 You have completed this procedure.

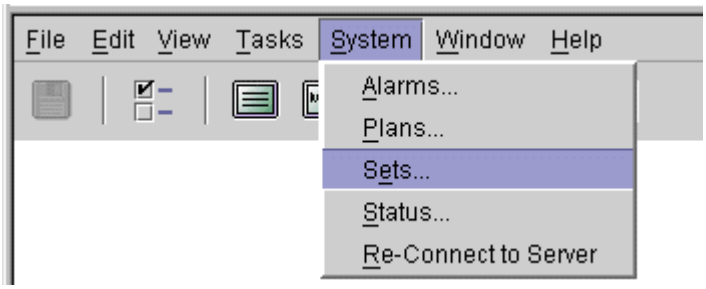
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

2 On the **System** menu, click **Sets...**.



The **Sets** window is displayed.

3 Click the **Set List** tab to display the list of defined sets.

4 Click one of the user-defined sets, then click **Edit** to display its details.

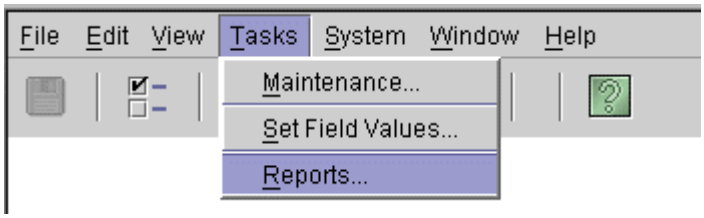
Note: Ignore all system-defined sets. These include the sets ALLDEVICES, ALLPATCHES, AUTOAPPLY, and NOSPAPP.

5 Record the details of the set.

6 Repeat steps 3 through 5 for each user-defined set.

7 Click **Close** to close the Sets window.

8 On the **Tasks** menu, click **Reports...**.



9 Click the **Report List** tab to display the list of defined reports.

10 Click one of the user-defined reports, then click **Edit** to display the details.

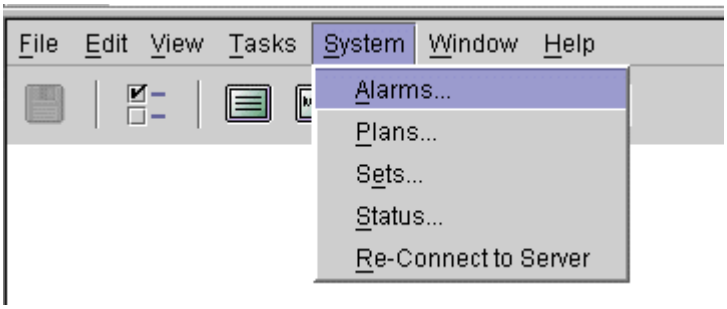
Note: Ignore all system-defined reports. These include ACTLIST, CALCLIST, DEVICE, DEVICELIST, DISABLEDAPPLIED, DISABLEDREMOVED, ENABLEDAPPLIED, ENABLEDREMOVED, FULLDEVICELIST, LOADLIST, PATCH, PATCHES_SINCE, PATCHINFO, and PATCHLIST.

11 Record the details of the report.

12 Repeat steps 9 through 11 for each user-defined report.

13 Click **Close** to close the Reports window.

14 On the **System** menu, click **Alarms...**.



15 Click the **Alarm List** tab to display the list of defined alarms.

16 Click one of the user-defined alarms, then click **Edit** to display its details.

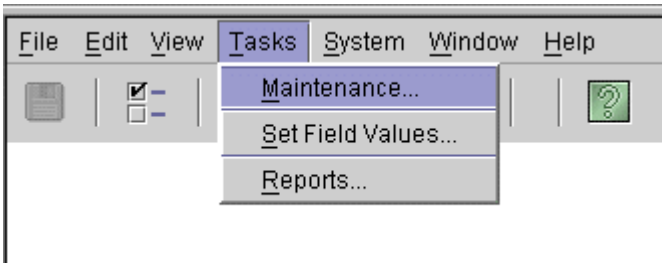
Note: Ignore all system-defined alarms. These include ACT_NOT_APP, ACT_NOT_ACT, DEVICE_ONHOLD, DNR_NOT_APP, OBE_NOT_REMOVED, DISABLED_APPLIED, ENABLED_REMOVED, OBS_NOT_REMOVED, DEBUG_APP, PATCH_ONHOLD, REMOVED_PATCHES, EMG_NOT_APP, GEN_NOT_APP, AND LTD_NOT_APP.

17 Record the details of the alarm.

18 Repeat steps 15 through 17 for each user-defined alarm.

19 Click **Close** to close the Alarms window.

20 On the **Tasks** menu, click **Maintenance...**.



21 Click the **Task List** tab to display the list of defined tasks.

22 Click one of the user-defined tasks, then click **Edit** to display its details.

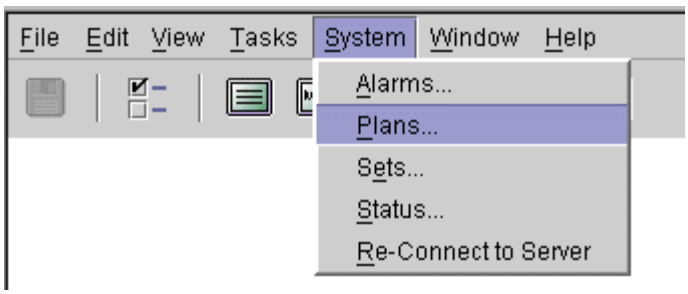
Note: Ignore all system-defined tasks. These include AUTOAPPLY, and AUDIT.

23 Record the details of the task.

24 Repeat steps 21 through 23 for each user-defined task.

25 Click **Close** to close the Tasks window.

26 On the **System** menu, click **Plans...**.



27 Click the **Plan List** tab.

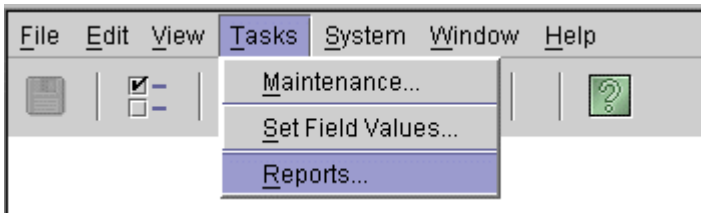
28 Click the **SYSTEMPLAN**, then click **Edit** to display its details.

29 If either (or both) are present, open the Tasks and/or Reports folders.

30 If the System Plan has been modified from its original version, record the changes at this time. The original version should show a Task folder with AUTOAPPLY in it.

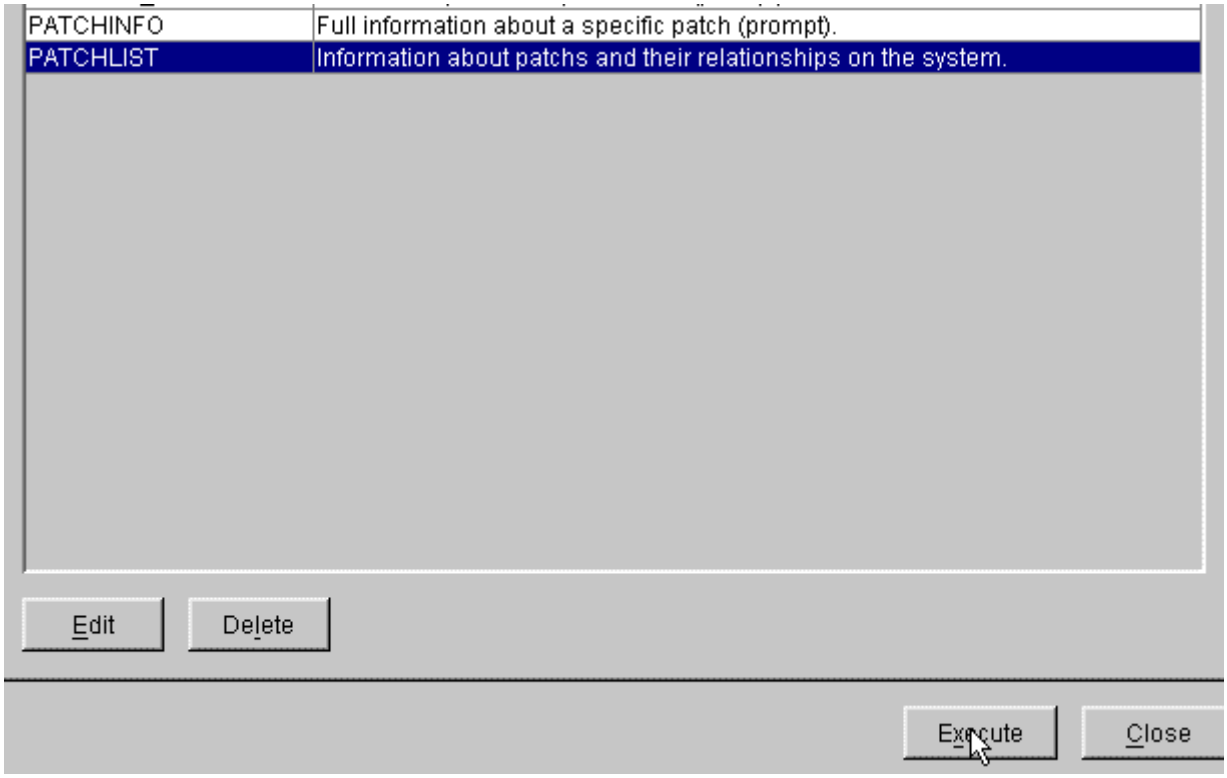
31 Click **Close** to close the Plans window.

32 On the **Tasks** menu, click **Reports...**.

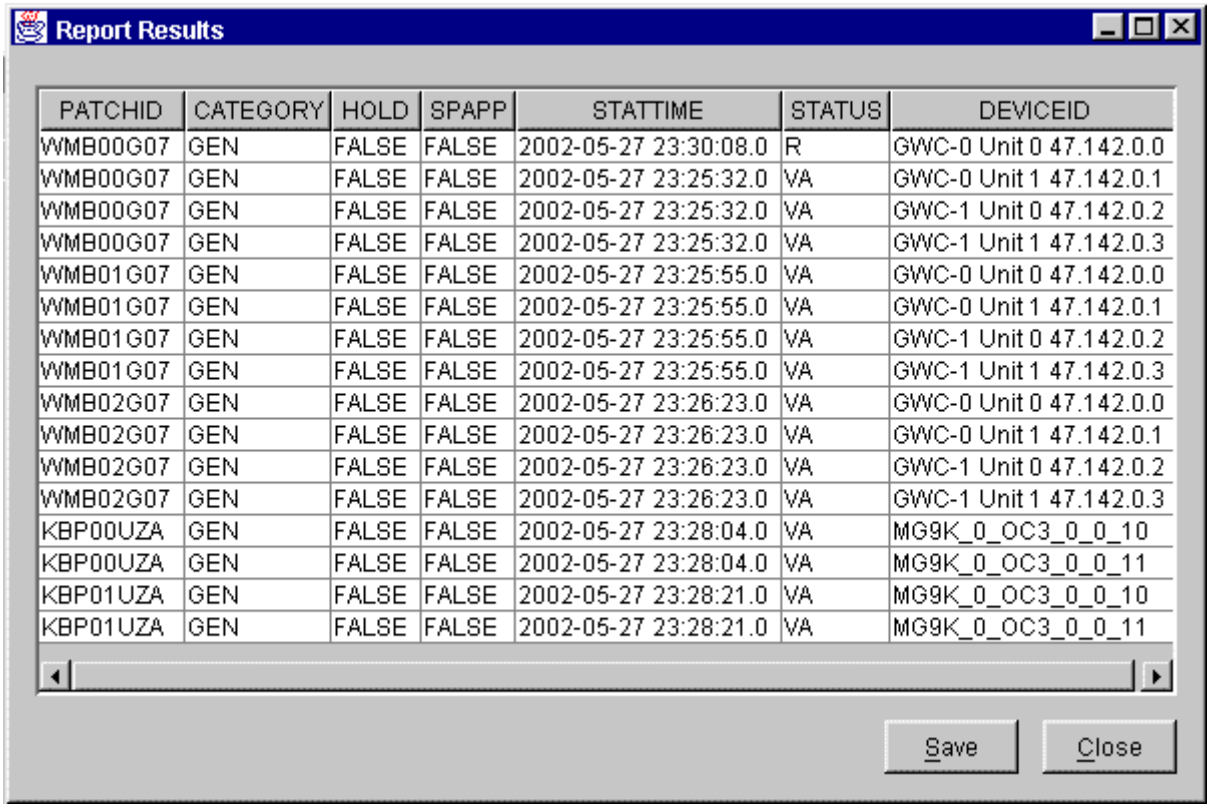


33 Click the **Reports List** tab to display the list of all reports.

34 Select **PATCHLIST**, then click **Execute** to run the PATCHLIST report.

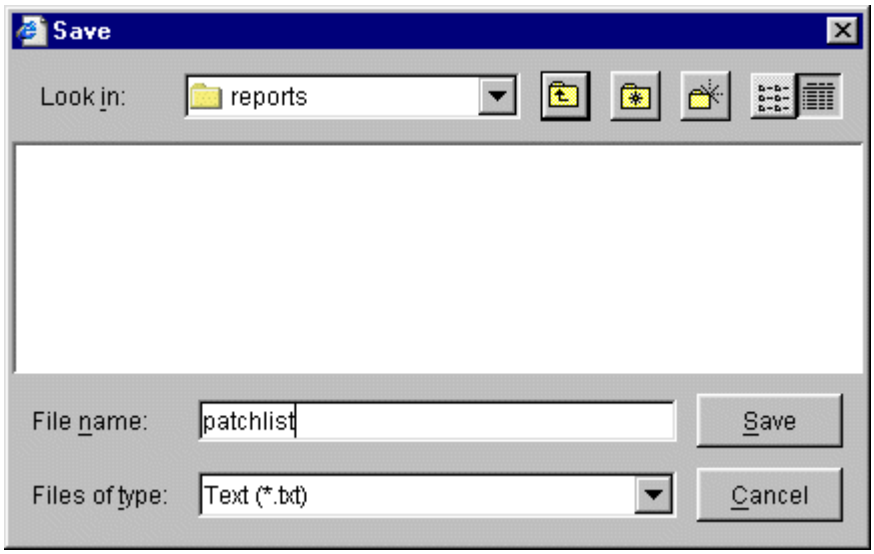


The **Reports Results** window is displayed.



35 Click **Save** to save the results of the PATCHLIST report.

36 In the **Filename** box enter a name for the saved report, then click **Save**.



37 You have completed this procedure.

Saving the NPM patch files

Application

Use this procedure prior to upgrading the Network Patch Manager (NPM) software. This procedure provides instructions on how to copy patch files information to a location that will be preserved over the upgrade.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify whether any NPM patch files exist as follows:

a Change directory to the NPM's patch file directory by typing

```
# cd /data/npm/Au
```

and pressing the Enter key.

b List the content of the directory by typing

```
# ls
```

and pressing the Enter key.

If patch files	Do
exist	step 6
do not exist	you have completed this procedure

6 Access the data directory by typing

```
# cd /data
```

and pressing the Enter key.

7 Make a directory to store the old NPM files by typing

```
# mkdir <npm_old>
```

where

npm_old
is a valid Unix directory name

8 Change directory to the directory you just created by typing

```
# cd <npm_old>
```

where

npm_old
is a valid Unix directory name

9 Create a temporary directory to hold the NPM backup data by typing

```
# mkdir <directory_name>
```

and pressing the Enter key.

where

directory_name
is a valid UNIX directory name

Example

```
# mkdir patch_data
```

10

ATTENTION

This step copies all or selected NPM patch files to a temporary location. If it is preferable to download the required patch files after the upgrade, this step may be skipped.

Save a copy of the needed patch files by performing the following steps.

Note: The NPM upgrade process normally does not remove the patch files present in the patch file repository. However, the NPM06 server may not be able to locate and utilize all the files. The NPM server and database will remain unaware of any patches present that are not yet applied to any working device.

a Change directory to the NPM's patch file directory by typing

```
# cd /data/npm/Au
```

and pressing the Enter key.

b Copy all patch files to the backup directory by typing

```
# cp *.ptch* <directory_path>
```

and pressing the Enter key.

where

directory_path
is the path to the directory you created in step 9

Example

```
# cp *.ptch* /data/npm_old/patch_data
```

c Ensure all patch files were copied to the backup directory by typing

```
# ls -l
```

and pressing the Enter key.

11 Return to the home directory of the UNIX host by typing

```
# cd
```

and pressing the Enter key.

12 You have completed this procedure.

Performing a backup of APS application files

Application

Use this procedure to back up APS application files.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the APS server

1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

At the APS server console

2 Log in to the server through the console (port A) using the root user ID and password.

3 Rewind the tape by typing

```
# mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.

4 Back up the APS application files by typing

```
# tar -cvf /dev/rmt/0c /PROV_data /audio_files
/user_audio_files /opt/uas/uas_conf_backup
```

and pressing the Enter key.

Note: When entering the command, you must ensure that a space is placed between the path names, “/PROV_data” and “/audio_files”, between “/audio_files” and “/user_audio_files”, and between “/user_audio_files” and “/opt/uas/uas_conf_backup”

5 Rewind the backup tape by typing

```
# mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.

6 To ensure that the backup was successful, list the content of the tape on the terminal screen by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.

7 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen), to prevent the data on the tape from being accidentally over-written. Store the tape for use later.

8 You have completed this procedure.

Preparing for the CS 2000 SAM21 Manager data migration

Application

Use this procedure to prepare for the migration of the CS 2000 SAM21 Manager from the CS 2000 Core Manager to the CS 2000 Management Tools server, prior to upgrading the CS 2000 Management Tools software to SN06 or higher.

ATTENTION

Once you prepare for the CS 2000 SAM21 Manager data migration, ensure no SAM21 nodes are added to the network until the entire upgrade of the CS 2000 Management Tools software is complete, and the CS 2000 SAM21 Manager is operating from the CS 2000 Management Tools server.

Prerequisites

The CS 2000 Core Manager must be at the CS2E00006 software release or higher.

Action

Perform the following steps to complete this procedure.

At the console connect to the CS 2000 Core Manager

1 Log on to the CS 2000 Core Manager through the console using the root user ID and password.

2 Verify that the Open SSH fileset is installed as follows:

a Access the Details level of the maintenance interface to display a list of the filesets installed on the CS 2000 Core Manager by typing

```
# sdmmtc details
```

and pressing the Enter key.

b Filter the display so that only the filesets with “ssh” in their name are displayed by typing

```
> filter ssh
```

and pressing the Enter key.

c Ensure that the OpenSSH fileset is applied.

If OpenSSH is	Do
applied	step 3
not applied	Refer to procedure "Installing or upgrading OpenSSH" in the CS 2000 Core Manager Upgrades section, NN10060-461. When complete, return to this procedure and continue with step 3.

3 Busy the CS 2000 SAM21 Manager as follows:

a Access the application level of the maintenance interface by typing

> **appl**

and pressing the Enter key.

b Busy the Succession SAM21 Manager application by typing

> **bsy <#>**

and pressing the Enter key.

where

#
is the number next to the Succession SAM21 Manager fileset

c Confirm the busy command by typing

> **y**

and pressing the Enter key.

The CS 2000 SAM21 Manager client application on the CS 2000 Core Manager shuts down after the busy command.

d Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

4 Run the pre-migration script to backup persistent data and create an SSPFS persistent data file by typing

\# **/sdm/snm/bin/sam21emPreMigration.sh**

and pressing the Enter key.

5 Return the CS 2000 SAM21 Manager application to service as follows:

a Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.

b Return the Succession SAM21 Manager to service by typing

```
> rts <#>
```

and pressing the Enter key.

Where:

#
is the number next to the Succession SAM21 Manager fileset

Note: The state changes to ISTb, then to in-service (represented by a dot) after approximately one minute.

6 You have completed this procedure.

Stopping the SESM server application

Application

Use this procedure to stop the SESM server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05	step 6
SN06 or SN06.1	step 7
SN06.2 or greater	step 8

6 For the SN05 release, stop the SESM server application by typing

```
# /opt/nortel/NTptm/bin/ptmctl stop
```

and pressing the Enter key.

7 For the SN06 or SN06.1 release, stop the SESM server application as follows:

a Stop the SESM server application including the Proxy Agent by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl -f stop
```

and pressing the Enter key.

b Verify the SESM server application stopped by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl status
```

and pressing the Enter key.

Example response (without stopping Proxy Agent):

```
SESM STATUS --------------------------------

  COMPONENT                    STATUS
  --------                     ------
 Proxy Agent                   NOT RUNNING
 RMI Registry                  NOT RUNNING
 Snmpfactory                   NOT RUNNING
 MI2 Server                    NOT RUNNING

Current number of SESM processes running: 0
(of 4)

SESM APPLICATION STATUS: No Applications are
ready
```

8 For the SN06.2 or greater release, stop the SESM server application by typing

Note: In a two-server configuration, perform the steps that follow on the active side.

```
# servstop SESMService
```

and pressing the Enter key.

9 Verify the SESM server application stopped by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

10 You have completed this procedure.

Stopping the NPM server application

Application

Use this procedure to stop the Network Patch Manager (NPM) server application.

Prerequisites

All users of the NPM CLUI and GUI should exit before stopping the NPM server application.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, stop the NPM server application as follows:

a Stop the NPM server by typing

```
# npmsrvr stop
```

and pressing the Enter key.

b Verify the NPM server application stopped by typing

```
# npmsrvr status
```

and pressing the Enter key.

7 For the SN06.2 or greater release, stop the NPM server application as follows:

Note: In a two-server configuration, perform the steps that follow on the active side.

a Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

b Verify the NPM server application stopped by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

8 You have completed this procedure.

Upgrading SSPFS software

Application

Use this procedure to upgrade the SSPFS software on the CS 2000 Management Tools server (Netra t1400) from the SN05 or SN06 release to the SN06.2 release.

Upgrading the SSPFS software updates the Solaris operating system and all platform common software. For a list of the new and updated 3rd party common software included with the SSPFS SN06.2 upgrade, refer to the CS 2000 Management Tools Basics document, NN10020-111.

Prerequisites

Ensure you have SSPFS Disk 1 and SSPFS Disk 2 for the SN06.2 release.

ATTENTION

SSPFS does not have a rollback command, therefore, ensure you performed procedures Performing a full backup of Oracle data on a Sun server and Performing a full backup of file systems in this document to back up your system before proceeding with this procedure. Returning to a previous version of your system, requires that you install the previous version of SSPFS software and restore the Oracle data and file systems using the backup tapes.

Ensure the site spec book is available with IP addresses, hostnames, and non-system logins.

Action

Perform the following steps to complete this procedure.

At the CS 2000 Management Tools server console

1 Log in to the CS 2000 Management Tools server through the console (port A) using the root user ID and password.

2 Verify that your system is running the version of the SSPFS by typing

```
# echo $SSPFS_VERSION
```

and pressing the Enter key.

Note: The command is case sensitive.

At the CS 2000 Management Tools server

3 Insert “SSPFS Disk 1” into the CD Rom drive.

At the CS 2000 Management Tools server console

4 Run the pre-upgrade script by typing

```
# /cdrom/cdrom0/s0/pre_upgrade
```

and pressing the Enter key.

The pre-upgrade script prepares the CS 2000 Management Tools server for the upgrade.

5 At the ok prompt, boot the system in single-user mode by typing

```
OK> boot -s
```

and pressing the Enter key.

6 When prompted, enter the root password. Do not press Ctrl-D.

7 Mount the drive by typing

```
# mount -F hsfs /dev/dsk/c0t6d0s0 /cdrom
```

and pressing the Enter key.

8 Start the upgrade process by typing

```
# /cdrom/upgrade
```

and pressing the Enter key.

Note: The execution of this step takes approximately 90 minutes to complete.

Once the upgrade is complete, the system reboots into single-user mode and prompts you for the root password.

9 When prompted, enter the root password. Do not press Ctrl-D.

At the CS 2000 Management Tools server

10 Remove “SSPFS Disk 1” from the cdrom drive and insert “SSPFS Disk 2” into the drive.

At the CS 2000 Management Tools server console

11 Mount the drive by typing

```
# mount -F hsfs /dev/dsk/c0t6d0s0 /cdrom
```

and pressing the Enter key.

12 Start the platform common service upgrade by typing

```
# /cdrom/upgrade
```

and pressing the Enter key.

Note 1: The execution of this step takes approximately 60 minutes to complete.

Note 2: You can ignore any “rpcbind” errors.

13 Once the system has rebooted, log in, then eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

14 You have completed this procedure.

Configuring the Patching Server Element on a Sun server

Application

Use this procedure to configure the Patching Server Element (PSE) on a Sun server.

Prerequisites

The SSPFS upgrade is complete.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where the PSE software resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “Succession Element Configuration” option by typing

```
select - 13
```

and pressing the Enter key.

Example response:

```
Succession Element Configuration
 1 - PSE Application Configuration
 2 - OMPUSH Application Configuration


 X - exit

select -
```

8 Select the “PSE Application Configuration” option by typing

```
select - 1
```

and pressing the Enter key.

Response

```
PSE Application Configuration
 1 - View_SESM_host_ip <View SESM hostname/ip
     address>
 2 - Update_SESM_host_ip <Update SESM
     hostname/ip address>
 3 - Create_PSE_Database (Initialize or
     re-initalize the PSE database)


 X - exit

select -
```

9 Select the “Update_SESM_host_ip” option by typing

```
select - 2
```

and pressing the Enter key.

10 When prompted, enter the host name or IP address of the Sun server where PSE resides.

11 When prompted, confirm the hostname or IP address by typing.

```
y
```

and pressing the Enter key.

12 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

13 You have completed this procedure.

Setting up the BootP file on SSPFS

Application

Use this procedure to set up the SSPFS platform as the bootp master and migrate the bootp entries from the CS 2000 Core Manager to the SSPFS platform.

Note: Only perform this procedure if the CS 2000 SAM21 Manager is in your network.

Prerequisites

This procedure has the following prerequisites:

- the OpenSSH fileset on the SDM (CS 2000 Core Manager) must be APPLIED

  Note: You can verify whether the OpenSSH fileset is APPLIED using command “sdmmtc details” at the CS 2000 Core Manager (SDM). If it is not applied, refer to procedure “Installing or upgrading OpenSSH” in document Upgrading the CS 2000 Core Manager, NN10060-461.

- you need the password for the root user on the SDM (CS 2000 Core Manager)
- you need the IP address of the SDM (CS 2000 Core Manager)

  Note: You can obtain the IP address of the SDM (CS 2000 Core Manager) using command “sdmmtc eth” at the SDM. Use the IP address associated with the host name of the SDM, which is the first one.

ATTENTION

Do no begin this procedure until the SSPFS software has been upgraded to the new release. If required, refer to procedure Upgrading SSPFS software in this document.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Configure the IP address of the SDM (CS 2000 Core Manager) as follows:

a Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

b Select the “OAMP Application Configuration” option by typing

```
select - 4
```

and pressing the Enter key.

Response

```
OAMP Application Configuration
 1 - sdm_conf (Configure SDM IP Address)
 2 - sdm_unconf (Unconfigure SDM IP Address)
 3 - cmClli_conf (Configure CM_CLLI Address)
 4 - cmClli_unconf (Unconfigure CM_CLLI IP
     Address)


 X - exit

select -
```

c Select the “sdm_conf” option by typing

```
select - 1
```

and pressing the Enter key.

d When prompted, enter the IP address for the SDM (CS 2000 Core Manager).

Example response

```
SDM IP: 47.152.34.56
SDM User Name: swld

Enter "ok" to accept current settings
```

e When prompted, confirm the current settings by typing

```
ok
```

and pressing the Enter key.

7 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

8 For the SAM21 Manager user, generate the ssh key pair needed for data transmission between the SAM21 Manager and the CS 2000 Core Manager as follows:

a Log on as the SAM21 user by typing

```
# su - sam21em
```

and pressing the Enter key.

b Generate the key pair by typing

```
$ ssh-keygen -t rsa
```

and pressing the Enter key.

Example response

```
Generating public/private rsa key pair.
Enter file in which to save the key
(/export/home/sam21em/.ssh/id_rsa):
```

c When prompted, press the Enter key to accept the default location and filename (“/export/home/sam21em/.ssh/id_rsa”) for the key.

Example response

```
Enter passphrase (empty for no passphrase):
```

d When prompted, press the Enter key to confirm an empty passphrase.

Example response

```
Enter same passphrase again:
```

e When prompted, press the Enter key again to confirm an empty passphrase.

Example response

```
Your identification has been saved in
/export/home/sam21em/.ssh/id_rsa.
Your public key has been saved in
/export/home/sam21em/.ssh/id_rsa.pub.
The key fingerprint is:
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37
bc:1e sam21em@znc0s0j6
```

9 Place the key information contained in file "/export/home/sam21em/.ssh/id_rsa.pub" on the CS 2000 Management Tools server, in file "/home/swld/.ssh/authorized_keys2" on the SDM (CS 2000 Core Manager) as follows:

Note: You need to know the password for the SDM root user to complete the following steps.

a Secure-append the public key to the authorized key's list that resides on the SDM (CS 2000 Core Manager) by typing

```
$ cat .ssh/id_rsa.pub | ssh root@$SDM_IP 'cat
>> /home/swld/.ssh/authorized_keys2'
```

and pressing the Enter key.

Example response:

```
The authenticity of host '47.142.128.16
(47.142.128.16)' can't be established. RSA
key fingerprint is
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37
bc:1e sam21em@znc0s0j6
Are you sure you want to continue connecting
(yes/no)?
```

b When prompted, confirm you want to continue connecting by typing

```
# yes
```

and pressing the Enter key.

Example response:

```
Warning: Permanently added '47.142.128.16'
(RSA) to the list of known hosts.
root@47.142.128.16's password:
```

c When prompted, enter the password for the SDM root user.

d Ensure the "authorized_keys2" file has the proper ownership on the SDM by typing

```
$ ssh root@$SDM_IP chown swld:swld
/home/swld/.ssh/authorized_keys2
```

and pressing the Enter key.

Example response:

```
root@47.142.128.16's password:
```

e When prompted, enter the password for the SDM root user.

f Copy the bootptab file from the CS 2000 Core Manager to the CS 2000 Management Tools server by typing

```
$ /opt/nortel/sspfs/Scripts/getbootp.ksh
```

and pressing the Enter key.

g When prompted, enter the password for the SDM root user.

Example response:

```
Successfully performed bootptab manipulation
```

Once complete, the SAM21 Manager application will have access to the needed directories and files on the CS 2000 Core Manager.

h Exit the SAM21 user by typing

```
$ exit
```

and pressing the Enter key.

10 You have completed this procedure.

Unconfiguring DCE on a Sun server

Application

Use this procedure to unconfigure the Distributed Computing Environment (DCE) on a Sun server following an SSPFS software upgrade. Only perform this procedure if DCE is used as an authentication mechanism. As of SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

Prerequisites

You need the DCE cell administrator password.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that uses DCE as an authentication method

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “DCE Configuration” option by typing

```
select - 3
```

and pressing the Enter key.

Response

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>
 2 - dce_unconf <Unconfigure the DCE Client>

 X - exit

select -
```

8 Select the “dce-unconf” option by typing

```
select - 2
```

and pressing the Enter key.

Example response

```
=== Executing "dce_unconf"
Gathering current configuration information...
Enter password for principal cell_admin:
```

9 Enter the cell administrator password and press the Enter key.

Example response

```
Start of DCE Host, znc0s0jy, will now begin.
RPC is already running.
The Security client is already running.
The Directory client is already running.

Unconfiguration of DCE Host, znc0s0jy, will now
begin.
Unconfiguring the DTS client...
Stopping the DTS client...
The DTS client was stopped successfully.
The DTS client will be completely unconfigured
when RPC is unconfigured.
Unconfiguration of this component has been
successful so far.
```

```
Unconfiguring the Directory client...

Stopping the Directory client...

The Directory client was stopped successfully.

The Directory client was unconfigured
successfully.

Unconfiguring the Security client...

Stopping the Security client...

The Security client was stopped successfully.

The Security client was unconfigured
successfully.

Unconfiguring RPC...

Stopping RPC...

RPC was stopped successfully.

RPC was unconfigured successfully.

Gathering component state information...


      Component Summary for Host: znc0s0jy
 Component   Configuration State   Running State

No DCE components are configured.

Unconfiguration of DCE Host, znc0s0jy, was
successful.

Unconfiguration completed successfully.

done unconfiguring DCE

=== "dce_unconf" completed successfully
```

10 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

11 You have completed this procedure.

Configuring DCE on a Sun server

Application

Use this procedure to configure the Distributed Computing Environment (DCE) on a Sun server following a Succession Server Platform Foundation Software (SSPFS) upgrade. Only perform this procedure if DCE is used as an authentication mechanism. As of SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

Prerequisites

This procedure has the following prerequisites:

- unconfigure DCE - refer to procedure Unconfiguring DCE on a Sun server in the CS 2000 Management Tools Configuration Management document, NN10106-511, if required
- obtain the following information
  - the DCE cell name for your customer-provided DCE cell

    Note: This should be the same DCE cell that contains the CS 2000 Core Manager.

  - the host name or IP address of the DCE Master Security Server (MSS)
  - the host name or IP address of the DCE Cell Directory Server (CDS)
  - the DCE cell administrator password.
  - the host name or IP address of the DCE Time Server (DTS)

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that uses DCE as an authentication method

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “DCE Configuration” option by typing

```
select - 3
```

and pressing the Enter key.

Response

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>
 2 - dce_unconf <Unconfigure the DCE Client>

 X - exit

select -
```

8 Select the “dce-conf” option by typing

```
select - 1
```

and pressing the Enter key.

Example response

```
DCE Cell Name(default:)
```

9 Enter the DCE Cell Name.

Example response

```
Master Security Server Name(default:)
```

10 Enter the host name or IP address of the MSS.

Example response

```
Time Server Name(default:)
```

11 Enter the host name or IP address of the DTS.

Example response

```
CDS Server Name(default:)
```

12 Enter the host name or IP address of the CDS

Example response

```
You have selected to configure your DCE
environment as the following:
Host Name                          : znc0s0jx
DCE Cell Name                      :
rtpptm.sdm.nortel.com
Time Server Name                   : wnc0s0j8
Master Security Server Host Name : wnc0s0j8
CDS Server Host Name               : wnc0s0j8
Continue with configuration?(default:Y[Y/N]
```

13 Continue the configuration by typing

y

and pressing the Enter key.

Example response

```
Synchronizing time with wnc0s0j8......
Tue Apr 16 15:00:47 2002
done synchronizing time with wnc0s0j8(0)
Configuring DCE.............................
Default DCE configuration timeout value
successfully changed.
Gathering current configuration information...
Enter password for principal cell_admin:
```

14 Enter the cell administrator password and press the Enter key.

Example response

```
Configuration of DCE Host, znc0s0jx, will now
begin.
Configuring RPC...
Starting RPC...
RPC was started successfully.
RPC configuration is complete.
Configuring the Security client...
Information from the /etc/krb5.conf.backup file
may need to be manually merged into the
/etc/krb5.conf file.
Starting the Security client...
The Security client was started successfully.
Security client configuration is complete.
Configuring the Directory client...
Starting the Directory client...
Waiting up to 10 minutes for the directory
server.
Contacted the directory server.
The Directory client was started successfully.
```

```
Waiting up to 10 minutes for DCED registration
to be functional.
Directory client configuration is complete.
Configuring the DTS client...
Starting the DTS client...
The DTS client was started successfully.
DTS client configuration is complete.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State   Running State
Security client      Configured         Running
RPC                 Configured         Running
Directory client     Configured         Running
DTS client           Configured         Running

The component summary is complete.
Configuration of DCE Host, znc0s0jx, was
successful.
Configuration completed successfully.
done configuring DCE
Gathering current configuration information...
Configuration of DCE Host, znc0s0jx, will now
begin.
There are no components in the request that need
to be configured.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State   Running State
Security client     Configured         Running
RPC                Configured         Running
Directory client    Configured         Running
```

```
DTS client          Configured          Running


The component summary is complete.

Configuration of DCE Host, znc0s0jx, was
successful.

Configuration completed successfully.

=== "dce_conf" completed successfully
```

15 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

16 You have completed this procedure.

Installing an HTTPS certificate on a Sun server

Application

Use this procedure to install an HTTPS certificate on a Sun Server. An HTTPS certificate enables HTTPS communications.

ATTENTION
An HTTPS certificate is preserved over an SSPFS upgrade. Therefore, you do not need to perform this procedure following an SSPFS upgrade if an HTTPS certificate was already installed on the server.

Prerequisites

This procedure has the following prerequisites:

- Obtain an X.509 certificate. You can purchase a certificate from a third-party Certificate Authority such as VeriSign. Nortel Networks recommends the installation of a unique certificate for each host.

  Note: The name of the certificate should match the host name of the server. A separate file contains the key, and should not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- The domain name service (DNS) must be enabled on the Sun server to allow the security certificates to work, and must be enabled prior to the installation of the certificate. Refer to procedure “Configuring Domain Name Service” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to install the HTTPS certificate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Place the certificate you obtained prior to the procedure, into the following file by typing

```
# /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

6 Place the key into the following file by typing

```
# /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

7 Change the certificate's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

8 Change the key file's owner and group by typing

```
# chown root:other
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

9 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

10 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

11 Restart the Apache web server by typing

```
# /etc/init.d/apache restart
```

and pressing the Enter key.

12 You have completed this procedure.

If you installed an HTTPS certificate on an existing Sun server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

Configuring the Apache Web Server for HTTPS proxy

Application

Use this procedure to configure the Apache Web Server for HTTPS proxy.

Note: You can provision a maximum of 6 IP addresses for use in HTTPS proxy.

ATTENTION
Only perform this procedure if STORage Management (STORM) units are configured in your network.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the Sun server console

1 Log in to the Sun server through the console (port A) using the root user ID and password.

2 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

3 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

4 Select the “Apache Proxy Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Example response

```
Apache Proxy Configuration
 1 - add_proxy_conf (Add an IP to the Apache
     Proxy Module configuration)
 2 - del_proxy_conf (Delete an IP from the
     Apache Proxy Module configuration)
 3 - list_proxy_conf (List the Apache Proxy
     Module configuration)

 X - exit

select -
```

5 Select the “add_proxy_conf” option by typing

```
select - 1
```

and pressing the Enter key.

6 When prompted, type the proxy IP address, and press the Enter key.

7 When prompted, type the hostname associated with the IP address you just entered, and press the Enter key.

8 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

9 You have completed this procedure.

Installing or upgrading the CS2M software

Application

Use this procedure to install or upgrade to the SN06.2 release of the CS 2000 Management Components (CS2M) software on the CS 2000 Management Tools server.

Prerequisites

Ensure you have the CD that contains the CS2M software for the SN06.2 release.

Action

Perform the following steps to complete this procedure.

At the CS 2000 Management Tools server

1 Insert the CD that contains the CS2M software into the CD-Rom drive of the CS 2000 Management Tools server.

At the CS 2000 Management Tools server console

2 Log in to the CS 2000 Management Tools server through the console (port A) using the root user ID and password.

3 Change directories by typing

```
# cd /cdrom/cdrom0/bin
```

and pressing the Enter key.

4 Upgrade or install the CS2M software by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

5 When prompted, confirm you want to upgrade or install by typing

```
# y
```

Note: The upgrade or installation takes approximately 20 minutes to complete.

6 Eject the CD that contains the CS2M software from the CD-Rom drive of the CS 2000 Management Tools server.

7 You have completed this procedure.

Initializing the NPM database

Application

Use this procedure to initialize the Network Patching Manager (NPM) database.

Prerequisites

Only the root user can perform this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “Succession Element Configuration” option by typing

```
select - 13
```

and pressing the Enter key.

Example response

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SAM21EM Application Configuration
 3 - PSE Application Configuration
 4 - OMPUSH Application Configuration


 X - exit

select -
```

8 Select the “NPM Application Configuration” option by typing

```
select - 1
```

and pressing the Enter key.

