Media Server 2000 Series Security and Administration

This NTP contains security and administration procedures for the Nortel Media Server 2000 Series and the Audio Provisioning Server (APS). These procedures are listed in tables shown below.

Media Server 2000 Series security and administration

The primary Media Server 2000 Series security and administration activities include changing the password for accessing the embedded web server utility and backing up the configuration files. These tasks, performed through the Media Server 2000 Series Configuration Tool and Embedded Web Server utility, are in the Media Server 2000 Series Configuration Management document (NN10340-511). This NTP does, however, include a procedure for Enabling HTTPS on Media Server 2000 devices.

APS security and administration

APS security and administration tasks include changing passwords for accessing the APS GUI and monitoring the APS provisioning database.

Security management procedures

The following table lists user-related security and administration procedures that pertain to the APS.

APS user-related security and administration procedures (Sheet 1 of 2)

Procedure and page	Interface/ Tool used
Obtaining an APS Client Certificate	APS CLI
Adding an APS to the Integrated EMS	Integrated EMS GUI
Logging in to the APS GUI	APS GUI

APS user-related security and administration procedures (Sheet 2 of 2)

Procedure and page	Interface/ Tool used
Logging out of the APS GUI	APS GUI
Changing the PMGRdaemon password	Desktop interface

The following table lists device-related security and administration procedures that pertain to the APS.

APS device-related security and administration procedures (Sheet 1 of 2)

Procedure and page	Interface/ Tool used
Listing APS patches and release information	APS GUI
Downloading the Java runtime environment plug-in	APS GUI
Running the APS command line interface	APS CLI
Displaying APS mounted file systems	Command line
Changing the APS IP/Hostname configuration	Command line
Monitoring nightly cleanup	Command line
Monitoring audio provisioning activity	Command line
Checking APS provisioning activity	Command line
Checking the APS Oracle database	Command line
Verifying that the APS CD drive is mounted	Command line
Set APS security	Command line
Setting the APS administrator (UNIX) password	Command line
Restarting the SNMP agent	Command line
Verifying that the Web server is running	Command line
Verifying that the Web server is running	Command line
Changing the APS Oracle account password	Command line
Performing a backup of APS audio files into a single tar archive (FTP)	Command line

APS device-related security and administration procedures (Sheet 2 of 2)

Procedure and page	Interface/ Tool used
Performing an APS-only Data Base Backup to Disk and to CD	Command line
Performing an APS-only Data Base Backup to 4mm DAT	Command line
Performing an APS-only Data Base Restore from a 4mm DAT	Command line
Performing an APS-only Database restore from a CD	Command line
Performing a restore of APS audio from 4mm DAT	Command line
Performing a restore of APS audio files from a TAR file	Command line

Enabling HTTPS on Media Server 2000 devices

The embedded web server on the Media Server 2000 can be secured using SSL (Secure Socket Layer). The SSL protocol provides confidentiality, integrity and authenticity of the web server.

Specifications for the SSL/TLS implementation are listed below.

- Supported transports: SSL 2.0, SSL 3.0, TLS 1.0
- Supported ciphers: DES, RC4 compatible
- Authentication: X.509 certificates

Considerations/Dependencies:

Enabling HTTPS on the Media Server 2000 requires Network Time Protocol (NTP) setup and configuration on a Media Server 2000 node. The node must be configured to use NTP to obtain the current date and time only if client certificates are used. Without a correct date and time, client certificates cannot work.

Enabling HTTPS on the Media Server 2000 also requires that the APS be enabled for HTTPS operation so audio distribution can occur using HTTPS. For example, if the Media Server 2000 is configured to only allow HTTPS, then the APS must be configured to use HTTPS for audio provisioning. The APS uses HTTP and/or HTTPS as a client to the Media Server 2000.

Any external management tool which accesses the Media Server 2000 device using HTTP may need to be configured to use HTTPS to the Media Server 2000.

There is an INI file parameter, “HTTPSOnly”, which controls whether “HTTPS only” operation is to be used on the media server. The possible values are 0 or 1, with the default of 0. If this parameter is set to 0, the Media Server 2000 communicates with the clients using either HTTP or HTTPS. If set to 1, the Media Server 2000 communicates with the clients using HTTPS only.

Media Server Security Certificates

Media Server 2000 devices are shipped with a working SSL configuration, consisting of a unique self-signed server certificate. When an Media Server 2000 device is upgraded to firmware version 4.6, a unique self-signed server certificate is created. If an organizational PKI (public key infrastructure) is in place, you may wish to replace this certificate with one provided by your security administrator.

