# Upgrading the Media Server 2000 Series

This document contains the procedures for upgrading and downgrading the Media Server 2000 Series software (Media Server 2010 and Media Server 2020).

**ATTENTION**

When applying a patch, refer to the instructions contained in the *Admin file* on the Patch CD or in the individual downloaded patch. The *Admin file* explains how to apply the patch and overrides this procedure. If no special instructions are contained in the *Admin file* and a reference to this document is provided, then continue using this document.

## IEMS GUI

The Integrated Element Management System GUI (IEMS GUI) access for the Media Server 2000 series is introduced in SN08. If you are upgrading the Media Server 2000 nodes to SN08, you must first upgrade to the IEMS. In order to change configuration settings for an SN08 Media Server node, you must use the IEMS GUI.

The IEMS GUI is the human interface to the Succession Operations and Maintenance Center Platform. To access the IEMS GUI, refer to the IEMS Basics document (NN10329-111).

## Media Server 2000 Series upgrade and downgrade

The Media Server 2000 Series upgrade procedure enables you to apply a maintenance release or “patch” to a Media Server 2000 Series node, or upgrade the node as part of a network-wide upgrade to a new release. The downgrade procedure enables you to remove a maintenance release or patch from a Media Server 2000 Series node, or downgrade the node as part of a network-wide downgrade to a previous release.

Beginning in SN08, the Media Server 2000 series is configured through the CS 2000 Management Tools GUI. In SN07, the Media Server 2000

series was configured through a command line User Interface (CLUI). This procedure covers the steps necessary to migrate from SN07 to SN08.

**CAUTION**

For the procedure used to upgrade the Media Server as part of an end-to-end software upgrade, refer to the solution upgrades document.

The following table lists the procedures used in upgrading and downgrading the Media Server 2010 or Media Server 2020.

**Media Server 2000 Series upgrade and downgrade procedures**

| Procedure and page |
| --- |
| Upgrading a Media Server 2000 node |
| Backing up the Current load files |
| Copying the files to the audiocodes directory |
| Pre-Migration steps for the Media Server 2000 |
| Migration of Media Server 2000 nodes into an Integrated EMS |
| Procedure to upgrade a Media Server 2000 |
| Editing and viewing object properties using Java Web Client |
| Editing and viewing object properties using Web Client |
| Downgrading a Media Server 2000 node |
| Backing up the Current load files |

# Upgrading a Media Server 2000 node

This procedure enables you to upgrade a Media Server 2000 node as part of a network-wide upgrade to a new release.

## Office impact

Upgrading a Media Server 2000 node as part of network-wide upgrade is dependent upon the upgrade of other network elements first being completed. Therefore, this procedure must be performed at the appropriate time within the network upgrade sequence.

When this procedure is performed in response to a network-wide upgrade, the Media Server 2000 node is not operational. Therefore, this procedure should be performed during an offline network maintenance window or when sufficient additional servers are available to maintain normal network operations while this node is out of service.

In this procedure each Media Server 2000 node in the network is to be updated one at a time.

When this upgrade procedure is successfully completed, INI files retrieved from the Media Server 2000 nodes will be encrypted.

**CAUTION**

During the upgrade procedure, you will perform a hard reset on the Media Server. If you are upgrading a 240 port Media Server 2010, the hard reset will take both Media Servers out of service. Any active calls will be dropped!

## Material requirements

This is a software-only procedure and doesn't require special tools. The following files are provided either on compact disc or through electronic software distribution (ESD).

- CMP file (software executable load)
- INI file (configuration file)
- DAT files containing specific information (such as Conference tones, and information to deliver test trunk functionality)

The client workstation must be running the following programs.

- Microsoft Windows 98, NT, 2000, XP, or 2003
- Netscape 6, or higher, or Microsoft Internet Explorer (IE) 6.0, or higher

## Backing up the Current load files

Before starting this procedure, review any documentation included with the software. The documentation included with the software may override or supplement this procedure.

For increased security, the CS 2000 Management Tool, and SDM logins, are equipped with login timeouts. If at any point in the procedure the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

### *At the Windows desktop interface*

1 Open a DOS window and enter the following three commands.

```
ping <IP address of router>
ping <IP address of CS 2000 Management Tool>
ping <IP address of SDM>
```

If a response displays for all three commands, continue with the next step. If a response does not display for any one of the three commands, check connections and configuration of the network settings for the PC (or laptop). Do not continue with this procedure until the ping commands all indicate successful connections.

2 Open a telnet connection to the CS 2000 Management Tool.

3 When prompted, enter nortel as the user name and nortel as the password.

4 Log in to the Media Server 2000 Series CLUI by entering the following commands.

```
cd /opt/nortel/NTsesm/bin/
./ms2000.sh
```

5 When prompted, enter nortel as the user name and nortel as the password.

The Media Server 2000 Series CLUI main menu displays.

```
** Media Server 2000 Series CLUI Main Menu **
1) Display list of MS 2000 series nodes
```

```
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
Enter selection (1-5, x)
>
```

6 Enter the number corresponding to “Backup INI file for all nodes”. This will retrieve a current copy of the INI file for each Media Server 2000 configured in the system.

***Note:*** The .ini files are backed up in a directory with the ams ip address as the directory name. The directory contains the last five backed up .ini files. Note the dates to determine which file is the most recent.

7 Press “x” to exit the Media Server 2000 Series CLUI.

8 Enter the following command.

**cd /data/loads/ams**

9 Create a backup directory with a descriptive name that includes today’s date and the current release version.

**mkdir ams_bku_<today’s date>_<release>**

**Example**
mkdir ams_bku_20031031_7.0

10 Back up the files by entering the following commands.

**cp -p *.cmp ams_bku_<today’s date>_<release>**

**cp -p *.dat ams_bku_<today’s date>_<release>**

***Note:*** If you receive an error such as “cp cannot access *.dat”, this indicates that there are no files of this type to back up.

11 Each Media Server 2000 node has a directory containing a copy of its INI file. The directory name is the IP address of the Media Server 2000 node. Make a backup copy of each Media Server 2000 directory by entering the following command at the command line for each Media Server 2000 node.

**cp -pr <MS 2010 ip address> ams_bku_<today’s date>_<release>**

where <release> is the current release

**Example**
cp -pr 172.17.40.230 ams_bku_20040501_7.0

**12** Change to the backup directory you created in step 9 above and verify that the files and directory are actually present.

## Copying the files to the audiocodes directory

***At the Windows desktop interface***

**1** Determine the source for the software upgrade files.

| If | Do |
|---|---|
| the software upgrade files are delivered through ESD | step 2 |
| the software upgrade files are on CD | step 11 |

**2** Log in to the server by typing

```
> telnet <server>
```

where

**server**
is the IP address or host name of the SSPFS-based server to which you want to transfer the software load

**3** When prompted, enter your user ID and password.

**4** Change to the root user by typing

```
$ su - root
```

**5** When prompted, enter the root password.

**6** Ensure enough disk space is available for the ESD software by typing

```
# df -k /
```

***Note:*** It is recommended to have a minimum of 800 MByte of available disk space.

*Example response*

```
# df -k /
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454     5%    /
```

2876454 / 1000 = 2876 MB free

The value under the avail column is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.

**7** Transfer the ESD software load from the drop box on the repository server to the SSPFS-based server as follows:

**a** Access the repository server through FTP by typing

```
# ftp <repository_server>
```

*where*

**<repository_server>**
is the machine owned by the operating company that was selected to be the destination for ESD software.

**b** Log in and change directory to the drop box location on the repository server.

**c** Change the transfer mode to binary by typing

```
ftp> bin
```

**d** List the contents of the drop box by typing

```
ftp> ls
```

**e** Transfer the ESD software load onto the SSPFS-based server by typing

```
ftp> get <iso_image>
```

*where*

**<iso_image>**
is the MS20x0 filename of the zipped version of the ISO image for the software load

**Example**
**ftp> get MS2000X0.X0.V.NCL.NAP.VAULT.X.D.tar.gz**

*Or*

**ftp> get MS2A00X0.X0.V.NCL.NAP.VAULT.X.D.tar.gz**

*where*

**MS2000X0.X0** or **MS2A00X0.X0** refers to the ordering code for the Media Server 2000 software for the SN0X release (this value changes for each release)

**V** refers to the product release (V for VO; R for Released)

**NCL** refers to the software load type (NCL for non-CM load; MNCL for maintenance non-CM load)

**NAP** refers to the processor type

**VAULT** refers to the Nortel software repository source

**X** refers to the Nortel software repository version (if applicable)

**D** refers to the software file format reason (Distribution)

**tar** refers to a tarred file (tape archive file)

**gz** refers to a zipped file

**f** End the FTP session by typing

```
ftp> bye
```

**g** Uncompress the software load file.

```
gzip -d MS2000X0.X0.V.NCL.NAP.VAULT.X.D.tar.gz
```

*Or*

```
gzip -d MS2A00X0.X0.V.NCL.NAP.VAULT.X.D.tar.gz
```

**h** Untar the software load file.

```
tar -xvf MS2000X0.X0.V.NCL.NAP.VAULT.X.D.tar
```

*Or*

```
tar -xvf MS2A00X0.X0.V.NCL.NAP.VAULT.X.D.tar
```

**i** Access the directory that contains the software load file by typing

```
cd MS2000X0.X0.V.NCL.NAP.VAULT.X.D
```

*Or*

```
cd MS2A00X0.X0.V.NCL.NAP.VAULT.X.D
```

and list the file in the directory.

**j** Change the name of the file in the directory by typing

```
mv MS2000X0_load.iso.tape MS2000X0_load.iso
```

*Or*

**mv MS2A00X0_load.iso.tape MS2A00X0_load.iso**

**8** Mount the ISO image as follows:

**a** Access the command line interface by typing

```
# cli
```

*Example response*

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

**b** Enter the number next to the “Other” option in the menu.

*Example response*

```
Other
 1 - Log Rotation
 2 - capt_files (Capture Various SSPFS
     Files/Logs For Debugging Purposes)
 3 - sun_explorer (Execute the Sun Explorer
     Data Gathering Tool)
 4 - mount_image (Mount A Generic Iso Image
     To The SSPFS Unit)
 5 - umount_image (Un-Mount A Generic Iso
     Image From The SSPFS Unit)
 X - exit
```

**c** Enter the number next to the “mount_image” option in the menu.

| If the response is | Do |
|---|---|
| `ISO Image Already Mounted` | substep d |
| `Enter the full path of the ISO image` | substep e |

**d** Enter the number next to the “umount_image” option in the menu and retry substep c.

***Note:*** If the umount_image or mount-image command is unsuccessful a second time, contact your next level of support.