Response

```
NPM Application Configuration
 1 - PFRS (Patch File Receipt System
     Configuration (PFRS))
 2 - CreateDB (Intialize or re-initialize the
     NPM database)


 X - exit

select -
```

9 Select the “CreateDB” option by typing

```
select - 2
```

and pressing the Enter key.

10 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

11 You have completed this procedure.

Setting up users on a Sun server

Application

Use this procedure to add new users on a Sun server and assign them to user groups, or assign existing users to user groups (see User groups).

ATTENTION
User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

The default authentication mechanism is UNIX. To change the authentication mechanism from UNIX to Distributed Computing Environment (DCE), refer to procedure “Changing the authentication mechanism between UNIX and DCE” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

User groups

Users of the Nortel Networks OAM&P client applications must belong to the primary user group “succssn” for login access. Users must also belong to one or more Secondary user groups listed in the table below, which specify the operations a user is authorized to perform.

Note: If upgrading from a release prior to SN06, existing users must be assigned to primary group “succssn” for login access, and to one or more Secondary user groups to specify the operations the user is authorized to perform, as shown in step 13 of this procedure.

User groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
trkro	lnro	mgcro	mgro	emsro

Secondary user groups

A secondary user group consists of a user group domain (see table User group domains), which defines the range of applications to which a user group applies, and a user group operation (see table User group operations), which dictates the operations a user can perform using the Nortel Networks OAM&P client applications.

User group domains

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operations

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.

User group operations

Operation	User role mapping
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

- Node provisioning operations
- Carrier provisioning operations
- Audit operations
- Alarm operations
- Internet transparency operations
- Trunk provisioning operations
- Trunk maintenance operations
- ADSL provisioning operations
- Line provisioning operations
- Line maintenance operations
- V5.2 provisioning operations
- CS 2000 SAM21 operations

For patching operations using the Network Patch Manager (NPM), assign users to the “emsadm” secondary user group.

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
disAssocMg		x			
assocMG		x			

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
changeMG		x			
querySiteInfo					x
queryGWC					x
queryMG					x
changeMGGWCEMData		x			
getPEPServerData					x
queryGWCPEPConn					x
getDQosPoliciesData					x

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
configureAudit	x				
runAudit	x				
getAuditDescription					x
getAuditConfiguration					x
getListOfRegisteredAudits					x
retrieveAuditReport					x
takeActionOnProblem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
addCarrier		x			
deleteCarrier		x			
getEndpoint					x
getCarrier					x
getCarrierByFilter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
set/unset ack			x		
all other functions (query related)					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
queryNAT					x
queryMP					x
ChangeAssocNAT		x			

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
getTuple					x
getTupleRange					x
getCMClli					x
addTuple		x			
replaceTuple		x			
delTuple		x			
listAllTuples	x				
suspendApplication	x				
restoreApplication	x				

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Post by trunk CLLI					x
D-channel Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
ICOT			x		
D-channel maintenance by trunk CLLI			x		
Post by gateway					x
QES by gateway					x
Set CM CLLI			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
getSubscriber					x
addSubscriber				x	
addCrossConnection				x	
modifySubscriber				x	
modifyCrossConnection				x	
deleteSubscriber				x	
deleteCrossConnection				x	

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
validateLineUsingDnClli					x
validateLineUsingTidClli					x

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
getLinePostInfo					x
bsyLine			x		
rtsLine			x		
frlsLine			x		
inbLine			x		
cancelDeload			x		
getCmClli					x
getEnpointState					x
getGwlp					x

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5Ring)					x					x
Add, modify, delete ringing cadence mapping (V5Ring)		x					x			

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View signalling characteristic profile, update list (V5Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
view carrier-to-interface and interface-to-carrier mappings					x					x

CS 2000 SAM21 operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
add, modify, or decommission a SAM21 network element		x			
reprovision a SAM21 node		x			
configure IPoA services, ATM PMC addresses		x			
view alarms, cards, subnet, shelf, mate shelf, mate card					x
lock/unlock a card			x		
perform diagnostics			x		
modify provisioning		x			
perform a swact			x		
firmware flash			x		
assign/unassign services		x			

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group “succssn” by typing

```
# useradd -g succssn <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table User groups) and any other user groups you noted in step 12 to which the user already belonged (include comma between groups, but no space)

userid
is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

Note: The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

14 You have completed this procedure.

Starting the SESM server application

Application

Use this procedure to start the SESM server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, start the SESM server application as follows:

a Start the SESM server by typing

```
# ptmctl -f start
```

and pressing the Enter key.

b Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

c Verify the SESM server application started by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS -------------------------------

  COMPONENT                    STATUS
  --------                     ------
 Proxy Agent                   RUNNING
 RMI Registry                  RUNNING
 Snmpfactory                   RUNNING
 MI2 Server                    RUNNING

Current number of SESM processes running: 4
(of 4)

SESM APPLICATION STATUS: All Applications
ready
```

7 For the SN06.2 or greater release, start the SESM server application as follows:

Note: In a two-server configuration, perform the steps that follow on the active side.

a Start the SESM server application by typing

```
# servstart SESMService
```

and pressing the Enter key.

b Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

c Verify the SESM server application started by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

8 You have completed this procedure.

Starting the NPM server application

Application

Use this procedure to start the Network Patch Manager (NPM) server application.

Prerequisites

Both CORBA and the database must be installed.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, start the NPM server application as follows:

a Start the NPM server application by typing

```
# npmsrvr start
```

and pressing the Enter key.

b Verify the NPM server application started by typing

```
# npmsrvr status
```

and pressing the Enter key.

Example response:

```
The NpmServer is running
```

Note: Wait approximately 1 min. before using the NPM.

7 For the SN06.2 or greater release, start the NPM server application as follows:

Note: In a two-server configuration, perform the steps that follow on the active side.

a Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

b Verify the NPM server application started by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

Note: Wait approximately 1 min. before using the NPM.

8 You have completed this procedure.

Configuring NPM for automatic patch file delivery

Application

Use this procedure to configure the Network Patch Manager (NPM) for automatic patch file delivery, which consists of enabling the Patch File Receipt System (PFRS). When the PFRS is enabled, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis. You can also use this procedure to verify whether the PFRS is already enabled.

Prerequisites

A valid secure ID and password is required to enable PFRS. This secure ID must belong to the primary user group “succssn” and the secondary user group “emsadm”. See “Setting up users on the Sun server” in the Administration and Security document, NN10281-600, if required.

CAUTION

To avoid failure of automatic patch file delivery, the secure id “pfrs” must remain locked (NOT assigned a password) and must use kshell.

For details, see Secure id pfrs restrictions and Query or configure the secure id pfrs.

Secure id pfrs restrictions

Observe the following restrictions to the secure id pfrs to avoid failure of automatic patch file delivery:

- Do not assign a password. Automatic patch delivery will fail when the password expires.
- Do not use other shells. Automatic patch delivery will fail until you reset the shell to kshell.
- Do not delete the pfrs secure id. If the pfrs secure id is deleted, contact your next level of support.

Query or configure the secure id pfrs

Use the secure id superuser to query or restore pfrs account defaults as follows:

- To display pfrs settings, use "logins -x -l pfrs".
- To lock pfrs, use "passwd -l pfrs"
- To set the default shell to kshell use "usermod -s /bin/ksh pfrs".

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where the NPM software resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “Succession Element Configuration” option by typing

```
select - 13
```

and pressing the Enter key.

Example response:

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SAM21EM Application Configuration
 3 - PSE Application Configuration
 4 - OMPUSH Application Configuration


 X - exit

select -
```

8 Select the “NPM Application Configuration” option by typing

```
select - 1
```

and pressing the Enter key.

Example response:

```
NPM Application Configuration
  1 - PFRS (Patch File Receipt System
      Configuration (PFRS))
  2 - CreateDB (Initialize or re-initialize the
      NPM database)

  X - exit

select -
```

9 Select the “PFRS” option by typing

```
select - 1
```

and pressing the Enter key.

If PFRS is	Do
disabled	step 10
enabled	you have completed this procedure

10 When prompted, confirm you want to enable PFRS by typing

y

and pressing the Enter key.

11 When prompted, enter a valid NPM Succession login ID.

12 When prompted, enter a valid password associated with the NPM Succession login ID.

13 When prompted, enter the host name or IP address of the interface server where patch files are to be delivered.

14 When prompted, enter the user ID that will be used to log in to the patch-file drop-off server.

Note: The user ID must have read, write, and overwrite privileges in the FTP user’s default directory on this server.

15 When prompted, enter the password associated with the patch-file drop-off server user ID.

16 When prompted, re-enter the password associated with the patch-file drop-off server user ID to confirm the password.

17 When prompted, enter the CLLI ID of the Communication Server 2000 associated with the office.

Note: You can obtain the CLLI ID from table OFCENG on the Communication Server 2000. Use the POS (position) command to locate the OFFICE_CLLI_NAME tuple. The value of this tuple, is the CLLI ID.

18 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

19 You have completed this procedure.

Restoring NPM data

Application

Use this procedure to restore any user-defined Network Patch Manager (NPM) data such as set definitions, report definitions, alarm definitions, plan definitions or SystemPlan modifications made in the release you upgraded from, that are to be carried over to the new release. This data should have been captured prior to the upgrade using procedure Saving user-defined NPM data using the NPM.

Note: NPM patch files are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support.

Prerequisites

The SSPFS and CS2M software upgrades are complete.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

At the NPM CLUI or GUI

5 With the information you collected prior to the upgrade using procedure Saving user-defined NPM data using the NPM, restore user-defined data from the previous release as follows:

a Restore all user-defined set definitions using procedure Defining sets using the NPM in this document, for each set you recorded.

b Restore all user-defined report definitions using procedure Defining reports using the NPM in this document, for each report you recorded.

c Restore all user-defined alarm definitions using procedure “Defining alarms with the NPM” in the ATM/IP Fault Management document, NN10325-900 for each alarm you recorded.

d Restore all user-defined patch definitions using procedure Saving a task using the NPM in this document, for each patch you recorded.

e Restore any modifications you made to the SystemPlan using procedure Defining a plan using the NPM in this document.

6 You have completed this procedure.

Modifying the QoS Collector Application

Application

Use this procedure to modify the configuration details for the QoS Collector Application (QCA) on the Sun server.

Prerequisites

You need the root user ID and password to log in to the Sun server where the QCA software resides.

Action

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where the QCA software resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Edit the QCA properties file by typing

 # vi /opt/nortel/qca/properties/qca.properties

and pressing the Enter key.

Example response

```
# QCA Properties file
# The QCA will have to be restarted for changes in the properties
# file to be reflected in the application's operation.

# port name to start application on.
# Default is 20000
portNumber=20001

# The maximum size of a file, in MBytes, before it is closed
# Range is 1 to 100
# Default is 1
MaxFileSize=10

# The maximum time, in minutes, a file can be open before it is
# closed
# Range is 1 to 240
# Default is 15
MaxFileTime=10

# How long, in days, the files are kept before deleting
# Range 1 to 30.
# Default is 5
RetainFileTime=3

# Hour of the day that the directory structure is recycled
# Range 0 (12:00 AM) to 23 (11:00 PM) Do NOT specify minutes.
# Default is 0
recycleToD=14

# File Extension used in the QCA output file name.
# Default is xml
fileExt=xml

# Node name to be used in the QCA output file name.
# Default in QCA.
nodeName=CS2K1

# 'true' or 'false' value indicating whether the output file
# should be compressed when closed. Default is true.
closedFileCompression=true

# 'true' or 'false' value indicating whether the file should be
# compressed at the first directory recycle
# Note: If closedFileCompression is true the value of the
# oldFileCompression property is negated as the files will have
# already been compressed. Default is true.
oldFileCompression=true
```

6 Modify the desired properties. The properties you can modify are described in the table below.

Name	Description	Range	Default
Port number (see Note 1)	The port number the QCA accepts connections on.	20000 to 20004	20000
MaxFileSize	The maximum size an output file can be before it is closed. ***Note:*** It is recommended to set this value to 10 MBytes. This reduces the number of file rotation during high traffic period.	1 to 100 MBytes	1
MaxFileTime	The maximum time the output file can be open before it is closed.	1 to 240 minutes	15
RetainFileTime	The length of time the output files should be retained.	1 to 30 days	5
RecycleToD	The hour in the day the directories are to be recycled. ***Note:*** It is recommended to set this value to a time of day when the traffic is low, such as 2.	0 to 23 hours	0
FileExt	The output file extension.	string	xml
NodeName	The node name to be used in the output files.	string	QCA
ClosedFileCompression (see Note 2)	The file should be compressed when closed and moved to today.	true or false	true
OldFileCompression (see Note 2 and Note 3)	The files should be compressed at the first directory recycle.	true or false	true

Note 1: A range of port numbers is provided for flexibility. The main use is for upgrade purposes where two QCA instances may be running on a single host. Multiple QCA instances, and therefore port numbers, should not be used to segregate QCA traffic.

Note 2: File compression may be required as there is limited disk space to store QCA IPDRs.

Note 3: If *ClosedFileCompression* is true, the value of the *OldFileCompression* is negated as the files will have already been compressed.

7 Exit the edit session and save the changes by typing

zz

and pressing the Enter key.

8 Stop and restart the QCA for the changes in the QCA properties file to take place. Refer to procedure “Starting and stopping the QoS Collector Application” in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required.

9 You have completed this procedure.

Installing the QCA software package on a separate server

Application

Use this procedure if you want to install the QCA software package on a separate server. In doing so, you will be able to perform in-service upgrades with no loss of records.

Note: Adding another QCA instance in the network requires that the GWC be associated with that QCA. Refer to the GWC Configuration Management document, NN10205-511, for instructions on how to associate a QoS collector to a GWC.

Prerequisites

The server must be running the SN06 release of the Succession Server Platform Foundation Software (SSPFS).

Action

Perform the following steps to complete this procedure.

At your workstation

1. Log in to the CS2000 Management Tools server where the first instance of QCA is running.
2. FTP the NTQCA.pkg onto the other server running SSPFS.
3. Telnet to that server by typing

   ```
   > telnet <server>
   ```

   and pressing the Enter key.

   where

   server
   is the IP address or hostname of the second server running SSPFS
4. When prompted, enter your user ID and password.
5. Change to the root user by typing

   ```
   $ su - root
   ```

   and pressing the Enter key.
6. When prompted, enter the root password.

7 Install the QCA software package by typing

```
# pkgadd -d NTQCA.pkg
```

and pressing the Enter key.

8 You have completed this procedure.

To configure QCA, refer to procedure Modifying the QoS Collector Application in this document.

Upgrading APS software

Application

Use this procedure to upgrade the APS software from release APS07 (SN05) or APS08 (SN06) to release APS08_2 (SN06.2) on the CS 2000 Management Tools server.

ATTENTION
Only perform this procedure if you are upgrading from SN05 or SN06 to SN06.2 where APS is on the same server as the CS 2000 Management Tools.

Prerequisites

Ensure you have the CD that contains the APS and IPS database software required for an upgrade to release APS08_2 (SN06.2).

Action

At the CS 2000 Management Tools server console

1 Log in to the CS 2000 Management Tools server through the console (port A) using the root user ID and password.

2 Uninstall the APS07 or APS08 software as follows:

a List the APS software package and any patches that have been applied by typing

```
# pkginfo | grep aps
```

and pressing the Enter key.

The existing installed APS07 or APS08 software package and any patches display.

b Remove any patches that were displayed in the previous step by typing

```
# pkgrm NTaps<aps_release>P<#>
```

and pressing the Enter key.

where

aps_release
is 07 or 08.

#
is an APS patch number.

Repeat this command for each patch listed in the previous step.

c Remove the APS software by typing

```
# pkgrm NORTips
```

and pressing the Enter key.

```
# pkgrm NTaps<aps_release>
```

and pressing the Enter key.

where

aps_release
is 07 or 08.

3 Install the APS08_2 software as follows:

a Insert the APS08_2 CD into the CD-ROM drive.

b Display the CD label by typing

```
# df
```

and pressing the Enter key.

c List the content of the CD by typing

```
# ls /cdrom/<cd_label>
```

and pressing the Enter key.

where

cd_label
is the CD label you obtained in the previous step

d Copy the software from the CD by typing

```
# cp /cdrom/aps08_2/* /
```

and pressing the Enter key.

e Install the APS software files by entering the following commands:

```
# pkgadd -d NTaps08_2-<xx.y>.pkg
```

and pressing the Enter key.

```
# pkgadd -d NORTips08_2-<xx.y>.pkg
```

and pressing the Enter key.

where

xx.y
is the version of the package listed on the CD

If the system prompts you about installing conflicting files, enter **n** (no). Enter **y** (yes) when the system prompts you to continue.

Note: This is a safe stopping point in this procedure.

f Run the APS software installation by typing

```
# ./start.sh 2>&1 | tee /startinstall.log
```

and pressing the Enter key.

Note: This is a safe stopping point in the procedure.

4 Eject the APS08_2 CD from the CD-ROM drive.

5 You have completed this procedure.

Proceed to procedure Configuring the SNMP agent in this document.

Note: To secure access to your APS system, perform procedure, “Setting the APS administrator password” in the UAS Security and Administration document, NN10161611.

Configuring the SNMP agent

Alarms are managed, sorted, and viewed on the Universal Audio Server Manager. The alarms are delivered to the Universal Audio Server Manager by system software known as the “Simple Network Management Protocol (SNMP) agent.” The Universal Audio Server Manager server IP address that the SNMP agent delivers alarms to is established immediately after installation of the APS system by performing the procedure below. This procedure is also used if the IP address of the Universal Audio Server Manager changes later on.

Configuring the SNMP agent

At the command line

1 Perform the following procedure:

a telnet to the CS 2000 Management Tools server

b log in using the “maint” login and password

c become the “root” user by entering:

```
su - root
```

2 Type the following command to stop the SNMP agent:

APSagentctl stop

Note: If this command is not found, enter the full path for the command, /opt/uas/SnmpAgent/bin/APSagentctl stop

3 After the system response, “APS Agent terminated” displays, type the following command:

configure_agent

Note: If this command is not found, enter the full path for the command, /opt/uas/SnmpAgent/bin/configure_agent

4 In response to the prompt, “Enter your selection,” enter either 1 or 2

where:

1
specifies that new configuration data is to be entered

2
specifies that previous configuration data is to be restored

If	Do
you entered 1	step 5
you entered 2	step 18

5 In response to the prompt, “What is the element manager’s IP address?” enter either 1 or 2

where:

1
specifies the default IP address

2
specifies that another IP address is to be entered

If	Do
you entered 1	step 7
you entered 2	step 6

6 In response to the prompt, “Enter the correct IP address” enter the IP address.

7 In response to the prompt, “What port does the element manager use to receive traps or alarms/logs?” enter either 1 or 2

where:

1
specifies the default port number, 162

2
specifies that another port number is to be entered

If	Do
you entered 1	step 9
you entered 2	step 8

8 In response to the prompt, “Enter the element manager’s port for receiving traps,” enter the port number.

9 In response to the prompt, “Should the agent forward alarms/logs to syslog?” enter either 1 or 2

where:

1
specifies “yes”

Note 1: APS system logs are available for viewing only in the var/log/ptmlog file.

Note 2: Forwarding alarms/logs to the syslog ensures backup access to this information.

2
specifies “no”

If	Do
you entered 1	step 10
you entered 2	step 11

10 In response to the prompt, “What is the logging level?” enter either 1, 2, or 3

where:

1
specifies “error messages”

2
specifies “error and warning messages”

3
specifies the default logging level, “error, warning, and information messages”

11 In response to the prompt, “What port does the agent use to receive SNMP messages from the element manager?” enter either 1 or 2

where:

1
specifies the default port number, 5161

2
specifies that another port number is to be entered

Note: If error messages display indicating that the port you have selected is already in use and cannot be used unless you specify it when you are logged in as the “root” user, either:

- log in again, restart the configure_agent program (see step 3), select 2 when you perform this step, and enter a different port number

or

- log in as the “root” user, restart the configure_agent program, and select 1 again when you perform this step

Note that the port number you select must also then be set in the Universal Audio Server Manager station when the APS is added to the network topology.

If	Do
you entered 1	step 13
you entered 2	step 12

12 In response to the prompt, “Enter the agent’s port for receiving SNMP messages,” enter the port number.

13 In response to the prompt, “What Read community string should the agent use to authenticate SNMP GET messages?” enter either 1 or 2

where:

1
specifies the default, “public”

2
specifies that another Read community string is to be entered

Note: You can enter 2 if you do not want a public SNMP read community string.

If	Do
you entered 1	step 15
you entered 2	step 14

14 In response to the prompt, “Enter the new Read community string,” enter the Read community string.

15 In response to the prompt, “What Write community string should the agent use to authenticate SNMP SET messages?” enter either 1 or 2

where:

1
specifies the default, “admin”

2
specifies that another Write community string is to be entered

Note 1: You can enter 2 if you do not want an admin SNMP Write community string.

Note 2: Make sure that you specify the same Write community string when you add an APS to the network topology through the Universal Audio Server Manager.

If	Do
you entered 1	step 17
you entered 2	step 16

16 In response to the prompt, “Enter the new Write community string,” enter the Write community string.

17 In response to the prompt, “What SNMP version should the agent use in sending SNMP messages? (enter either 1, for v1, or 2, for v2 (default))

18 After the system response, “Saving information to ApsAgent.conf” and “Saving information to ApsSnmpAgent.sh” displays, a UNIX shell prompt will display. Enter, then, the following command to start the SNMP agent:

/opt/uas/SnmpAgent/bin/APSagentctl start

Note: This step manually restarts the SNMP agent. If the command is not used, the SNMP agent is automatically restarted when the system is rebooted.

19 Verify that the agent has started by entering the following command:

`more /opt/uas/aps/scripts/SnmpAgent.pid`

If the agent has started, a process id (pid) displays.

20 Verify that the process is running by entering:

`ps -ef | grep nnnn`

where *nnnn* is the process id that was displayed in step 19.

21 You have completed this procedure.

Migrating the CS 2000 SAM21 Manager data

Application

Use this procedure to migrate the CS 2000 SAM21 Manager data from the CS 2000 Core Manager to the CS 2000 Management Tools server.

ATTENTION

Rollback after this point requires that you perform procedure Performing a rollback of the CS 2000 SAM21 Manager in this document.

Prerequisites

Procedure Preparing for the CS 2000 SAM21 Manager data migration was completed prior to the upgrade.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Stop the SAM21 Manager server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

Example response

```
Stopping group using servstop

Stopping the Succession SAM21 Element Manager:

 SAM21 Element Manager Server has been TERMinated and unregistered with pmfadm.

 SNMP Access Gateway has been TERMinated and unregistered with pmfadm.

SAM21EM Stopped
```

6 Migrate the SAM21 Manager data from the CS 2000 Core Manager to the CS 2000 Management Tools server by typing

```
# /opt/nortel/sam21em/bin/migration/sam21emMigration.sh
```

and pressing the Enter key.

This script imports backup data from the CS 2000 Core Manager using scp, and populates the SAM21EM database.

Example response

```
SAM21 Element Manager Server Persistent Data Migration
==============================================
Transferring data from 47.142.128.16 (SDM IP configured on SSPFS).
Checking if persistent data already exists...
Secure copying sam21emMigration.tar from SDM
sam21emMigration.tar 100%
|*****************************************************
10240          00:00
Retrieving Oracle SAM21 EM Password...
Extracting persistence.
Processing file: /tmp/scusql1.txt
Log file for /tmp/scusql1.txt available at: /tmp/scusql1.txt.log
Attempting to reserve physical and logical IPs
based on SAM21 EM provisioned card data.
Successfully reserved IP addresses from provisioned card data.
SAM21 Element Manager persistent data successfully migrated.
```

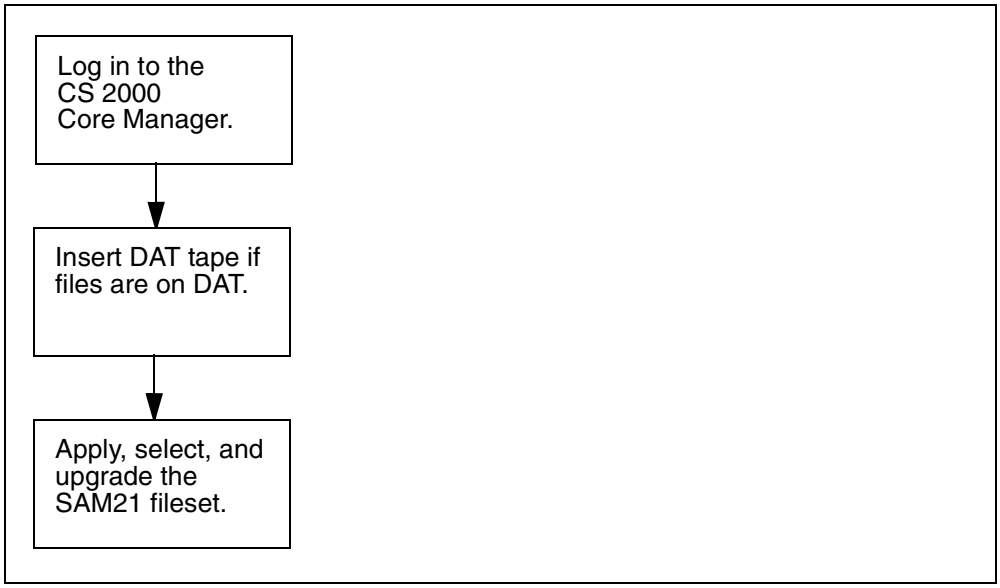
7 You have completed this procedure.

Installing SAM21 fileset

This procedure installs the Shelf Controller software on the CS 2000 Core Manager so that the CS 2000 Core Manager can serve the software to a BOOTP request from a Shelf Controller. Before performing this procedure, upgrade the CS 2000 SAM21 Manager server software on the CS 2000 Core Manager and install the CS 2000 SAM21 Manager package on the CS 2000 Management Tools server. Refer to *Upgrading the CS 2000 Management Tools*, NN10062-461.

Do not remove old SAM21 Shelf Controller fileset (NCL and MNCL filesets of the same release) unless there is not enough disk space in the `/swd/sam21` volume to apply new releases. If required, follow the procedure listed in section Old fileset removal on page 136.

The following figure summarizes the procedure.



At the SDM frame

1 If the SAM21 fileset is on Digital Audio Tape (DAT), insert the DAT tape in slot 2 or slot 13.

At the Core Manager console or terminal window

2 Log in to the CS 2000 Core Manager as the root user.

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

3 Enter the SDM maintenance level by typing

#sdmmtc

4 Enter the Software Installation Menu level by typing

>swim

5 Enter the Apply level by typing

>apply

6 Retrieve the fileset from tape by typing

>source <dat_no>

dat_no
is 0 or 1. Use 0 if the DAT is in slot 2 and 1 if the DAT is in slot 13.

7 Select the new SAM21 Platform software from the Apply menu by typing

>select <fileset_no>

fileset_no
is an integer value and represents the new SAM21 Platform fileset such as “1”.

APPLY level of the CS 2000 Core Manager

```
    SDM        CON      NET      APPL     SYS      HW     CLLI: clli_name
     .          .        .        .        .       .      Host: hostname
                                                             Fault Tolerant
Apply
 0 Quit      Source: the tape drive 0 (DAT 0).
 2           Filter: OFF
 3 Source       # Fileset Description          Current        Available
 4 Reload       1 SAM21 Platform               NA             9.0.xxx.0
 5 Eject                        Filesets on the source: 1 to 1 of 1
 6
 7 Select
 8 Apply
 9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
  root
Time 11:22    >
```

The example is for an upgrade to a new release, such as SN05 to SN06. If the upgrade is a maintenance release upgrade, then the value under the “Available” column ends in a value equal to or greater than 1, such as 9.0.66.3, and the value under the “Current” column ends in a value less than “Available.”

8 Upgrade the SAM21 Platform software by typing

>apply

if this is a standard upgrade such as 8.0.10.0 to 9.0.xxx.0 and the CURRENT version is NA as indicated in the figure above

or

>upgrade

if this is a maintenance upgrade such as 9.0.xxx.y to 9.0.xxx.(y+n)

Note: The new SAM21 Platform software and flash are available to upgrade the software on the Shelf Controllers. The CS 2000 Core Manager installs these files in the /swd/sam21 directory.

9 Confirm the change by typing **YES** at the prompt. Enter **NO** to cancel the fileset upgrade.

```
> YES
```

Example of succesful application:

```
Command completed with no errors
```

At the SDM frame

10 Press the Eject button and remove the tape.

11 This procedure is complete.

Additional information

Do not use links in the filesystem for bootloads. Links defeat the caching mechanism and increase the time required to boot a Shelf Controller.

Old fileset removal

To remove old SAM21 Shelf Controller filesets, perform the following procedure.

At the Core Manager console or terminal window

1 Change directory to `/var/adm/sam21`:

```
# cd /var/adm/sam21
```

2 Copy the custlog, designlog, and statlog configuration files to a backup version in the `/var/adm` directory:

```
# cp custlog ../custlog.bak
# cp designlog ../designlog.bak
# cp statlog ../statlog.bak
```

3 Remove the old SAM21 Shelf Controller fileset at the SWIM level of the **sdmmtc** tool.

4 Make the `/var/adm/sam21` directory:

```
# mkdir -p /var/adm/sam21
```

5 Change directory to `/var/adm`, the location of the backup configuration files:

```
# cd /var/adm
```

6 Move the backup configuration files into the `/var/adm/sam21` directory, and remove the backup suffix:

```
# mv custlog.bak sam21/custlog
# mv designlog.bak sam21/designlog
# mv statlog.bak sam21/statlog
```

7 Reapply the current SAM21 Shelf Controller NCL fileset and then apply the current MNCL fileset again using the **sdmmtc apply** tool.

Starting the SAM21 Manager server application

Application

Use this procedure to start the SAM21 Manager server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, start the SAM21 Manager server application as follows:

a Start the SAM21 Manager server application by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl start
```

and pressing the Enter key.

b Verify the SAM21 Manager server application started by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl status
```

and pressing the Enter key.

7 For the SN06.2 or greater release, start the SAM21 Manager server application as follows:

Note: In a two-server configuration, perform the steps that follow on the active side.

a Start the SAM21 Manager server application by typing