If you plan to use the APS to provision announcements using HTTPS, replace the certificate with a custom company supplied certificate.

A Certificate Authority (CA) certificate can be generated by a number of third party companies. Contact your security administrator for CA certificates generated for your company.

ATTENTION
The information below applies only if you choose to use the domain name as the subject name to generate the server certificate signing request.

Your network administrator should allocate a unique DNS name for the Media Server 2000 (for example, dns_name.corp.customer.com); this name is used to access the device, and needs to be listed in the server certificate.

As an alternative, the serial number of the Media Server 2000 server can be used for the subject name to generate the server certificate signing request.

1 Login to the Media Server 2000 embedded web server

2 Select the “STATUS and DIAGNOSTICS” option from the left panel of the Media Server 2000 web server page.

The “Device Information” heading displays.

3 Select “Device Information”.

4 Locate the Serial number of the device under the “General” heading and record it.

Example

General configuration parameters

Device Information	
General	
MAC Address	00908f042eba
Serial Number	123456

5 Open a web browser to the following URL (case-sensitive) for a media server.

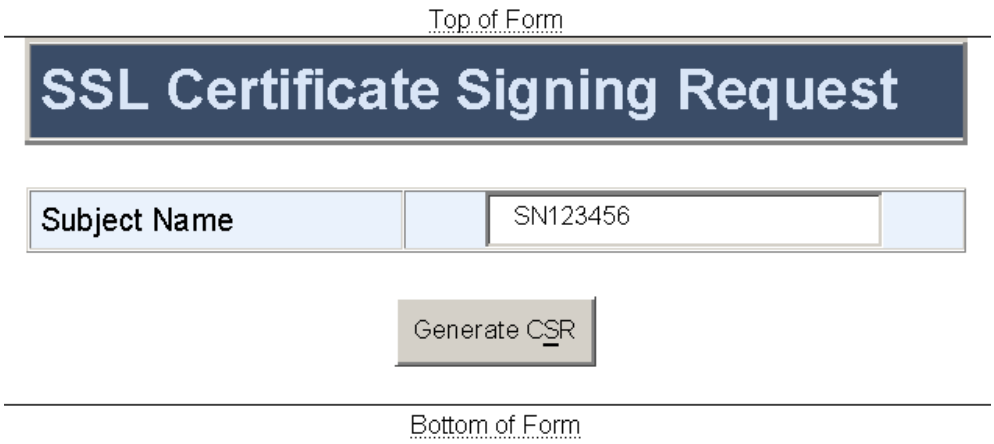
`https://dns_name.corp.customer.com/SSLCertificateSR`

If this link does not work, try the following link.

`http://dns_name.corp.customer.com/SSLCertificateSR`

6 Enter the subject name (for example, SN<serial-number>, IP address, or domain name).

Example



7 Copy the certificate signing request, and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBUjCBvAIBADATMREwDwYDVQQDEwhTTjI3NDEwNjCBnzANBgk
qhkiG9w0BAQEFAAOBjQAwgYkCgYEAufcqYpdohmc5N22cX/o5Tv
XsCpLzBijsbqErdSeJoNkC2+9jSKt/Cd3xZTHxBqBpZ/as+GE5I
+talwnC2kzGOVZLLHGg5I9XhCy4mhnkYxYMdxQSmCscOq9hnZek
i/Sx4UODi20qWA8YqessdqgQW734VccbJyGBDD2B6FcInZUCAwE
AAaAAMA0GCSqGSIb3DQEBBAUAA4GBAGiqCtn4I4mvG4dMNAkWXe
1O6nIn9uGAYCRT4kS8whvmMWzeY86XaH9VHyWUSeE7eql8rqwZ1
/Jx+9NL7tioZ5AdDUDcdrzCZ+HwZt3eaUyX65bx8ycgh/9DVq1W
da4oSF8EdO4MYw5aMLz5qvYuHd+xxRIE3TmnCB4kAoeCfhMH
-----END CERTIFICATE REQUEST-----
```

8 The web page displays a textual certificate signing request, containing the SSL device identifier. Copy this text and send it to your security provider.

9 Save the certificate in a file (for example, cert.txt). Make sure the file is plain-text with the "BEGIN CERTIFICATE" header.

Below is an example of a base64-encoded X.509 certificate.

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJG
UjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBTZXJ2
ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMC
RlIxEzARBgNVBAoTCkNlcnRpG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2Vy
dmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGR
x8bQrhZkonWnNm+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qI
JcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lR
efiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDlUP1F1jMa+LPwv
REXfFcUW+w==
-----END CERTIFICATE-----
```

Troubleshooting: If the link above does not work, set HTTPSONLY=0 in the Media Server 2000 device INI file. This gives you a method of accessing the device in case the new certificate is not working. Restore the previous setting after testing the configuration.