**e** When prompted, enter the full path name of the ISO image on the server from the root.

**Example**

**/MS2000X0.X0.V.NCL.NAP.VAULT.X.D/MS2000X0_load.iso**

*Or*

**/MS2A00X0.X0.V.NCL.NAP.VAULT.X.D/MS2A00X0_load.iso**

The contents of the ESD software file are placed in directory /tmpmnt.

The following message displays.

```
=== "mount_image" completed successfully
```

***Note:*** Do not attempt to access the /tmpmnt directory until the mount command is complete.

| If the response is | Do |
|---|---|
| `Is is very important for the user of this command to know that if you mount an iso image. It is a MUST that you umount an image before removing the image file. If the file is deleted while the OS has it mounted, it can be harmful to the runtime applications on this unit` | step f |
| `Provided full path to ISO image does not exist` | Verify the location and name of the ISO 9660 image. |
| `Error creating the image device location` | This response indicates an operating system error with the loopback file driver. Retry the command, and if it fails a second time, contact your next level of support. |
| `ERROR MOUNTING <ESD_filename>` | This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt` directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support. |

**f** Exit each menu level of the command line interface to return to the root level prompt, by typing **x** and pressing Enter.

**9** Enter the following commands.

**cd /tmpmnt**

**ls**

Verify the content of the /tmpmnt directory by referring to the patch or release installation instructions to determine the correct release content. You may see .ini, .dat, and .cmp files listed, as well as an installation script (<filename>.sh or <filename>.pl). There may also be some documentation or a README.file.

**10** Proceed to step 14.

**11** Insert the CD into the CD drive.

**12** Enter the following command.

```
cd /cdrom/cdrom0
```

**13** Enter the following command.

```
ls
```

Verify the content of the CD that displays by referring to the patch or release installation instructions to determine the correct release content. You may see .ini, .dat, and .cmp files listed, as well as an installation script (<filename>.sh or <filename>.pl). The CD may also contain some documentation or a README.file.

**14** Copy the files to the audiocodes directory by entering the following commands.

```
cp -r * /data/loads/audiocodes
```

```
cp * /data/loads/audiocodes
```

**15** Enter the following commands.

```
cd /data/loads/audiocodes
```

```
ls -ltr
```

Ensure that the files you copied are present in the directory. The newer files will appear near the bottom of the listing.

***Note:*** Make a note of the full path name of the .cmp file for use later in this procedure.

**16** Prepare the .dat file and the .ini file.

**a** Refer to the release notes and consult with your network administration regarding the tones file to determine if a customized toneset .DAT file is appropriate for your network.

**b** Login as root.

**c** Change to the audiocodes tools directory by entering the following command.

```
cd /data/loads/audiocodes/Tools
```

***Note 1:*** Check the /data/loads/audiocodes/( IP address) directory for the .DAT and .INI files. If you do not find the files, check the /data/loads/ams/( IP address) directory.

***Note 2:*** If the SESM and IEMS are on the different boxes, FTP the .ini file from the /data/loads/ams/( IP address) directory on SESM to /data/loads/audiocodes/(IP address) directory on the IEMS.

**d** Perform an upgrade to the .ini file by entering the following command.

```
perl iniupgrade.pl
/data/loads/audiocodes/AMS_DefaultConfig_<.ini file
from audiocodes> /data/loads/audiocodes/<SN06.2 .ini
or SN07 .ini file from step 6 > <SN08 .ini filename>
```

***Note:*** SN06.2 and SN07 use different directories as shown in the examples below.

### Example for SN06.2

```
perl iniupgrade.pl
/data/loads/audiocodes/AMS_DefaultConfig_IP_v204.ini
/data/loads/ams/10.69.33.1/2005-03-04_10:56:33.Board
.ini SN08_new.ini
```

### Example for SN07

```
perl iniupgrade.pl
/data/loads/audiocodes/AMS_DefaultConfig_IP_v204.ini
/data/loads/audiocodes/10.69.33.1/2005-03-04_10:56:3
3.Board.ini SN08_new.ini
```

**17** Make a note of the .DAT and .INI file names for use later in this procedure.

**18** Copy the INI file you created in step 16d above to the proper directory on the IEMS server. This allows the INI file to appear in the Media Server 2000 Configuration and Maintenance GUI during the node upgrade.

**a** Enter the following commands to change directories.

```
> cd /data/loads/audiocodes
```

```
> cd <ip address of the Media Server 2000
node>
```

**b** If the directory does not exist, create the directory for this node by entering the following command.

```
>mkdir <ip address of the MS2000 node>
```

**c** Copy the upgraded INI file to this directory as shown below.

```
>cp /data/loads/audiocodes/Tools/<ini file
created in step 16d>
/data/loads/audiocodes/<ip address of
node>/.
```

**19** If you acquired the the software upgrade files from CD, eject the CDRom and store in a secure location. Eject the CDRom by entering the following commands.

```
# cd /
```

```
# eject cdrom
```

**20** If you acquired the software upgrade files through ESD, remove the directory and files created in the Copying the files to the audiocodes directory procedure.

**Example**

```
cd /
```

```
rm -r /MS2000X0.X0.V.NCL.NAP.VAULT.X.D
```

*Or*

```
rm -r /MS2A00X0.X0.V.NCL.NAP.VAULT.X.D
```

## Pre-Migration steps for the Media Server 2000

Prior to upgrading the Media Server 2000 node you need to check the following items.

- the IP address on which the IEMS application is running
- the trusted managers table for the IEMS IP

If an SN07 Media Server 2000 node existed in the network prior to upgrading SESM, the Media Server 2000 trusted managers table must either be emptied or the IP address on which the IEMS server runs must be added to the list. Because the trusted managers table was introduced in SN07, previous loads do not have this requirement.

**CAUTION**

Deleting or adding the wrong entries in the trusted manager table can cause loss of communication to the Media Server 2000 node. Read this entire procedure before making any trusted manager table changes.

***Collect the following information. It is used to complete some of the steps.***

1 Record the IP address on which the SESM application is running.

**Example**

```
# getpip.ksh
47.20.10.1
```

**CAUTION**

If you are deleting all entries from the trusted managers table, then the SESM IP must be the last entry deleted from the table.

2 Record the IP address on which the IEMS application is running.

***Note:*** The IEMS application frequently runs on a virtual IP. Do not rely on the external IP address of the server itself.

```
bash-2.05$ getpip.ksh iems
47.142.100.15
```

***Procedure for updating trusted manager table for migrating Media Server 2000 node.***

3 Launch the Media Server 2000 CLUI from the SESM node and list the trusted managers table. (If the table is empty, no action is required and you have completed this procedure.)

```
bash-2.05$ /opt/nortel/NTsesm/bin/ms2000.sh
```

```
************************************************
Nortel Media Server 2000 Series Configuration Tool
                  version 2.05
************************************************
```

**4** Enter the user name and password when prompted.

```
Enter user name > iemslab
Enter password  >
```

The Media Server 2000 Series CLUI Main menu displays.

```
ORBWrapper orb initialized
****Media Server 2000 Series CLUI Main Menu ***
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
Enter Selection (1 - 5, x)
>
```

**5** Enter 2 to select the Node Maintenance and Configuration menu.

**6** When prompted, enter the IP address of the Media Server 2000 node.

The maintenance and configuration Main Menu displays.

***Note:*** The maintenance and configuration Main Menu shows the type of Media Server based on the IP you entered. For this example, the following IP address is for a Media Server 2010. The screen output is slightly different for a Media Server 2020.

```
*** Main Menu for MS2010 at 47.142.134.127 ***
1) Maintenance Menu
2) Configuration Menu
x) EXIT
Enter Selection (1 - 2, x)
>
```

**7** Enter 2 to select the Configuration menu.

The Main Configuration Menu displays.

```
***** Main Configuration Menu for MS2010 at
47.142.134.127 *****
1) Display this nodes current configuration
2) General node configuration
3) Configure Network Time settings
4) SNMP configuration and security
x) EXIT
Enter Selection (1 - 4, x)
>
```

**8** Enter 4 to select SNMP configuration and security.

The SNMP Configuration and Password Management Menu displays.

```
*** SNMP Configuration and Password Management
Menu for MS2010 at 47.142.134.127 ***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and
password
?) Help
x) EXIT
Enter Selection (1 - 4, ?, x)
>
```

**9** Enter 1 to select Setup Trusted SNMP Managers.

The Trusted Mangers Configuration Menu displays.

```
*** Trusted Mangers Configuration Menu for
MS2010 at 47.142.134.127 ***
1) List configured trusted managers
2) Add a trusted manager
3) Delete a trusted manager
?) Help
x) EXIT
Enter Selection (1 - 3, ?, x)
```

```
>
```

**10** Enter 1 to list the trusted managers.

A list of the trusted managers displays.

```
List of Trusted Managers
========================
IP = 47.142.10.1
IP = 47.142.100.15
IP = 47.140.4.0
```

***Note:*** If there are no trusted managers, the following message displays.

```
There are no Trusted Managers defined
Press <enter> to continue
```

**a** If the table is empty then the procedure is completed. Do nothing to the trusted manager table. Continue with the next section, Loss of communication with the node.

**b** If the trusted manager table contained entries, check to see if the IP address on which the IEMS application runs is in the list. If the IP address on which the IEMS application runs is in the list then the procedure is completed. Do nothing to the trusted manager table. Continue with the next section, Loss of communication with the node.

**c** If the trusted managers table is not empty *and* does not already contain the IP address that the IEMS application runs on then you have two choices. You can add the IEMS application IP address to the list or delete all entries in the list. If you choose to delete all of the trusted managers you *must* delete the IP address that the SESM application is running on *last*. The safest action is to add the IEMS application IP address to the list. Once this is done, you can go to the IEMS application and launch the Media Server 2000 Configuration and Maintenance tool from the node (provided it is already in the IEMS topology). If the Media Server 2000 Configuration and Maintenance tool can communicate with the device, the IEMS has its IP address in the trusted manager table correctly.

**i** Add the IEMS application IP address to the list. Once this is done, you can go to the IEMS application and launch the Media Server 2000 Configuration and Maintenance tool from the node (provided it is already in the IEMS topology). If the Media Server 2000 Configuration and

Maintenance tool can communicate with the device, the IEMS IP address has been added to the trusted manager table correctly.

*Or*

ii Delete all entries in the list. If you choose to delete all of the trusted managers, the IP address on which the SESM application is running *must be deleted last*.

***Note:*** The safest action is to add the IEMS application IP address to the list.

### Loss of communication with the node

If you lose communication with the node but the node is still in service, there are two possible causes.

- The node has a trusted manager defined and the machine you are attempting to access the node from is not in the trusted manager list.

  *Or*

- There is a SNMP community string mismatch.

In either case, the node will have to reloaded by performing the following steps.

1 Access the web interface of the node.

2 Perform a backup of the INI file.

3 Edit/correct the trusted managers file and correct the SNMP community strings.

***Note:*** Remember, whatever the community strings are set to in the INI file must match those used by the Media Server 2000 CLUI or the IEMS Media Server 2000 Maintenance and Configuration Tool.