```
# servstart SAM21EM
```

and pressing the Enter key.

b Verify the SAM21 Manager server application started by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

8 You have completed this procedure.

Launching CS 2000 Management Tools client applications

Application

Use this procedure to launch any one of the following CS 2000 Management Tools client application graphical user interfaces (GUIs):

- Trunk Maintenance Manager
- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

  Note: The Network Patch Manager also has a command line user interface (CLUI). Refer to procedure Accessing the Network Patch Manager CLUI in this document.

- Batch Configuration Monitor

This procedure offers the following four methods to launch a CS 2000 Management Tools client application:

- Launching applications from a web browser. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching applications from a desktop icon or Start menu (Windows only).

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching specific applications using a URL.

Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section “Client workstation requirements” in the CS 2000 Management Tools Basics document, NN10020-111.

ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you may experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following URL: http://developer.java.sun.com/developer/bugParade/bugs/4713003.html. A workaround for this issue is to download the latest ATI graphics driver from the following web site http://mirror.ati.com/support/driver.html. Contact your IT support team if you need assistance.

You need the IP address or host name of the CS 2000 Management Tools server, and a valid user name and password to launch an application.

Note: Users of the CS 2000 Management Tools client applications must belong to the primary user group “succssn” for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN102172-611.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.1_02.

Action

Launching applications from a web browser

At your workstation

1 Launch your web browser.

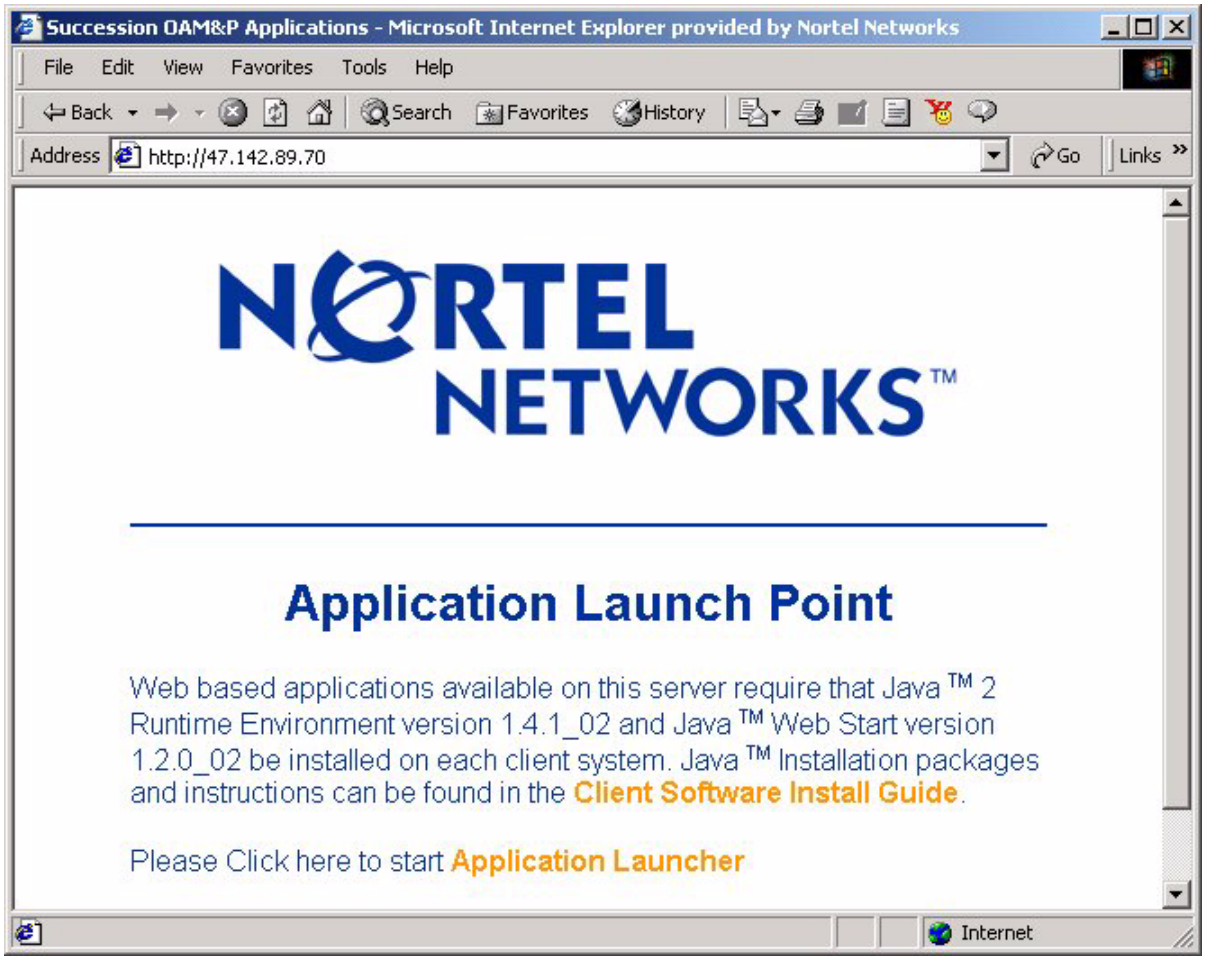
2 Access the CS 2000 Management Tools server by typing

>http://<host>

where

<host>
is the name or IP address of the CS 2000 Management Tools server where the CS2M software package is installed

The “Application Launch Point” page appears.



3 Refer to the following table to determine your next step.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 4
you do not know which version of JRE and JWS you have	step 4

4 Click **Client Software Install Guide** and follow the instructions under “How to check version” to verify your client setup.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 5

5 Click **Java 2 Runtime Environment Install Guide** under “Microsoft Windows” or “Sun Solaris” for system requirements and installation instructions.

6 Once you have read through the “Java 2 Runtime Environment Install Guide”, click the **Back** button to return to the “Client Software Installation” page.

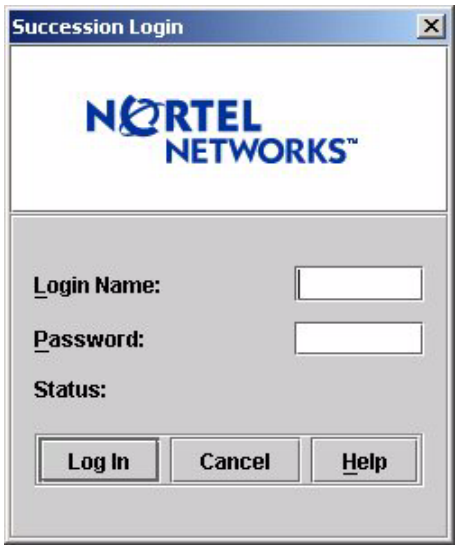
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

8 Click the **Back** button to return to the “Application Launch Point”.

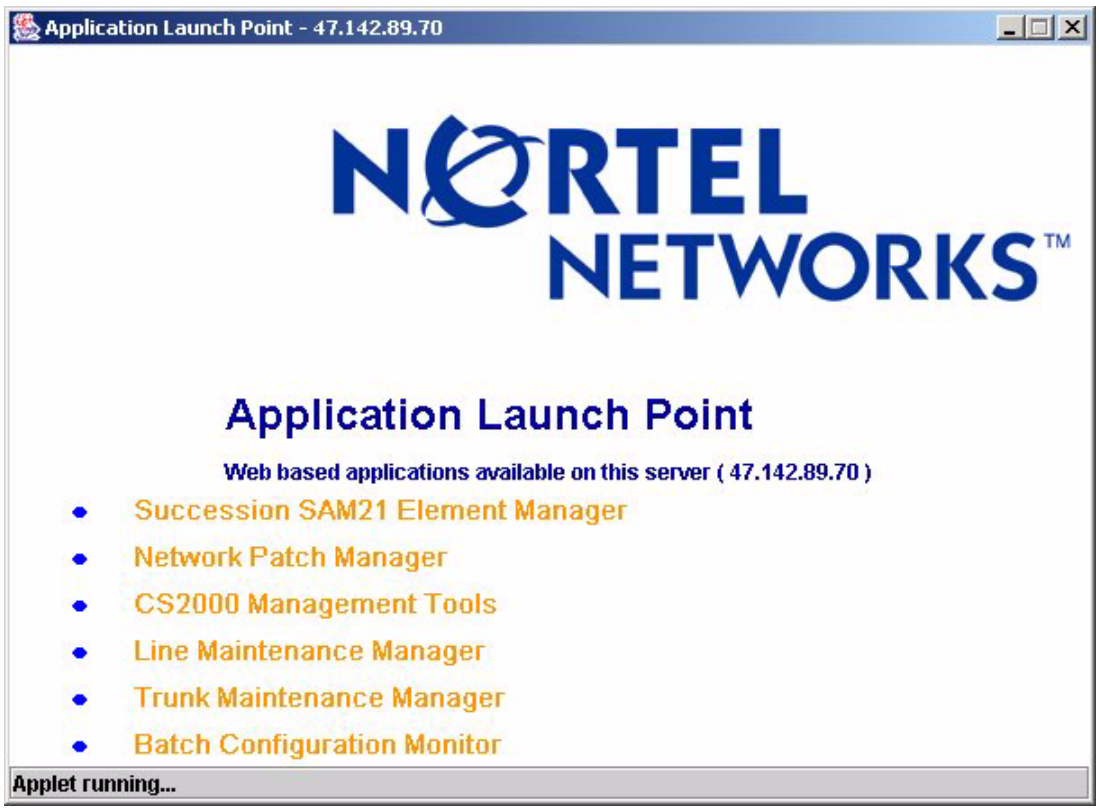
9 Click **Application Launcher**.

The Login window appears.



10 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



11 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

12 You have completed this procedure.

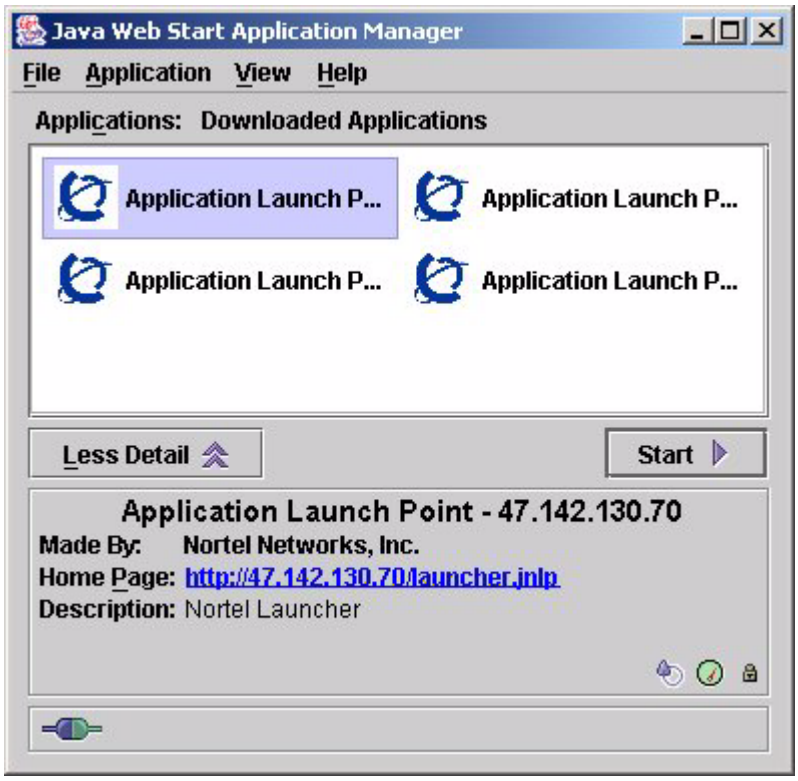
Launching applications from the JWS Application Manager

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Launch the Java Web Start Application Manager.

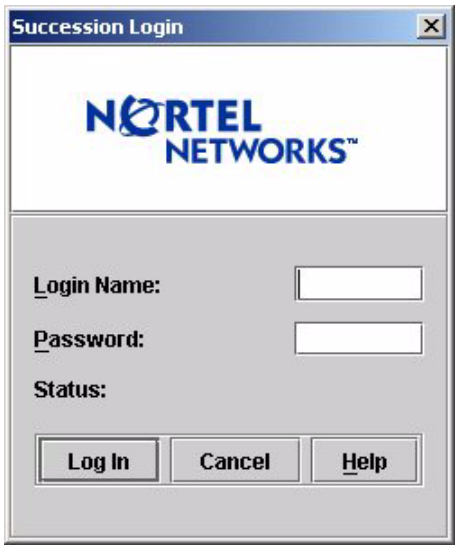


Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

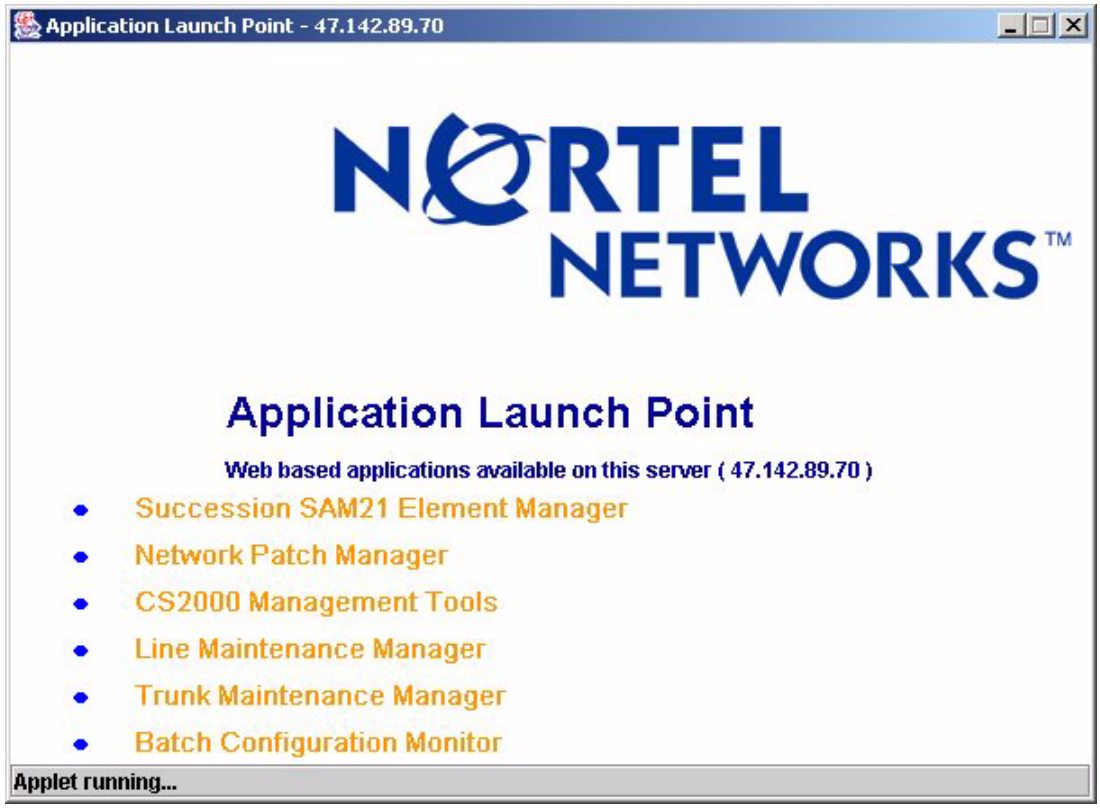
2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

The Login window appears.

3 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



4 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

5 You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

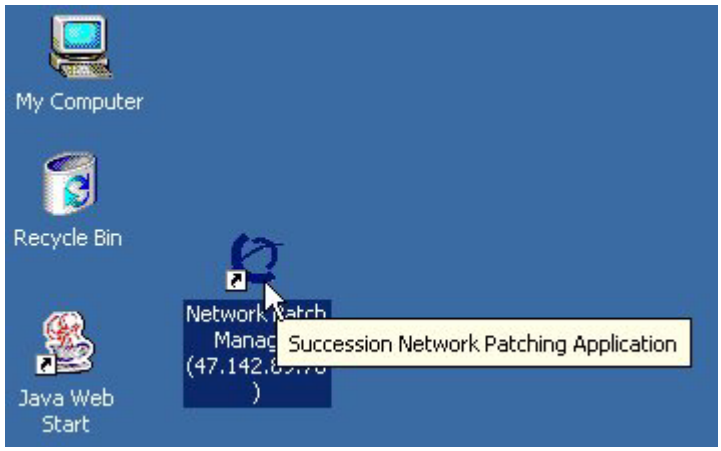
ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Perform step a to launch an application from a desktop icon, or b to launch an application from the Start menu.

a Locate the short-cut icon on your desktop, and double click on it to start the application.

Note: For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.

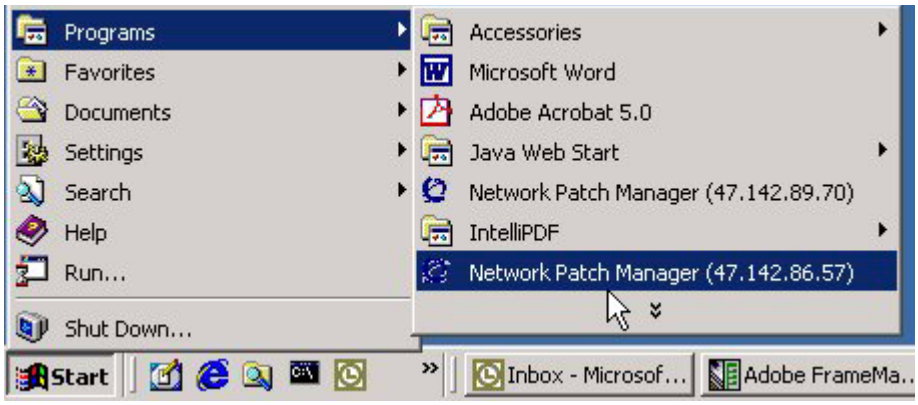


The Login window appears.

Proceed to step 2.

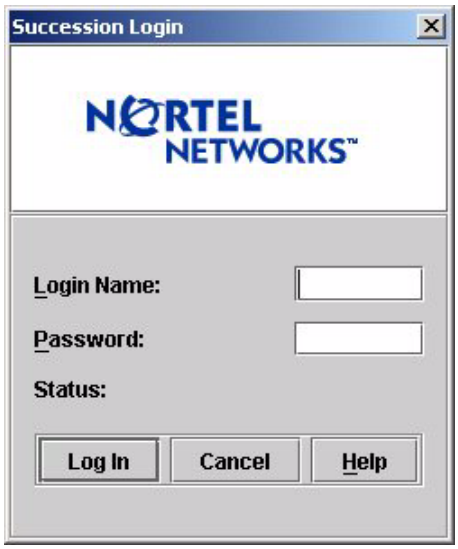
OR

b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click on the CS 2000 Management Tools client application you want to launch.

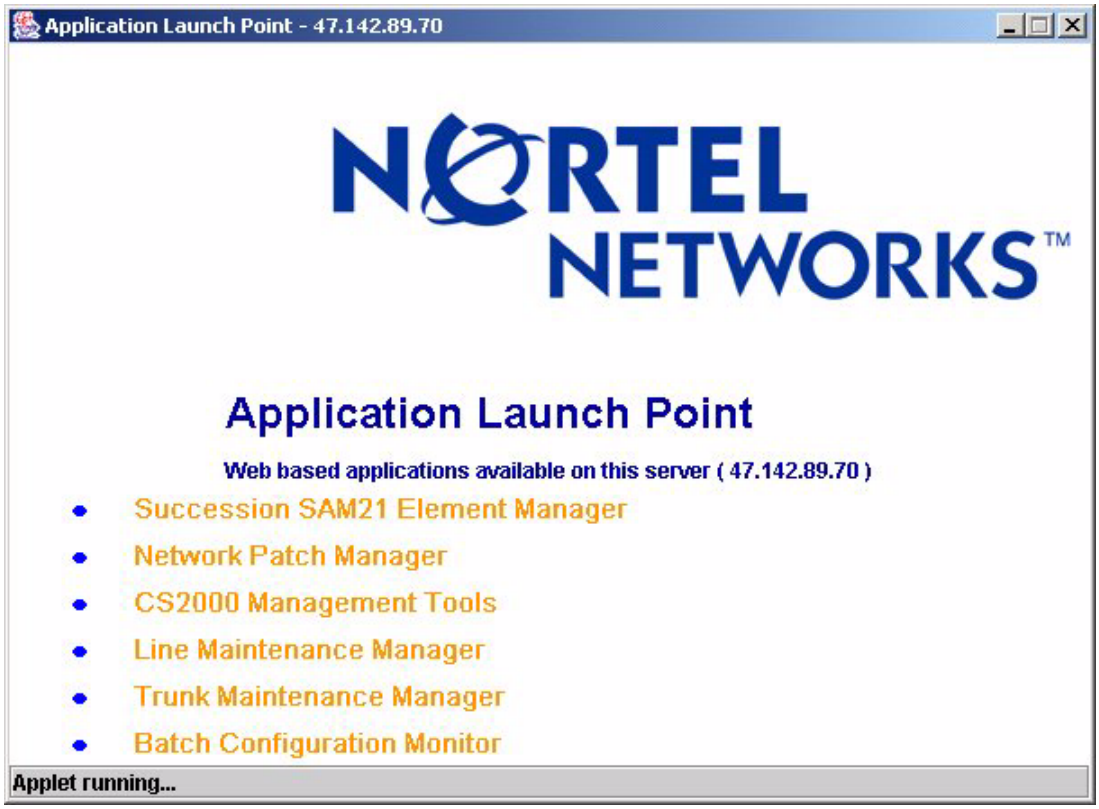


The Login window appears.

2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



3 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

4 You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure Launching applications from a web browser.

At your workstation

1 Launch your web browser.

2 In the Address field, enter one of the following URLs for the application you want to launch:

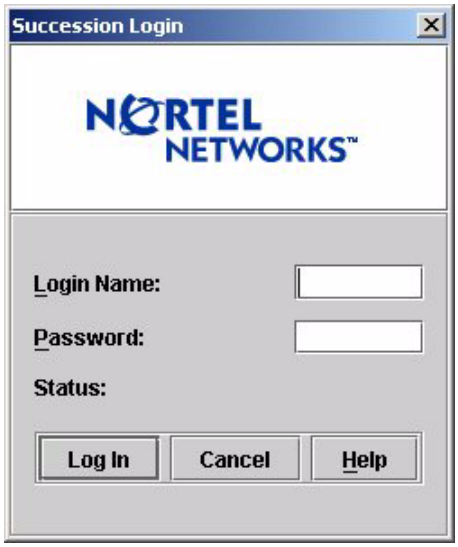
- CS2000 Management Tools - http://<host>/sesm/sesm.jnlp
- Line Maintenance Manager - http://<host>/sesm/lmm.jnlp
- Trunk Maintenance Manager - http://<host>/sesm/tmm.html
- Batch Configuration Monitor - http://<host>/sesm/bpt.html
- CS2000 SAM21 Manager - http://<host>/sam21em/sam21em.jnlp
- Network Patch Manager - http://<host>/npm/npm.jnlp

Where

host
is the host name or IP address of the CS 2000 Management Tools server

The Login window appears.

3 Enter your user name and password, then click **Log In**.

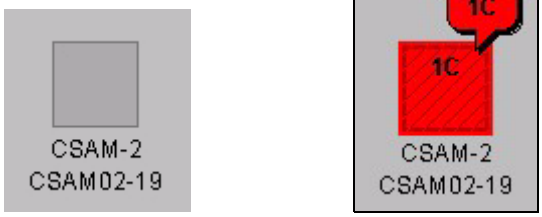


The interface for the application you launched, is displayed.

4 You have completed this procedure.

Upgrading software on the shelf controller

If this is an SN05 software upgrade to SN06, the shelf icon will appear isolated.



Not isolated Isolated

ATTENTION

During an upgrade to SN06, after the following procedure is completed, it is necessary to perform a Swact, Lock, and Unlock on the Shelf Controller that was upgraded first so that firmware parameters can be configured.

Monitor the progress text at the States tab as each Shelf Controller boots. The Shelf Controller that is upgraded first configures the second Shelf Controller. In order to configure the first Shelf Controller, it must be locked and unlocked so that the second Shelf Controller can configure it. This additional step is only performed once for each SAM21 shelf.

Before the firmware parameters for a Shelf Controller are configured, the progress text at the States tab includes the following lines:

```
Lock started
Locking in progress
Checking if SC firmware parameters are up to date
SC firmware parameters are not up to date
Configuring SC firmware parameters
Configuring netboot parameters
Configuring environment parameters
Saving configuration
SC firmware parameters configuration completed
Lock completed successfully
```

After the firmware parameters for a Shelf Controller are configured, the progress text at the States tab includes the following lines:

```
Lock started
Locking in progress
Checking if SC firmware parameters are up to date
SC firmware parameters are up to date
Lock completed successfully
```

Ensure that the progress text for both Shelf Controllers includes `SC firmware parameters are up to date.`

Client interfaces

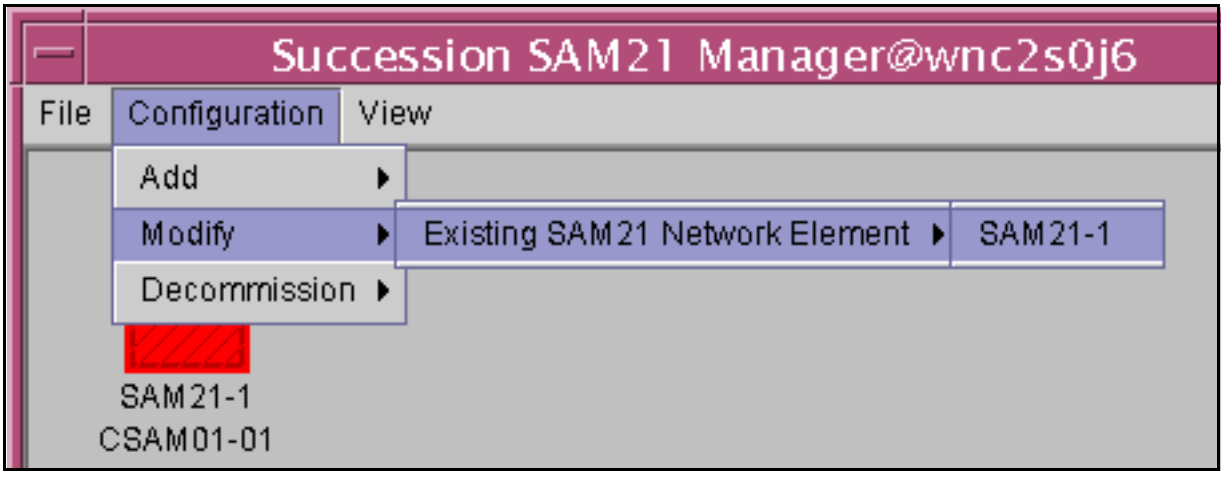
For the upgrade to SN06, two versions of the CS 2000 SAM21 Manager client are used. Use the Java Web Start client hosted by the CS 2000 Management Tools server to reprovision the software load in steps 1, 2, and 3. Use the client hosted by the CS 2000 Core Manager and started with the **/sdm/bin/sam21gui** to lock and unlock the Shelf Controllers as well as for SWACT in steps 5 through 10.

Detailed procedure

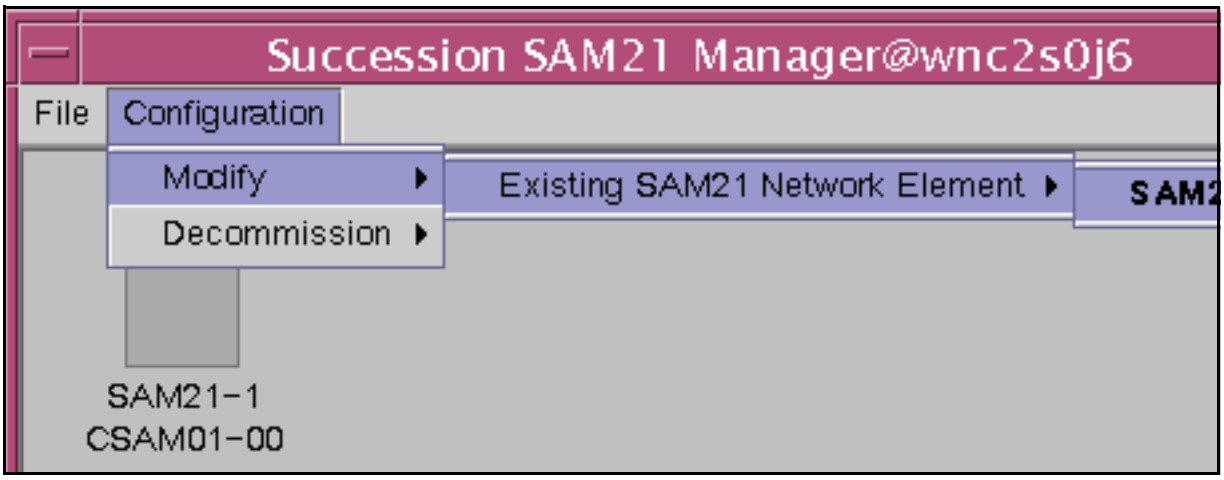
At the CS 2000 SAM21 Manager client (Java Web Start client)

1 From the Subnet View, select Configuration, Modify and then the SAM21 shelf with the Shelf Controllers to upgrade.

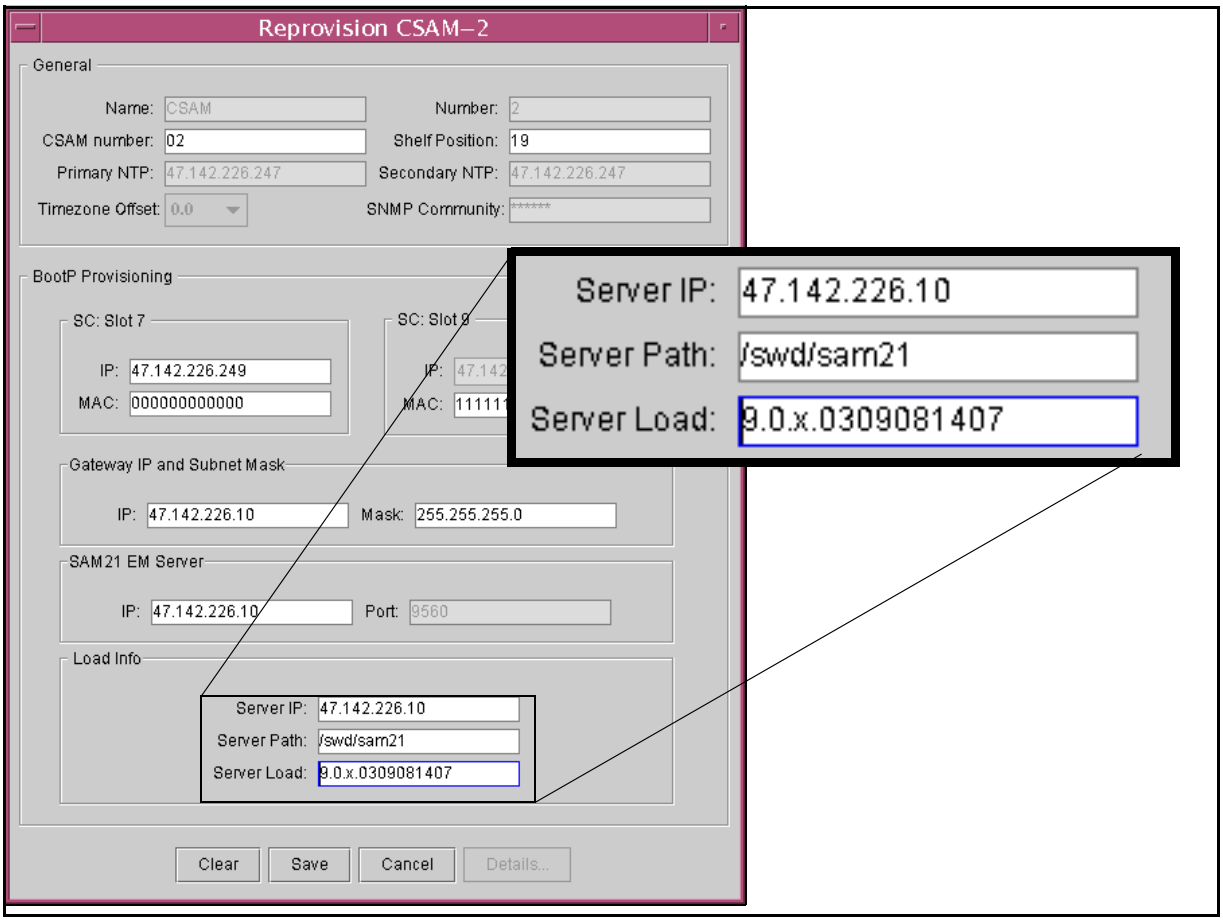
Upgrade to SN06



Upgrade from SN06 to SN06 or newer



2 Enter the new software load name in the Server Load field on the Reprovision window.



Note 1: For upgrades such as SN05 to SN06, x is equal to zero. For maintenance release upgrades, x is greater than or

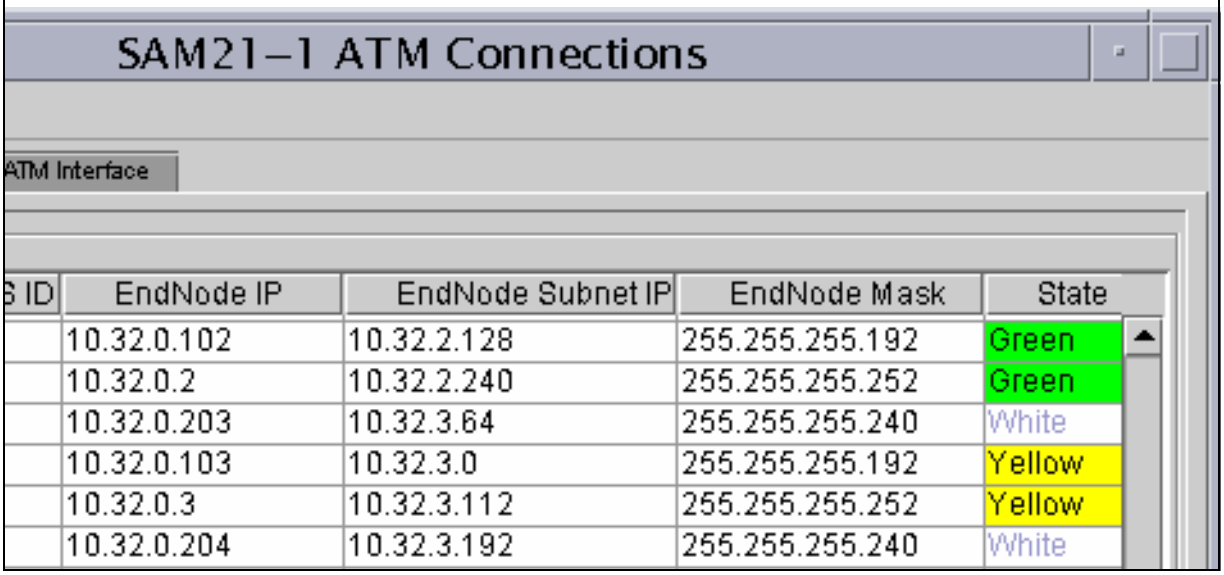
equal to zero. Refer to page 1-1 of the *SAM21 Platform Base Release Notes* for the correct value.

Note 2: This graphic shows the SN05 to SN06 upgrade. In SN06 to SN06 or newer upgrades, the Primary NTP, Secondary NTP, and Timezone Offset fields are available. During these same upgrades, the IP address, Gateway IP address, Server IP, and Server Path fields are unavailable.

3 Click Save on the Reprovisioning window to save the data and close the Reprovisioning window.

4 If the Shelf Controllers are provisioned with ATM interfaces, verify that the inactive Shelf Controller does not carry the active ATM link. Select Configuration and then IPOA Services from the subnet view to open the ATM Connections window.

Green - active ATM link is on active Shelf Controller
Yellow - active ATM link is on inactive Shelf Controller
Red - connection between Shelf Controller and end node existed but is currently broken
White - connection between Shelf Controller and end node is provisioned, but never connected



If all the connections are yellow, then SWACT the Shelf Controller at a period of low activity before proceeding. If some connections are green and some are yellow, as in the example, then check for alarms at the ATM equipment between the Shelf Controller and the end node with the yellow connection. Correct the condition, check again that all connections are green, and then proceed.

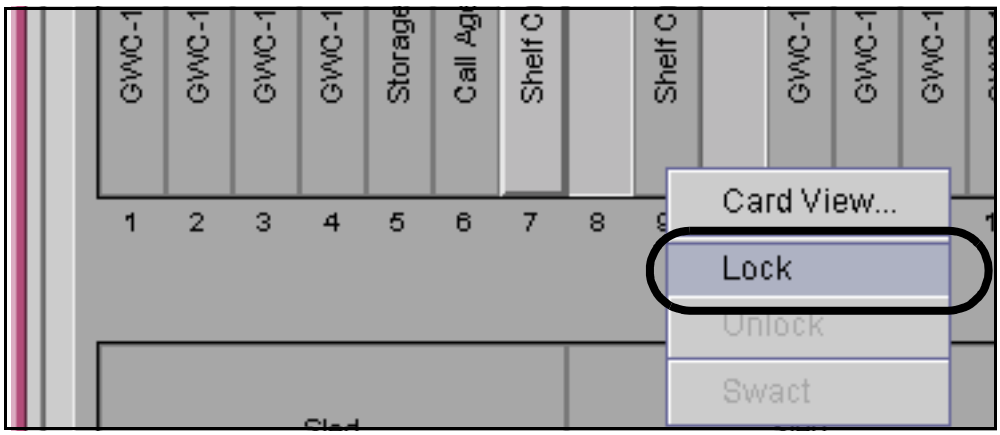
5

ATTENTION

If this is an SN05 to SN06 upgrade, perform steps 5 through 10 from the client that is hosted by the CS 2000 Core Manager and is started with the `/sdm/bin/sam21gui` command.

From the Shelf View window, right click on the card icon for the inactive Shelf Controller and select Lock from the context menu.

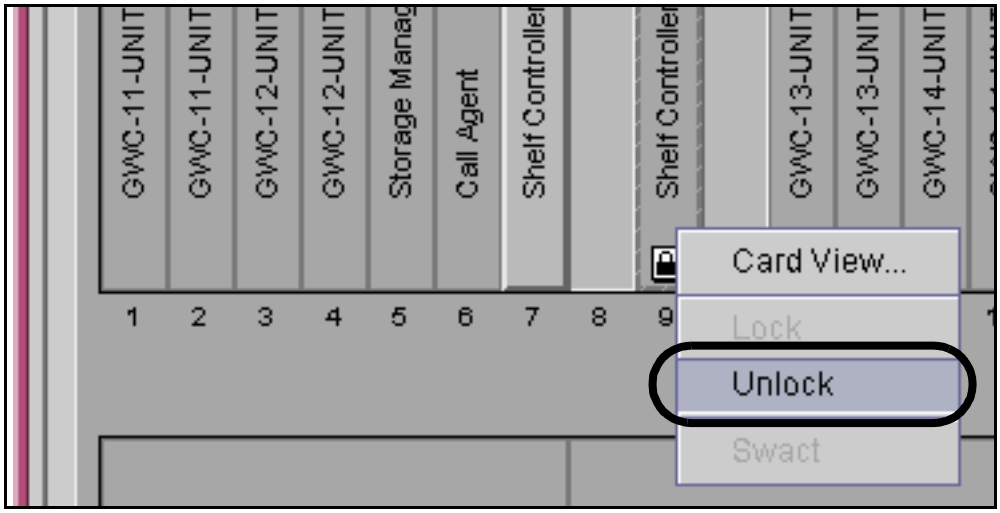
Note: The Lock menu option is only available for the inactive Shelf Controller.



6 Wait for the Lock icon to appear on the Shelf Controller icon and the other Shelf Controller to indicate that it is in simplex (alarm 2C on the other Shelf Controller).

Note: If the CS LAN is provided by Nortel Networks Passport 8000 series router switches, reprovision the port on the Passport to auto-negotiate. Refer to Reprovision Passport port to auto-negotiate on page 160.

7 Right click on the same Shelf Controller and select Unlock from the context menu and optionally verify that calls can originate and complete. The unlock request can require up to 10 minutes.



Note: Optionally monitor the download and boot of the card from the States tab of the Card View window. If the card does not boot or if the *SAM21 Base Platform Release Notes* indicates that upgraded firmware is included in the load, refer to procedure Shelf Controller does not unlock on page 164 for information about configuring firmware parameters.

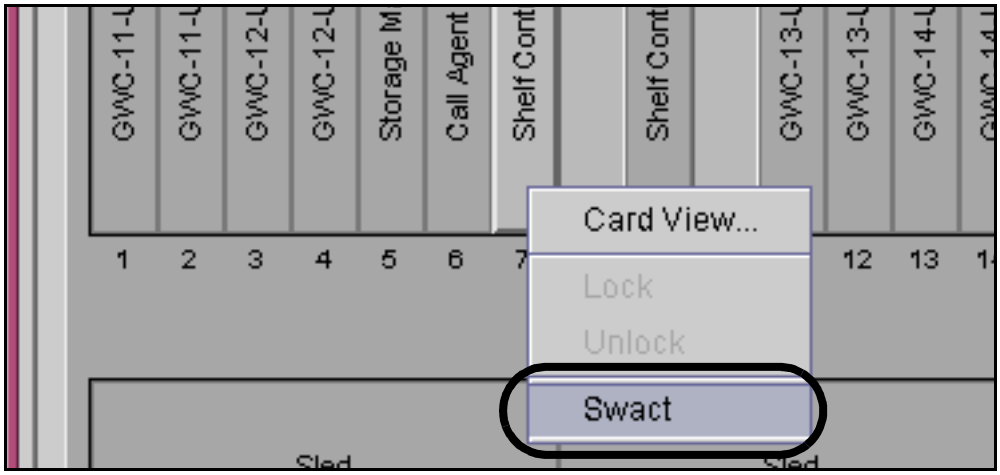
A successful boot reports the following message at the States tab of the Card View window:

```
Unlock started
Establishing control
Waiting for board to initialize
Beginning network boot
Issuing boot request
Unlock in progress
Waiting for SC to boot
SC is booting...
Unlock completed successfully
```

8 If required by operating company personnel, soak the new software load. If rollback to the previous release is required, refer to Rollback software on the shelf controller on page 281.

9 After the hashed outline disappears from the Inactive Shelf Controller, right click on the icon for the Active Shelf Controller and select Swact from the context menu.

If required by telephone operating company personnel, soak the new software and firmware after the Swact.



10

ATTENTION
Rollback is not supported after this step is completed.

Lock and unlock the newly Inactive card as in steps 5 and 7. If firmware configuration was required with the first card, perform the firmware configuration on the newly inactive card.

11 If this is the initial upgrade to SN06, Swact the Shelf Controllers again, and then Lock and Unlock the Shelf Controller that was upgraded first. This step ensures that the firmware parameters are configured correctly. Monitor the progress text at the States tab as the Shelf Controller boots.

12 This procedure is complete.

Reprovision Passport port to auto-negotiate

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Passport router switch.

At the CLI for the Passport

1 Determine the slot and port on the Passport that connects to the device:

`> show ip arp info <ip_address>`

ip_address
is the physical IP address of the SAM21 Shelf Controller, the Gateway Controller, or USP

The slot and port are reported.

```
prompt:cpu> show ip arp info 172.30.242.25
================================================================================
                                      Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
172.30.242.25    00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

Note: *If the response indicates MLT instead of the slot and port, perform this operation from the mate Passport unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.*

2 Set the slot and port to auto-negotiate:

`> config ethernet <slot>/<port> auto-negotiate enable`

The slot and port are reconfigured to auto-negotiate and the prompt returns.

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

3 Verify the port configuration:

`> show ports info config <slot>/<port>`

The slot and port configuration is displayed.

```
prompt:cpu> show ports config info 1/2

================================================================================
                                      Port Config
================================================================================

PORT                 AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT
NUM   TYPE           NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID
--------------------------------------------------------------------------------
1/2   100BaseTX      true  false  half  100   full  100   fals  core  1   0
```

4 Commit the change:

```
> save config
```

Shelf Controller does not unlock

If the Shelf Controller does not unlock and the lock icon persists on the SAM21 Shelf View, then the Shelf Controller failed to boot.

At the CS 2000 SAM21 Manager client workstation

1 Ensure that the Shelf Controller has enough time to boot. A Shelf Controller can take up to 4 minutes to boot on a slow network.

If the Shelf Controller has enough time to boot and still has a lock icon and a hashed outline, continue with this procedure.

At the SAM21 frame

2 Verify that the Shelf Controller is fully seated in the slot.

Note: Do not push on the faceplate to seat the card; use the levers.

3 Connect a VT100 terminal or a PC with terminal application software to the serial port labeled COM1 on the rear of the SAM21 shelf. If the Shelf Controller in slot 7 does not boot, connect to slot 7. If the Shelf Controller in slot 9 does not boot, connect to slot 9.

a To start the HyperTerminal application, click Start menu, click Programs, click Accessories, and click HyperTerminal.

b Double click the Hyperterm.exe icon to open a new connection.

The system displays the Connection Description box.

c Enter SC in the Name field and click OK.

The system displays the Phone Number box.

d Select Direct to COM1 from the “Connecting using:” list. Leave other entries in the box empty. Click OK.

e Open the COM1 Properties box and set the port settings to the following:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Flow control: Hardware

Click OK.

f Press the Enter key.

The system displays a new Hyperterm window with a login prompt.

4 Press the reset button on the faceplate while the console is connected and verify that the firmware revision is RM12 or the firmware revision indicated in the *SAM21 Platform Base Release Notes*.

```
Copyright Motorola Inc. 1988-2000, All Rights Reserved

PPC1 Debugger/Diagnostics Release Version 4.9 - 07/12/01 HA RM12
COLD Start

Local Memory Found=08000000 (&134217728)

MPU Clock Speed=367Mhz

BUS Clock Speed=67Mhz

WARNING: Keyboard Not Connected

Reset Vector Location   : ROM Bank B
Mezzanine Configuration : Single-MPU
Current 60X-Bus Master  : MPU0
Idle MPU(s)             : none

L2Cache                 : 1024KB, 147Mhz
System Memory           : 128MB, ECC Enabled (ECC-Memory Detected)


HA Mesquite Abbreviated Self-Tests about to Begin...
ISABRIDGE IRQ: Interrupt Request.....Running--->   PASSED

SelfTest/Boots about to Begin... Press <BREAK> at anytime to Abort ALL

NetBoot about to begin... Press <ESC> to Bypass, <SPC> to Continue
```

Firmware revision RM12

5 Press the **Esc** key to bypass NetBoot and access the PPC-Bug prompt.

6 Type **cnfg** at the PPC-Bug prompt and press Enter.

Note: The MAC address of the Shelf Controller card should be displayed. Verify that this is the address used in the CS 2000 SAM21 Manager client on the Reprovisioning window.

7 Type **niot** at the PPC-Bug prompt and press Enter.

8 The Shelf Controller software provides a series of prompts. Accept the default values except the following options in bold. For the options in bold, enter the value indicated in the table.