In the SSLCertificateSR web page, locate the server certificate upload section. Click "Browse" and locate the cert.txt file, then click "Send File". When the operation is complete, save the configuration and restart the device; the web server now uses the provided certificate.

Note 1: The certificate replacement process may be repeated as necessary, for example, when the new certificate expires.

Note 2: It is possible to set the subject name to the IP address of the device (e.g. “10.3.3.1”) instead of a qualified DNS name.

10 Create a file with the certification signing request from the previous step. The file can have a filename of “cert.txt”.

11 Send the file to your local security administrator or certificate authority to generate a signed server certificate. This procedure is not provided in this document since there are a number of tools current in the marketplace used to perform this function and local company practices for generating security certificates may differ.

Note: In the next step a custom certificate from a certificate authority has been obtained. If you do not have a certificate from a CA, do not continue past this step. The CA will give you a CA cert and a signed server certificate.

12 Access the device again using to following URL.

`https://dns_name.corp.customer.com/SSLCertificateSR`

13 Under the "SSL Files" Panel, press the "SSL Trusted Root Certificate Store" Browse button.

14 Select the file with the certificate for the certificate authority in steps 9 and 10 above.

15 Press the SendFile button. This loads the server certificate.

16 Save the configuration and perform a soft reset of the Media Server 2000.

Note: The following step is needed only if a client certificate is used.

17 Enable NTP (network time protocol) on the Media Server 2000 node. This is accomplished by adding a line to the Media Server 2000 configuration INI file.

18 Pull the existing configuration INI file from the Media Server 2000.

19 Add the following line to the INI file.

```
NTPServerIP= <IP_address_of_NTP_server>
```

20 Reload the INI file onto the Media Server 2000.

21 Perform a software reset on the Media Server 2000 to activate the change.

22 If announcements are used on the Media Server 2000 and there is an APS in the network, perform the procedure Obtaining an APS Client Certificate.

23 You have completed this procedure.

Obtaining an APS Client Certificate

By default, web servers using Secure Socket Layer (SSL) provide one-way authentication, the client is certain that the information provided by the web server is authentic. When an organizational PKI is in place, two-way authentication may be desired, both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the management PC, and uploading the same certificate (in base64-encoded X.509 format) to the Media Server 2000 device's Trusted Root Certificate Store. The Trusted Root Certificate file should contain both the certificate of the authorized user, and the certificate of the CA.

Since X.509 certificates have an expiration date and time, the Media Server 2000 must be configured to use Network Time Protocol (NTP) to obtain the current date and time. Without a correct date and time, client certificates cannot work.

To upload the Trusted Root Certificate file

1 Open a web browser to the following URL (case-sensitive) for a media server.

`https://dns_name.corp.customer.com/SSLCertificateSR`

2 Locate the trusted root certificate upload section.

3 Click "Browse" to locate the Trusted Root Certificate file, then click "Send File".

4 When the operation is complete, set the ini file parameter HTTPSRequireClientCertificates=1.

5 Save the configuration and restart the device.

When a user connects to the secure web server:

- If the user has a client certificate from a CA listed in the Trusted Root Certificate file, the connection is accepted and the user is prompted for the system password.
- If both the CA certificate and the client certificate appear in the Trusted Root Certificate file, the user is not prompted for a password. (This provides a single-sign-on experience. The authentication is performed using the X.509 digital signature.)
- If the user does not have a client certificate from a listed CA, the connection is rejected.

Note: Installing a client certificate for your web browser or the APS, is beyond the scope of this document. For more

information, refer to your web browser or operating system documentation, and consult your security administrator.

Because the APS uses HTTP and/or HTTPS to communicate to the Media Server 2000, then a client certificate can be used on the APS.

The Client Certificate is created by a Certificate Authority. Contact your security administer for client side certificates created and used by your company.

Configuring HTTPS on the APS devices

This procedure enables the APS to communicate to the Media Server 2000 device in the network more securely using HTTPS. To enable HTTPS on the Media Server 2000 servers, refer to the *Enabling HTTPS on Media Server 2000 devices* in the *Media Server 2000 Series Security and Administration (NN10337-611*) document.