## Migration of Media Server 2000 nodes into an Integrated EMS

In SN06.2 and SN07, configuration and maintenance of the Media Server 2000 nodes (IP Media Server 2010 and the ATM Media Server 2020) was handled through a command line tool running on the SESM application. With the SN08 software release, Media Server 2000 node configuration and maintenance is handled under the IEMS software using a GUI client.

In SN06.2 the Media Server 2000 CLUI (Command Line User Interface) provided the user with the ability to set a single web server user name and password that would be used by all devices. In SN07, the Media Server 2000 CLUI (Command Line User Interface) provided the user

with the ability to set the community string and web server passwords on the Media Server 2000 nodes. The tool stored these encrypted passwords to use when communicating with the node.

In SN08, the Media Server 2000 Configuration and Maintenance GUI will also need to use these passwords for communication with the nodes. Because of this, any password changes that were made to the Media Server 2000 nodes will need to be manually entered into the IEMS Media Server 2000 node properties.

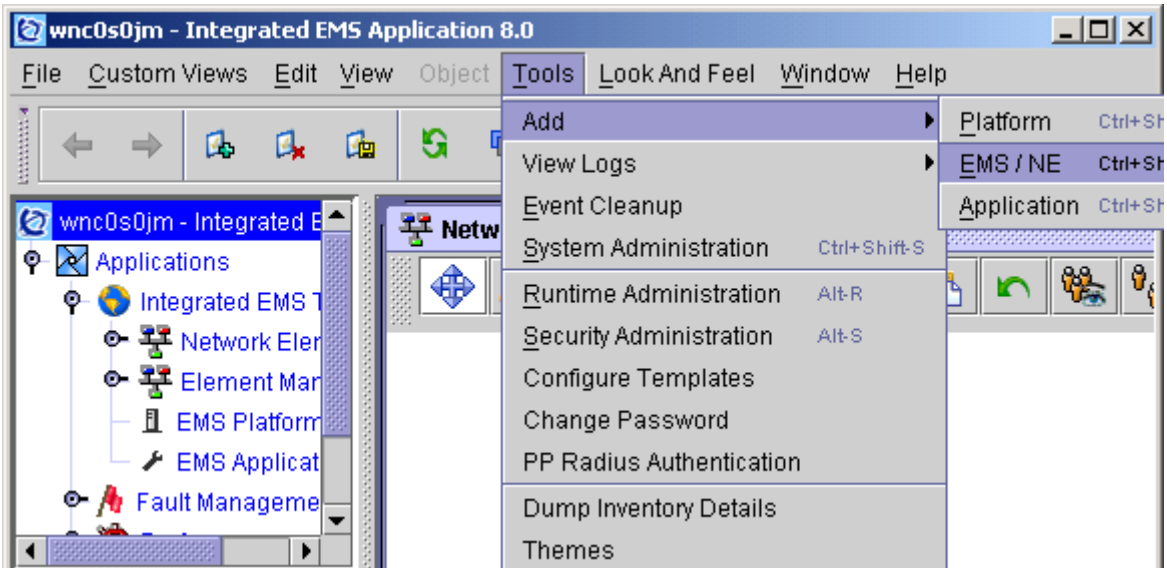
There are three scenarios for migrating or upgrading an SN06.2 or SN07 Media Server 2000 node into an SN08 IEMS.

- Scenario 1 - SN06.2 or SN07 Media Server 2000 node existed in the network but was not previously managed by IEMS (refer to Procedure for Scenario 1).
- Scenario 2 - SN07 Media Server 2000 node existed in IEMS and used default settings for web server and SNMP community strings (refer to Procedure for Scenario 2).
- Scenario 3 - SN07 Media Server 2000 node existed in IEMS with modified settings for web server and SNMP community strings (refer to Procedure for Scenario 3).

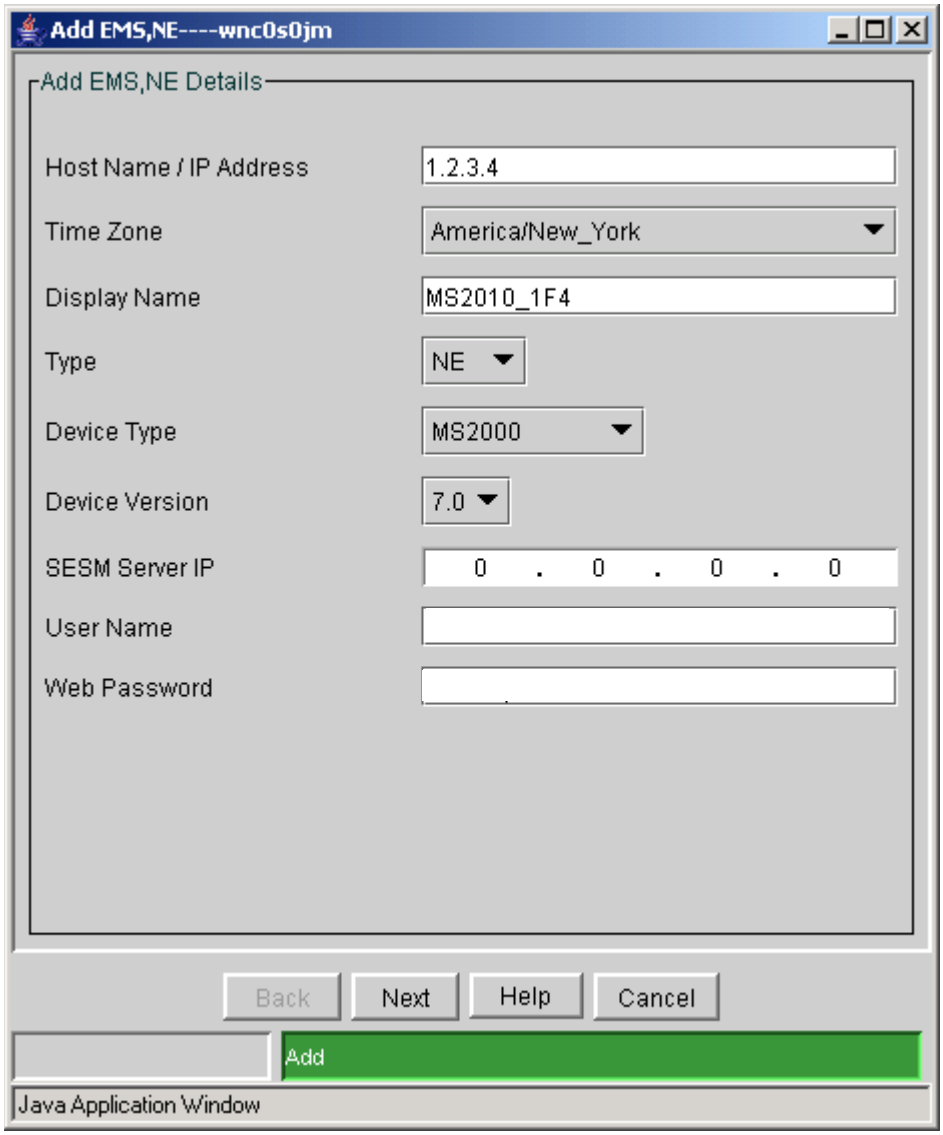
### *Procedure for Scenario 1*

A Media Server 2000 node was present in SN06.2 or SN07 network but did not exist in IEMS.

**1** Add the Media Server 2000 node to the IEMS by selecting the Add NE menu item under Tools menu.



The add EMS/NE wizard opens.




2 Select a type of “NE”, Device Type of “MS2000”, and Device Version.

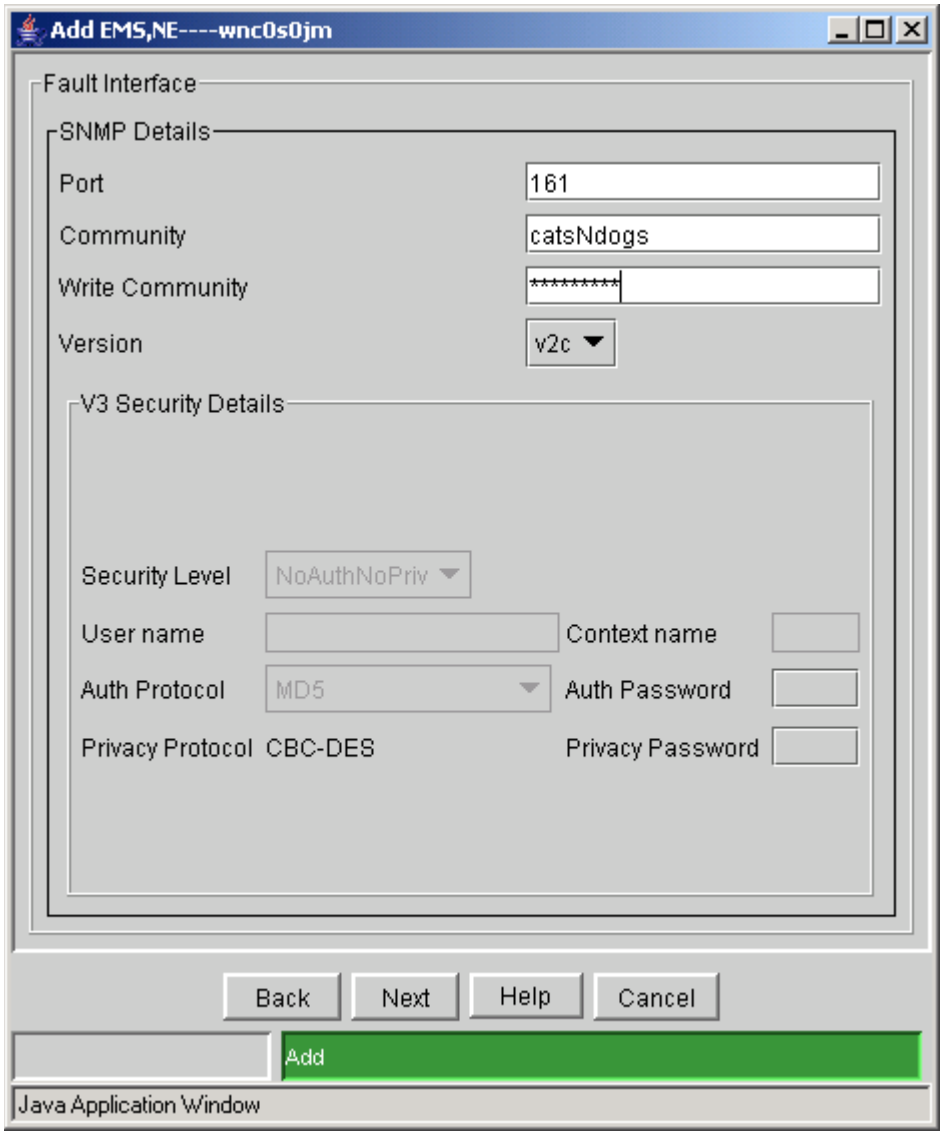
***Note:*** If you are upgrading from SN06.2, the IEMS does not support management of an SN06.2 Media Server 2000 node. However, you can add the node into the IEMS as an "8.0" Device version in order to upgrade it. Because the IEMS cannot collect alarms or performance metrics from the SN06.2 node, the node will have some alarms registered against it until it is upgraded to the SN08 load.