Note: If an error is entered, type **.** (period) and press Enter to quit. Restart niot by typing **niot** and pressing Enter.

Prompt	Value
Controller LUN	00
Device LUN	00
Node Control Memory Address	07F9E000
Client IP Address	**0.0.0.0**
Server IP Address	**0.0.0.0**
Subnet IP Address Mask	255.255.255.0
Broadcast IP Address	255.255.255.255
Gateway IP Address	**0.0.0.0**
Boot File Name	NULL
Argument File Name	NULL
Boot File Load Address	001F0000
Boot File Execution Address	001F0000
Boot File Execution Delay	00000000
Boot File Length	00000000
Boot File Byte Offset	00000000
BOOTP/RARP Request Retry	**00**
TFTP/ARP Request Retry	**00**
Hardware Error Retry Attempts	**20**
Trace Character Buffer Address	00000000
BOOTP/RARP Request Control	**A**

Prompt	Value
BOOTP/RARP Reply Update Control	**N**
Update Non-Volatile RAM (this prompt only appears if a change has been made)	**Y**

9 Type **env** at the PPC-Bug prompt and press Enter.

10 The Shelf Controller software provides a series of prompts. Accept the default values except the following options in bold. For the options in bold, enter the value indicated in the table.

Prompt	Value
Bug or System Environment	B
Field Service Menu Enable	N
Probe System for Supported I/O Controllers	Y
Auto-Initialize of NVRAM Header Enable	Y
Network PReP-Boot Mode Enable	**Y**
SCSI Bus Reset on Debugger Startup	N
Primary SCSI Bus Negotiations Type	A
Primary SCSI Data Bus Width	N
Secondary SCSI Identifier	07
NVRAM Boot List (GEV.fw-boot-path) Boot Enable	N
NVRAM Boot List (GEV.fw-boot-path) Boot at power-up only	N
NVRAM Boot List (GEV.fw-boot-path) Boot Abort Delay	5

Prompt	Value
Auto Boot Enable	N
Auto Boot at power-up only	N
Auto Boot Scan Enable	N
Auto Boot Scan Device Type List	FDISK/CDROM/TAPE/HDISK/
Auto Boot Controller LUN	00
Auto Boot Device LUN	00
Auto Boot Partition Number	00
Auto Boot Abort Delay	7
Auto Boot Default String	NULL
ROM Boot Enable	N
ROM Boot at power-up only	Y
ROM Boot Abort Delay	5
ROM Boot Direct Starting Address	FFF00000
ROM Boot Direct Ending Address	FFFFFFFC
Network Auto Boot Enable	**N**
Network Auto Boot at power-up only	N
Network Auto Boot Controller LUN	00
Network Auto Boot Device LUN	00
Network Auto Boot Abort Delay	5
Network Auto Boot Configuration Parameters Offset (NVRAM)	00001000
Watchdog prior status ignored at autoboot	**Y**
Watchdog reset at board reset	**Y**

Prompt	Value
Reset Ethernet chip after file reception	**Y**
Stop Auto Boot After Selftest Failure	N
Memory Size Enable	Y
Memory Size Starting Address	00000000
Memory Size Ending Address	08000000
DRAM Speed in NANO Seconds	50
ROM First Access Length (0-31)	10
ROM Next Access Length (0-15)	0
DRAM Parity Enable [On-Detection/Always/Never - O/A/N]	O (letter O)
L2Cache Parity Enable [On-Detection/Always/Never - O/A/N]	O (letter O)
PCI Interrupts Route Control Registers (PIRQ0/1/2/3)	0A050000
Serial Startup Code Master Enable	N
Serial Startup Code LF Enable	N
Claim domain A	N
Claim domain B	N
Slot power control word	00000000
Ignore healthy control word	00000000
Firmware Command Buffer Enabled	**Y**
Firmware Command Buffer Delay	**20**

Prompt	Value
Firmware Command Buffer	**cboot**<Enter key> **pboot 14 0**<Enter key> **nbo**<Enter key> <Enter key> **ma ;l**<Enter key> (letter L) **ma cboot**<Enter key> **NULL**
Update Non-Volatile RAM (this prompt appears only when a change is made)	**Y**
Reset local system (CPU)	Y

11 The Shelf Controller reboots.

12 Optionally verify that calls can originate and complete.

13 If this problem persists, contact Nortel Networks support personnel.

14 This procedure is complete.

Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server

Application

Use this procedure to migrate each provisioned SAM21network element from the CS 2000 SAM21 Manager on the CS 2000 Core Manager, to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server.

ATTENTION

This procedure requests that you reprovision each SAM21 network element using the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server and the CS 2000 SAM21 Manager client on the CS 2000 Core Manager. It is important that you reprovision the SAM21 network elements using both clients.

Prerequisites

None

Action

Launch the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server

At your workstation

1 Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

2 Reprovision each SAM21 network element, which involves changing the IP address in the “SAM21 EM Server” field to the IP address of the CS 2000 Management Tools server. Refer to procedure “Change the CS 2000 SAM21 Manager server address” in document Upgrading the SAM21 Shelf Controller, NN10067-461, and perform steps 1 and 2.

At this point, the CS 2000 Management Tools server bootp has updated the CS 2000 Core Manager bootp with the SAM21 EM server IP address change. However, the CS 2000 SAM21 network elements are still communicating with the CS 2000 SAM21 Manager on the CS 2000 Core Manager.

Launch the CS 2000 SAM21 Manager client on the CS 2000 Core Manager

At the client workstation

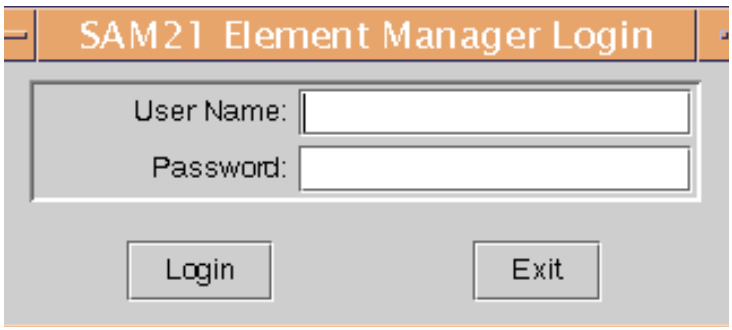
3 Log on to the client workstation using the correct user ID and password. Do not log on as the root user.

4 Launch the SAM21 Manager client application that resides on the CS 2000 Core Manager by typing

```
# /sdm/bin/sam21gui
```

and pressing the Enter key.

The user authentication window appears.



5 Enter a valid user name and password, and click **Login**.

6 Reprovision each SAM21 network element, which involves changing the IP address in the “SAM21 EM Server” field to the IP address of the CS 2000 Management Tools server. Refer to procedure “Change the CS 2000 SAM21 Manager server address” in document Upgrading the SAM21 Shelf Controller, NN10067-461, and perform steps 1 and 2.

An SNMP message is sent to both SAM21 shelf controllers with the IP and port of the CS 2000 Management Tools server. Within approximately 1 minute, the node recovers from isolation on the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server. Within approximately 2 minutes, the node will be isolated on the CS 2000 SAM21 Manager that resides on the CS 2000 Core Manager.

7 Decommission the isolated shelf. Refer to procedure “Deprovision a SAM21 shelf” in the SAM21 Shelf Controller Configuration Management document, NN10111-511, if required.

Persistent storage for the shelf is removed.

Note: The bootp entries on the CS 2000 Core Manager are not removed by the CS 2000 SAM21 Manager.

8 Remove the CS 2000 SAM21 Manager from the client workstation as follows:

a Log on to the client workstation using the root user ID and password.

b Remove the contents of the “/sdm” directory by typing

```
# rm -r /sdm/snm
```

and pressing the Enter key.

```
# rm -r /sdm/bin
```

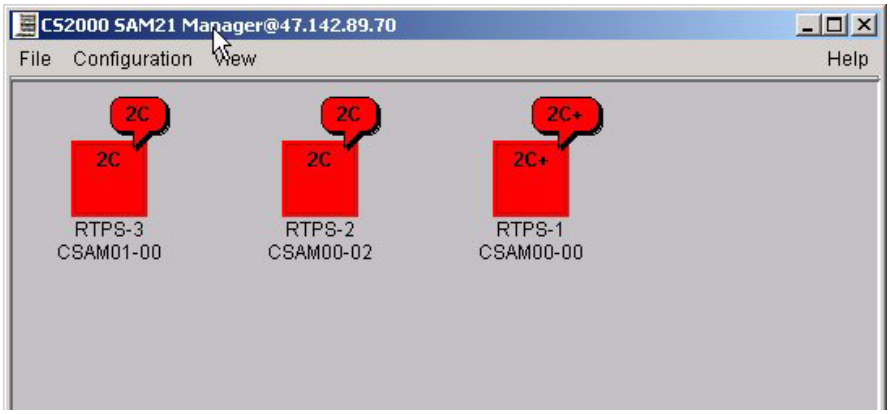
and pressing the Enter key.

At the CS 2000 SAM21 Manager client on the CS 2000 Management Tools server

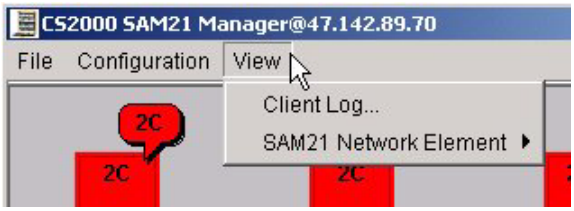
9 Verify that all SAM21 network elements are communicating with the CS 2000 SAM21 Manager on the CS 2000 Management Tools server as follows:

a Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server if not already available. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

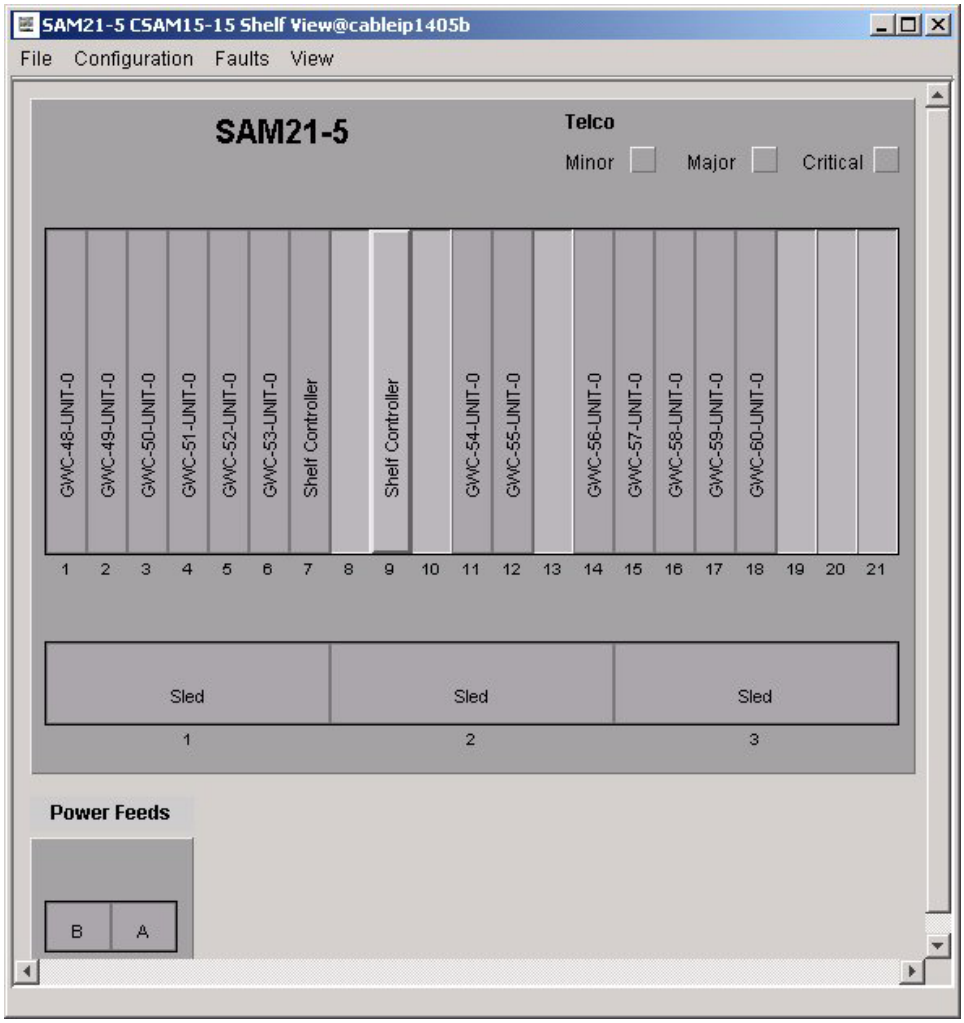
When you launch the CS2000 SAM21 Manager, the subnet view, similar to the following, is displayed.



b On the **View** menu, select **SAM21 Network Element**, and then select the first SAM21 network element in the list, or double click on the icon of the first SAM21 network element in the subnet display.



The shelf view of the SAM21 network element, similar to the following, is displayed.



c Repeat substep b to display the shelf view of each SAM21 network element.

If you	Do
cannot display the shelf view of the SAM21 network elements	substep d
can display the shelf view of the SAM21 network elements	you have completed this procedure

d Ensure you performed each step in this procedure. Contact support if necessary.

10 You have completed this procedure.

Completing the CS 2000 SAM21 Manager migration

Application

Use this procedure to run the SAM21 EM post-migration script and remove the Succession SAM21 Manager fileset from the CS 2000 Core Manager.

ATTENTION
Rollback after this point requires that you boot the CS 2000 Core Manager from the backup tape to rollback to the CS 2000 SAM21 Manager on the CS 2000 Core Manager.

Prerequisites

ATTENTION
Ensure you completed all the steps in procedure Migrating the SAM21 network elements to the CS 2000 SAM21 Manager on the CS 2000 Management Tools server in this document.

You need the root user ID and password for the CS 2000 Core Manager.

Action

At the CS2000 Core Manager console

1 Log on to the CS 2000 Core Manager using the root user ID and password.

2 Busy the CS 2000 SAM21 Manager as follows:

a Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.

b Busy the CS 2000 SAM21 Manager by typing

> **bsy <#>**

and pressing the Enter key.

Where:

<#>
is the number next to the Succession SAM21 Manager fileset

c Confirm the busy command by typing

> **y**

and pressing the Enter key.

The CS 2000 SAM21 Manager client application on the CS 2000 Core Manager shuts down after the busy command.

d Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

3

ATTENTION

This step deletes all persistent data for the CS 2000 SAM21 Manager in sdm/configdata/snm/persistence. Ensure you successfully migrated the data to the CS 2000 Management Tools server and reprovisioned all the SAM21 network elements to communicate with the CS 2000 Management Tools server before you proceed.

Run the SAM21 Manager post-migration script by typing

```
# /sdm/snm/bin/sam21emPostMigration.sh
```

and pressing the Enter key.

Example response:

```
SAM21 Element Manager Post Migration
====================================
WARNING:  This action will DELETE all persistent
data for the SAM21 Element Manager from
sdm/configdata/snm/persistence.
Please ensure you have successfully migrated the
data to the SSPFS platform and decommissioned
all nodes via the Element Manager before
proceeding.
```

Note: This step applies only for upgrades from SN05 or earlier.

4 Confirm the command by typing

```
# yes
```

and pressing the Enter key.

Example response:

```
SAM21EM post migration successful
```

5 Remove the Succession SAM21 Manager fileset as follows:

a Access the SWIM level by typing

```
# sdmmtc swim
```

and pressing the Enter key.

b Access the Details level by typing

```
> details
```

and pressing the Enter key.

c Select the Succession SAM21 Manager application by typing

> **select <#>**

and pressing the Enter key.

where

#
is the number next to the Succession SAM21 Manager fileset

d Remove the Succession SAM21 Manager application by typing

> **remove**

and pressing the Enter key.

e Confirm the removal by typing

> **y**

and pressing the Enter key.

Note: The remove command also removes the older version of the SAM21 platform fileset.

f Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

6 You have completed this procedure.

Transferring patches to the NPM database manually

Application

Use this procedure to manually transfer patches to the Network Patch Manager (NPM) database and retrieve them for processing. Patches can be delivered either on a CD or electronically.

> ***Note:*** You can enable automatic patch file delivery to the NPM database, including patch retrieval for processing, by enabling the Patch File Receipt System (PFRS). Refer to procedure “Configuring NPM for automatic patch file delivery” in the CS 2000 Management Tools Configuration Management documentm, NN10106-511, to enable PFRS or determine if it is already enabled.

Also use this procedure when you are attempting to audit or apply patches that have a blank patch category or patch status field.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Use the following table to determine how to proceed.

If patches were delivered	Do
on CD	step 2
electronically	step 3

2 Insert the CD that contains the patches into the CD drive of the Sun server where NPM resides.

At your workstation

3 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

4 When prompted, enter your user ID and password.

5 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If patches were delivered	Do
on CD	step 8
electronically	step 13

8 Make a temporary directory for the patchlist file by typing

```
# mkdir /data/npm/tmp
```

and pressing the Enter key.

9 Change the permissions on the temporary directory by typing

```
# chmod 777 /data/npm/tmp
```

and pressing the Enter key.

10 Create the .patchlist file for all the patches that are on the CD, in the temporary directory by typing

```
# find /cdrom -name "*.patch" >
/data/npm/tmp/current.patchlist
```

and pressing the Enter key.

11 Access the directory you just created by typing

```
# cd /data/npm/tmp
```

and pressing the Enter key.

12 Proceed to step 23.

13 Make a directory for the patch files you want to install by typing

```
# mkdir /data/npm/patch_upgrade
```

and pressing the Enter key.

14 Change the permissions on the newly created directory by typing

```
# chmod 777 /data/npm/patch_upgrade
```

and pressing the Enter key.

15 Access the newly created directory by typing

```
# cd /data/npm/patch_upgrade
```

and pressing the Enter key.

16 FTP to the ESD server by typing

```
# ftp <ESD_server>
```

and pressing the Enter key.

where

ESD_server
is the IP address of the ESD server

17 When prompted, enter your user ID and password for the ESD server.

18 Set the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

19 Transfer all the patches from the ESD server to the NPM by typing

```
ftp> mget *.patch
```

and pressing the Enter key.

Note: To transfer individual patch files, enter the following command:

ftp> get <patch_filename>

20 Exit FTP by typing

```
ftp> quit
```

and pressing the Enter key.

21 Verify the patches are in the temporary directory on the Sun server by typing

```
# ls
```

and pressing the Enter key.

22 Change permissions for the patch files in the directory by typing

```
# chmod 777 *
```

and pressing the Enter key.

23 Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
not running	step 24
running	step 25

24 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

25 Access the NPM command line user interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

26 When prompted, enter your user ID and password.

Note: Do not change directory.

27 Retrieve the patch files for the NPM to process as follows

If	Type
You want to retrieve the patch files copied from the CD	# **getpatch current.patchlist**
You want to retrieve the patch files copied from the electronic service delivery system (ESD)	# **getpatch <patch_filename>**

and press the Enter key.

where

patch_filename
is either the name of the file that contains names of the patch files to retrieve (must end with ".patchlist"), or an actual patch file

28 Eject the CD from the drive by typing

cd eject cdrom

and pressing the Enter key.

Note: You must change directory from the cdrom directory using the "cd" command for the "eject cdrom" command to execute successfully.

If you have	Do
other patch CDs	insert the next CD and go to step 10
no other patch CDs	close the cdrom tray

29 You have completed this procedure.

Accessing the Network Patch Manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

Note: The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure Launching CS 2000 Management Tools client applications in this document.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter 'npm' commands, help
or quit to exit.

npm>
```

5 You have completed this procedure.

Performing a device audit using the NPM

Application

Use this procedure to perform a device audit using the Network Patch Manager (NPM). You can perform a device audit using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

An audit determines whether the NPM database has accurate device patch information. If the patch category or patch status fields are blank for any patches, complete procedure Transferring patches to the NPM database manually in this document.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Audit the device by typing

`npm> auditd <devices>`

and pressing the Enter key.

where

devices
is a list of one or more device IDs for which you want to run the audit - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Note: Enclose the <deviceid> for GWC devices in single quotes (‘).

Example
`npm> auditd` ‘gwc3 Unit 1 47.142.108.39’

3 You have completed this procedure.

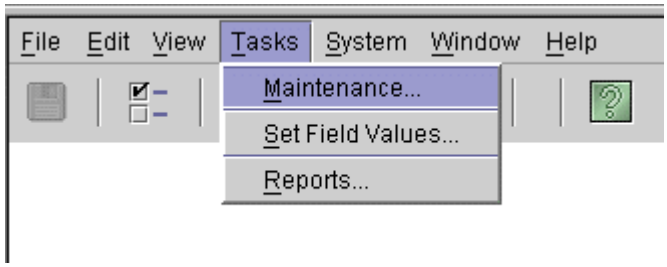
Using the NPM GUI

At your workstation

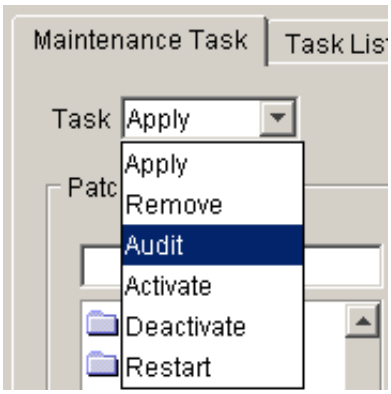
1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

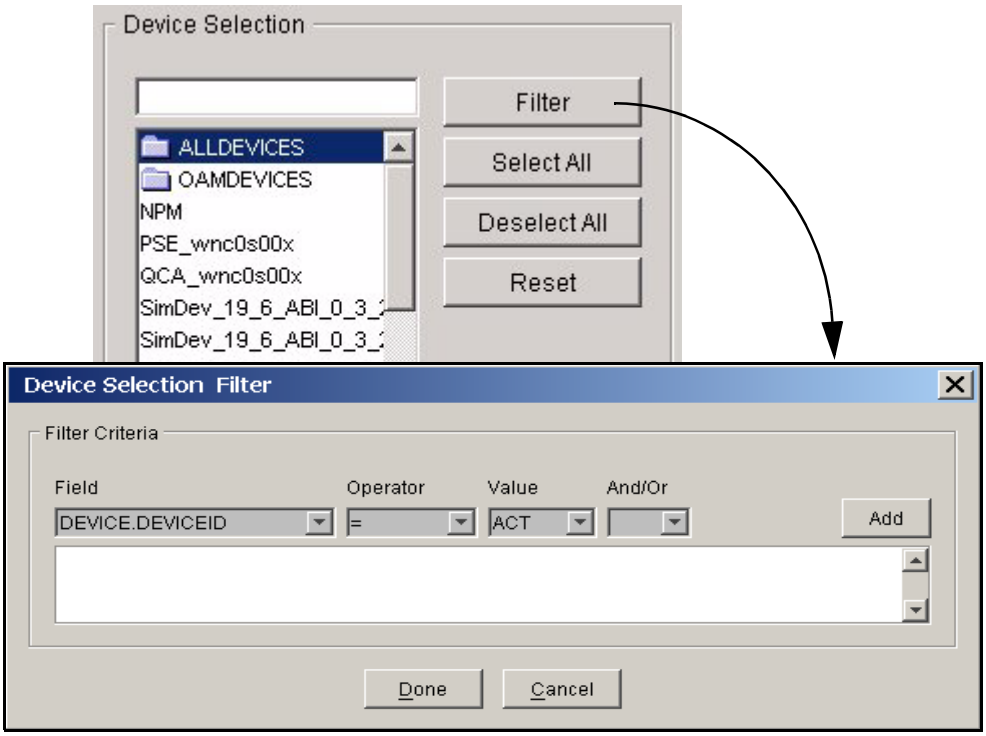
2 On the **Tasks** menu, click **Maintenance...**.



3 In the **Task** list, click **Audit**.

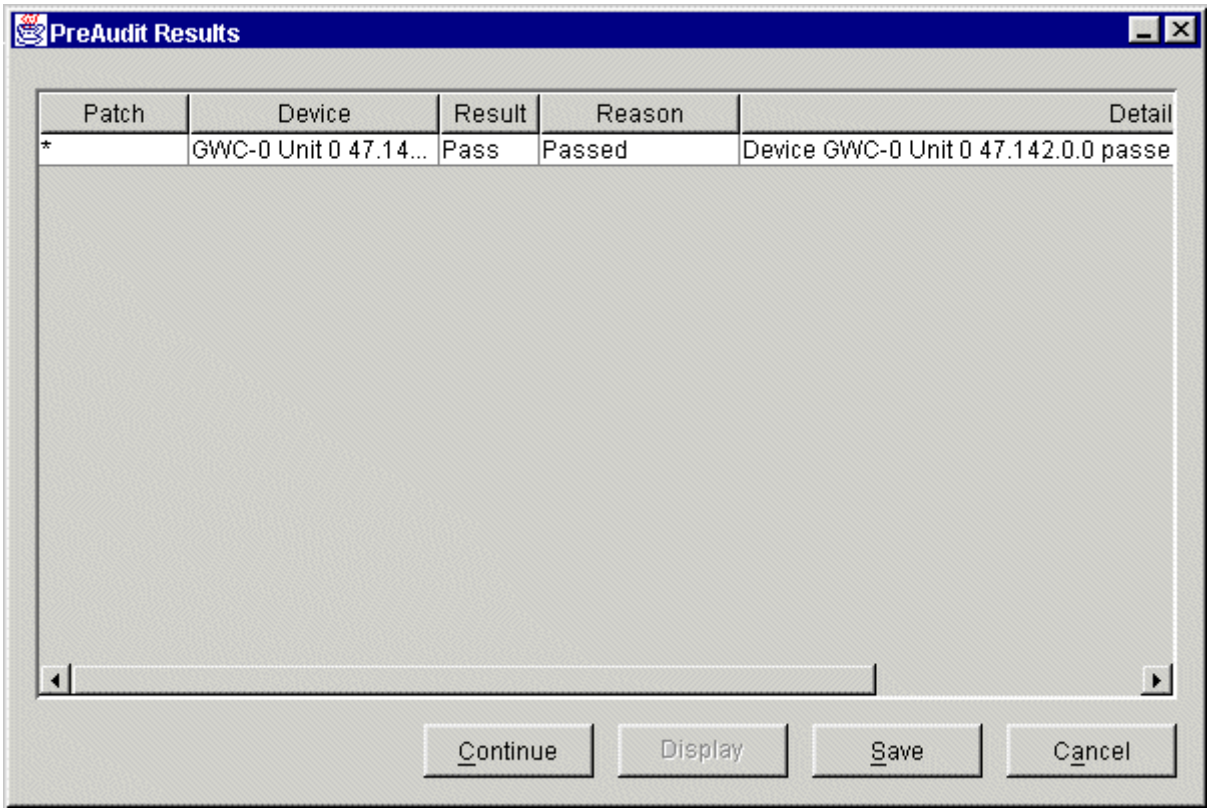


4 In the **Device Selection** list, select the devices or device sets you want to audit, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



5 Click **Execute** to begin the audit process.

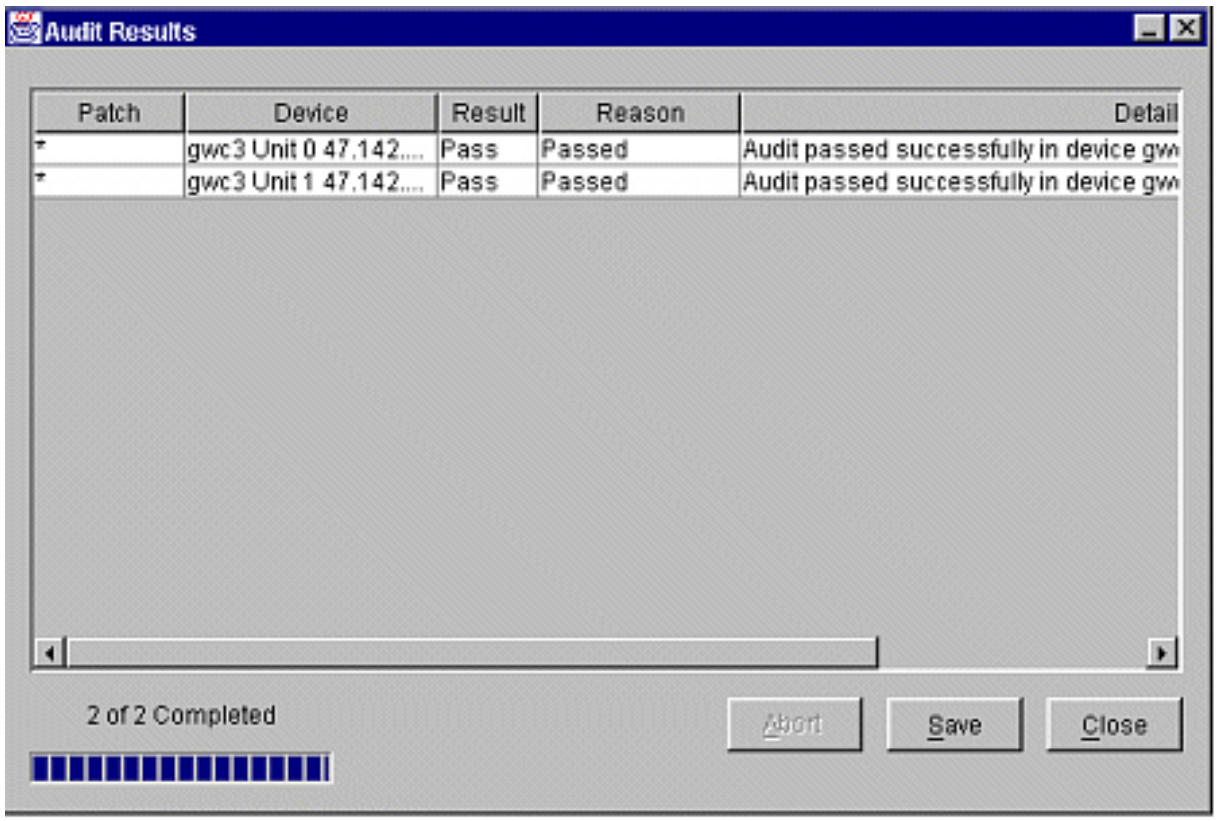
The results of the PreAudit phase are displayed.



6 Review the PreAudit Results, then click **Continue** to proceed.

Note: The Patch field in the Results Table will indicate an asterisk (*) for each operation since only the device is related to the operation.

The Audit Results window is displayed with results added as each action is completed. Failures from the PreAudit phase are also included in the results.



7 Click **Save** to save the results to a file, or click **Close**.

Note: If the audit does not successfully complete, abort the audit procedure and contact your next level of support.

8 You have completed this procedure.

Applying patches using the NPM

Application

Use this procedure to apply patches using the Network Patch Manager (NPM). You can apply patches using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Prerequisites

The patches must have already been installed in the NPM database. Contact your network administrator to determine if this has already been done. If required, refer to procedure Transferring patches to the NPM database manually in this document, to install the patches in the NPM database.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Apply one or more patches to one or more devices by typing

`npm> apply <patches> [in <devices>]`

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to apply - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices
is a list of one or more device IDs to which you want to apply the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and applies them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Note: Enclose the <deviceid> for GWC devices in single quotes (‘).

Example
`npm> apply` ACT02GAX in ‘gwc3 Unit 1 47.142.108.39’

3 When prompted, press the Enter key.

4 Generate a device query report to verify the patches are applied by typing

`npm> q device`

5 Enter the device name in the format **‘<deviceid>’** that you input in step 2.

Note: The GWC <device id> must be enclosed in single quotes (‘) only when the GWC device id has spaces, dashes or periods as part of its name.

A device report of known patch activity for the particular device associated with the <device id> is returned.

6 Verify from the report that the desired patches are applied (status =A).

Note: If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

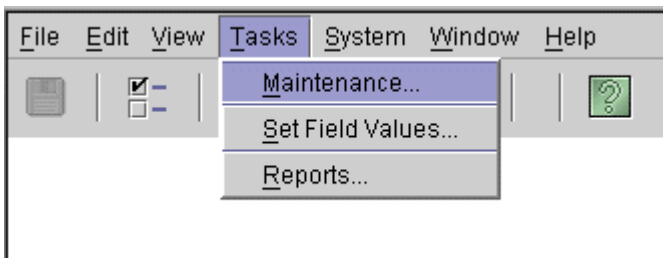
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

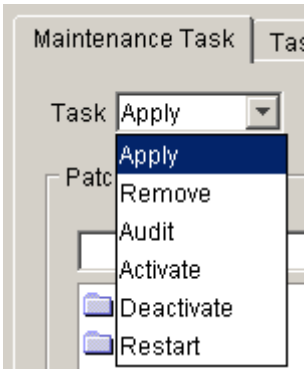
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

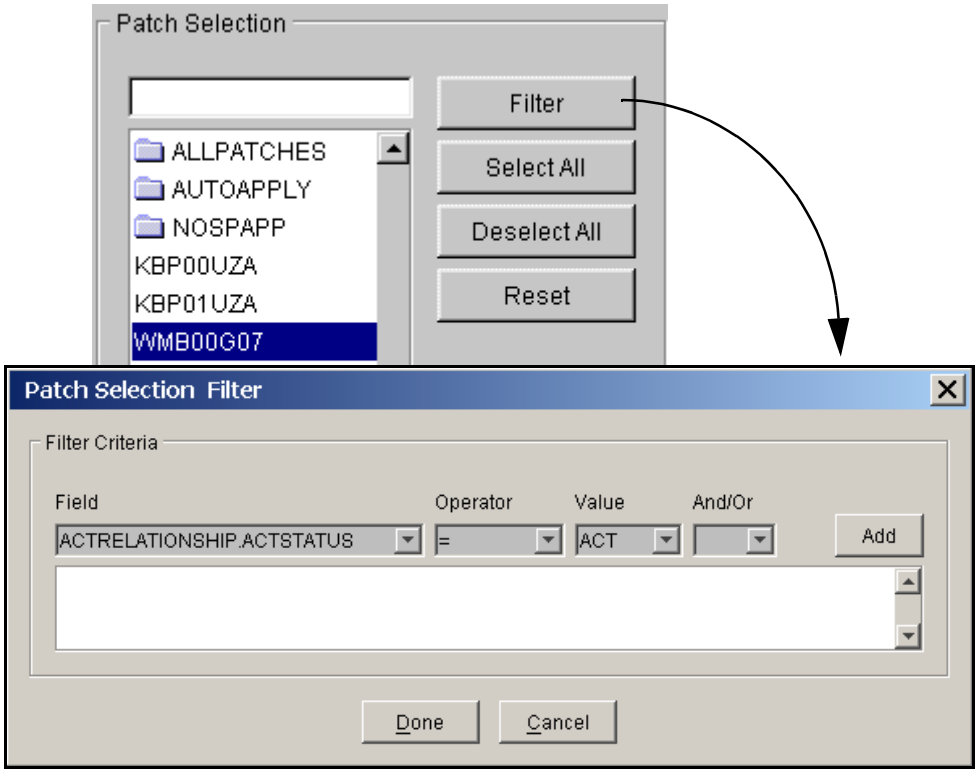


The Maintenance window is displayed.

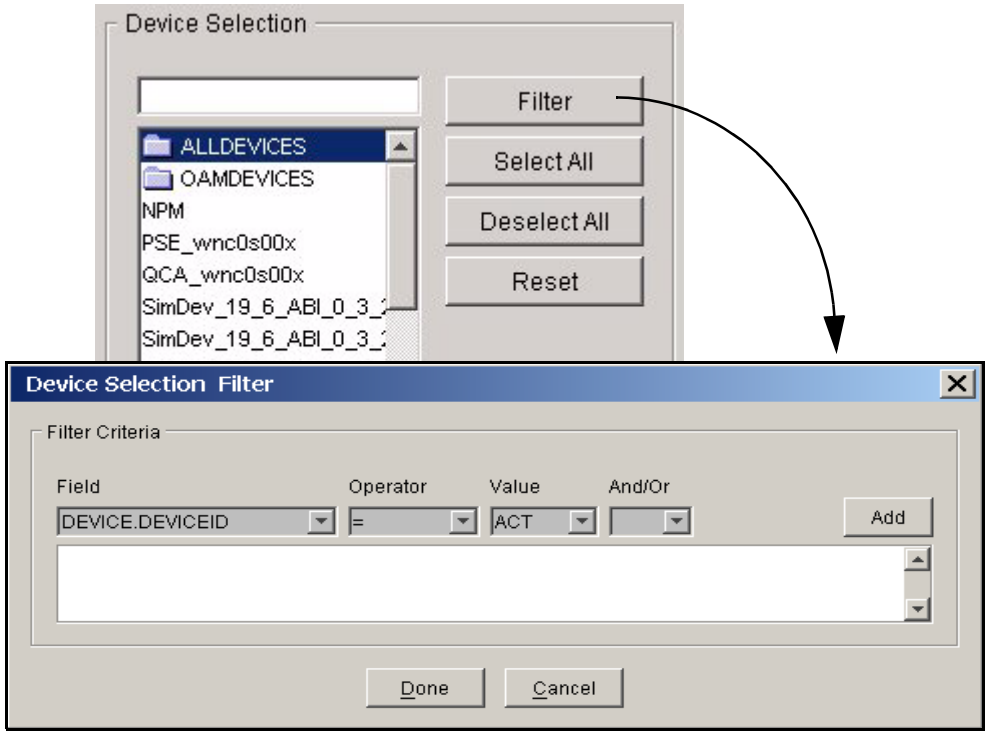
3 In the **Task** list, click **Apply**.



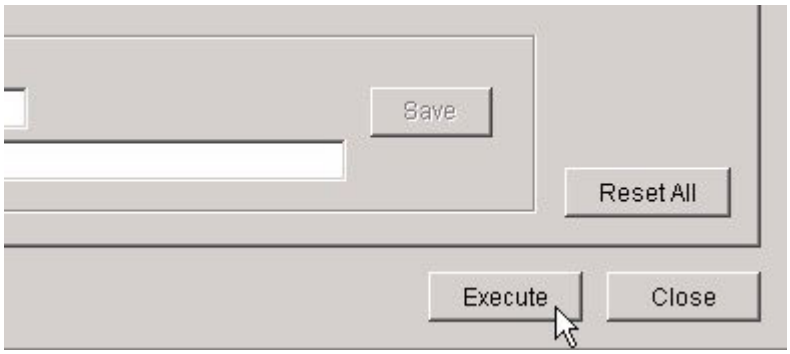
4 In the **Patch Selection** list, select the patch files or patch sets you want to apply, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



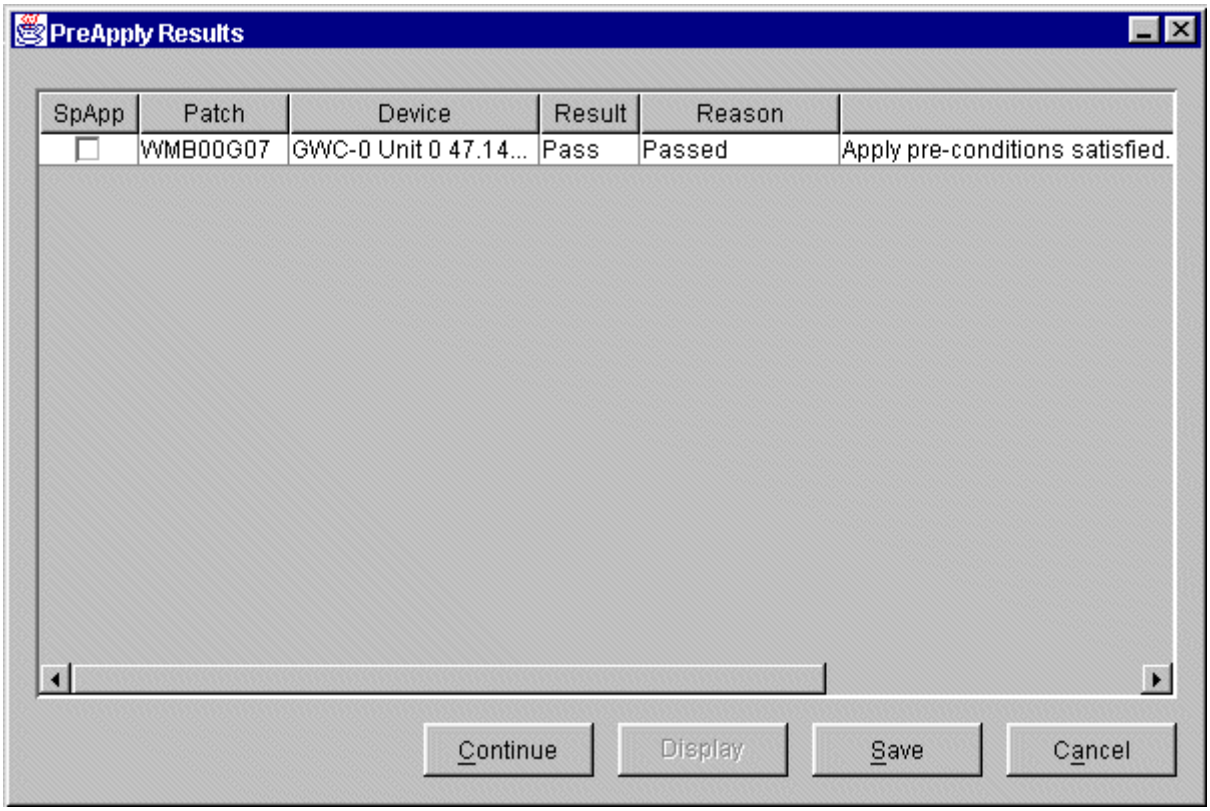
5 In the **Device Selection** list, select the devices or device sets to which you want to apply the patches, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



6 Click **Execute** to begin the patching process.



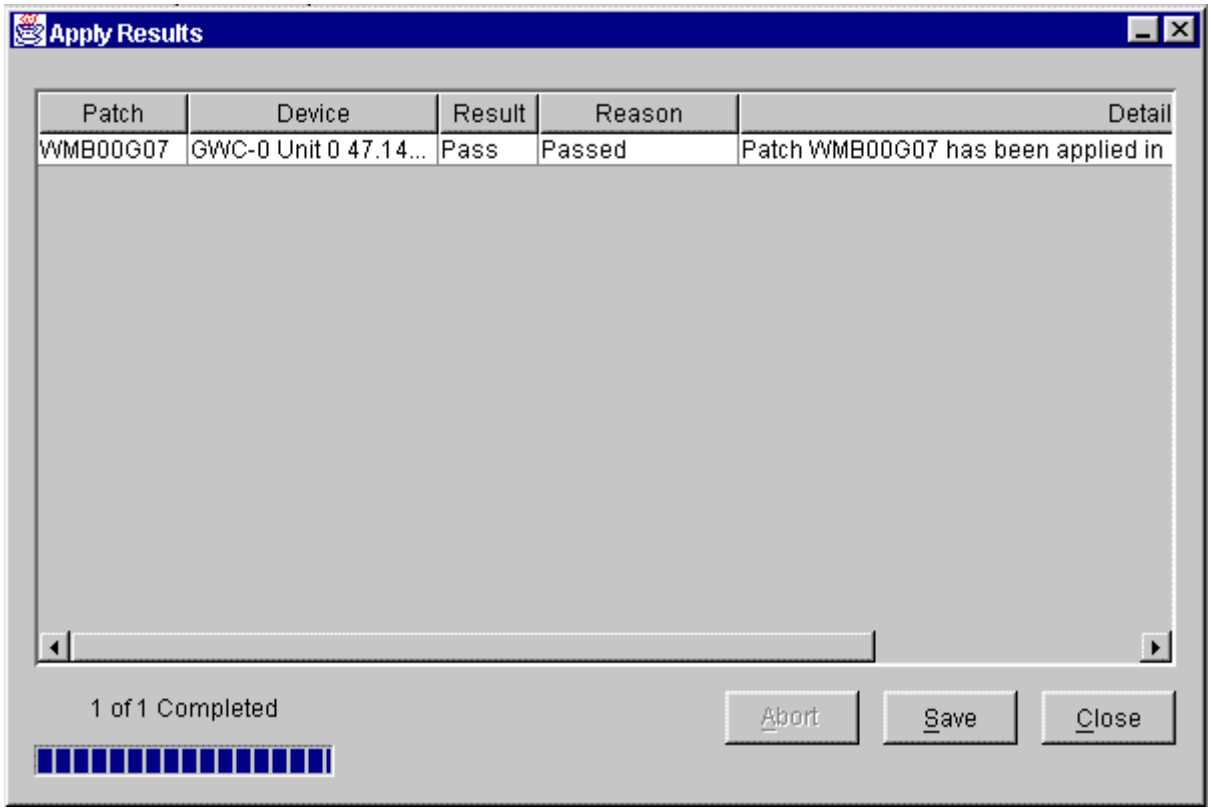
The results of the PreApply phase are displayed.



7 Review the PreApply Results, then click **Continue** to proceed.

Note: If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Apply Results window is displayed with results added as each action is completed. Failures from the PreApply phase are also included in the results.



8 Click **Save** to save the results to a file, or click **Close**.

Note: If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

9 You have completed this procedure.

Removing patches using the NPM

Application

Use this procedure to remove patches using the Network Patch Manager (NPM). You can remove patches using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Prerequisites

Before you remove ACT category patches, you must first deactivate the patches. Refer to procedure Deactivating patches using the NPM in this document.

Ensure the patch is not on hold.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Remove one or more patches from one or more devices by typing