Create the CA certificate

1. Log in to the APS server as the root user.
2. Access the server via telnet.
3. Become the root user by entering the following command.

   # su - root
4. Launch the apscli tool by entering the following command.

   # apscli

   The APS Command Line Interface *MAIN MENU* displays.

```
APS Command Line Interface MAIN MENU
 1) Database Queries, Reports, Status, Checks
 2) Audio Provisioner Actions
 3) Restart APS Server Processes
 4) Software Listing and Inventory
 5) APS Database and Application File Backups,
    Restores
 6) APS SNMP Agent, configure, start, stop.
 7) LOG files, Accessing and Viewing
 8) View, access UAS node(s) conf file(s) backup
    directory
 9) Determine if APS Server Processes are running.
10) Audits and aps checking utilities.
```

```
11) Configure Audio Distribution HTTP/HTTPS
X) Exit

Enter a number or (X)
```

5 Enter 11 to select Configure Audio Distribution HTTP/HTTPS. The following menu displays.

```
1) Display Existing Configuration
2) Use Only HTTP
3) Use Only HTTPS
4) Use HTTPS If possible (Uses HTTP if HTTPS fails)
5) Configure CA Certificate
6) Configure Client Certificate
7) Set Client Certificate Pass Phrase
8) Validate Configuration
X) Exit
Enter a number
```

6 Enter 1 to display the current configuration. A sample output display is shown below.

```
Upload Protocol:        1 (HTTP)
CA Certificate:         none
Client Certificate:     none
Client Certificate Pass Phrase:          none
Enter return to continue:
```

7 Press return to continue and return to the menu options.

8 Select option 3 or 4 to designate HTTPS.

IMPORTANT
Use Option 4 if there are both SN07 (4.4) and SN08 (4.6) Media Server 2000 devices in your network. SN07 devices do not support HTTPS. APS will use HTTP for SN07 devices and HTTPs for SN08 devices.

The following menu displays.

```
1) Display Existing Configuration
2) Use Only HTTP
3) Use Only HTTPS
4) Use HTTPS If possible (Uses HTTP if HTTPS fails)
5) Configure CA Certificate
6) Configure Client Certificate
7) Set Client Certificate Pass Phrase
8) Validate Configuration
X) Exit
Enter a number
```

9 Enter menu option 5 to Configure a CA certificate.

10 Enter the path to the CA certificate.

11

If	Do
you are configuring a client certificate	step 12
you are not configuring a client certificate	step 13

12 Enter 6 to configure a client certificate and a pass phrase.

a If you are using client certificates, enter the path to the client certificate.

b If you are using client certificates, enter the client pass phrase (required).

13 Select menu option “8” to validate the configuration.

14 Press x to exit to the main “apscli” menu and restart the APS server processes.

15 You have completed this procedure.

Adding an APS to the Integrated EMS

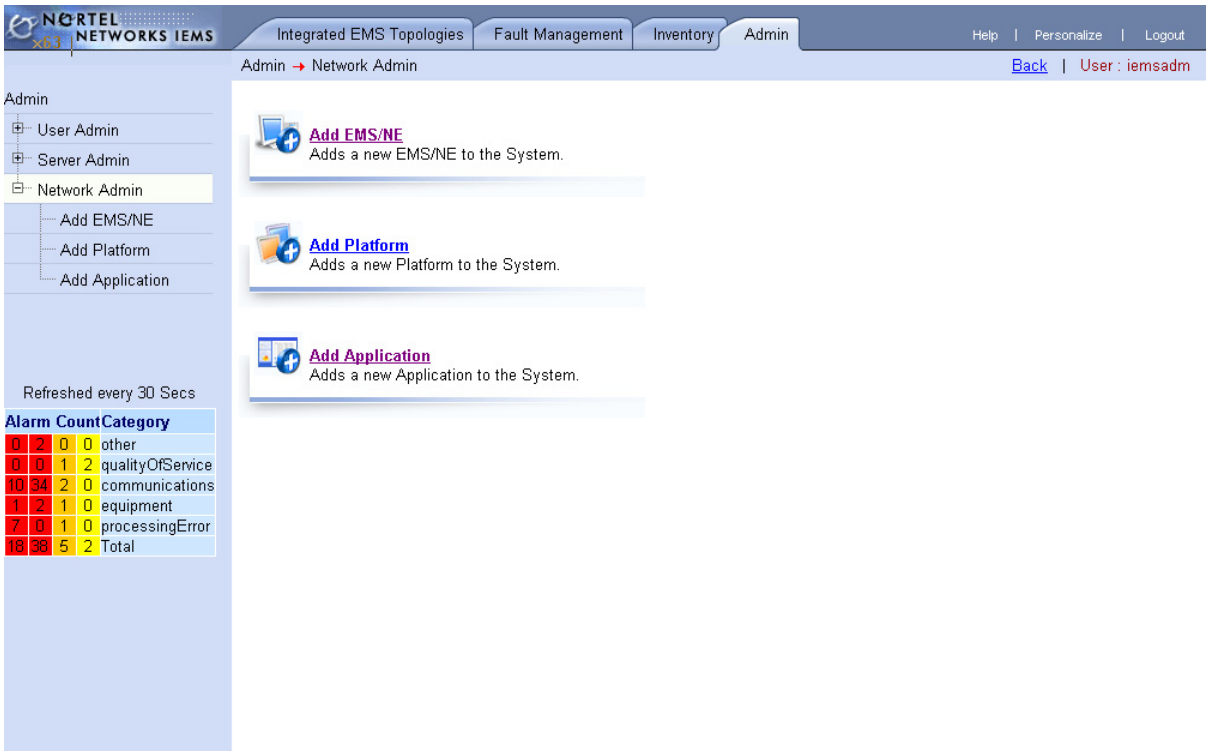
This procedure enables you to add an APS to the Integrated EMS.