The panel adds the fields to enter the web server “User Name” and “Web Password”.

3 If the web user name and password were modified in SN06.2 or SN07, enter the modified values in the NE properties for the Media Server 2000 node. If the web server user name and password are still the node default values, enter a user name of “Admin” and a password of ”Admin”.

***Note:*** Failure to put the correct values here will cause the Maintenance and Configuration tool to fail when it attempts to perform file transfers to and from the node.

The next figure panel illustrates setting up the Fault Interface. The SNMP Read and Write Community Strings will be setup for the node.



4 If the node has previously had its community strings changed from the default values then the new values need to be entered here. If the default values for the node are still being used then enter a read community of “public” and write community of “private”.

***Note 1:*** If the community strings were changed by the Media Server 2000 CLUI in SN07, then both the read and write community string will be the same value. These can be changed after this procedure is completed by using the Media Server 2000 Configuration and Maintenance tool from the Media Server 2000 device menu.

***Note 2:*** Failure to put the correct read community string for the node here will prevent the Media Server 2000 Configuration and Maintenance tool from communicating with the node. When the tool is launched for this node a “Request Timeout” will occur while trying to retrieve the node information. If the write community string is not correct then the tool will fail whenever any configuration or maintenance activity attempts to change settings on the node. Again this will appear as a “Request Timeout” to the node.

5 Fill in the appropriate community strings for the node.

### *Procedure for Scenario 2*

A Media Server 2000 node was present in an SN07 IEMS and used the default file transfer / web server password and SNMP community string.

There is *No* action required. When a Media Server 2000 node in an SN07 IEMS is upgraded it is assigned the default values used by the node for web server user name (“Admin”) and password (“Admin”) and the default SNMP read (“public”) and write (“private”) community strings.

### *Procedure for Scenario 3*

A Media Server 2000 node was present in an SN07 IEMS and the file transfer / web server password or SNMP community string was changed.

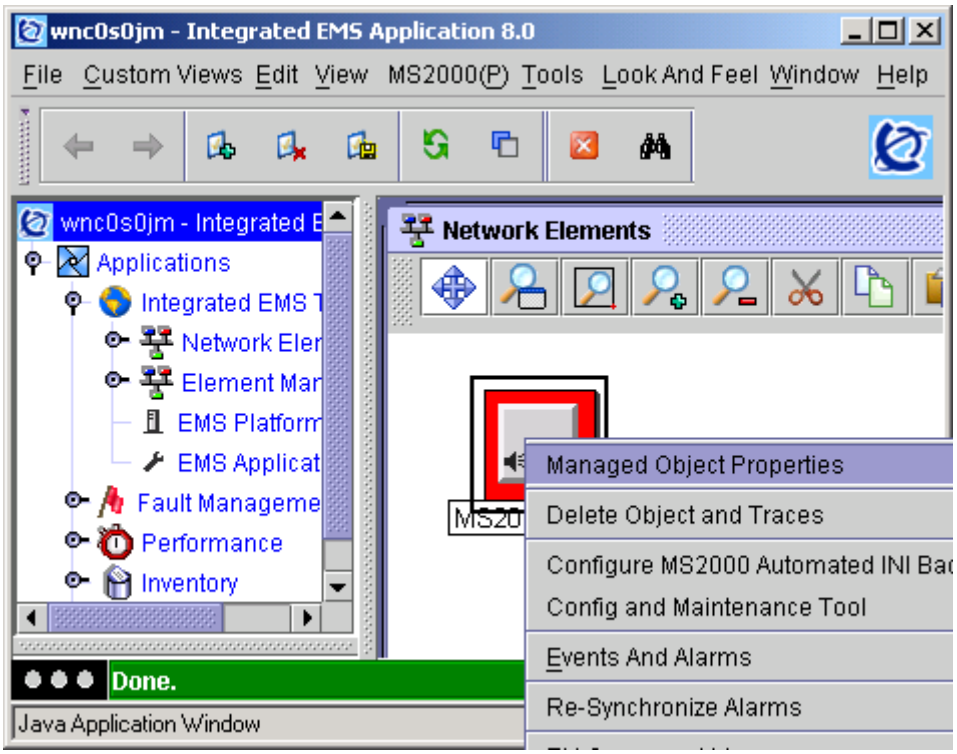
1 Once the IEMS is running on an SN08 load you can modify the properties of the existing Media Server 2000 node and change the settings of the web user name and password as well as the SNMP community strings if necessary.

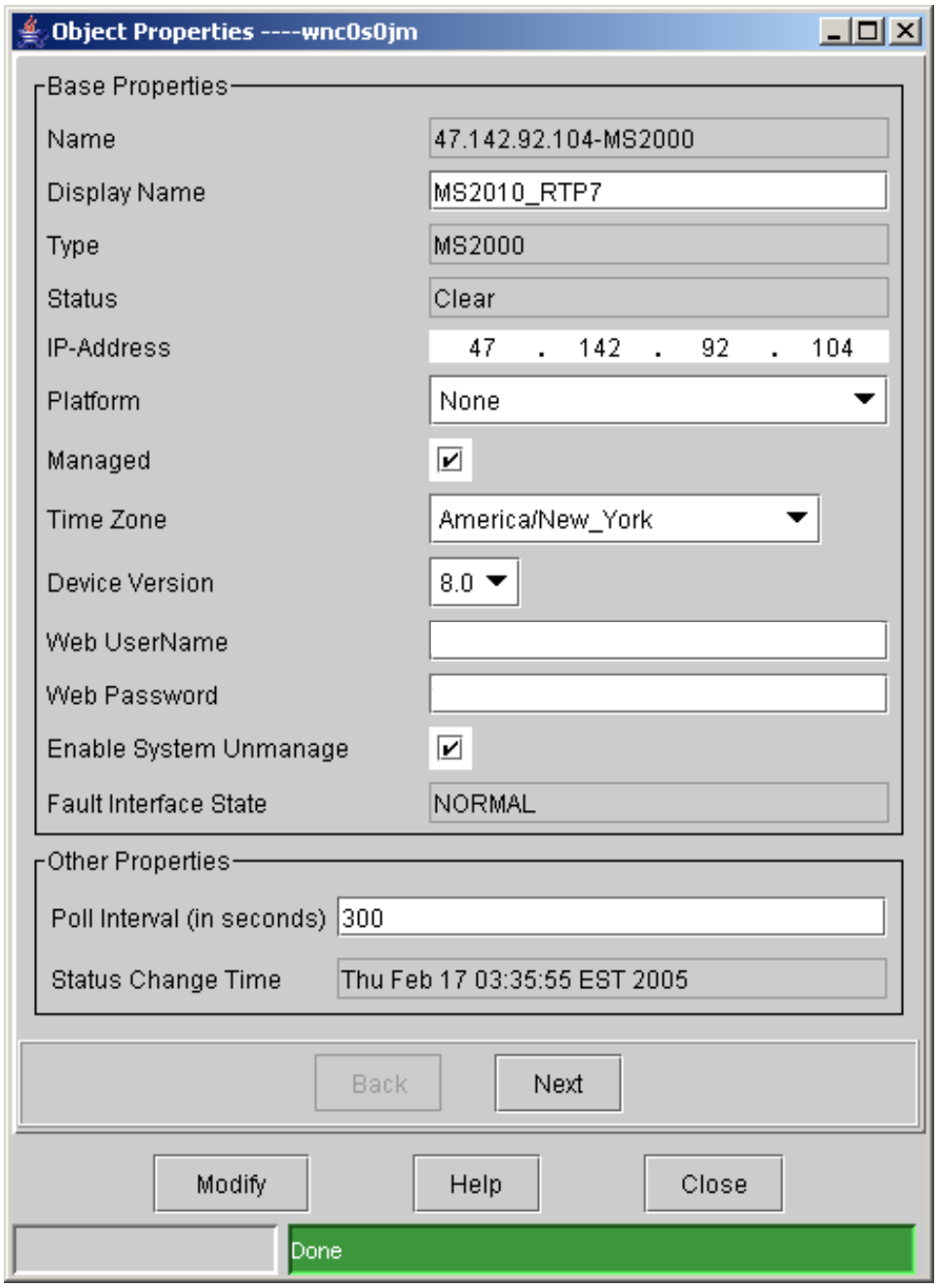
2 From the Media Server 2000 network element icon right-click on the node and select the “Managed Object Properties” menu item.

This brings up the “Object Properties” for this node. On the first panel there are entries for the webserver User and Password. After upgrading from SN07 these will be set to the default values for the node. Namely the web user and password will be set to “Admin”.

3 If the web server username or password was previously changed in an SN06.2 or SN07 release, they will need to be updated here to the correct values.