```
npm> remove <patches> [in <devices>]
```

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to remove - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices
is a list of one or more device IDs from which you want to remove the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and removes them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Note: Enclose the <deviceid> for GWC devices in single quotes (‘).

Example
`npm> remove` ACT02GAX in ‘gwc3 Unit 1 47.142.108.39’

3 When prompted, press the Enter key.

4 Generate a device query report to verify the patches are removed by typing

`npm>` **`q device`**

5 Enter the device name in the format **‘<deviceid>’** that you input in step 2.

Note: The GWC <device id> must be enclosed in single quotes (‘) only when the GWC device id has spaces, dashes or periods as part of its name.

A device report of known patch activity for the particular device associated with the <device id> is returned.

6 Verify from the report that the desired patches are removed.

Note: If the patches do not successfully remove, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

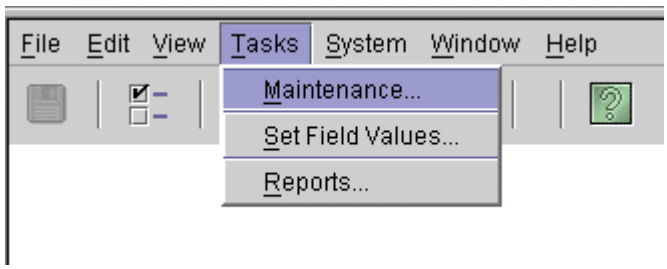
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

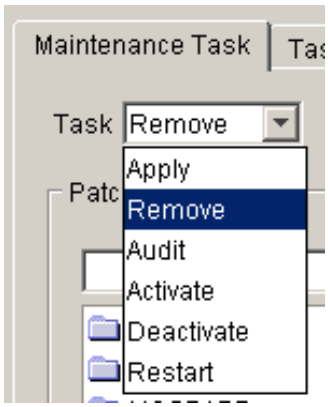
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

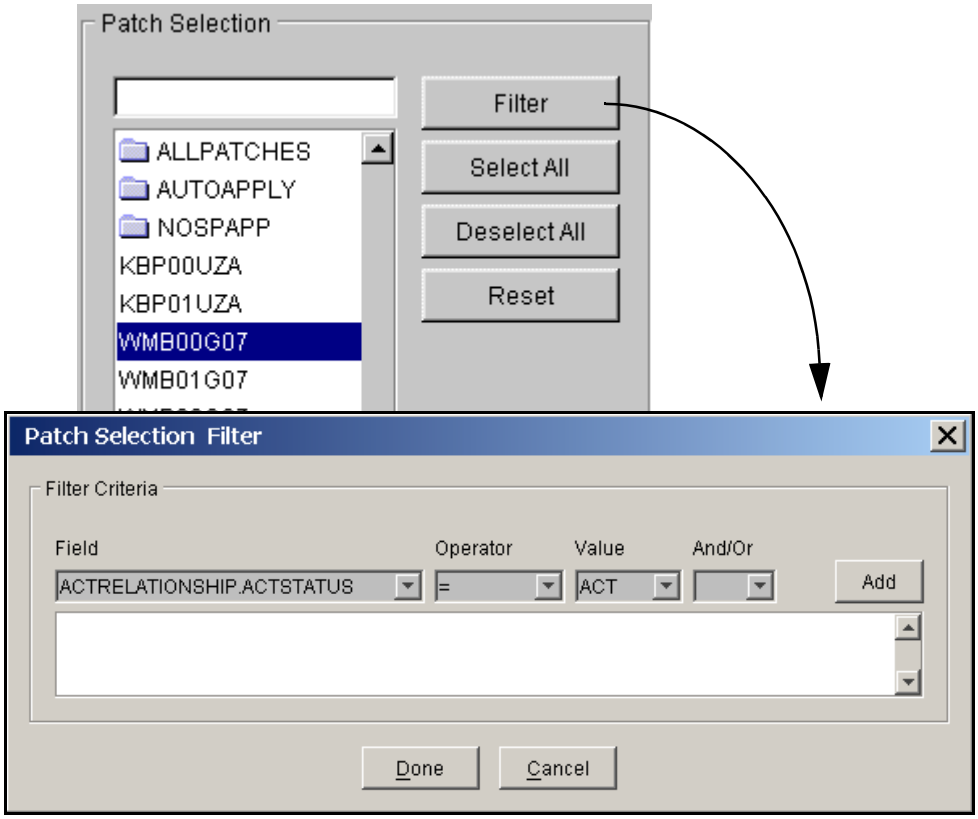


The Maintenance window is displayed.

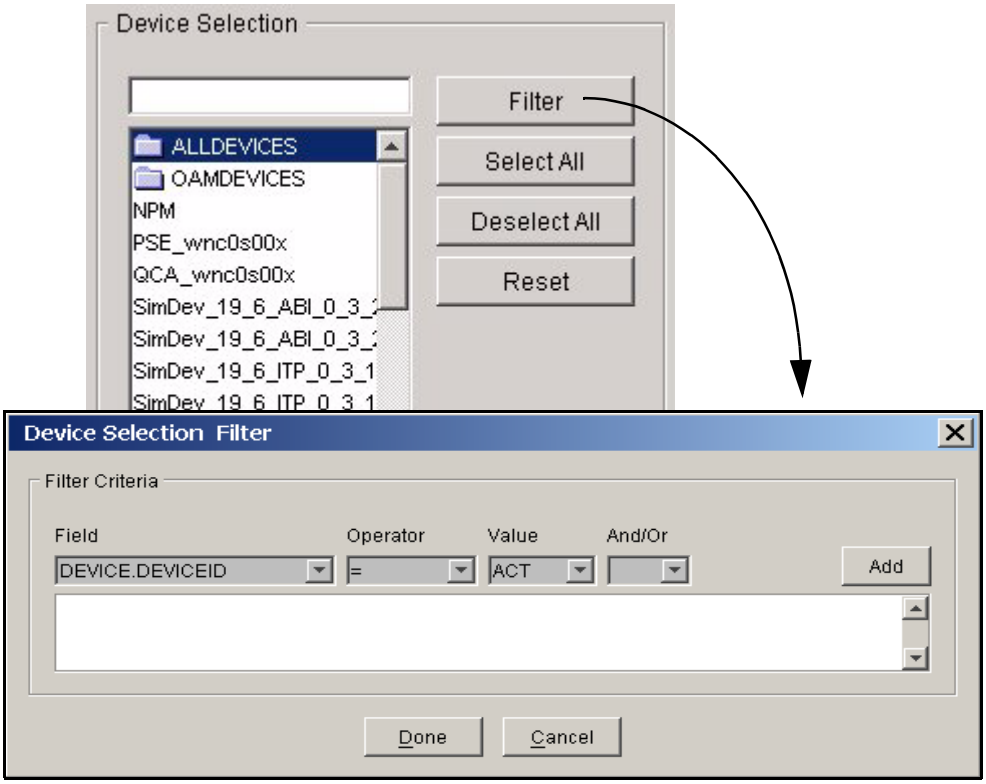
3 In the **Task** list, click **Remove**.



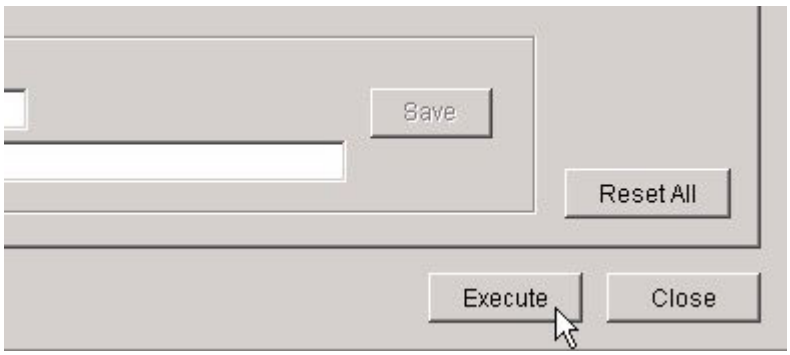
4 In the **Patch Selection** list, select the patch files or patch sets you want to remove from the Patch Selection list, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box..



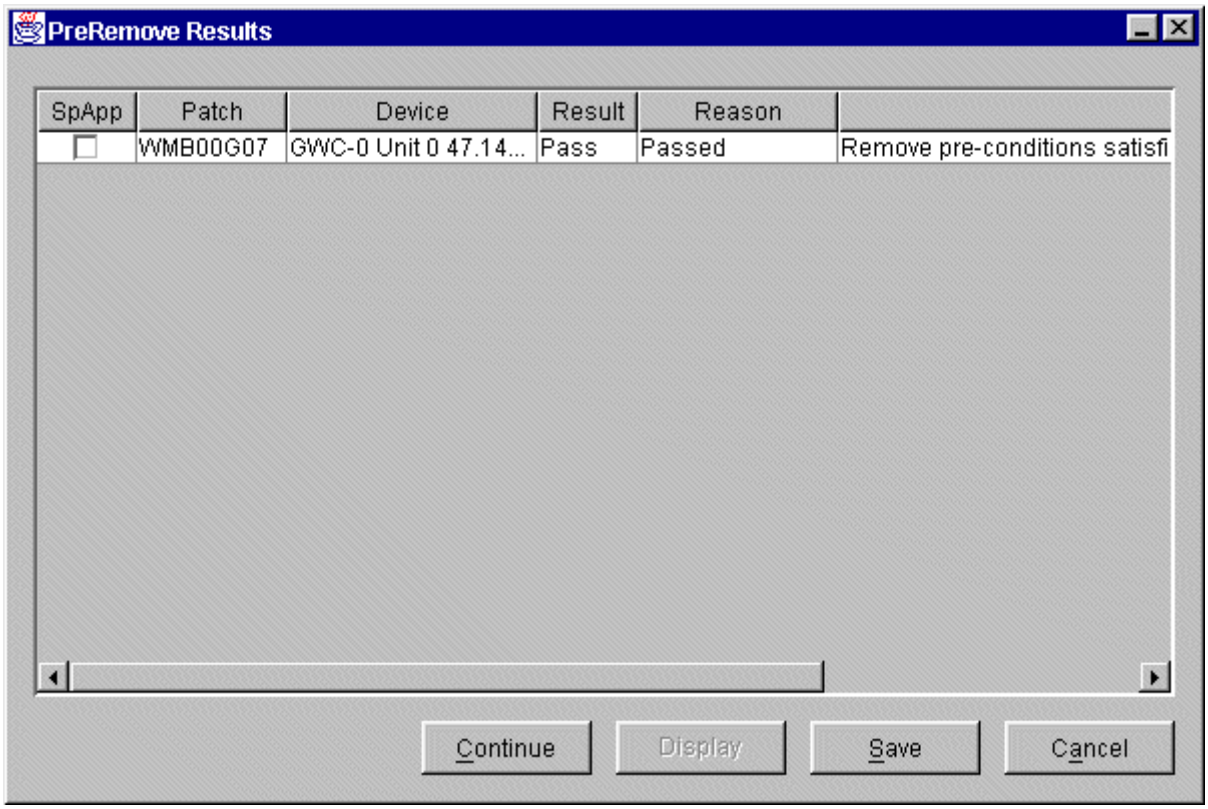
5 In the **Device Selection** list, select the devices or device sets from which the patches will be removed, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



6 Click **Execute** to begin the patch removal process.



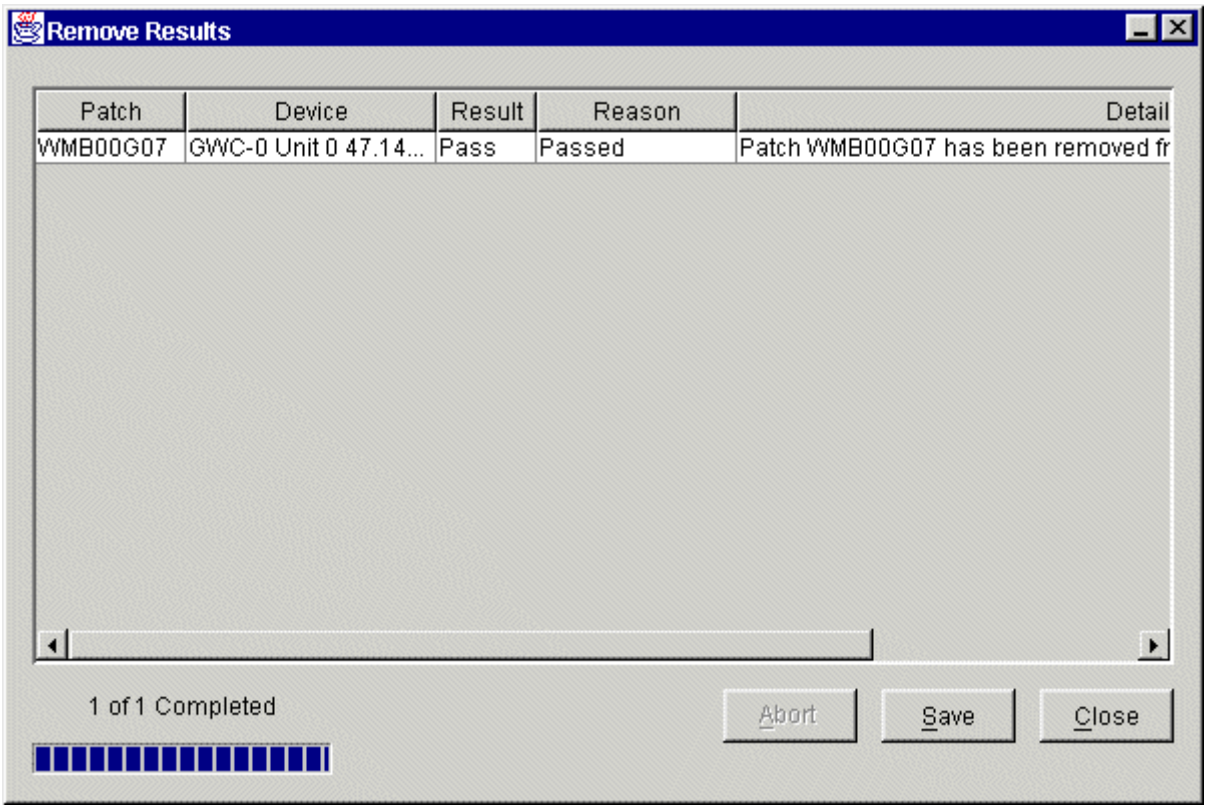
The results of the PreRemove phase are displayed.



7 Review the PreRemove Results, then **Continue** to proceed.

Note: If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Remove Results window is displayed with results added as each action is completed. Failures from the PreRemove phase are also included in the results.



8 Click **Save** to save the results to a file, or click **Close**.

Note: If the patches do not successfully remove, abort the patching procedure and contact your next level of support.

9 You have completed this procedure.

Deactivating patches using the NPM

Application

Use this procedure to deactivate one or more ACT category patches using the Network Patch Manager (NPM). You can deactivate patches using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Note: Currently, only GWC can have ACT category patches.

Prerequisites

You can deactivate a patch if the following criteria apply:

- the patch to be deactivated has been identified by your support team and Nortel as being applicable for your site and be recommended for deactivation
- the patch has been activated
- the patch is not on hold

CAUTION

Do not deactivate patches for your components that have not been identified as needing deactivation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Query the NPM for a list of patches that are activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message “Empty Results”.

3 Deactivate one or more patches for one or more devices by typing

```
npm> deactivate <patches> [in <devices>]
```

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to deactivate - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices
is a list of one or more device IDs for which you want to deactivate the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and deactivates them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Note: Enclose the <deviceid> for GWC devices in single quotes (‘).

Example
`npm> deactivate` ACT02GAX in ‘gwc3 Unit 1 47.142.108.39’

4 When prompted, press the Enter key.

5 Query the NPM to verify the patches are deactivated by typing

`npm>` **`q actlist`**

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

6 Verify from the list that the desired patches are deactivated.

Note: If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

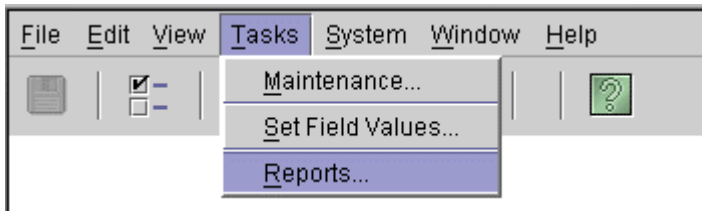
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

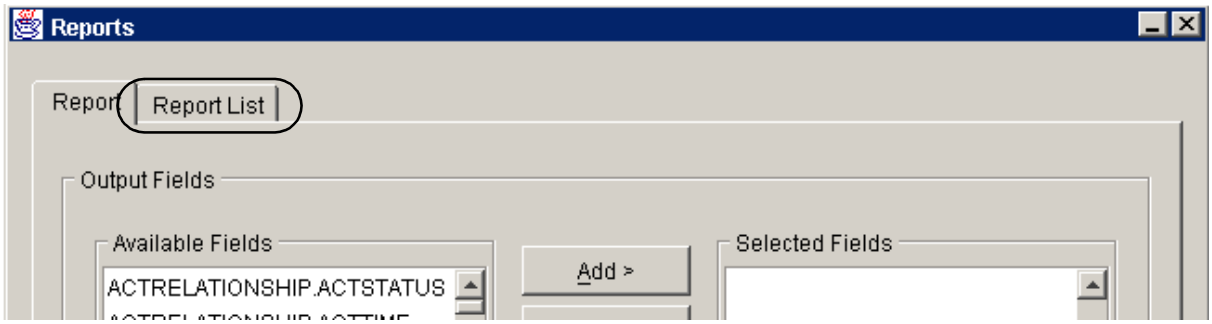
At the NPM GUI

2 On the **Tasks** menu, click **Reports...**.

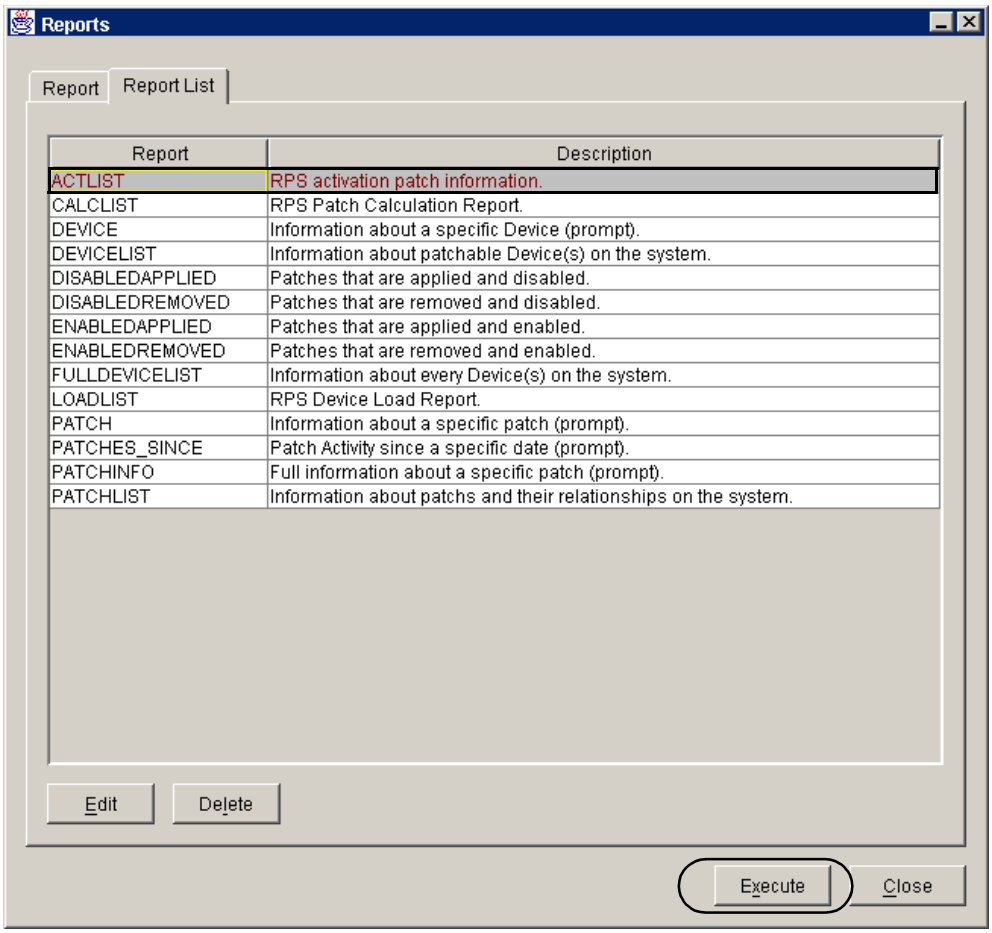


The Reports window is displayed.

3 Click the **Report List** tab.

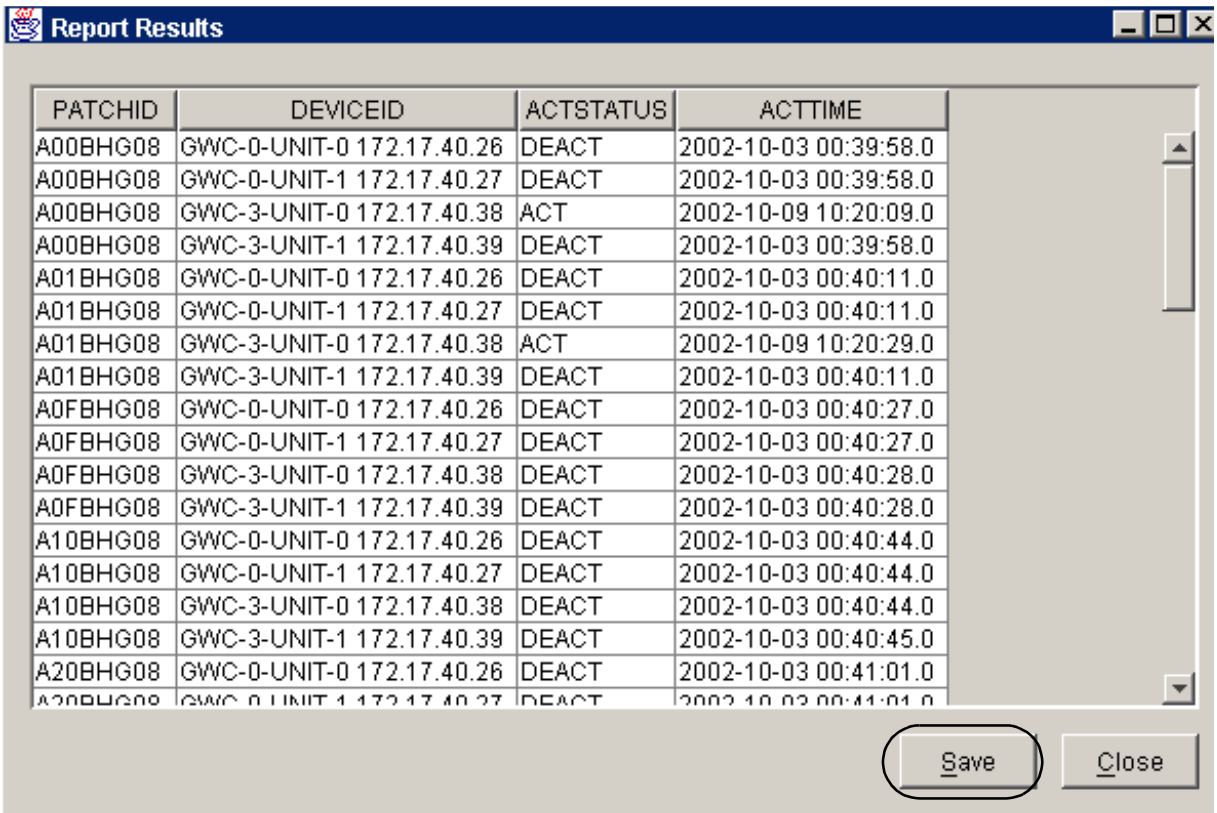


4 Click the **ACTLIST** entry in the **Report** field, then click **Execute**.



5 Review the list of patches displayed and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and should be deactivated.

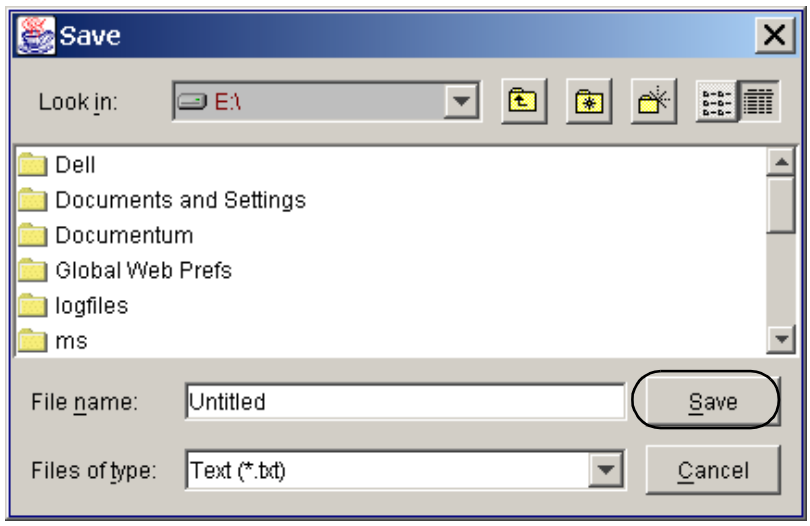
Note: If there are no patches to deactivate, the system returns a dialog box indicating that the report has “empty results”.



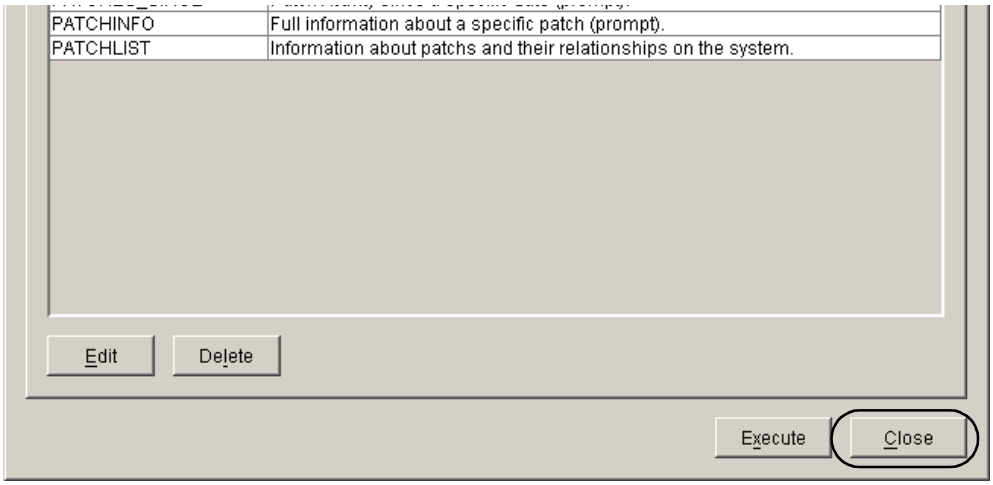
6 If necessary, save a copy of the report to a text file as follows:

a Click **Save**.

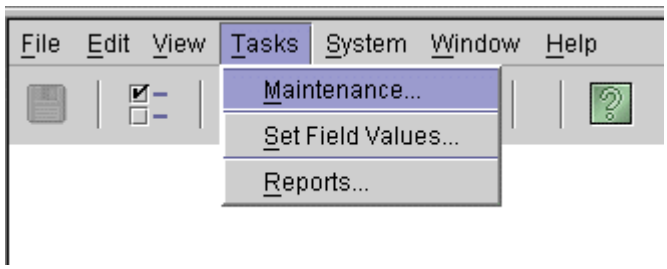
b Type a file name in the **File name:** box, and click **Save**.



7 Click **Close** to close the Reports window.

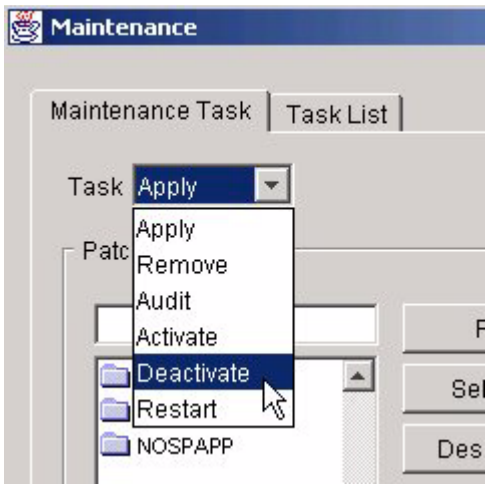


8 On the **Tasks** menu, click **Maintenance...**.

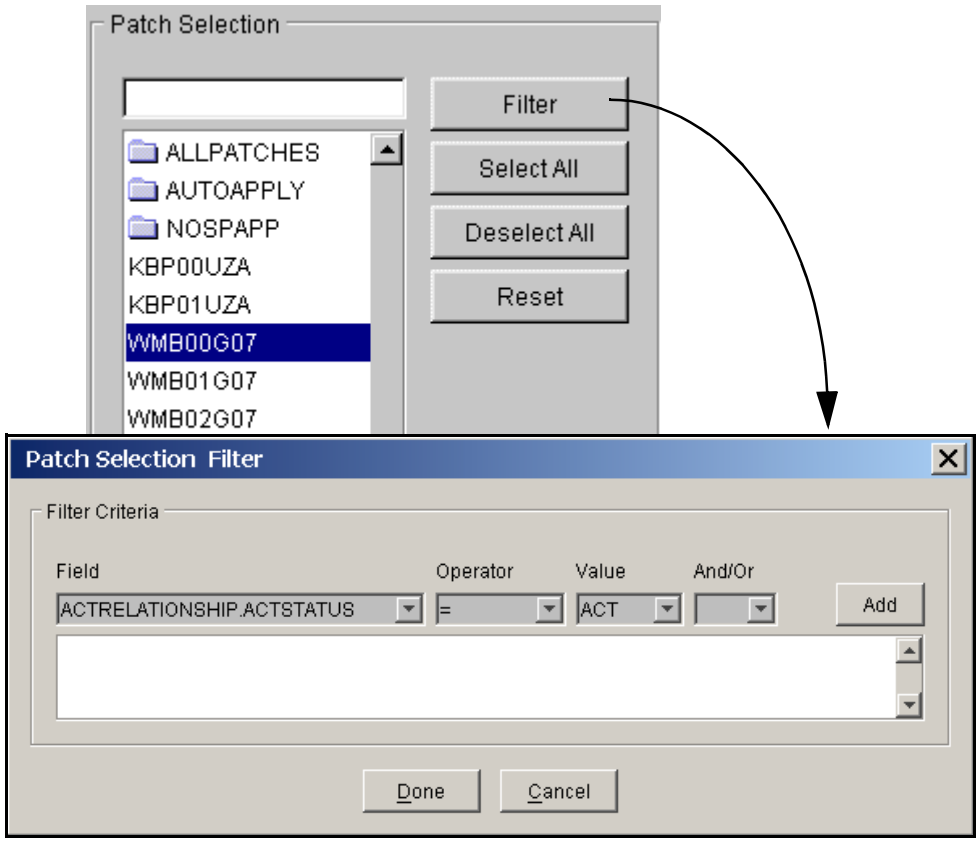


The Maintenance window is displayed.

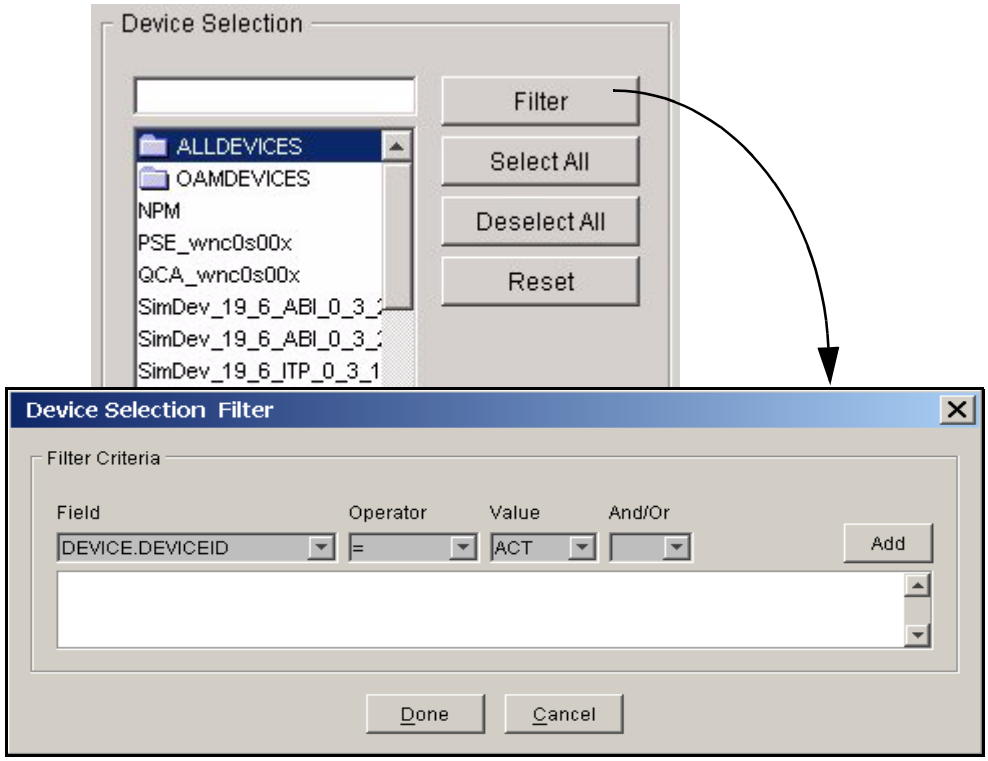
9 In the **Task** list, click **Deactivate**.



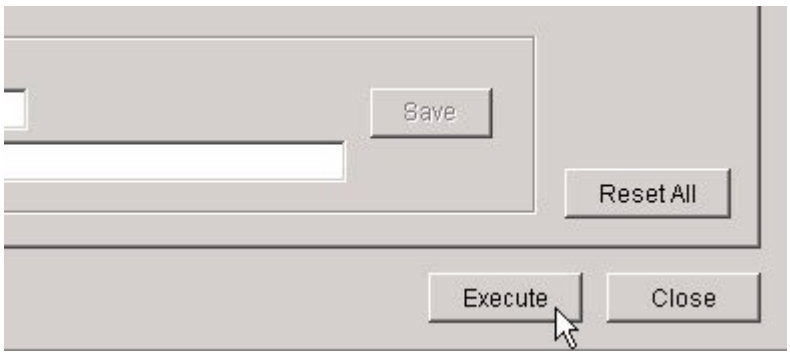
10 In the **Patch Selection** list, select the patch files or patch sets you want to deactivate, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box..



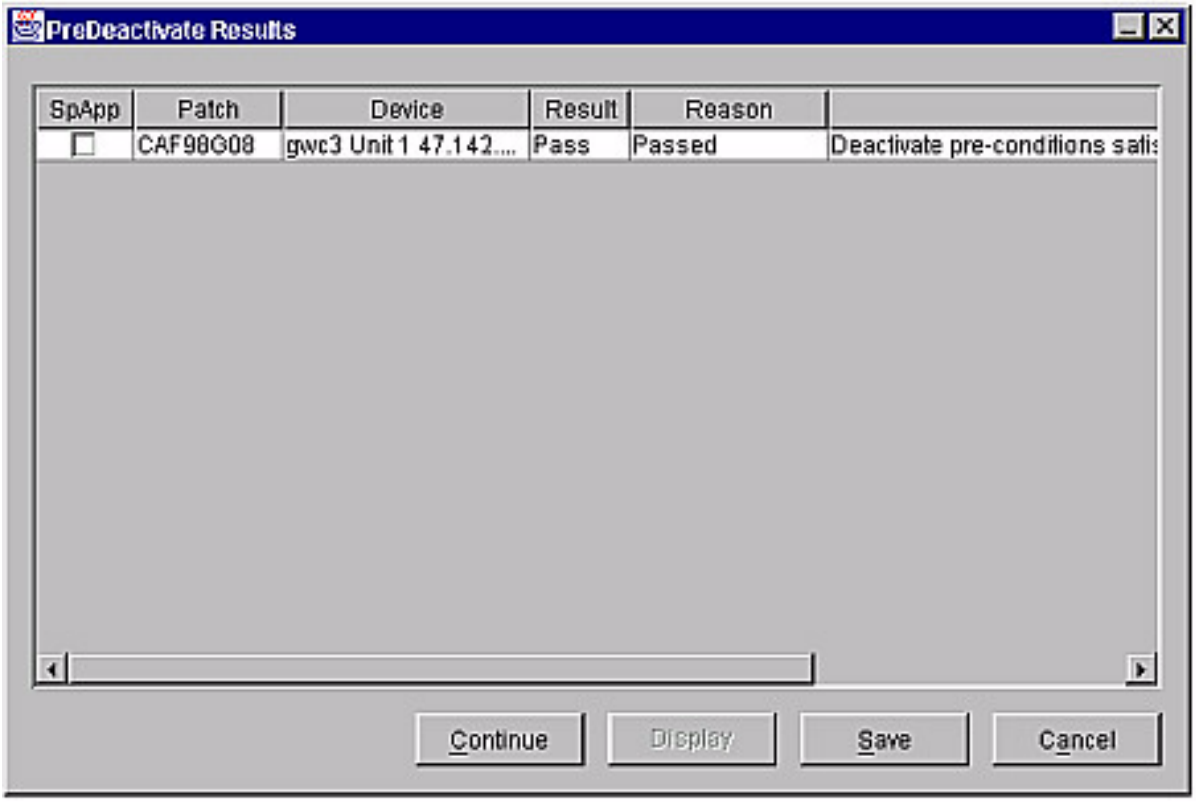
11 In the **Device Selection** list, select the devices or device sets for which you are deactivating the patches, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



12 Click **Execute** to begin the patch deactivation process.

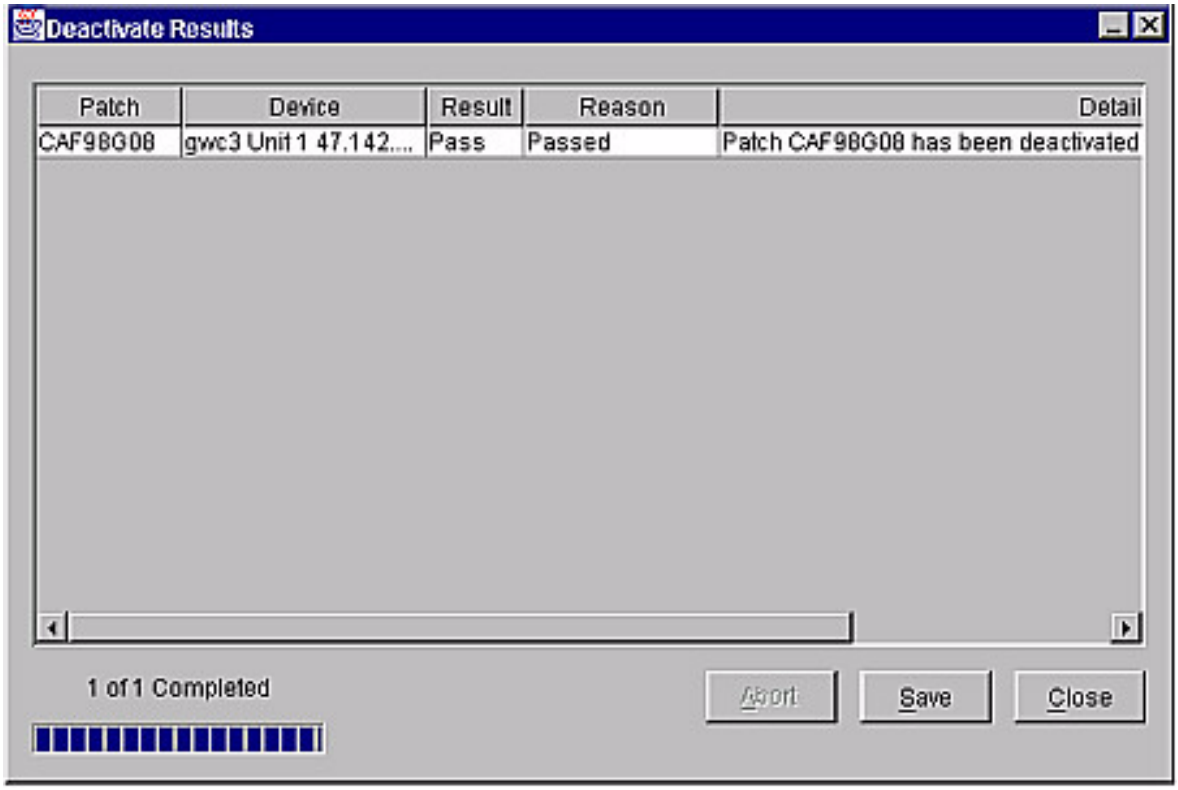


The results of the Pre-deactivate phase are displayed.



13 Review the PreDeactivate Results, then click **Continue** to proceed.

The Deactivate Results window is displayed with results added as each action is completed. Failures from the PreDeactivate phase are also included in the results.



14 Click **Save** to save the results to a file, or click **Close**.

Note: If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

15 You have completed this procedure.

Restarting a device using the NPM

Application

Use this procedure to restart a device using the Network Patch Manager (NPM). You can restart a device using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

You must restart a device to enable an OAM patch after it is applied, or disable an OAM patch after it is removed.

Note: Ensure you have applied all the necessary patches to the device, or removed all the unnecessary patches from the device before you restart the device.

Prerequisites

If you are enabling an OAM patch, the patch must have been applied. If you are disabling an OAM patch, the patch must have been removed.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

CAUTION

Stop or complete any maintenance activities associated with the patched device before you begin the restart.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Restart a device by typing

```
npm> restart <devices>
```

and pressing the Enter key.

where

devices
is a list of one or more device IDs you want to restart - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Note: Enclose the <deviceid> for GWC devices in single quotes (‘).

Example
`npm> restart` ‘gwc3 Unit 1 47.142.108.39’

3 When prompted, confirm you want to continue with the device restart by typing

y

and pressing the Enter key.

Example output

```
SpAPP: false
Patch: *
Device: SESM
Result: true
Reason: Passed
Details: Device SESM passed preRestart.
If you wish to continue with this maintenance
request, enter Yes (Y or y). Otherwise, just
enter return.
```

4 When prompted, confirm you want to continue with the device restart by typing

y

and pressing the Enter key.

Example output

```
npm>
Patch: *
Device: SESM
Reason: Passed
Detail: Restart passed on device SESM.
Hit <CR> to continue...
```

5 When prompted, press the Enter key.

Note: Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

Once the device has been successfully restarted, Nortel Networks recommends that you perform an audit on the device to synchronize the NPM database with the updates to the patches on the device. The audit will automatically occur at a specified time, however, to perform an audit manually, see Performing a device audit using the NPM in this document.

6 You have completed this procedure.

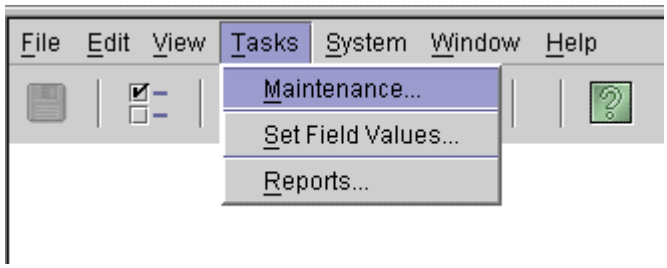
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

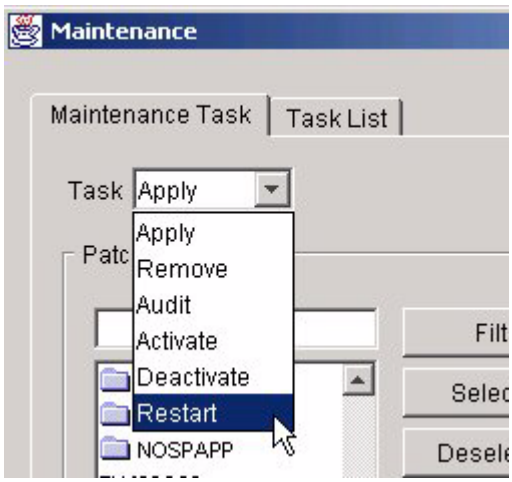
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

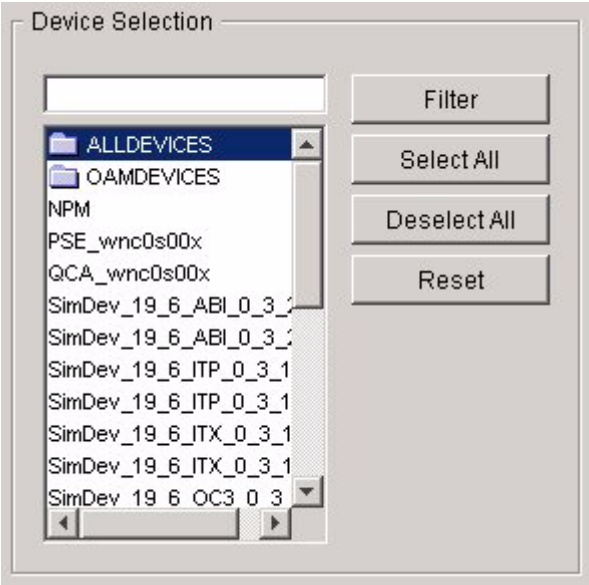


The Maintenance window is displayed.

3 In the **Task** list, click **Restart**.

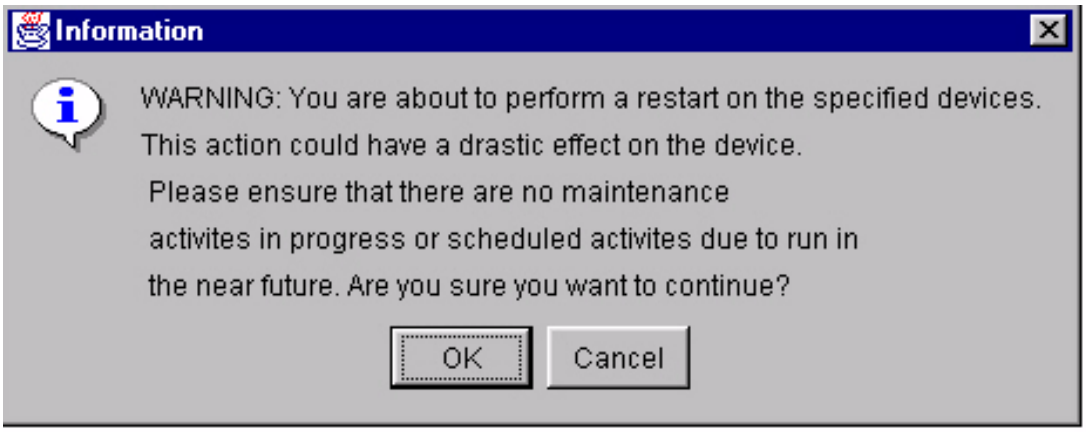


4 In the **Device Selection** list, select the device, device list, or device set that you want to restart.



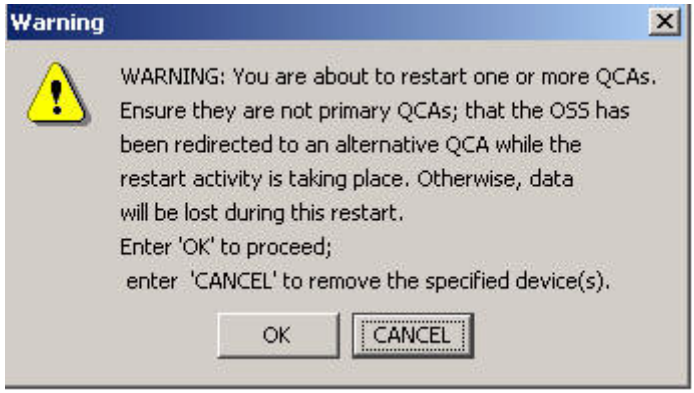
5 Click **Execute** to begin the restart.

The system returns the following dialog box.



6 Click **OK** to begin the restart.

If you are restarting a QCA device, the system returns the following warning:

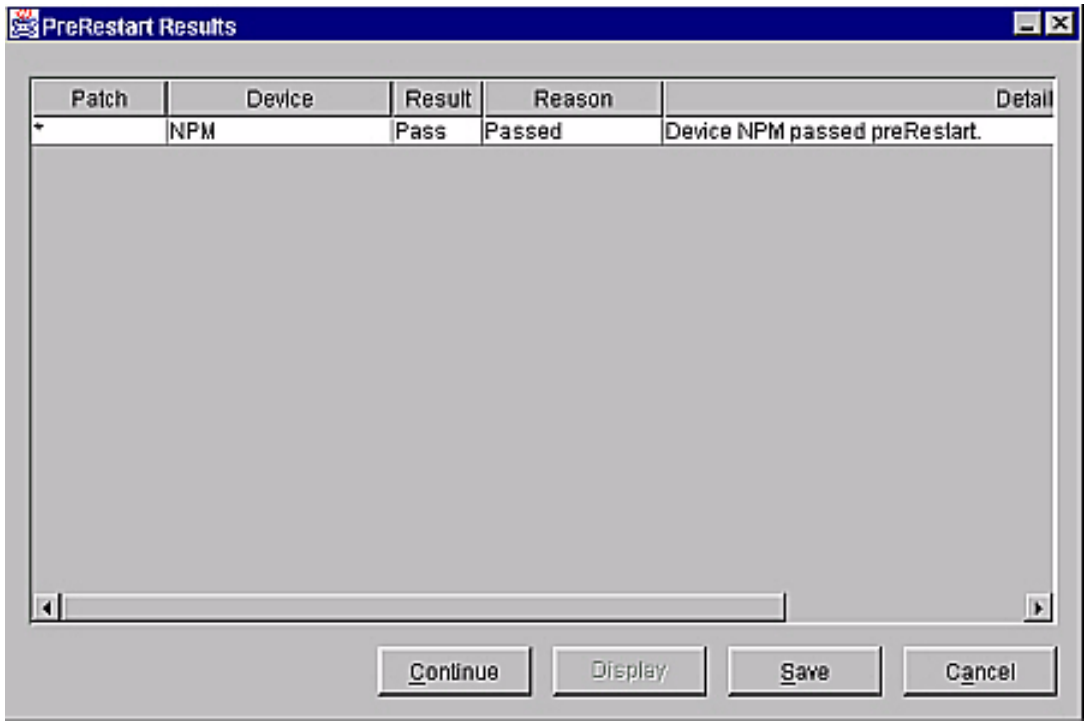


7

CAUTION
Loss of data
Carefully read the warning about QCAs before you proceed with a QCA restart.

If restarting a QCA is acceptable, click **OK** to proceed with the restart.

The results of the PreRestart phase are displayed.



8 Review the PreRestart Results, then click **Continue** to proceed.

Note: Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

Once the device has been successfully restarted, Nortel Networks recommends that you perform an audit on the device to synchronize the NPM database with the updates to the patches on the device. The audit will automatically occur at a specified time, however, to perform an audit manually, see Performing a device audit using the NPM in this document.

9 You have completed this procedure.

Defining sets using the NPM

Application

Use this procedure to define sets using the Network Patch Manager (NPM). You can define sets using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Sets provide a convenient grouping of patches and devices used in routine patching tasks. The sets are dynamic, based on database query statements, and are evaluated at execution time.

The NPM is initially configured with the following defined sets:

- ALLDEVICES - all registered devices on the system
- ALLPATCHES - all patches on the system
- AUTOAPPLY - all patches that can be auto-applied
- NOSPAPP - all patches with no special applications
- OAMDEVICES - all registered devices that are of device type OAM (PSE, SESM, CS 2000 SAM21 Manager, MG 9000 Manager, QCA, and NPM)
- AUTORESTARTDEVICES - all registered devices that are of device type OAM and can be auto-restarted (this excludes QCA)

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN102172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

1 Define a set by typing

```
npm> newset <report_type> <name> <description>
<fields> where <criteria>
```

and pressing the Enter key.

where

report_type
is either REPORT, PATCHSET, or DEVICESET

name
is the name of the set to be created

description
is a short description of the set

fields
is the name of one or more fields, separated by a space, to be included in the set

criteria
is the SQL statement that identifies the criteria by which to search the NPM database

Example

```
npm> newset PATCHSET BR12345PATCH “Patches for
CSR BR12345” where PATCH.CSR=’BR12345’”
```

2 You have completed this procedure.

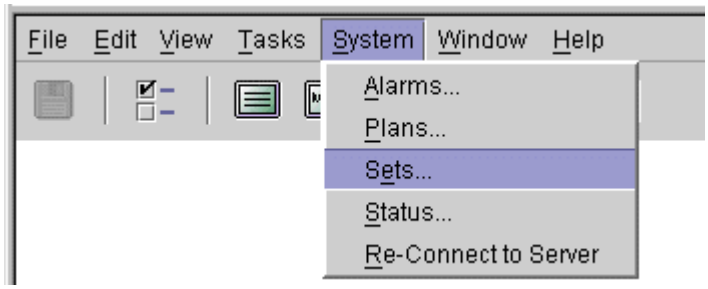
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

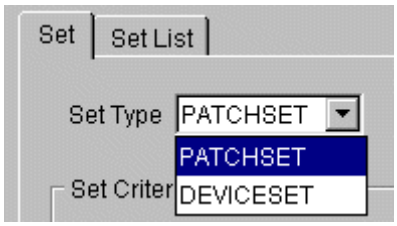
1 On the **System** menu, click **Sets...**.



The **Sets** window is displayed.

2 In the **Set Type** list, select PATCHSET to define a set of patches, or DEVICESET to define a set of devices.

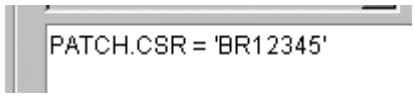
Note: You can also edit an existing set definition listed under the **Set List** tab, that contains similar criteria to the set you want to create, and save it under a new name.



3 In the **Set Criteria** area, specify the criteria for the set using substep a or b

a Type the criteria for the set in the text box.

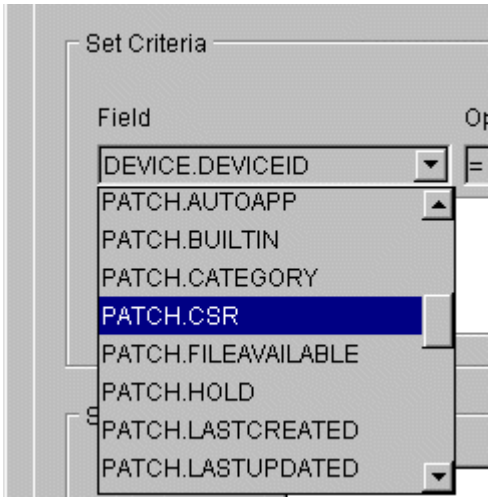
Note: Parenthesis "()" may be inserted to define precedence for multiple criteria statements.



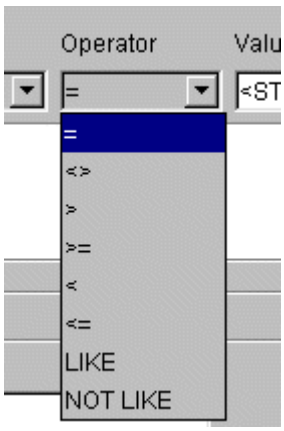
OR

b Specify the set criteria as follows:

i In the **Field** list, click the field of your choice.



ii In the **Operator** list, click the operator of your choice.

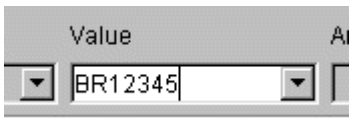


The following table lists the supported operators and their meaning.

Operator	Meaning
=	Equal
<>	Not equal
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal
LIKE	Matches string with wildcard (%)
NOT LIKE	Does not match string with wildcard (%)

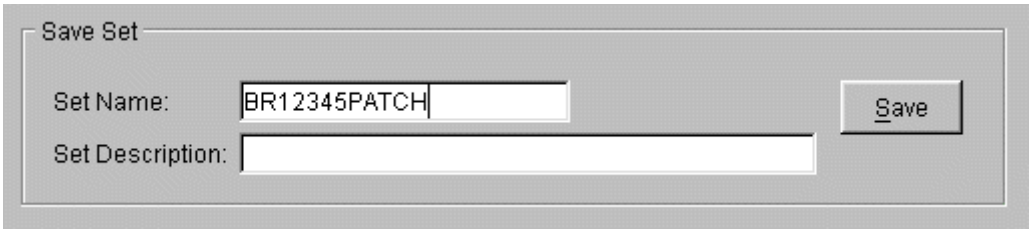
iii In the **Value** list, select the value of your choice.

Note: The data type in the **Value** list will change depending on the data type selected in the **Field** list. For alphanumeric data, type the value. For boolean data, select the value.

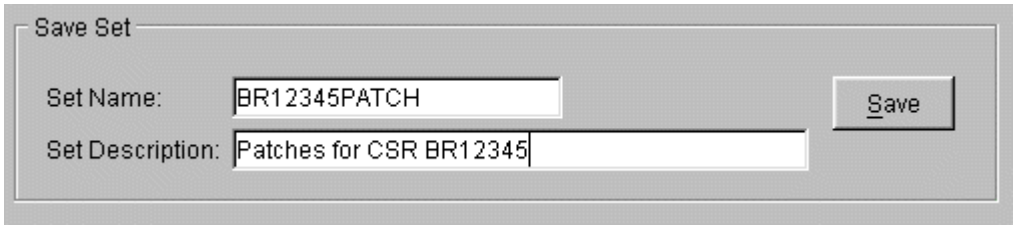


To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

4 Type a unique name for the set in the **Set Name** box.

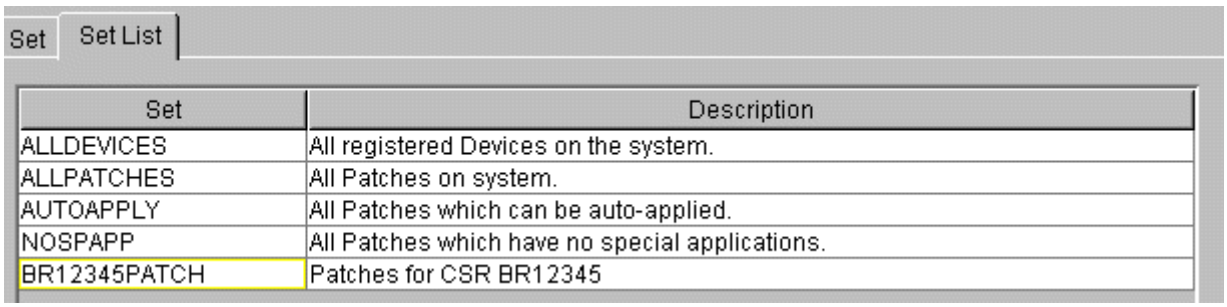


5 Type a description of the set in the **Set Description** box if desired.



6 Click **Save** to save the set.

The new set will be reflected under the **Set List** tab once the system has saved it.



7 You have completed this procedure.

Saving a task using the NPM

Application

Use this procedure to save a task using the Network Patch Manager (NPM). You can save tasks using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

A task is a definition of one type of maintenance activity that involves devices and may involve patches. The Network Patch Manager (NPM) allows tasks to be saved for automated execution.

The NPM is initially configured with the following defined tasks:

- AUTOAPPLY
- AUTORESTART
- AUDIT

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Define the task by typing

```
npm> newtask <task_name> <task_type>
<task_desc> <task_patchlist> <task_devicelist>
```

and pressing the Enter key.

where

task_name
the name of the task to be created

task_type
determines the type of task (APPLYTASK, REMOVETASK, ACTIVATETASK, DEACTIVATETASK, AUDITTASK, or RESTARTASK)

task_desc
is the description of the task

task_patchlist
is the set of patches associated with the task

Note: The task_patchlist field is not used with AUDITTASK. For an AUDITTASK, use "" (two double quotes together).

task_devicelist
is the set of devices associated with the task

Following is an example to apply all NOSPAPP patches to all devices.

```
npm> newtask NOSPAPPALL APPLYTASK "NOSPAPP for
ALLDEVICES" NOSPAPP ALLDEVICES
```

Following is an example to audit all devices.

```
npm> newtask AUDITALL AUDITTASK "Audit all
devices" "" ALLDEVICES
```

3 You have completed this procedure.

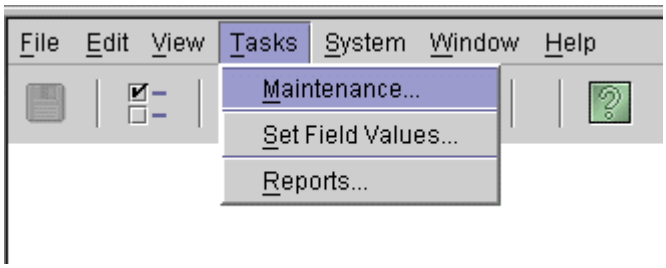
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

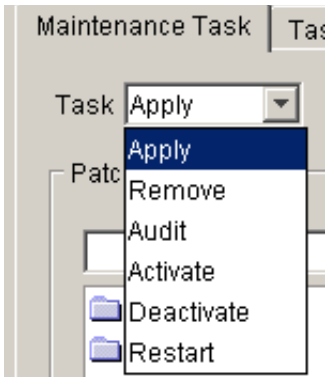
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

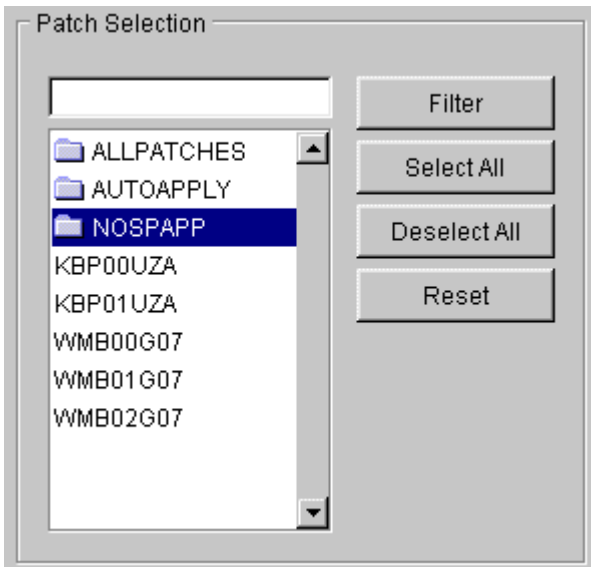


The **Maintenance** window is displayed.

3 In the **Task** list, click the task of your choice.

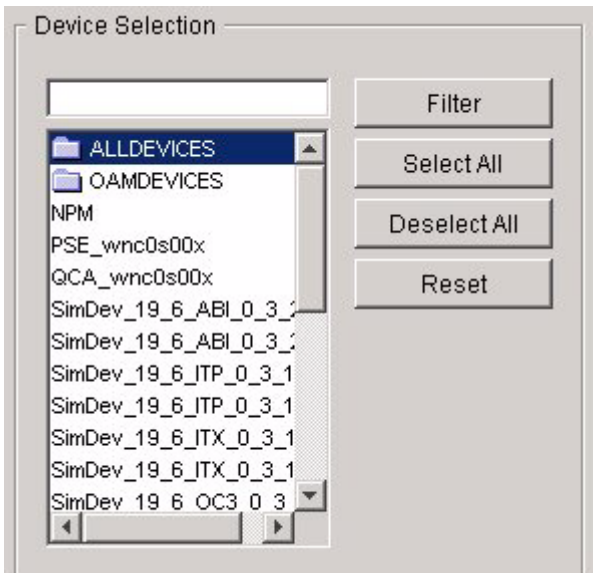


4 In the **Patch Selection** list, select the patch set (if applicable) you want to associate with the task.

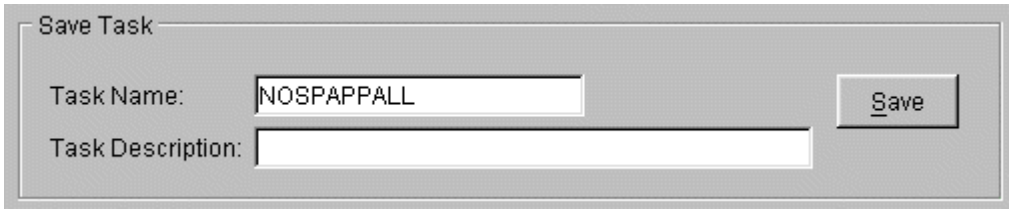


Note: Saved tasks can only contain patchsets or devicesets, not single patches or devices. You can save a task that applies one patch to one device by putting the patch in a single-member patchset and the device in a single-member deviceset and then applying the patchset to the deviceset.

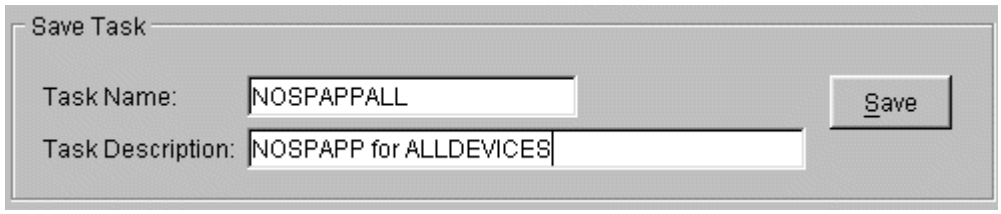
5 In the **Device Selection** list, select the device set you want to associate with the task.



6 Type a unique name for the task in the **Task Name** box.

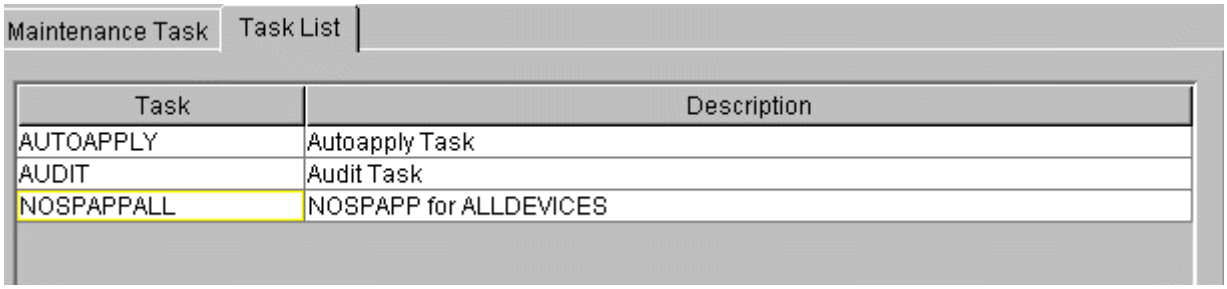


7 Optionally, type a description of the task in the **Task Description** box.



8 Click **Save** to save the task.

The new task will be displayed under the **Task List** tab once the system has saved the task.



9 You have completed this procedure.

Setting field values using the NPM

Application

Use this procedure to set field values using the Network Patch Manger (NPM). You can set field values using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

The NPM allows the exclusion and inclusion of patches or devices from manual or automated patching tasks. This is accomplished by setting database field values using the “assign” command. An example of when this option could be used is when a new patch is to be applied to a single device for a test period, without applying the patch to the remaining devices. After the test period, the patch would then be applied to the remaining devices.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM CLUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Assign field values by typing

```
npm> assign <pd_option> <val_field> <val_value>
<val_idset> <val_set>
```

and pressing the Enter key.

where

pd_option
identifies what is being assigned (PATCH or DEVICE)

val_field
is the field to be assigned (PATCH.HOLD or DEVICE.HOLD)

val_value
is the new value for the field (Y or N)

val_idset
identifies if you are assigning a singe patch or device or a set of patches or devices (ID or SET)

val_set
is the patch, device, or set to be assigned

Example

```
npm> assign PATCH PATCH.HOLD Y ID WMB00G07
```

Using the table below, determine the Field and Values to select.

Field and Value combinations

Field	Value	Result
PATCH.HOLD	N	The patch will be applied to the remaining devices. This is typically after the test period is over.
PATCH.HOLD	Y	The patch will be excluded from manual or automated patching activities.
DEVICE.HOLD	N	The device will be included in patching tasks. This is typically after the test period is over.
DEVICE.HOLD	Y	The device will be excluded from manual or automated patching activities.

3 You have completed this procedure.

Using the NPM GUI

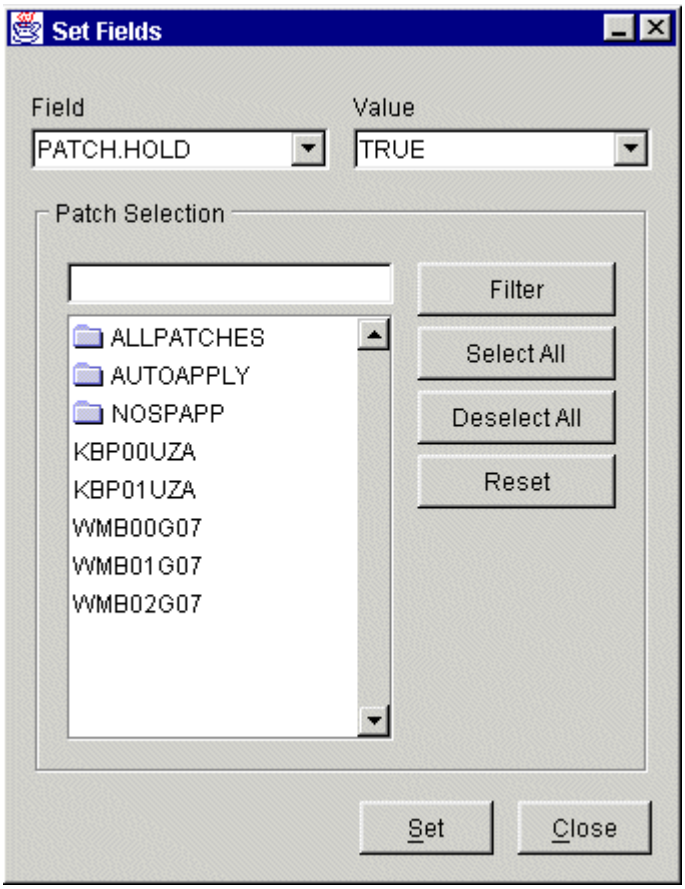
At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

2 On the **Tasks** menu, click **Set Field Values...**.

The **Set Field** window is displayed.

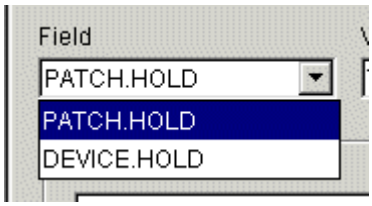


3 Using the table below, determine the Field and Values to select.

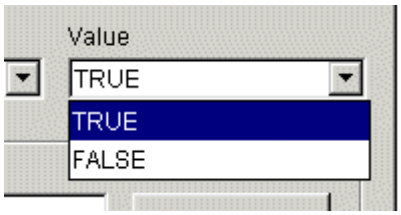
Field and Value combinations

Field	Value	Result
PATCH.HOLD	FALSE	The patch will be applied to the remaining devices. This is typically after the test period is over.
PATCH.HOLD	TRUE	The patch will be excluded from manual or automated patching activities.
DEVICE.HOLD	FALSE	The device will be included in patching tasks. This is typically after the test period is over.
DEVICE.HOLD	TRUE	The device will be excluded from manual or automated patching activities.

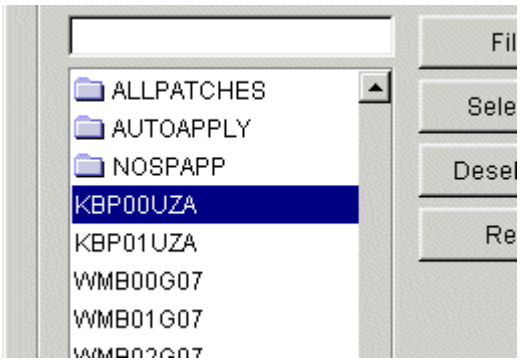
4 In the **Field** list, click PATCH.HOLD or DEVICE.HOLD.



5 In the **Value** list, click TRUE or FALSE.

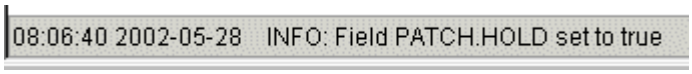


6 In the **Patch Selection** list (if you clicked PATCH.HOLD), select one or more patches, or in the **Device Selection** list (if you clicked DEVICE.HOLD), select one or more devices.



7 Click **Set**, to apply the changes.

The system displays a confirmation message at the bottom of the Network Patch Manager window.



8 You have completed this procedure.

Defining reports using the NPM

Application

Use this procedure to create a user-defined report and generate it using the Network Patch Manager (NPM). You can define reports using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

The reporting feature of the Network Patch Manager (NPM) allows you to select information from the database and display it. Report criteria determines what is displayed. In addition to the predefined reports for the NPM, users can create and save their own reports according to their application-specific criteria.

The NPM is initially configured with the following defined reports:

- ACTLIST - RPS activation patch information
- CALCLIST - RPS patch calculation report
- DEVICE - Information about a specific device (prompt report)
- DEVICELIST - Information about patchable devices on the system
- DISABLEDAPPLIED - patches that are applied but disabled
- DISABLEDREMOVED -patches that are disabled and removed
- ENABLEDAPPLIED - patches that are applied and enabled
- ENABLEDREMOVED - patches that are applied but removed
- FULLDEVICELIST - Information about every device on the system
- LOADLIST - RPS device load report
- PATCH - Information about a specific patch (prompt report)
- PATCHES_SINCE - Patch activity since a specific date (prompt report)
- PATCHINFO - Full information about a specific patch (prompt report)
- PATCHLIST - Information about patches and their relationships on the system

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

1 Define the report by typing