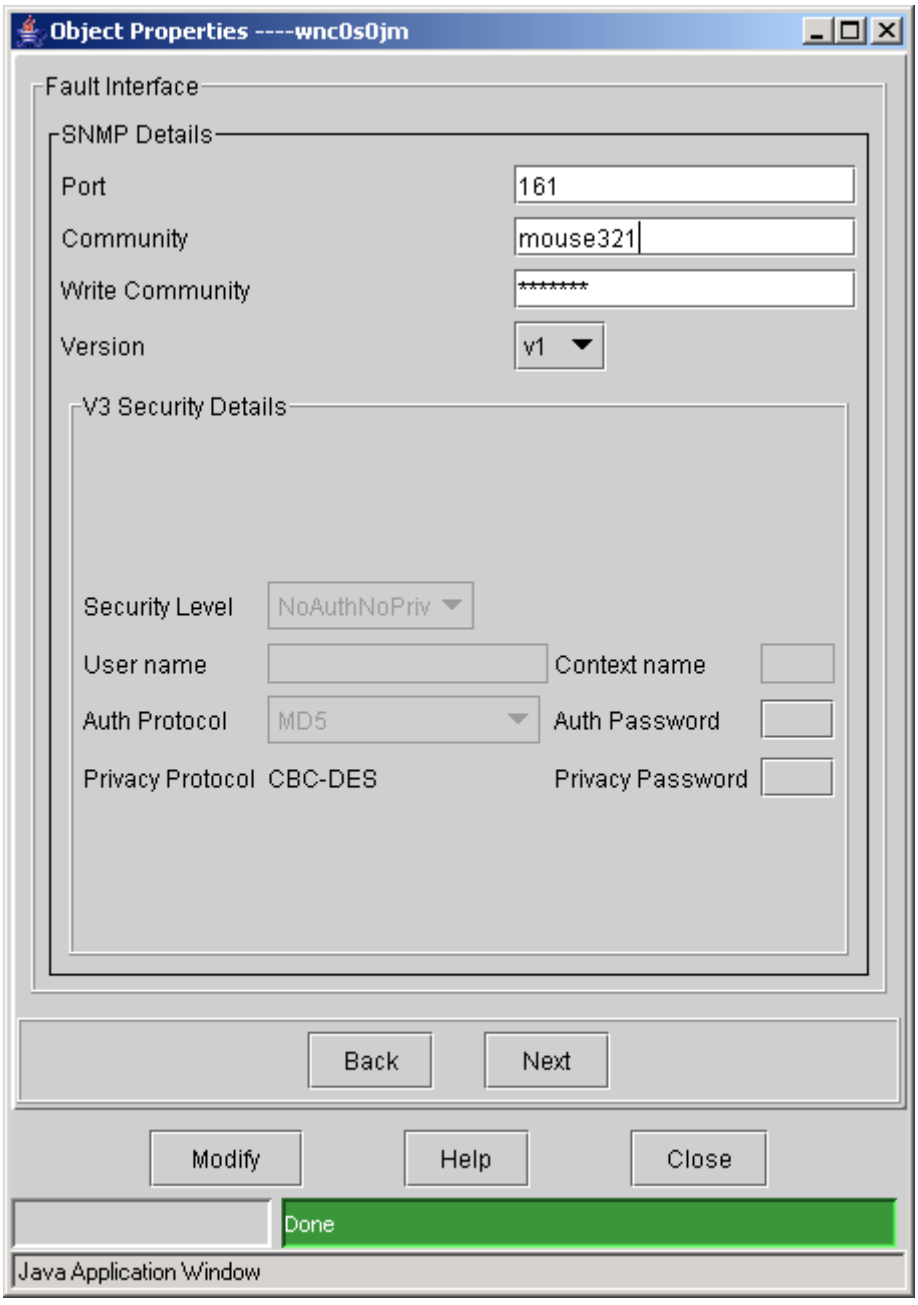
***Note:*** Failure to put the correct values here will cause the Maintenance and Configuration tool to fail when it attempts to perform file transfers to and from the node.






The object properties for the fault interface displays. Here the SNMP Read and Write Community Strings will be setup for the node. After an upgrade the node will be set with the default values.

4 If the SN07 node has previously had its community strings changed from the default values of read community “public” and write community of “private”, enter the new values.



***Note 1:*** If the community strings were changed by the Media Server 2000 CLUI in SN07, both the read and write community string will be the same value. These can be changed after this procedure is completed by using the Media Server 2000 Configuration and Maintenance tool from the Media Server 2000 device menu.

***Note 2:*** Failure to have the correct read community string for the node will prevent the Media Server 2000 Configuration and Maintenance tool from communicating with the node. When the tool is launched for this node a “Request Timeout” will occur while trying to retrieve the node information. If the write community string is not correct then the tool will fail whenever any configuration or maintenance activity attempts to change settings on the node. This will appear as a “Request Timeout” to the node.

## Procedure to upgrade a Media Server 2000

Before starting this procedure, review any documentation included with the software. The documentation included with the software may override or supplement the procedure described below.

For increased security, the CS 2000 Management Tool, and SDM logins, are equipped with login timeouts. If at any point the procedure the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

### *At the Windows desktop interface*

**1** Enter the following commands

```
cd /data/loads/ams
```

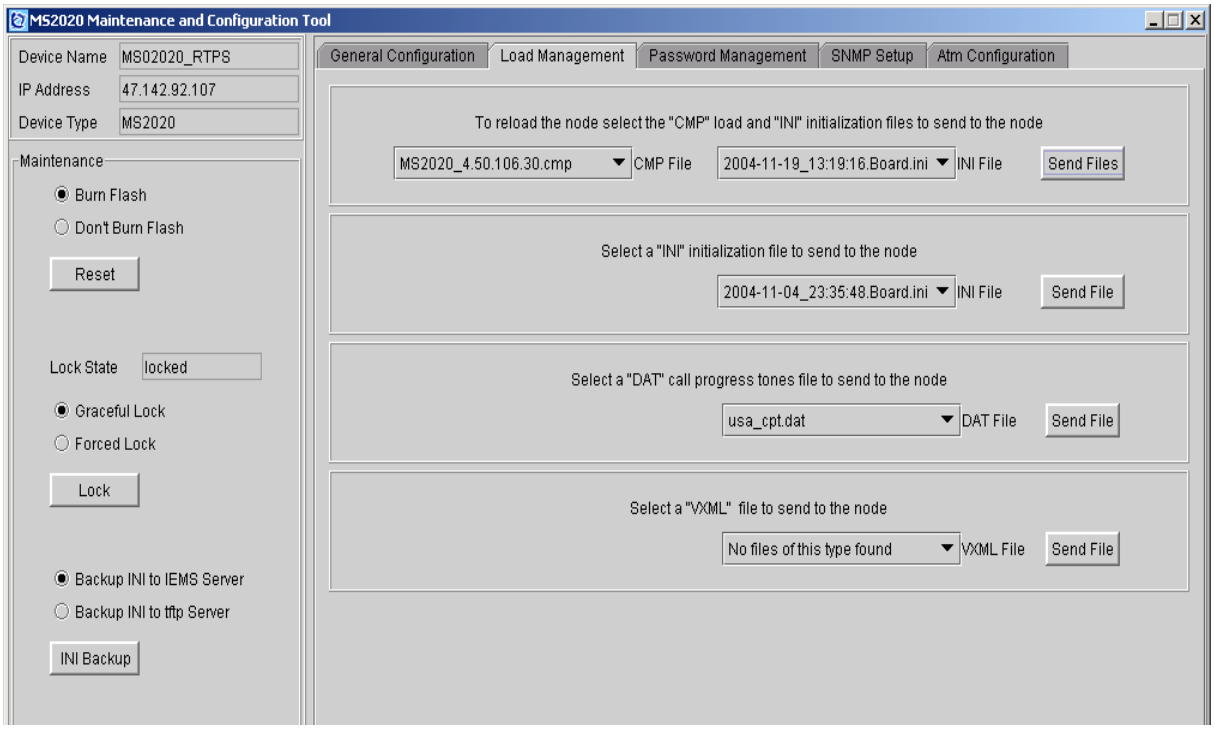
```
ls -ltr
```

Ensure that the files you copied are present in the directory. The newer files will appear near the bottom of the listing.

***Note:*** Make a note of the full path name of the .cmp file for use later in this procedure.

**2** From the IEMS client, launch the MS2000 Configuration and Maintenance GUI. Consult your system administrator for instructions about how to do access the GUI.

**3** Select the Media Server 2000 node to upgrade and then select the Load Management tab as shown in the following figure.




**4** On the left side of the window, choose the Graceful Lock or the Forced Lock radio button to lock the node. (You will actually initiate the lock in the next step.)

**CAUTION**

Performing a *Graceful Lock* on the node will take it out of service after any active calls have completed.

**CAUTION**

Performing a *Forced Lock* on the node will take it out of service immediately. Active calls will be dropped.

**5** Select *Lock* to lock the node.

**6** Select the *CMP* and *INI* files to upload from the pull down menus at the top of the Load Management page.

***Note 1:*** The *CMP* and *INI* files associated with the new software load must be installed on the Media Server 2000

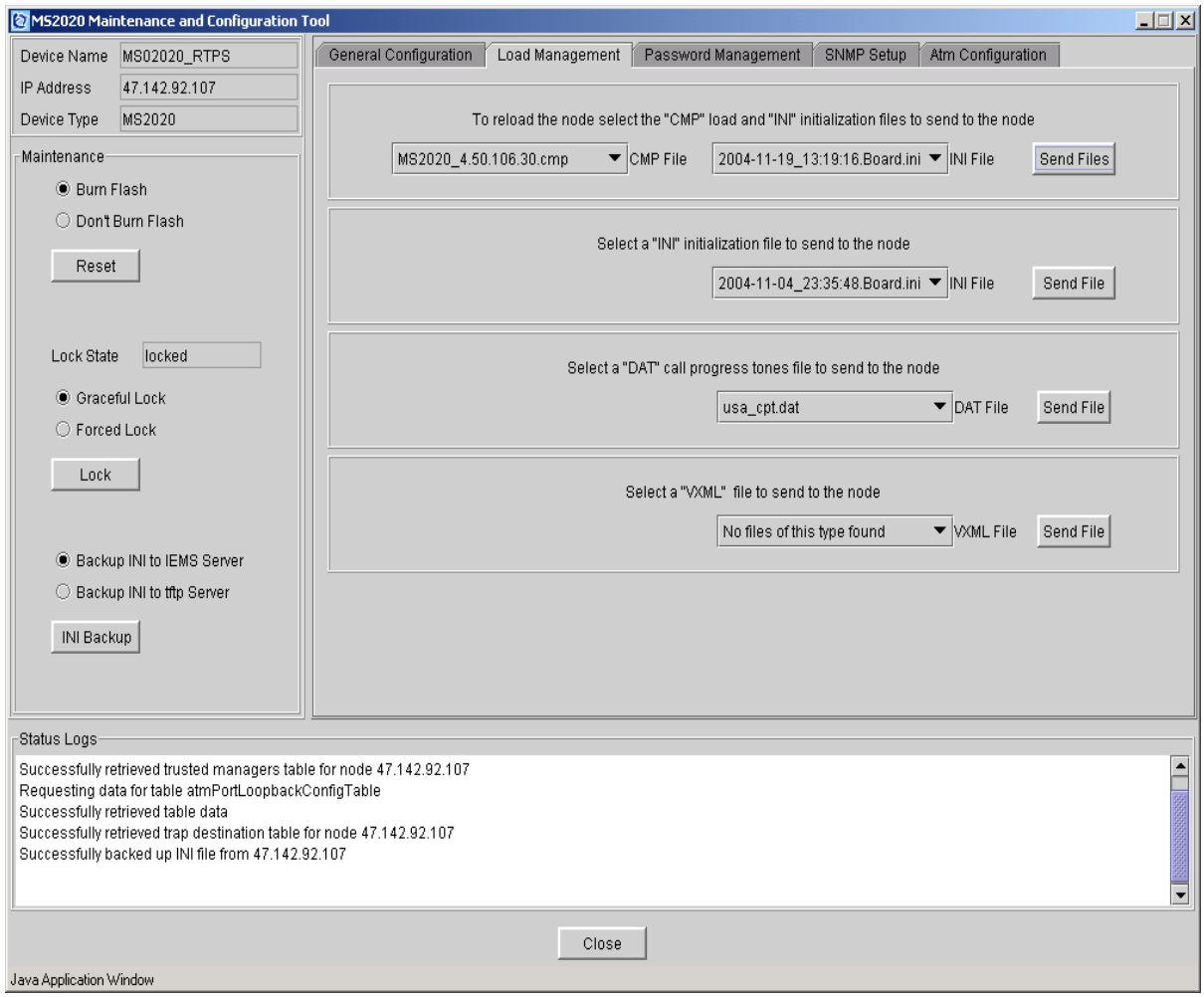
nodes. These are the files you copied in the Copying the files to the audiocodes directory section above.