```
npm> newset REPORT <report_name> <report_desc>
<report_fields> where <report_criteria>
```

and pressing the Enter key.

where

report_name
the name of the report to be created

report_desc
is a short description of the report

report_fields
is the name of one or more fields, separated by a space, to be included in the report

report_criteria
is the SQL statement that identifies the criteria by which to search the NPM database

Example

```
npm> newset REPORT DEVHOLDFALSE “All devices
with HOLD=FALSE” “DEVICE.DEVICEID DEVICE.HOLD
where DEVICE.HOLD=’FALSE’”
```

2 Generate the report by typing

```
npm> query <report_name>
```

and pressing the Enter key.

where

report_name
the name of the report you previously created

3 You have completed this procedure.

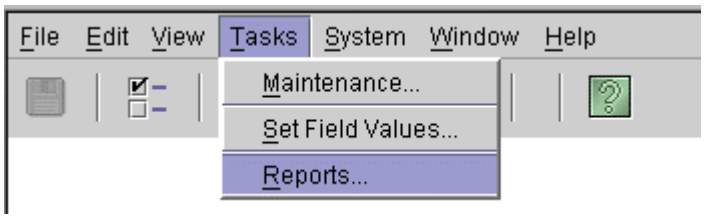
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

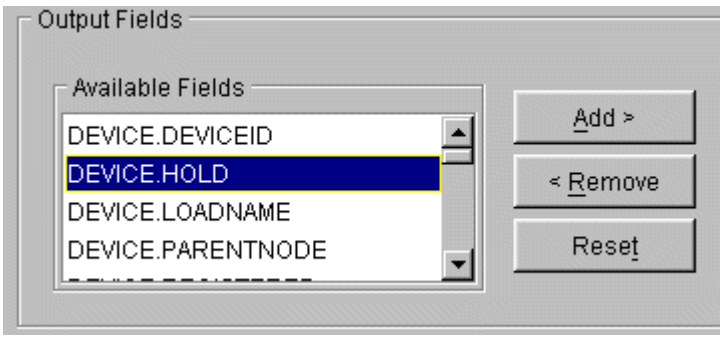
1 On the **Tasks** menu, click **Reports...**.



2 Specify the fields to be included in the new report as follows:

Note: You can also edit an existing report listed under the **Report List** tab, that contains similar criteria to the report you want to create, and save it under a new name.

a In the **Available Fields** list, click a field of your choice.



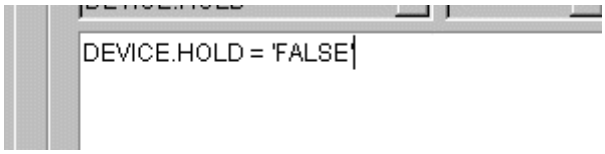
b Click **Add** to add the field to the **Selected Fields** list.

c Repeat Steps 2a and 2b for each field, then proceed to step 3.

3 In the **Report Criteria** area, specify the criteria for the report using substep a or b

a Type the criteria for the report in the text box.

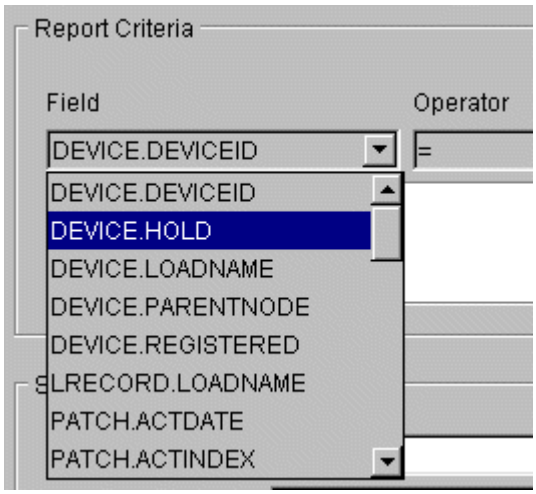
Note: Parenthesis "()" may be inserted to define precedence for multiple criteria statements.



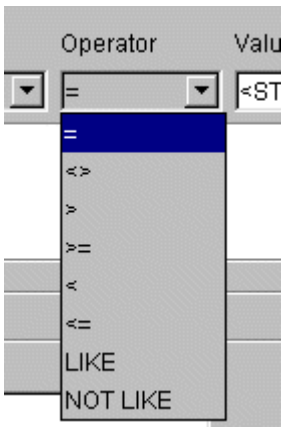
OR

b Specify the report criteria as follows:

i In the **Field** list, click the field of your choice.



ii In the **Operator** list, click the operator of your choice.

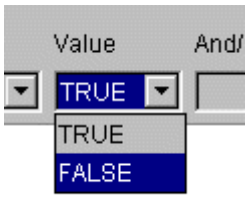


The table below lists the supported operators and their meaning.

Operator	Meaning
=	Equal
<>	Not equal
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal
LIKE	Matches string with wildcard (%)
NOT LIKE	Does not match string with wildcard (%)

iii In the **Value** list, select the value of your choice

Note: The data type in the **Value** list will change depending on the data type selected in the **Field** list. For alphanumeric data, type the value. For boolean data, select the value.

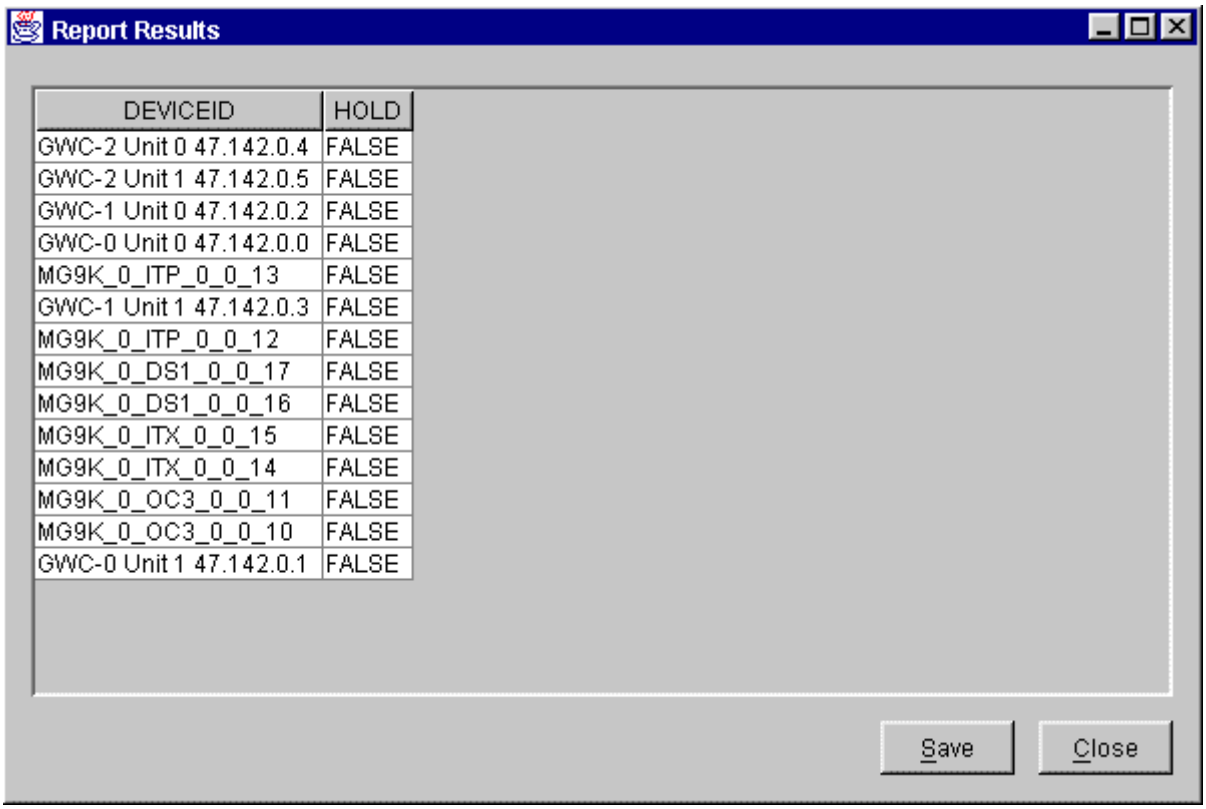


To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

4 Click **Execute** to generate the report.

The system displays the Report Results window.

Note: The time required to generate the report depends on the number of patches and devices in the database and the complexity of the search criteria.



5 You have completed this procedure.

Defining a plan using the NPM

Application

Use this procedure to define a plan using the Network Patch Manager (NPM). You can define a plan using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

A Plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule may specify either a one time execution at a given time or repeated execution according to a frequency definition. A Plan may include the following tasks: apply, remove, audit, and reports.

There is one system-defined plan named SYSTEMPLAN. It cannot be renamed, but it can be modified or deleted. The SYSTEMPLAN is initially defined with the AUTOAPPLY and AUTORESTART tasks.

A maximum of 5 plans can be defined in addition to the SYSTEMPLAN.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Define the plan by typing

```
npm> newplan <plan_name> <plan_freq>
<date_time> <max_time> <plan_desc>
```

and pressing the Enter key.

where

plan_name
is the name of the plan

plan_freq
is how often the plan should execute (Once, Hourly, Daily, Weekly, or Monthly)

date_time
is the date and time the plan is to be executed in mm-dd-yy hh:mm format. Plans executed more than once will begin executing at this time of day each interval.

max_time
is the maximum amount of time to execute the plan (No_Limit, 15_min, 30_min, 1_Hr, 2_Hr, 4_Hr, 8_Hr, or 16Hr)

plan_desc
is a brief description of the plan

Example

```
npm> newplan <plan_name> Weekly "07-15-03
16:59" 4_Hr "NPM weekly scheduled routine
activities"
```

3 Enable the plan by typing

```
npm> enableplan <plan_name> ON
```

and pressing the Enter key.

where

plan_name
is the name of the plan

4 Add a task to the plan by typing

```
npm> sched <plan_name> <tr_option> <tr_name>
<add_delete>
```

and pressing the Enter key.

where

plan_name
is the name of the plan

tr_option
determines whether a Task or Report is being added (TASK, REPORT)

tr_name
is the name of the task or report

add_delete
determines if the task or report is being added to or removed from the SystemPlan

Example

```
npm> sched <plan_name> TASK AUDIT ADD
```

5 You have completed this procedure.

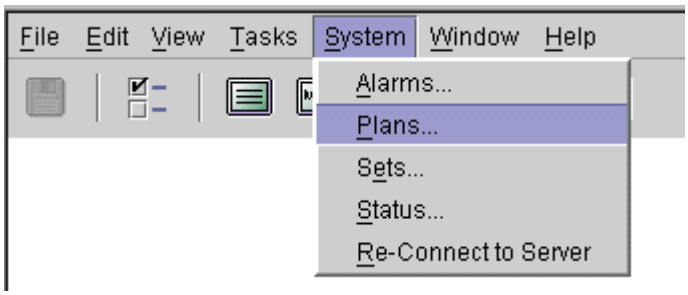
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

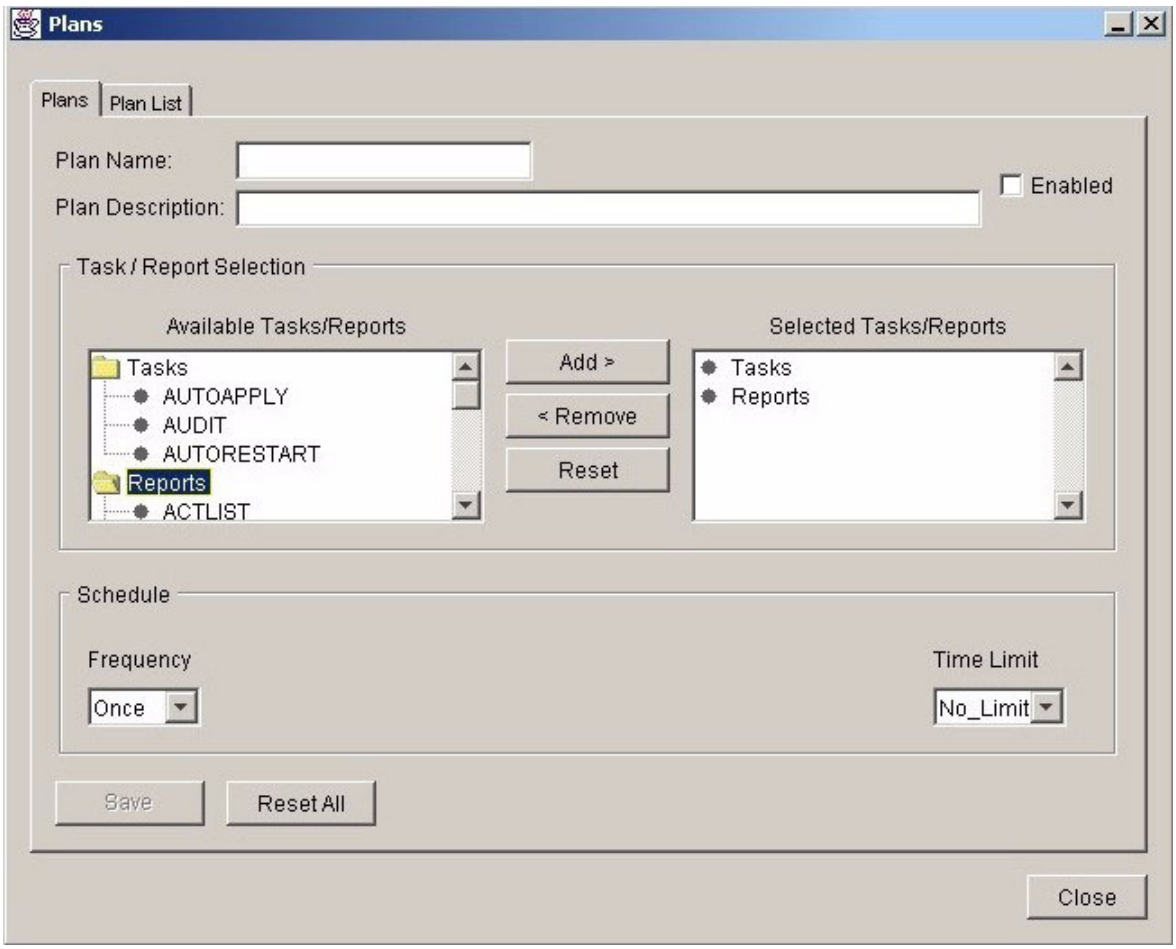
At the NPM GUI

2 On the **System** menu, click **Plans...**.



The **Plans** window opens.

3 Click the **Plans** tab if not already displayed, and click **Reset All**.



4 In the **Plan Name** box, type a unique name for the plan, and in the **Plan Description** box, type a description of the plan (optional).

5 Click the **Enabled** check box.

6 Add tasks or reports to the plan as follows:

a In the **Available Tasks/Reports** list, double click on the **Tasks** or **Reports** folder to didplay the available tasks or reports.

b Click the task or report you want to add to the plan.

Note: Only add reports that do not require any user input when they are run as a user may not be present at the time the plan runs. This includes pre-defined reports and user-defined reports. The pre-defined reports that require user input are as follows:

- DEVICE
- PATCH
- PATCHES_SINCE
- PATCHINFO

c Click **Add** to add the task or report to the **Selected Tasks/Reports** list.

Note: The order in which the tasks and reports appear in the Selected Tasks/Reports list, is the order in which they will execute. The tasks in a plan are executed sequentially.

d Repeat step 6a and 6b for each task or report you want to add to the plan.

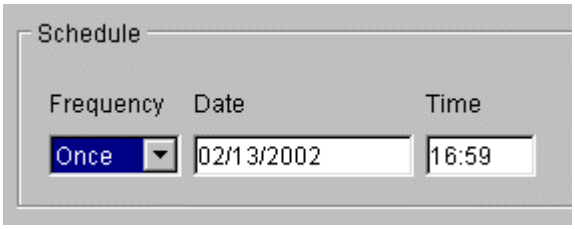
Note: You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

7 Specify the execution schedule in the **Schedule** are as follows:

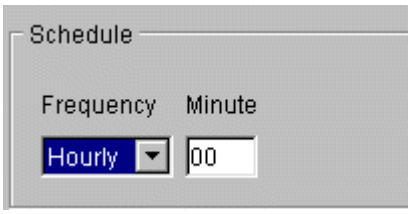
a In the **Frequency** list, click the frequency option of your choice.

When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

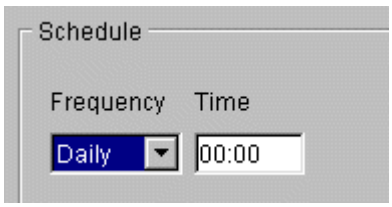
Once option



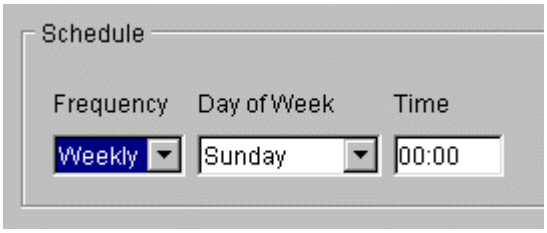
Hourly option



Daily option



Weekly option

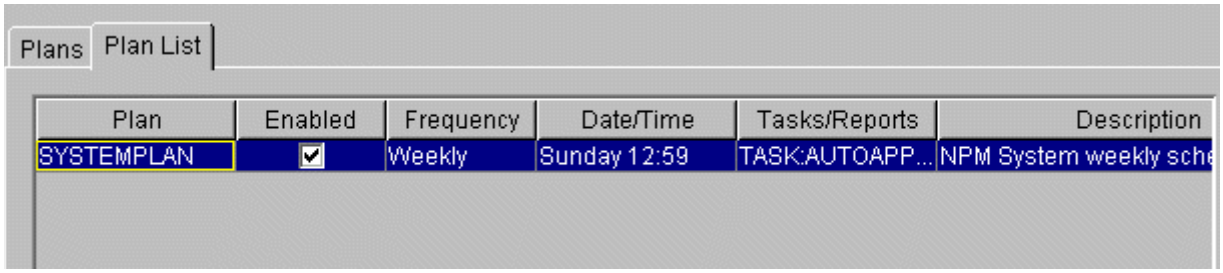


b Enter the appropriate scheduling information for the frequency option you selected.

c In the **Time Limit** list, click the time limit of your choice. The time limit defines how long the plan will be allowed to run.

8 Click **Save** to save the plan.

The new plan will be reflected on the **Plan List** tab once the NPM has saved the plan.



9 Click **Close** to close the Plans window.

10 You have completed this procedure.

Modifying a plan using the NPM

Application

Use this procedure to modify a plan using the Network Patch Manager (NPM). You can modify a plan using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

A Plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule may specify either a one time execution at a given time or repeated execution according to a frequency definition. A Plan may include the following tasks: apply, remove, audit, and reports.

There is one system-defined plan named SYSTEMPLAN. It cannot be renamed, but it can be modified or deleted. The SYSTEMPLAN is initially defined with the AUTOAPPLY and AUTORESTART tasks.

A maximum of 5 plans can be defined in addition to the system-defined plan, SYSTEMPLAN.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Enable the plan by typing

```
npm> enableplan ON
```

and pressing the Enter key.

Note: If the start time for the plan has already passed, this step will fail. To correct this, modify the plan schedule to change the start time (see step 4). Then perform this step again.

3 Add or delete a task to or from the plan by typing

```
npm> sched <tr_option> <tr_name> <add_delete>
```

and pressing the Enter key.

where

tr_option
is TASK or REPORT, which indicates whether a Task or Report is being added or deleted

tr_name
is the name of the task or report being added or deleted

add_delete
is ADD or DELETE, which indicates whether the task or report is being added or deleted to or from the plan

Example

```
npm> sched TASK AUDIT ADD
```

4 Update the plan schedule in the database by typing

```
npm> updplan <plan_freq> <date_time> <max_time>
<plan_desc>
```

and pressing the Enter key.

where

plan_freq
is Once, Hourly, Daily, Weekly, or Monthly, which indicates how often the plan should execute

date_time
is the date and time the plan is to be executed in mm-dd-yy hh:mm format. Plans executed more than once will begin executing at this time of day each interval.

max_time
is No_Limit, 15_min, 30_min, 1_Hr, 2_Hr, 4_Hr, 8_Hr, or 16Hr, which indicates the maximum amount of time to execute the plan

plan_desc
is a brief description of the plan

Example

```
npm> updplan Weekly "02-15-02 16:59" 4_Hr "NPM
System weekly scheduled routine activities"
```

5 You have completed this procedure.

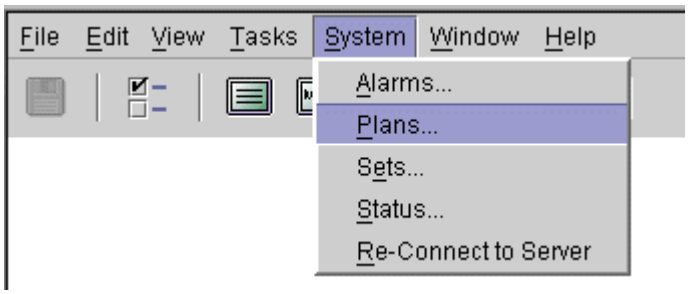
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

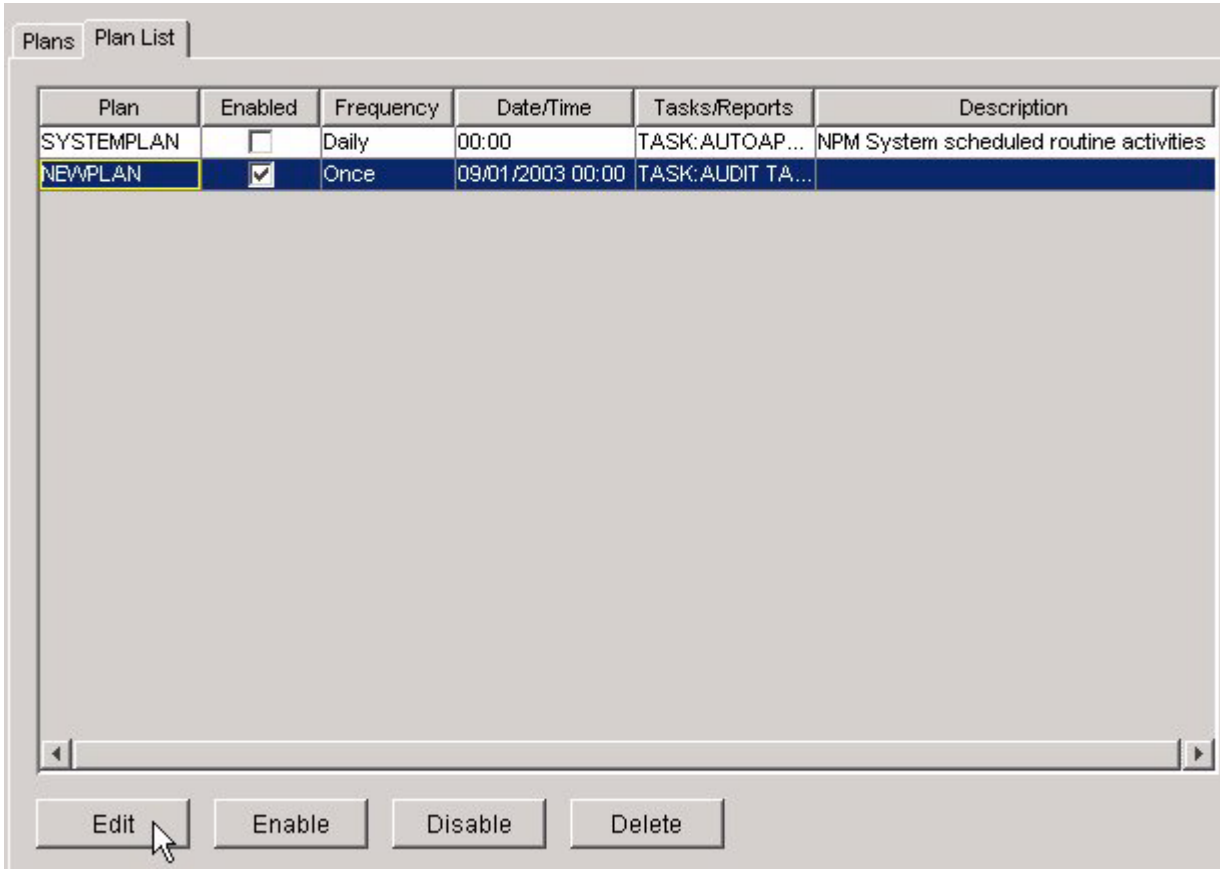
2 On the **System** menu, click **Plans...**.



The **Plans** window opens.

3 Click the **Plan List** tab.

4 In the **Plans List** tab, click the plan you want to modify, then click **Edit**.



5 In the **Plan Description** box, type a new description of the plan (optional).

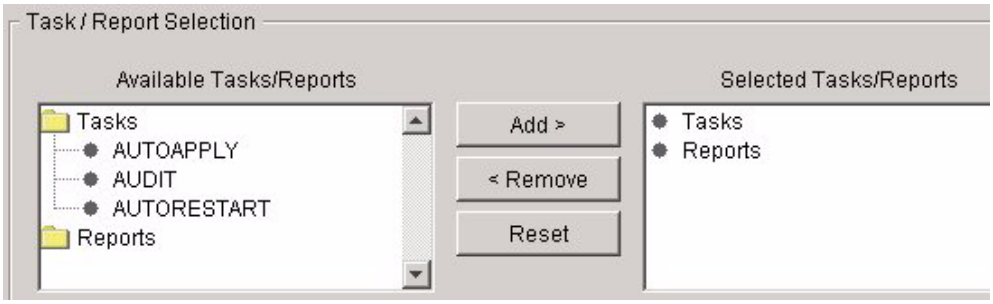
6 Click the **Enabled** check box to enable (checked) or disable (unchecked) the execution of the scheduled plan if required.

7 Use the following table to determine your next step.

If you want to	Do
add tasks or reports to the plan	step 8
delete tasks or reports from the plan	step 9

8 Add tasks or reports to the plan as follows:

a In the **Available Tasks/Reports** list, double click on the **Tasks** or **Reports** folder to didplay the available tasks or reports.



b Click the task or report you want to add to the plan.

Note: Do not add reports that require user input when they execute, as a user may not be present at the time those reports execute. This includes pre-defined reports and user-defined reports. The pre-defined reports that require user input, and that you must not add, are as follows:

- DEVICE
- PATCH
- PATCHES_SINCE
- PATCHINFO

c Click **Add** to add the task or report to the **Selected Tasks/Reports** list.

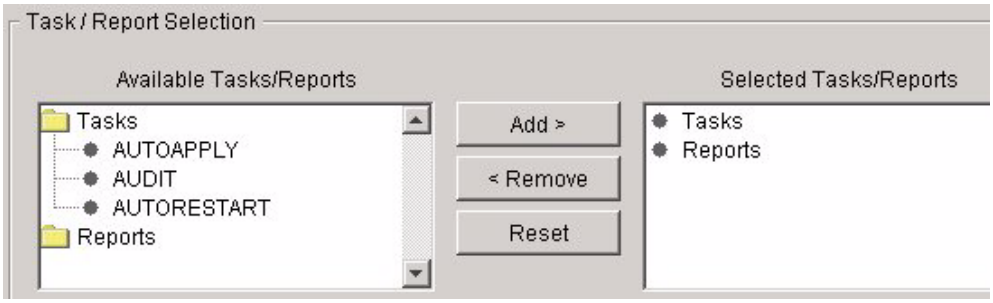
Note: The order in which the tasks and reports appear in the Selected Tasks/Reports list, is the order in which they will execute. The tasks in a plan are executed sequentially.

d Repeat step 8a and 8b for each task or report you want to add to the plan.

Note: You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

9 Delete tasks or reports from the plan as follows:

a In the **Selected Tasks/Reports** list, double click on the **Tasks** or **Reports** folder to didplay the selected tasks or reports.



b Click the task or report you want to delete from the plan.

c Click **Remove** to delete the task or report from the **Selected Tasks/Reports** list.

d Repeat step 9a and 9b for each task or report you want to remove from the plan.

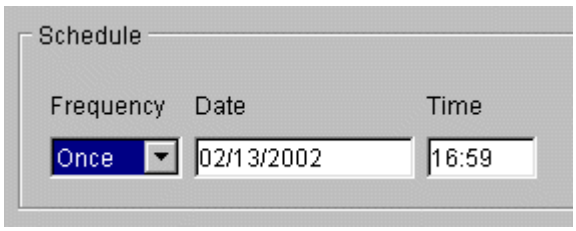
Note: You can use the **Shift** key to select multiple tasks or reports consecutively, or the **Ctrl** key to select multiple tasks or reports non-consecutively.

10 In the **Schedule** area, update the plan schedule if required, as follows:

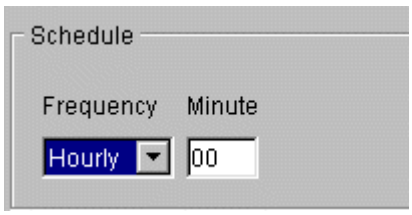
a In the **Frequency** list, click the frequency option of your choice.

When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

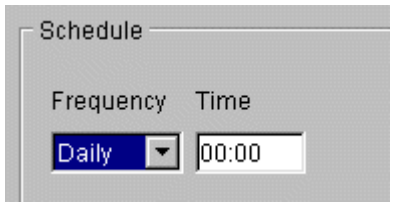
Once option



Hourly option



Daily option



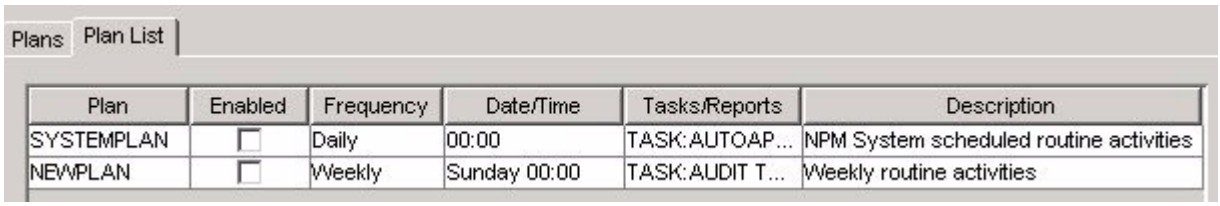
Weekly option

b Enter the appropriate scheduling information for the frequency option you selected.

c In the **Time Limit** list, click the time limit of your choice. The time limit defines how long the plan will be allowed to run.

11 Click **Save** to save the plan.

The modified plan will be reflected on the **Plan List** tab once the NPM has saved the plan.



12 Click **Close** to close the Plans window.

13 You have completed this procedure.

Deleting a plan using the NPM

Application

Use this procedure to delete a plan using the Network Patch Manager (NPM). You can delete a plan using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

A Plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule may specify either a one time execution at a given time or repeated execution according to a frequency definition. A Plan may include the following tasks: apply, remove, audit, and reports.

There is one system-defined plan named SYSTEMPLAN. It cannot be renamed, but it can be modified or deleted. The SYSTEMPLAN is initially defined with the AUTOAPPLY and AUTORESTART tasks.

A maximum of 5 plans can be defined in addition to the system-defined plan, SYSTEMPLAN.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Disable the plan by typing

`npm> enableplan <plan_name> OFF`

and pressing the Enter key.

where

plan_name
is the name of the plan

3 Delete the plan by typing

`npm> delplan <plan_name>`

and pressing the Enter key.

where

plan_name
is the name of the plan

4 You have completed this procedure.

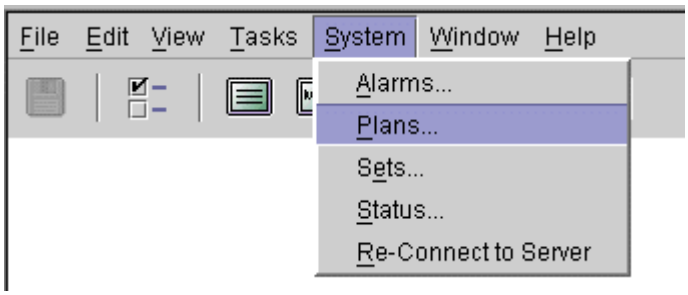
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

2 On the **System** menu, click **Plans...**.



The **Plans** window opens.

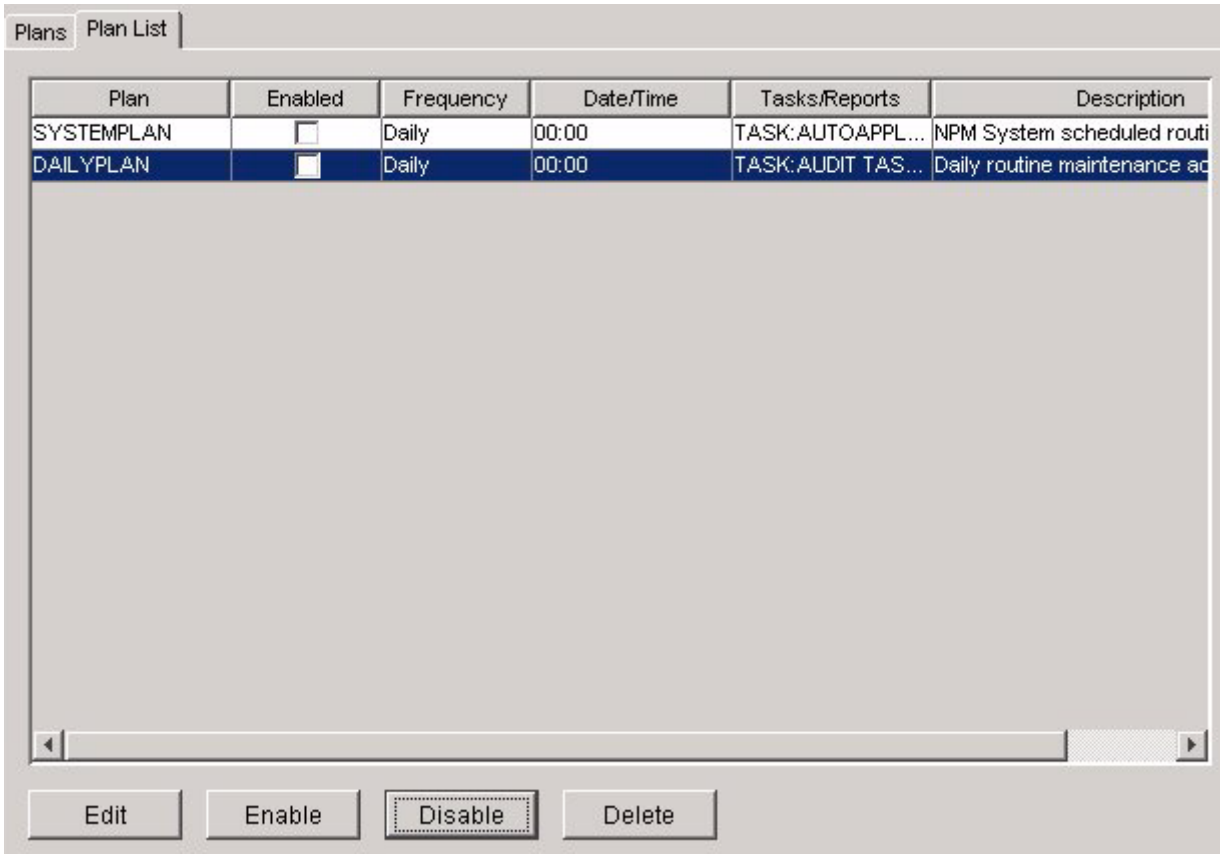
3 Click the **Plan List** tab.

4 In the **Plan List** tab, click the plan you want to delete.

If the plan is	Do
enabled	step 5
not enabled	step 6

5 Click **Disable**.

6 Click **Delete**.



7 Click **Close** to close the Plans window.

8 You have completed this procedure.

Prioritizing a patching maintenance request using the NPM

Application

Use this procedure to move a specific patching maintenance request to the top of the queue for processing, using the Network Patch Manager (NPM). You can prioritize a request using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 List the queued maintenance requests and their task ID by typing