***Note 2:*** If you upgraded the INI file in step 16 of the Copying the files to the audiocodes directory section above, you will see the upgraded file in the pull down list. Select this upgraded INI file to upload for the Media Server 2000 node.

**7** Select the *DAT* file to upload from the pull down menus in the middle of the Load Management page.

***Note:*** The *DAT* file is the .dat file you copied in the step 10 of the Backing up the Current load files section above.

**8** Select the *Send Files* button to start the upgrade (load the files to the node).



The status logs section at the bottom of the Load Management window displays the load that is being sent. Also, periodic updates display information on how long the burn process has been progressing.

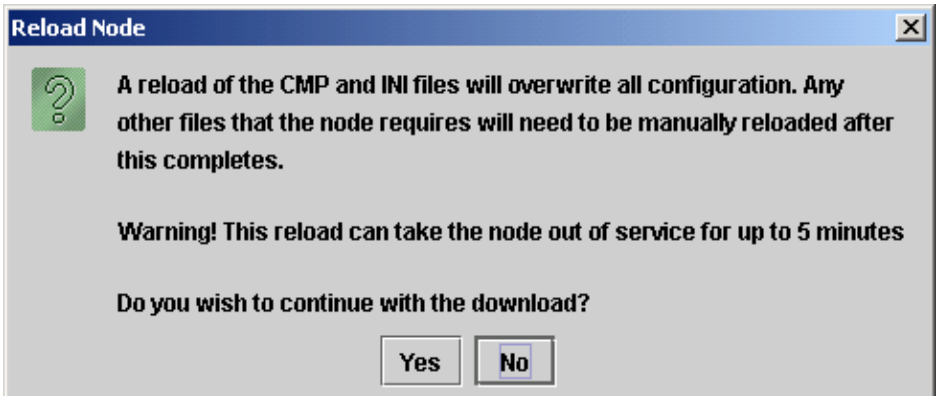
**Example**
Waiting for load to be burned into flash. Time from burn start is 2 minutes 1 secs

Waiting for load to be burned into flash. Time from burn start is 2 minutes 21 secs

Download of 2004-11-19_13:19:16.Board.ini starting.

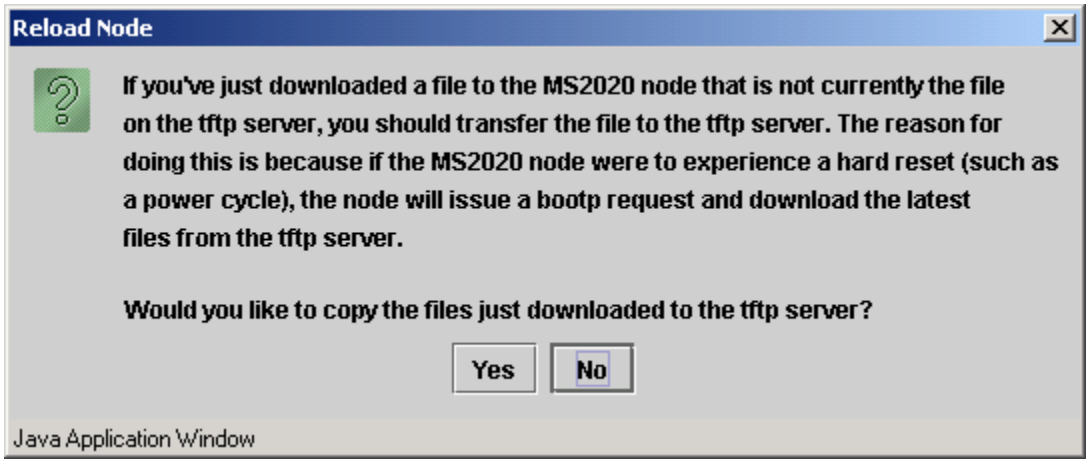
Download of 2004-11-19_13:19:16.Board.ini completed.

While executing the upgrade, the following message displays.



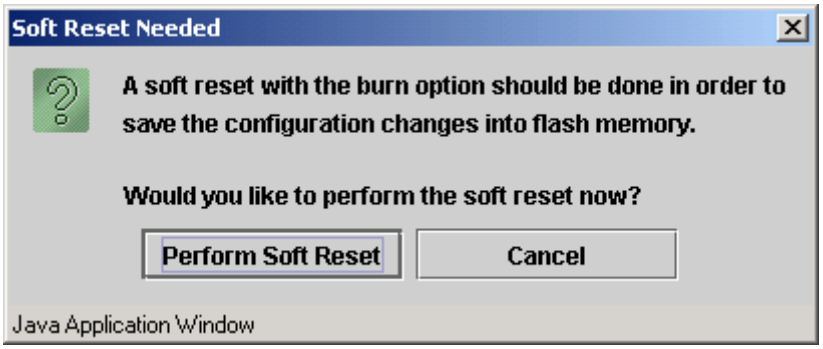

**9** Select *Yes* to proceed with the upgrade.

Once the loads have been sent the following screen displays prompting you to save the file to the tftp server if it is different than the file already there. Because this is an upgrade, the file you just loaded is not yet on the tftp server.



10 Select *Yes* to save the file to the tftp server.

11 After the upgrade completes, the following screen displays.




**CAUTION**

If you are upgrading a 240 port Media Server 2010, the hard reset will take both Media Servers out of service. Any active calls will be dropped! Make sure both Media Servers are locked before proceeding.

12 Select *Perform Soft Reset*.

13 On the left side of the Configuration and Maintenance GUI window, select *Unlock* to unlock the node.

14 To upgrade additional Media Server 2000 nodes, do the following:

**a** complete step 16d, step 17 and step 18 of Copying the files to the audiocodes directory on page 6

**b** complete Procedure to upgrade a Media Server 2000 on page 26

15 Edit the object properties in the IEMS for the MS2000 network element you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field.

- Editing and viewing object properties using Java Web Client
- Editing and viewing object properties using Web Client

16 You have completed this procedure.

# Editing and viewing object properties using Java Web Client

## Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

## Prerequisites

None

## Action

***At the IEMS workstation***

**1** Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *Integrated EMS Basics*, NN10329-111.

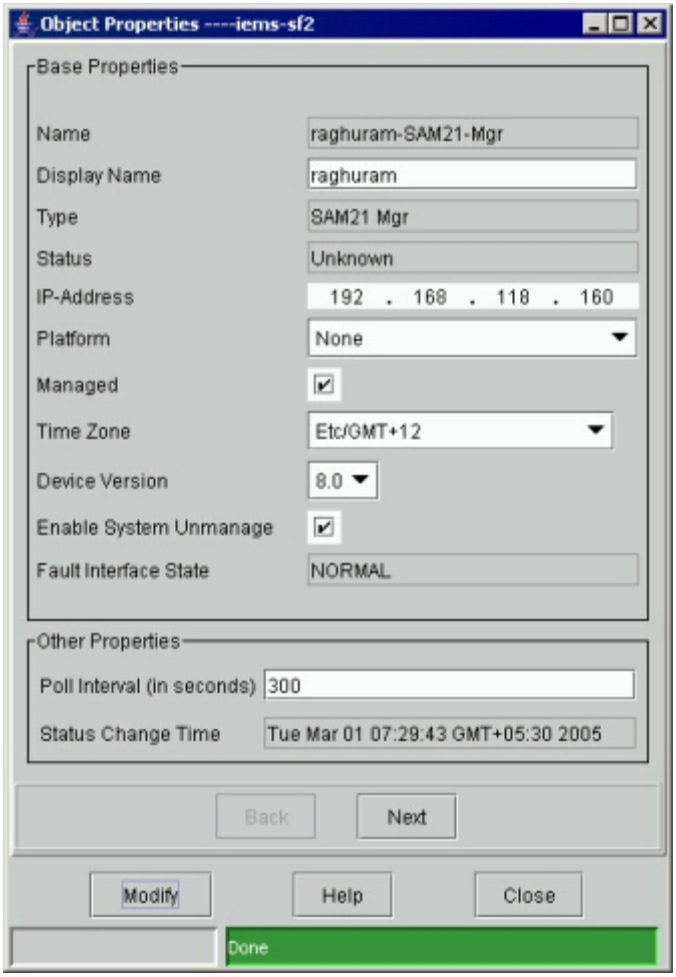
**2** Select the required object in the Integrated EMS Topologies tree under Applications.

***Note:*** The properties of an object from the Inventory panel of Integrated EMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree under Applications to open the Inventory view. Double-click the required row in the Inventory view.

**3** Right-click the map symbol and select the **Managed Object Properties** menu item or double-click the map symbol to open the Object Properties window.

***Note:*** The object properties displayed can differ for each component.

*A window similar to the following figure opens.*




**4** Modify the object properties listed in the table below if required.

**Managed object properties in Java Web Client**

| Field | Description |
|---|---|
| Name | Displays a unique name for the object |
| Display Name | Edit the name displayed in the topology for the object |
| Type | Displays the type of object (element manager, EMS, EMS platform or NE) |
| Status | Displays the status of the object |
| IP-Address | Edit the IP address of the object |

**Managed object properties in Java Web Client**

| Field | Description |
|---|---|
| Platform | Select the platform where the object resides from the drop-down list |
| Managed | Indicates whether the object is managed or unmanaged |
| Time Zone | Select the time zone of the geographical location where the object exists from the drop-down list |
| Device Version | Select the device version of the managed object from the drop-down list |
| Enable System Unmanage | Enable or disable the System_Unmanaged state. Refer to the System_Unmanaged state section of Configuring the Message Overload Controller parameters in *Integrated EMS Fault Management*, NN10334-911. |
| Poll Interval | Edit the Poll Interval for status updates |
| Status Change Time | Displays the last status change time of the object |
| ***Note:*** For the following objects, only the Display Name and the Managed field can be modified.<br>• SDM platform, APS EMS application, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Proxy, Media Gateway 7480/15000, MSS 15000 | |

**5** Select your next step.

| If | Do |
|---|---|
| you do not want to modify any other properties | go to step 6 |
| you want to view or modify the fault interface or performance interface properties | go to step 8 |

**6** Click the **Modify** button to update the changes.

**7** Go to step 16.

**8** Click the **Next** button to proceed to the Fault Interface window.

*A window similar to the following figure opens.*


**9** Edit or view the fault interface properties of the object as required.

***Note:*** The Details panel dynamically changes according to the fault interface of the EMS/NE.

**10** Select your next step.

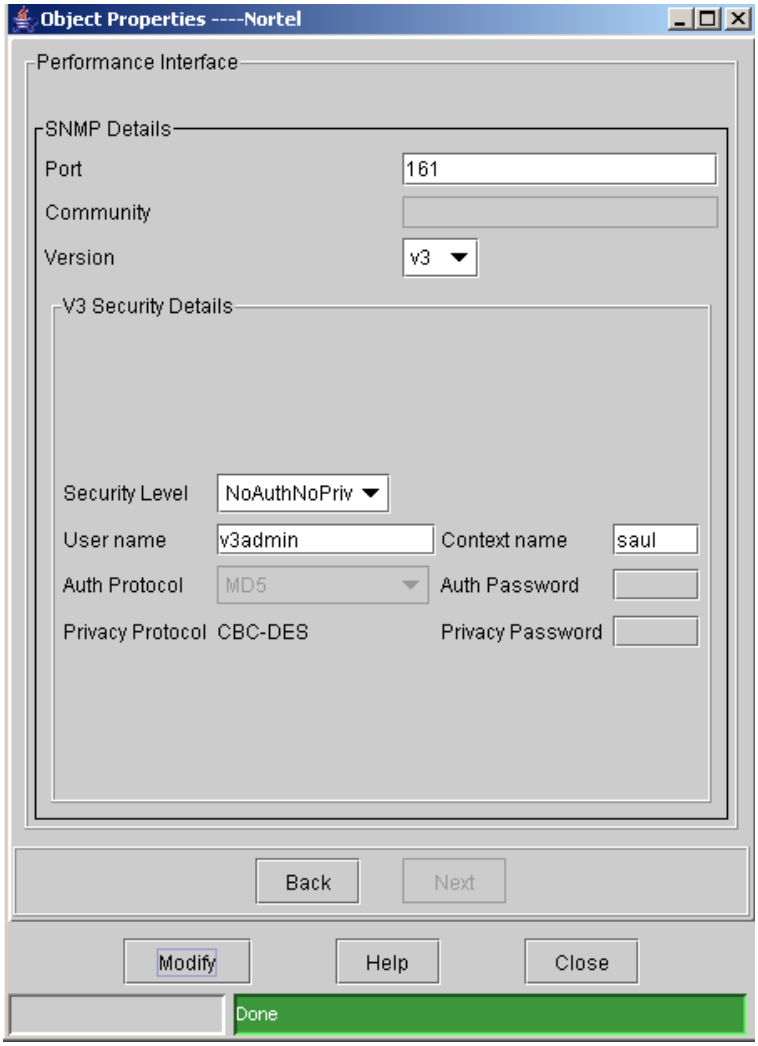
| If | Do |
|---|---|
| you do not want to modify any other properties | step 11 |
| you want to view or modify the performance interface properties | step 13 |

**11** Click the **Modify** button to update the changes.

12 Go to step 16.

13 Click the **Next** button to proceed to the Performance Interface window.

*A window similar to the following figure opens.*




14 Edit or view the performance interface properties of the object as required.

15 Click the **Modify** button to update the changes.

16 You have completed this procedure.

# Editing and viewing object properties using Web Client

## Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

## Prerequisites

None

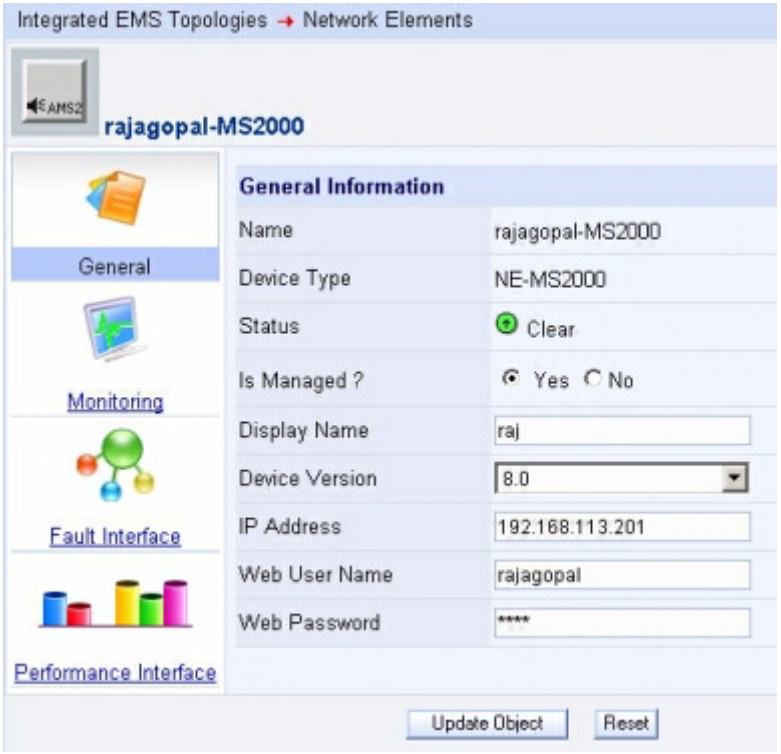
## Action

***At the IEMS workstation***

1. Launch the IEMS Web Client. Refer to Launching the IEMS Web Client in *IEMS Basics*, NN10329-111.
2. Select the **Integrated EMS Topologies** tab.
3. Navigate to the required topology node in the Integrated EMS Topologies tree.
4. Click the map symbol label to open the **General Information** window.

   ***Note:*** The object properties displayed can differ for each component.

   *A window similar to the following figure opens.*




**5** Select each vertical tab and modify the object properties listed in the table below if required.

**Managed object properties in Web Client**

| Field | Description |
|---|---|
| **General** | |
| Name | Displays the unique object name of the managed object |
| Device Type | Displays the type of object (element manager, EMS, EMS platform or NE) |
| Status | Displays the status of the object |
| Is Managed? | Indicates whether the object is managed or unmanaged |
| Display Name | Displays the name or label displayed in map symbol |
| Device Version | Select the version of the device from the drop-down list |

**Managed object properties in Web Client**

| Field | Description |
|---|---|
| IP Address | Modify the IP address of the object |
| Web User name | Enter your web user name |
| Web Password | Enter your web password |
| **Monitoring** | |
| Last Status Update Time | Displays the time when the status of the managed object last changed |
| Last Status Change Time | Displays the time when the status of the managed object last changed |
| Status Polling Interval (secs) | Modify the Poll Interval for status updates |

**Managed object properties in Web Client**

| Field | Description |
|---|---|
| **Fault Interface** | |
| If the details are present for the selected object, the details can be modified. | |
| **Performance Interface** | |
| If the details are present for the selected object, the details can be modified. | |

6 Click the **Update Object** button to update the changes.

7 You have completed this procedure.

# Downgrading a Media Server 2000 node

This procedure enables you to downgrade a Media Server 2000 node to a previous release.

## Office impact

In this procedure each Media Server 2000 node in the network is to be downgraded one at a time

**CAUTION**

During the downgrade procedure, you will perform a hard reset on the Media Server. If you downgrade a 240 port Media Server 2010, the hard reset will take both Media Servers out of service. Any active calls will be dropped!

## Material requirements

This is a software-only procedure and doesn't require special tools. The following files are provided either on compact disc or through electronic software distribution (ESD):

- CMP file (software executable load)
- INI file (configuration file)
- DAT files containing specific information (such as Conference tones, and information to deliver test trunk functionality)

The client workstation must be running the following programs:

- Microsoft Windows 98, NT, 2000, XP, or 2003
- Netscape 6, or higher, or Microsoft Internet Explorer (IE) 6.0, or higher

## Backing up the Current load files

Before starting this procedure, review any documentation included with the software. The documentation included with the software may override or supplement the procedure described below.

For increased security, the CS 2000 Management Tool, and SDM logins, are equipped with login timeouts. If at any point in the procedure the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

***At the Windows desktop interface***

1 Open a DOS window and enter the following three commands:

```
ping <IP address of router>
ping <IP address of CS 2000 Management Tool>
ping <IP address of SDM>
```

If a response displays for all three commands, continue with the next step. If a response does not display for any one of the three commands, check connections and configuration of the network settings for the PC (or laptop). Do not continue with the procedure below until the ping commands all indicate successful connections.

## Downgrading a Media Server 2000 node

Before starting this procedure, review any documentation included with the software. The documentation included with the software may override or supplement the procedure described below.

For increased security, the CS 2000 Management Tool, and SDM logins, are equipped with login timeouts. If at any point the procedure the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

### Loss of communication with the node

***If you lose communication with the node but the node is still in service, there are two possible causes.***

1 The node has a trusted manager defined and the machine you are attempting to access the node from is not in the trusted manager list.

*Or*

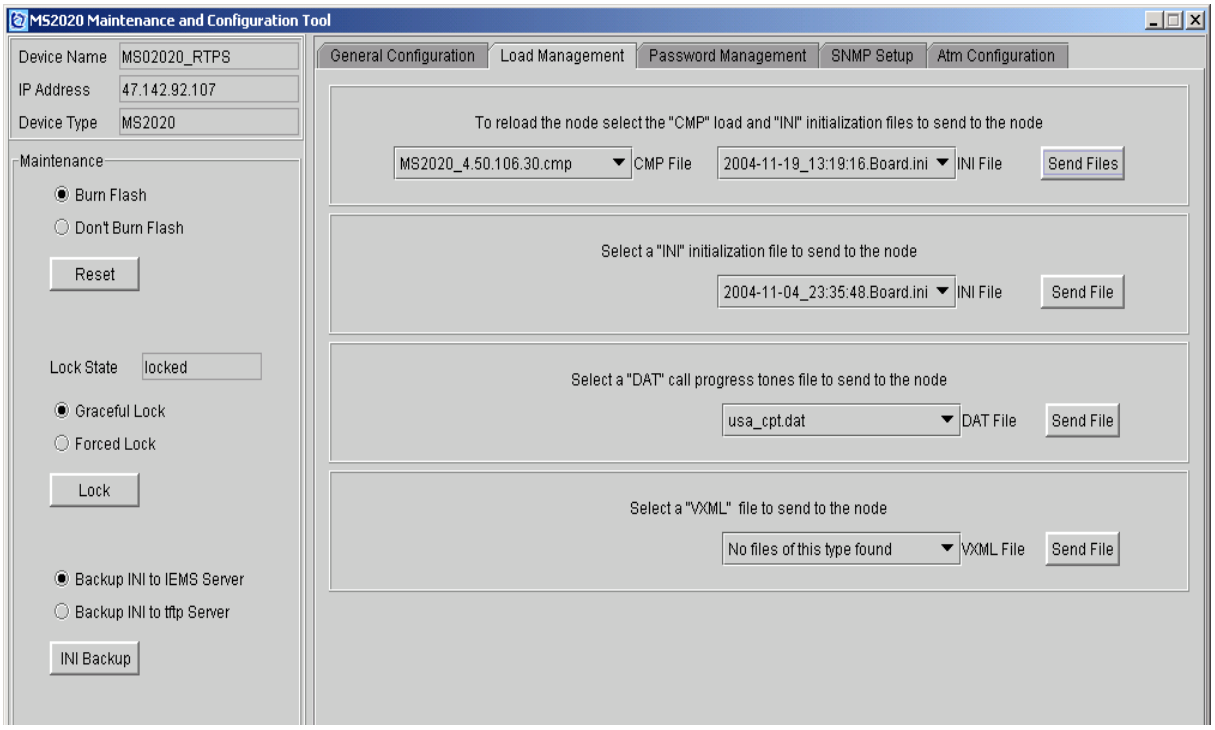
2 There is a SNMP community string mismatch.