```
npm> qrunning
```

and pressing the Enter key.

3 Move a specific maintenance request to the top of the processing queue by typing

`npm> priority <task ID>`

and pressing the Enter key.

where

task ID
is the number next to the task

The system moves the task to the top of the queue for processing.

4 You have completed this procedure.

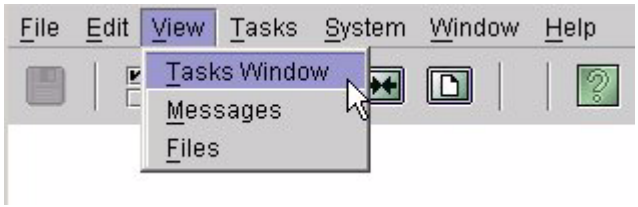
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

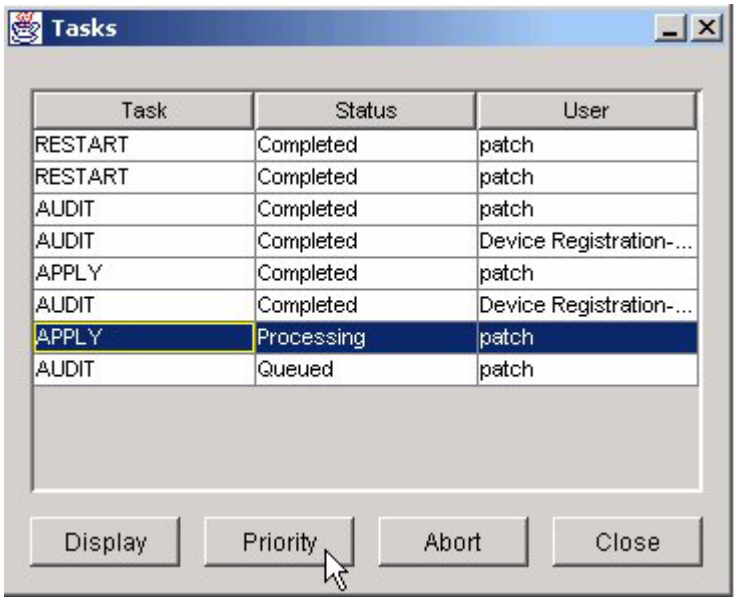
At the NPM GUI

2 On the **View** menu, click **Tasks Window**.



The **Tasks** window is displayed.

3 Select the queued task you want to move to the top of the processing queue, and click **Priority** .



The system moves the task to the top of the queue for processing.

4 You have completed this procedure.

Migrating the SAM21 network elements back to the CS 2000 SAM21 Manager on the CS 2000 Core Manager

Application

Use this procedure to migrate the SAM21network element back to the CS 2000 SAM21 Manager on the CS 2000 Core Manager.

Prerequisites

None

Action

Launch the CS 2000 SAM21 Manager client that resides on the CS 2000 Core Manager

At the client workstation

1 Log on the client workstation using the correct user ID and password. Do not log on as the root user.

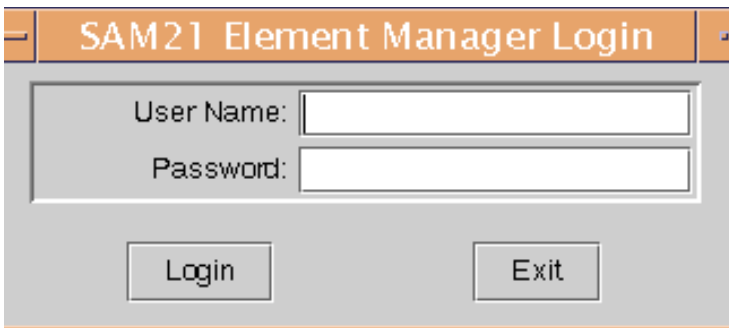
2 Launch the SAM21 Manager client application that resides on the CS 2000 Core Manager by typing

```
# /sdm/bin/sam21gui
```

and pressing the Enter key.

The user authentication window appears.

User authentication window



3 Enter a valid user name and password, and click the “Login” button.

4 Reprovision each SAM21 network element, which involves changing the IP address in the “SAM21 EM Server” field to the IP address of the CS 2000 Core Manager. Refer to procedure “Reprovision a CS 2000 SAM21 network element” in the SAM21 Shelf Controller Configuration Management document, NN10111-511, if required.

An SNMP message is sent to both SAM21 shelf controllers with the IP and port of the CS 2000 Core Manager. Within approximately 1 minute, the SAM21 network element recovers from isolation on the CS 2000 SAM21 Manager that resides on the CS 2000 Core Manager. Within approximately 2 minutes, the SAM21 network element is isolated on the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server.

Launch the CS 2000 SAM21 Manager client that resides on the CS 2000 Management Tools server

At your workstation

1 Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server. Refer to procedure “Accessing the GUI for the CS 2000 SAM21 Manager” in this document, if required.

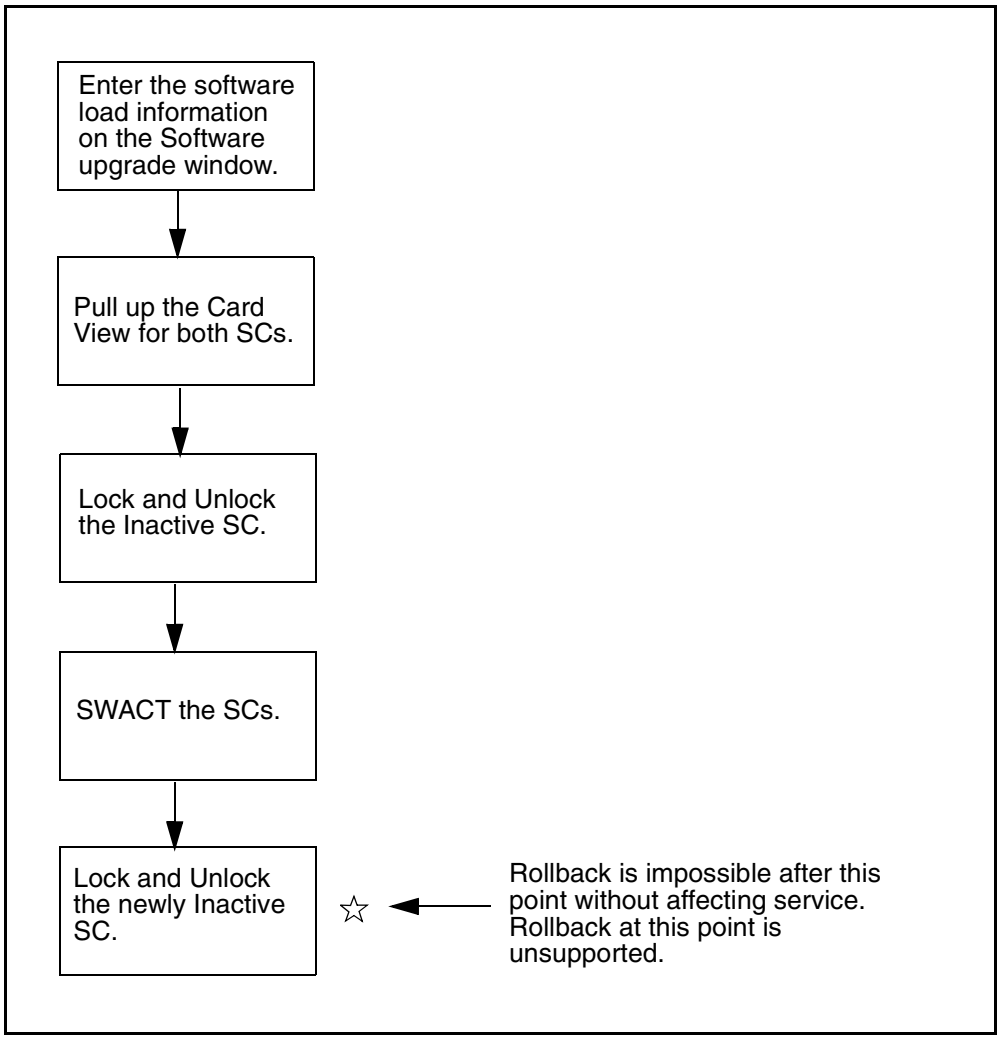
2 Reprovision each SAM21 network element by changing the IP address in the “SAM21 EM Server” field to the IP address of the CS 2000 Core Manager. Refer to procedure “Reprovision a CS 2000 SAM21 network element” in the SAM21 Shelf Controller Configuration Management document, NN10111-511, if required.

All non-isolated shelves are communicating with the CS 2000 SAM21 Manager on the CS 2000 Core Manager.

3 You have completed this procedure.

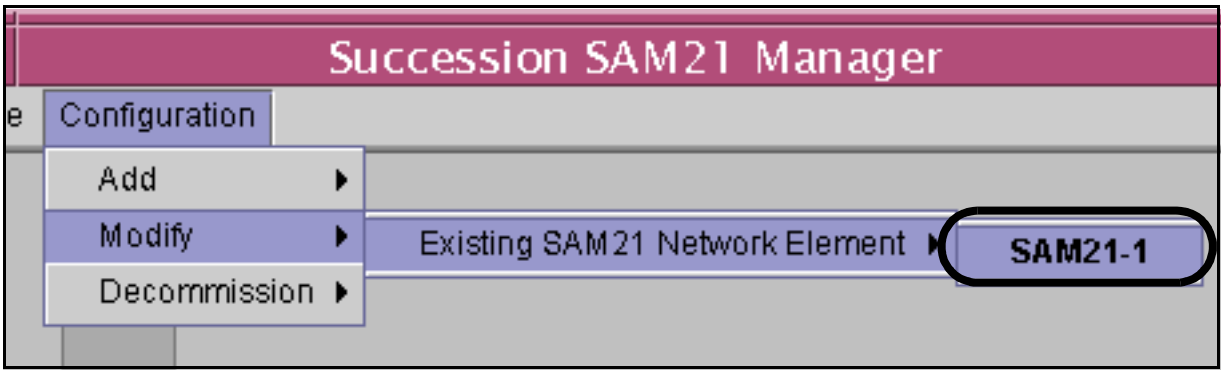
Rollback software on the shelf controller

The following figure summarizes the upgrade procedure. Rollback is available until the second Shelf Controller is upgraded. This point is indicated with the star.

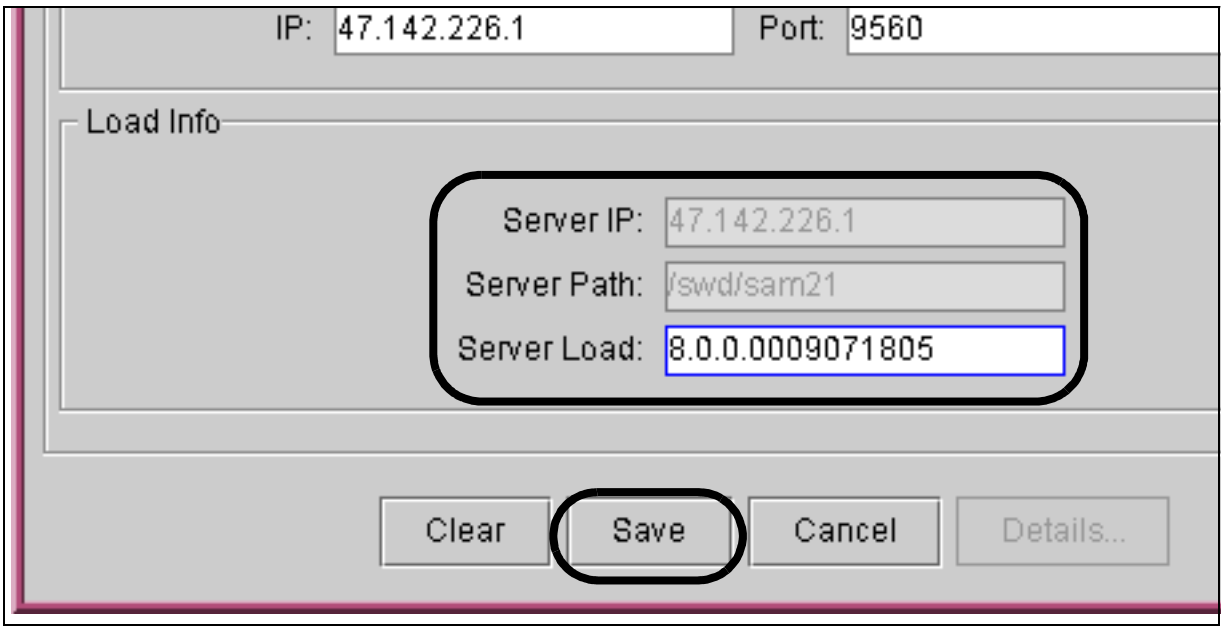


At the CS 2000 SAM21 Manager client (Java Web Start client)

1 From the Subnet View, select Configuration, Modify and then the SAM21 shelf with the Shelf Controllers to revert.



2 Enter the software loadname of the old software load on the Reprovisioning window. For example, if the upgrade was from 8.0.0.0009071805 to 9.0.0.0301120523, enter 8.0.0.0009071805 to revert to the old software load.



3 Click Save.

4

ATTENTION

If this was an SN05 to SN06 upgrade, perform steps 4 through 8 from the client that is served by the CS 2000 Core Manager and is started with the `/sdm/bin/sam21gui` command.

If the active Shelf Controller is running SN06, right click on the card icon and select Swact from the card context menu. Wait for completion of SWACT.

From the Shelf View, right click on the inactive Shelf Controller and select Lock from the card context menu.

Note: This Shelf Controller is the card that was loaded with the software upgrade and is being reverted to the previous software load.

5 Wait for the lock icon to appear on the inactive Shelf Controller.

6 From the Shelf View, right click on the inactive Shelf Controller and select Unlock from the card context menu.

7 Wait for the hashed outline to disappear from the Inactive Shelf Controller.

8 This procedure is complete.

Performing a rollback of the CS 2000 SAM21 Manager

Application

Use this procedure to rollback the CS 2000 SAM21 Manager from the CS 2000 Management Tools server to the CS 2000 Core Manager.

ATTENTION
This procedure deletes all provisioned data for the CS 2000 SAM21 Manager from the database on the CS 2000 Management Tools server.

Prerequisites

None

Action

At the CS 2000 Management Tools server

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Stop the SAM21 Manager server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

6 Change directory by typing

```
# cd /opt/nortel/sam21em/bin/migration
```

and pressing the Enter key.

7 Run the SAM21 Manager rollback script by typing

```
# ./sam21emRollback.sh
```

and pressing the Enter key.

Example response:

```
SAM21 Element Manager Server Persistent Data
Migration Rollback
==============================================
This script should only be executed to rollback
from the SSPFS SAM21 EM to the CS2E SAM21 EM.

WARNING: This script deletes all provisioned
data from the SAM21 EM database.

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N")
```

8 Confirm that you want to proceed with the rollback by typing

```
# y
```

and pressing the Enter key.

Example response:

```
Retrieving Oracle SAM21 EM Password...

Clearing the SAM21EM Database Tables...
SAM21 Element Manager Persistent data migration
rollback successful.
```

9 You have completed this procedure.

Reverting to the previous release of the SSPFS software

Application

Use this procedure if you have upgraded the SSPFS software to the SN06.2 release and want to revert to the previous release, which can be one of the following:

- Reverting to the SN05 release
- Reverting to the SN06 release

Prerequisites

You must have “SSPFS Disk 1” and “SSPFS Disk 2” for the release you want to revert to, either SN05 or SN06.

Action

Perform the steps under Reverting to the SN05 release or Reverting to the SN06 release to complete this procedure.

Reverting to the SN05 release

At the CS 2000 Management Tools server console

1 Bring your system to the OK prompt by typing

```
init 0
```

and pressing the Enter key.

2 Insert “SSPFS Disk 1” into the CD Rom drive.

3 Boot the system from the CD Rom by typing

```
# boot cdrom
```

and pressing the Enter key.

4 When prompted, acknowledge your use of the software by typing

```
# ok
```

and pressing the Enter key.

5 When prompted, enter the hostname for this system.

6 When prompted, enter the IP address associated with the hostname you just entered.

7 When prompted, enter the subnet mask for the network.

8 When prompted, enter the IP address for the network’s router.

9 When prompted, enter the timezone for the system.

Note: Type **`Help`** or **`?`** for a list of timezones.

10 When prompted, confirm this system will host a database by typing

```
# yes
```

and pressing the Enter key.

11 When prompted, indicate whether this system uses DNS (Domain Name Service).

If you enter	Do
no (does not use DNS)	step 15
yes (uses DNS)	step 12

12 When prompted, enter the DNS domain for the system.

13 When prompted, enter the IP address of a DNS server.

Note: You can enter a maximum of 5 IP addresses. If you have less than 5, leave blank and press the Enter key.

14 When prompted, enter a DNS search domain.

Note: You can enter a maximum of 5 DNS search domains. If you have less than 5, leave blank and press the Enter key.

15 When prompted, review the current settings, and if correct, accept them by typing

```
# ok
```

and pressing the Enter key.

This step takes approximately 65 minutes to complete. When complete, the system ejects “SSPFS Disk 1” and reboots.

16 When prompted, enter the root password.

Note: If you do not want a root password, press the Enter key twice.

17 When prompted, enter the root password again.

18 Remove “SSPFS Disk 1” from the CD Rom drive, and insert “SSPFS Disk 2”.

19 When prompted, confirm you are ready to proceed by typing

```
# ok
```

and pressing the Enter key.

This step takes approximately 40 minutes to complete. When complete, the system ejects “SSPFS Disk 2” and reboots.

20 When prompted, enter the root user ID and password-.

21 You have completed this procedure.

Reverting to the SN06 release

At the CS 2000 Management Tools server console

1 Bring your system to the OK prompt by typing

```
init 0
```

and pressing the Enter key.

2 Insert “SSPFS Disk 1” into the CD Rom drive.

3 Boot the system from the CD Rom by typing

```
# boot cdrom
```

and pressing the Enter key.

4 When prompted, acknowledge your use of the software by typing

```
# ok
```

and pressing the Enter key.

5 When prompted, confirm this system will host a database by typing

```
# yes
```

and pressing the Enter key.

The system defaults to factory set values.

Note: Entering “no” allows you to change the database IP if required.

6 When prompted, review the current settings, and if correct, accept them by typing

```
# ok
```

and pressing the Enter key.

Note: Entering “no” allows you to change the current settings if they are not correct.

This step takes approximately 65 minutes to complete. When complete, the system ejects “SSPFS Disk 1” and reboots.

7 Remove “SSPFS Disk 1” from the CD Rom drive, and insert “SSPFS Disk 2”.

8 When prompted, confirm you are ready to proceed by typing

```
# ok
```

and pressing the Enter key.

This step takes approximately 40 minutes to complete. When complete, the system ejects “SSPFS Disk 2” and reboots.

After the reboot, the logon prompt is displayed, and the system is ready for use.

9 When prompted, enter the root user ID and password.

10 You have completed this procedure.

Restoring root file systems

Application

Use this procedure to restore the root file systems from disk.

This procedure only applies to systems running SSPFS SN05, SN06, or SN06.1. For system running SSPFS SN06.2, refer to procedure "Performing a full system restore (SN06.2 or greater)" in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the CS 2000 Management Tools server console

1. Log in to the CS 2000 Management Tools server through the console using the root user ID and password.
2. Insert the backup tape into the drive.
3. Insert SSPFS CD disk#1 into the CD-ROM drive.
4. Enter the following commands:

   ```
   # metadetach d2 d1
   # metaroot /dev/dsk/c0t0d0s1
   # init 6
   ```

5. When prompted, log on as root.
6. Enter the following commands:

   ```
   # metaclear -r d2
   # metaclear d1
   # init 0
   ```

7. At the ok prompt, boot the system from the CD Rom by typing

   ```
   ok boot cdrom -s
   ```

   and pressing the Enter key.

8 Enter the following commands:

```
# mount /dev/dsk/c0t0d0s1 /a
# cp /a/etc/system /a/etc/system.unmirror
# cp /a/etc/vfstab/ /a/etc/vfstab.unmirror
# cd /a
# ufsrestore rfs /dev/rmt/0 1
```

Note: The system can take between 20 and 45 min. to process the above command.

```
# rm restoresymtable
# cd /
# cp /a/etc/system.unmirror /a/etc/system
# cp /a/etc/vfstab.unmirror /a/etc/vfstab
# umount /a
# fsck /dev/rdsk/c0t0d0s1
# installboot /usr/platform/`uname -i`
/lib/fs/ufs/bootblk /dev/rdsk/c0t0d0s1
```

Note: The above command is entered on one line, and a space is required between "`-i``" and "`/lib/fs/ufs/bootblk`".

```
# init 6
```

9 When prompted, log on as root.

Note: The root password required is the restored root password and not the default root password.

10 Enter the following commands:

```
# metainit -f d0 1 1 c0t0d0s1
# metainit d1 1 1 c0t1d0s1
# metainit d2 -m d0
# metaroot d2
# lockfs -fa
# init 6
```

11 When prompted, log on as root.

12 Enter the following commands:

```
# metattach d2 d1
# init 6
```

13 When prompted, log on as root.

14 Remove the tape from the drive and store it in a safe place.

15 Eject the SSPFS CD disk#1 from the CD-ROM drive by entering the following commands:

```
# cd /
# eject cdrom
```

16 You have completed this procedure.

Restoring non-root file systems

Application

Use this procedure to restore all of the non-root file systems from disk.

This procedure only applies to systems running SSPFS SN05, SN06, or SN06.1. For system running SSPFS SN06.2, refer to procedure “Performing a full system restore (SN06.2 or greater)” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

ATTENTION

The root user must be under the default command shell when performing the whole restore file systems procedure. Do not switch to any other command shell such as the Korn or Bash shell, since under the Korn or Bash command shell, the system will be frozen when you issue the “init 1” command.

At the CS 2000 Management Tools server console

1. Log in to the CS 2000 Management Tools server through the console using the root user ID and password.
2. Insert the backup tape into the drive.
3. Enter the following command:

   ```
   # init 1
   ```

4. When the system prompts you to either enter the root password or press Control-D, enter your root password to continue the maintenance process.

5 Enter the following command:

```
# ufsrestore tfs /dev/rmt/0 1 | grep audio_files
```

If	Do
the response to the command is similar to `321287 ./audio_files`	substep a
the command produces no output	substep b

a Enter the following series of commands:

Note: The restore time is dependent on the size of the filesystem, therefore varies between filesystems.

```
# cd /audio_files
# ufsrestore rfs /dev/rmt/0 2
# rm restoresymtable

# cd /data
# ufsrestore rfs /dev/rmt/0 3
# rm restoresymtable

# cd /opt
# ufsrestore rfs /dev/rmt/0 4
# rm restoresymtable

# cd /opt/nortel
# ufsrestore rfs /dev/rmt/0 5
# rm restoresymtable

# cd /PROV_data
# ufsrestore rfs /dev/rmt/0 6
# rm restoresymtable

# cd /user_audio_files
# ufsrestore rfs /dev/rmt/0 7
# rm restoresymtable

# cd /var
# ufsrestore rfs /dev/rmt/0 8
# rm restoresymtable
```

b Enter the following series of commands:

```
# cd /data
# ufsrestore rfs /dev/rmt/0 2
# rm restoresymtable
```

```
# cd /opt
# ufsrestore rfs /dev/rmt/0 3
# rm restoresymtable

# cd /opt/nortel
# ufsrestore rfs /dev/rmt/0 4
# rm restoresymtable

# cd /var
# ufsrestore rfs /dev/rmt/0 5
# rm restoresymtable
```

6 Enter the following command:

```
# init 6
```

7 Remove the tape from the drive and store it in a safe place.

8 You have completed this procedure.

Restoring application data to the Oracle database

Application

Use this procedure to restore the application data to the Oracle database from a backup tape.

Prerequisites

You need the tape on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the CS 2000 Management Tools server

1 Insert the backup tape into the drive.

At your workstation

2 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Stop the SESM, SAM21EM, and NPM server applications that run on the CS 2000 Management Tools server. Refer to the procedure that corresponds to the application in the CS 2000 Management Tools Administration and Security document, NN10172-611, for instructions on how to the stop the server application if required.

7 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

8 Perform the restore command by typing

```
$ /opt/nortel/sspfs/bks/rsimpora
```

and pressing the Enter key.

9 Quit the Oracle user by typing

```
$ exit
```

and pressing the Enter key.

10 Remove the tape from the drive and store it in a safe place.

11 Start the SESM, SAM21EM, and NPM server applications that run on the CS 2000 Management Tools server. Refer to the procedure that corresponds to the application in the CS 2000 Management Tools Administration and Security document, NN10172-611, for instructions on how to the stop the server application if required.

12 You have completed this procedure.

Clearing the JWS cache on a client workstation

Application

Use this procedure to clear the Java ™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client worksation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

Prerequisites

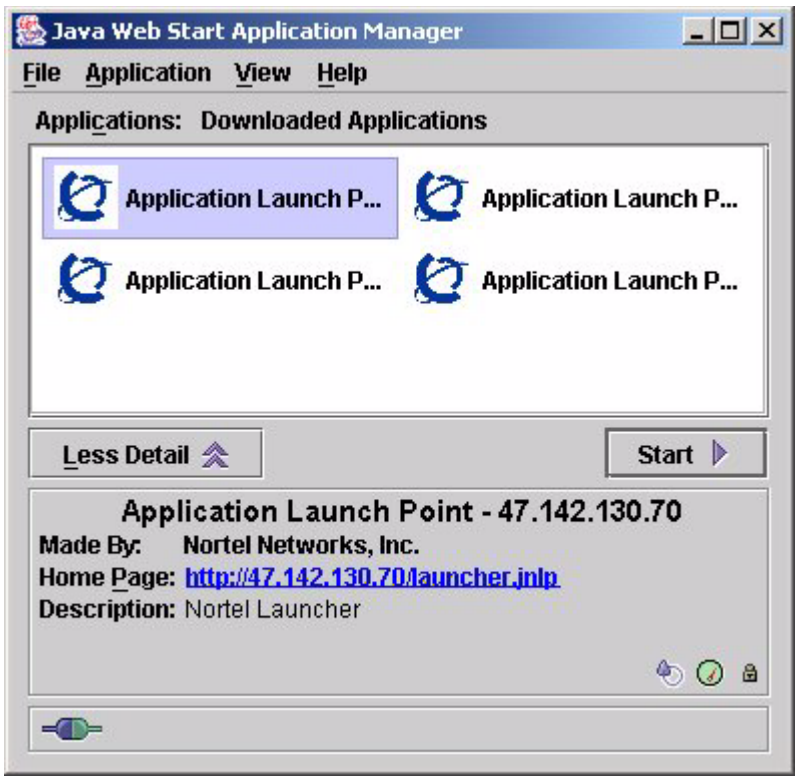
None

Action

Perform the following steps to complete this procedure.

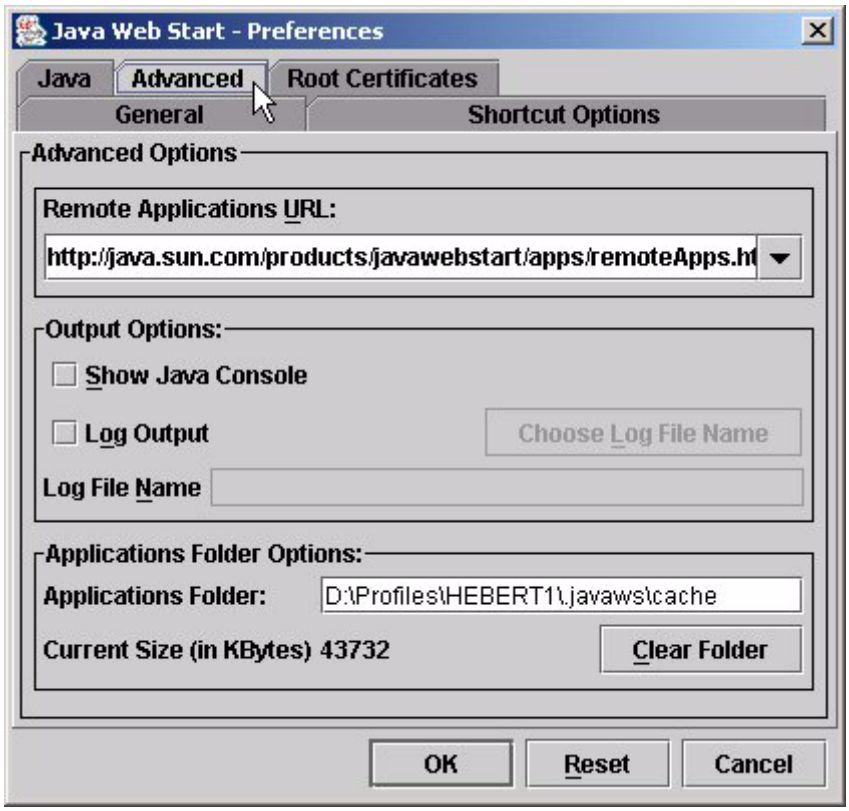
At your workstation

1 Access the Java Web Start Application Manager.

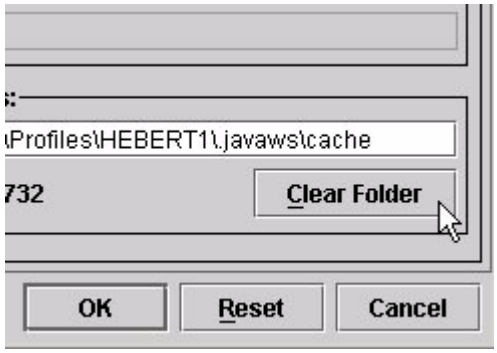


2 Access the Preferences panel by clicking **File->Preferences**.

3 Access the Advanced panel by clicking the **Advanced** tab.



4 Clear the cache by clicking **Clear Folder**.



5 Confirm you want to clear the cache (remove all downloaded resources) by clicking **Yes**.

6 You have completed this procedure.

Verifying the upgrade was successful

Application

Use this procedure to verify the upgrade was successful.

Prerequisites

The CS2M software has been upgraded.

Action

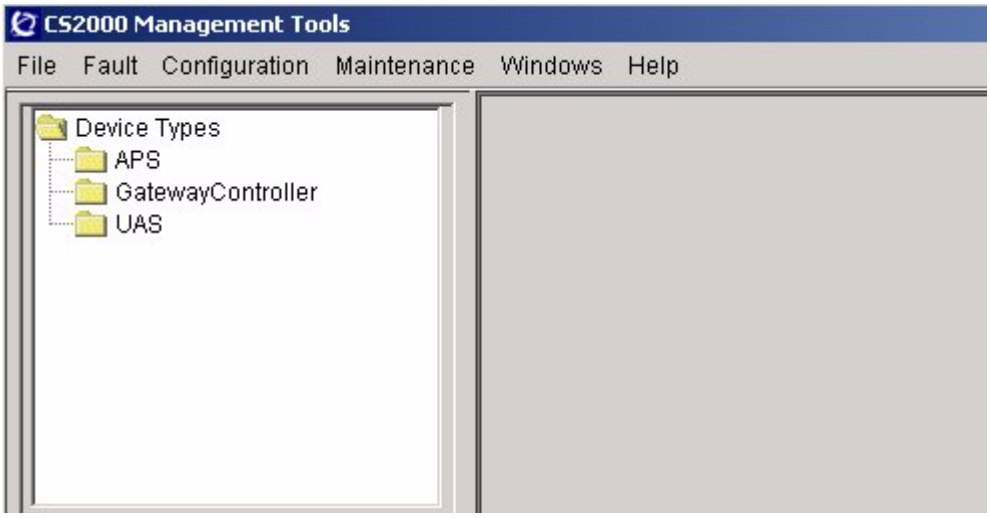
Perform the following steps to complete this procedure.

ATTENTION
If you encounter a problem during any one of the steps in this procedure, contact your next level of support.

At your workstation

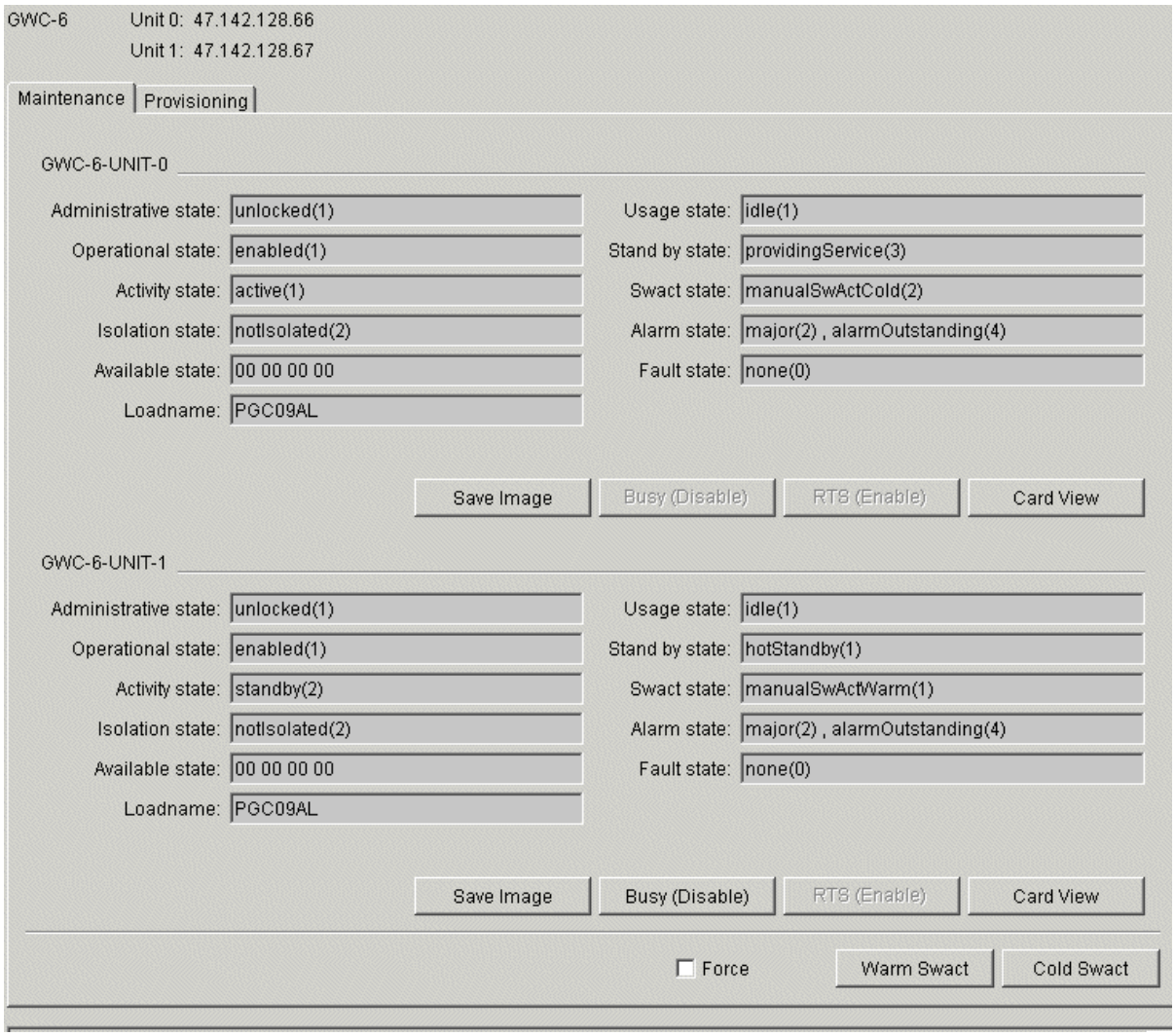
1 Launch the CS2000 Management Tools application GUI and ensure the topology is displayed correctly as shown in the figure below. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

This verifies correct restoration of the database.



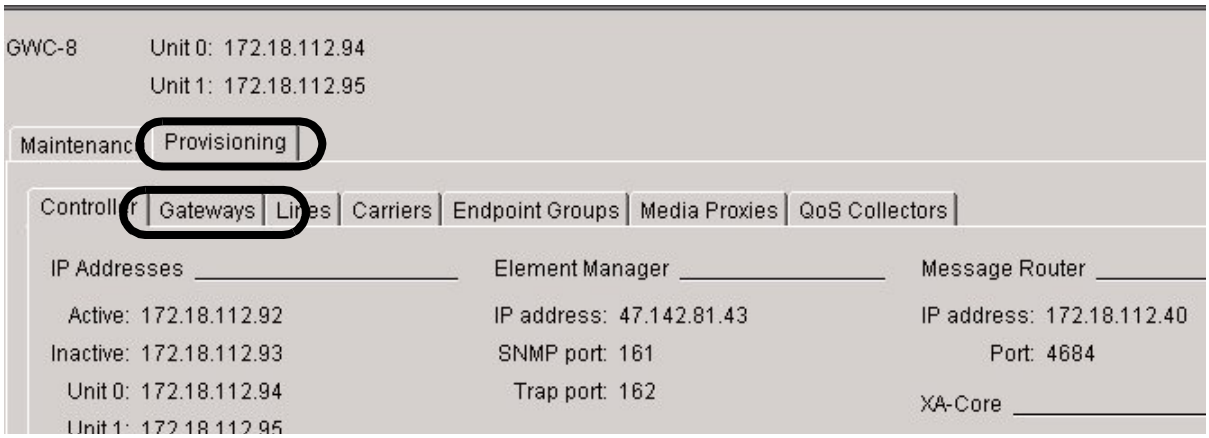
2 Click on **GatewayController**, then select a GWC from the list, and ensure correct maintenance states are displayed for the active and inactive units as shown in the figure below.

This verifies GWC SNMP communication.

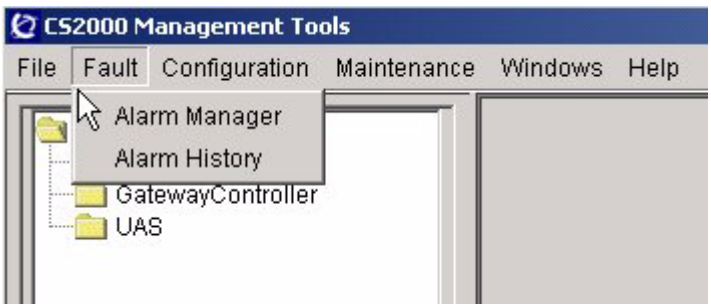


3 Click the **Provisioning** tab, then the **Gateways** tab as shown in the figure below, and then click **Retrieve All** to retrieve all subtending gateways.

This verifies correct restoration of the database.



4 On the **Fault** menu, click **Alarm Manager** as shown in the figure below, and verify alarms show up when a maintenance attempt is performed on a GWC unit.



5 Click the **Maintenance** tab, then click **Card View** to launch the CS 2000 SAM21 Manager card view.

This verifies correct operation of the CS 2000 SAM21 Manager application GUI.

6 Connect to OSSGate. Refer to the associated procedure in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required. Query a provisioned line (line solutions) or trunk (trunk solutions). Refer to the associated procedures in the OSSGate user guide, if required.

This verifies the SDM OSS APS, DDMS, and core communication path.

7 For line solutions, launch the line maintenance manager (LMM) application GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required. Post, busy, and return a line to service. Refer to associated procedures in the CS 2000 Management Tools Fault Management document, NN10084-911, if required.

This verifies the SDM - DMA, BMI, and core communciation path.

8 For trunk solutions, launch the trunk maintenance manager (TMM) application GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required. Post, busy, and return a trunk to service. Refer to associated procedures in the CS 2000 Management Tools Fault Management document, NN10084-911, if required.

This verifies the SDM - DMA, BMI, and core communciation path.

9 You have completed this procedure.

Stopping the PSE server application on a Sun server

Application

Use this procedure to stop the Patching Server Element (PSE) server application on a Sun server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where PSE resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Stop the PSE server application by typing

```
# servstop PSE
```

and pressing the Enter key.

6 Verify the PSE server application stopped by typing

```
# servman query -status -group PSE
```

and pressing the Enter key.

7 You have completed this procedure.

Starting the PSE server application on a Sun server

Application

Use this procedure to start the Patching Server Element (PSE) server application on a Sun server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where PSE resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Start the PSE server application by typing

```
# servstart PSE
```

and pressing the Enter key.

6 Verify the PSE server application started by typing

```
# servman query -status -group PSE
```

and pressing the Enter key.

7 You have completed this procedure.