In either case, the node will have to reloaded by accessing the web interface of the node and performing a backup of the INI file. The file then needs to be edited correcting the trusted managers and/or SNMP community strings. Remember, whatever the community strings are set to in the INI file must be what the Media Server 2000 CLUI or the IEMS Media Server 2000 Maintenance and Configuration Tool uses.

### *At the Windows desktop interface*

1 Log in to the CS 2000 Management Tools GUI. Consult your system administrator for instructions about how to do access the GUI.

2 Select the Media Server 2000 node to downgrade and then select the Load Management tab as shown in the following figure.




3 On the left side of the window, choose the Graceful Lock or the Forced Lock radio button to lock the node. (You will actually initiate the lock in the next step.)

**CAUTION**

Performing a *Graceful Lock* on the node will take it out of service after any active calls have completed.

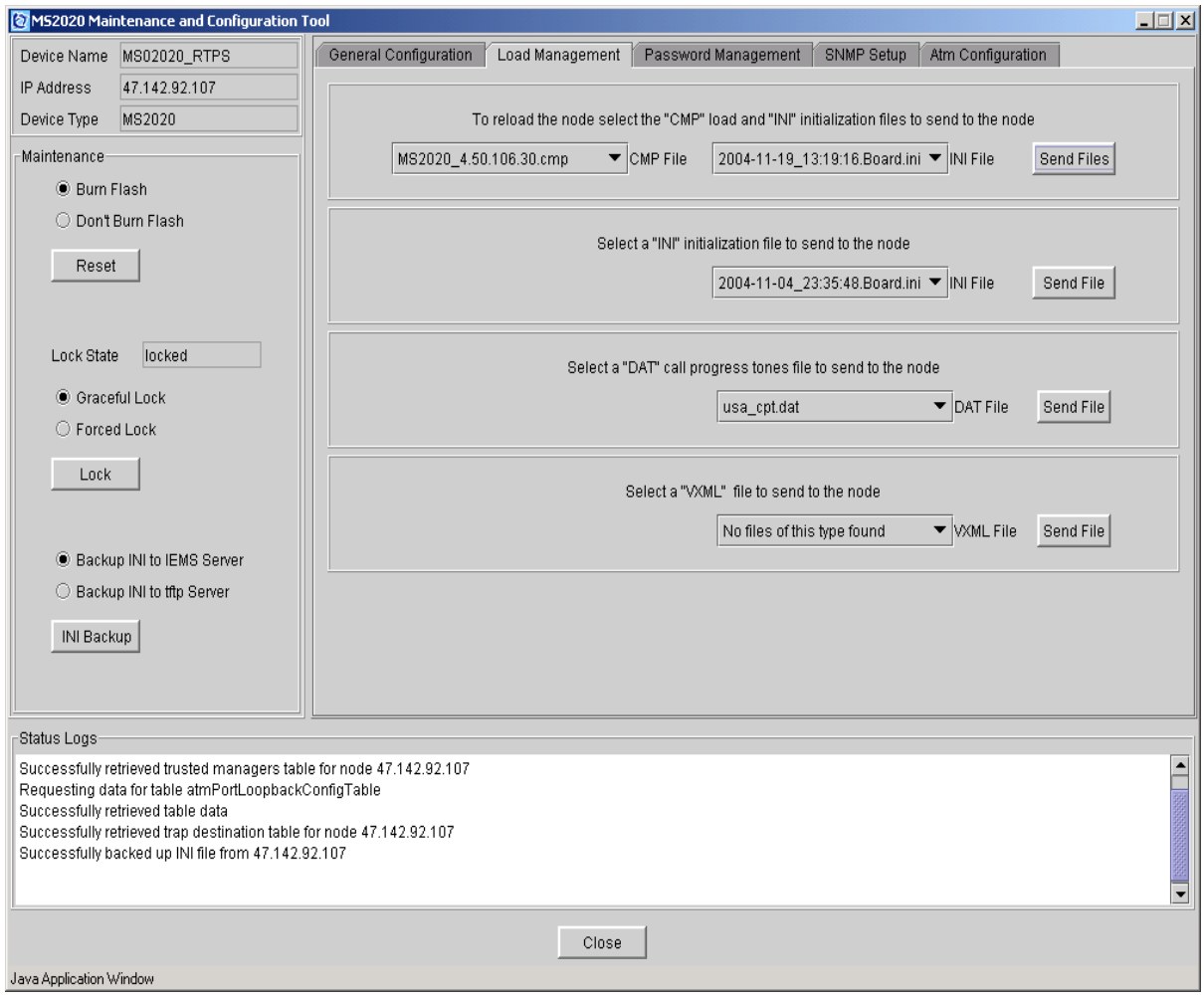
**CAUTION**

Performing a *Forced Lock* on the node will take it out of service immediately. Active calls will be dropped.

4 Select *Lock* to lock the node.

5 Select the *CMP* and *INI* files to upload from the pull down menus at the top of the Load Management page.

6 Select the *Send Files* button to start the downgrade (load the files to the node).



The status logs section at the bottom of the Load Management window displays the load that is being sent. Also, periodic updates display information on how long the burn process has been progressing.

**Example**

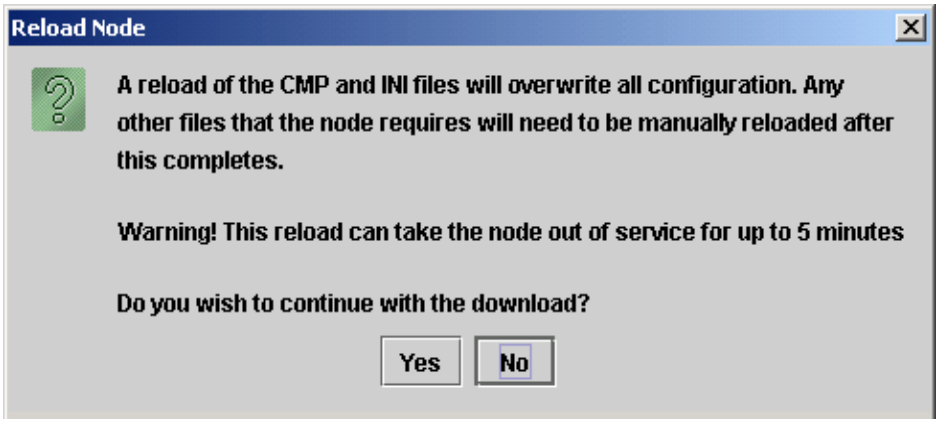
Waiting for load to be burned into flash. Time from burn start is 2 minutes 1 secs

Waiting for load to be burned into flash. Time from burn start is 2 minutes 21 secs

Download of 2004-11-19_13:19:16.Board.ini starting.

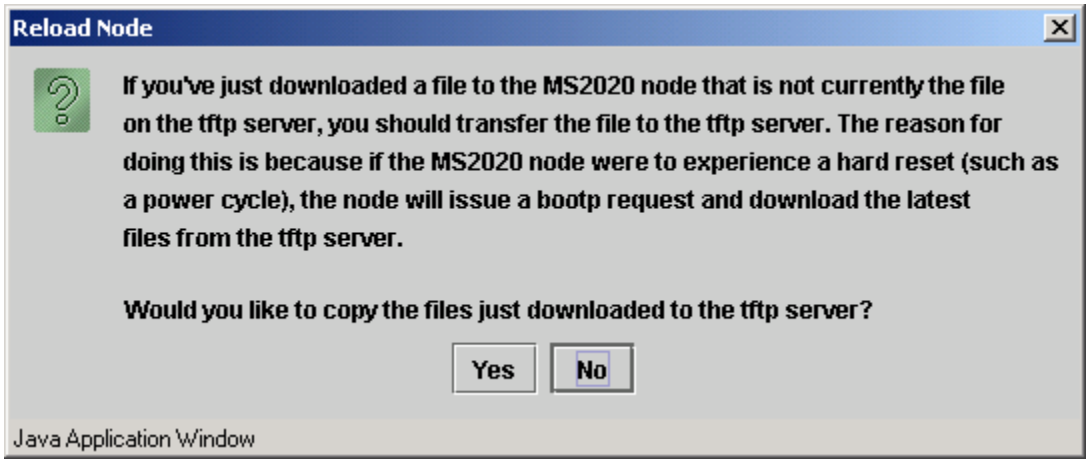
Download of 2004-11-19_13:19:16.Board.ini completed.

While executing the downgrade, the following message displays.



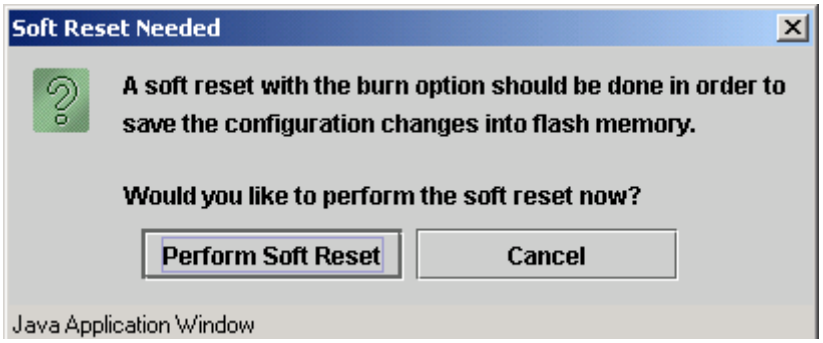

7 Select *Yes* to proceed with the downgrade.

Once the loads have been sent the following screen displays prompting you to save the file to the tftp server if it is different than the file already there.



8 Select *Yes* to save the file to the tftp server.

9 After the downgrade completes, the following screen displays.




**CAUTION**

If you are downgrading a 240 port Media Server 2010, the hard reset will take both Media Servers out of service. Any active calls will be dropped! Make sure both Media Servers are locked before proceeding.

10 Select *Perform Soft Reset* to completed this procedure.

11 Perform this procedure for additional Media Server 2000 nodes you are downgrading.

12 You have completed this procedure.