Refer to the *Integrated EMS Basics (NN10329-111)* to log into the Integrated EMS GUI.

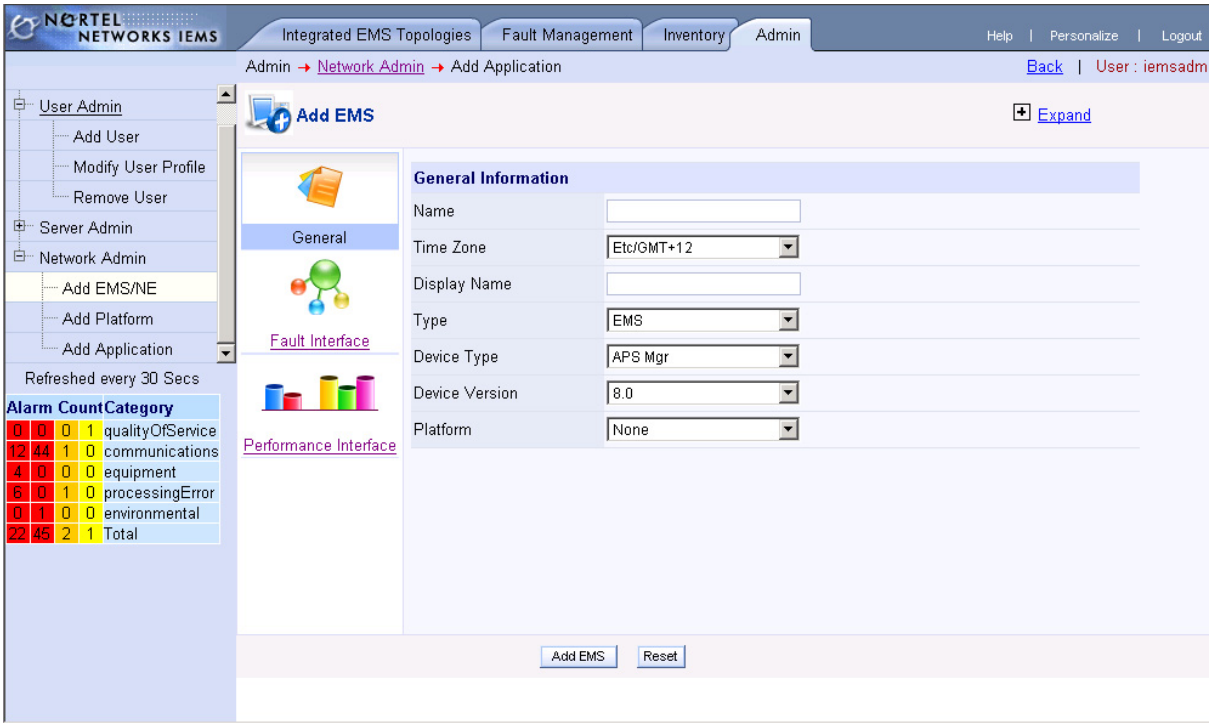
From the Integrated EMS GUI main window

1 Select the *Admin* tab at the top of the window.

2 Select *Network Admin* from the list on the left side of the window.



3 Select *Add EMS/NE*. The Add EMS General Information screen displays.

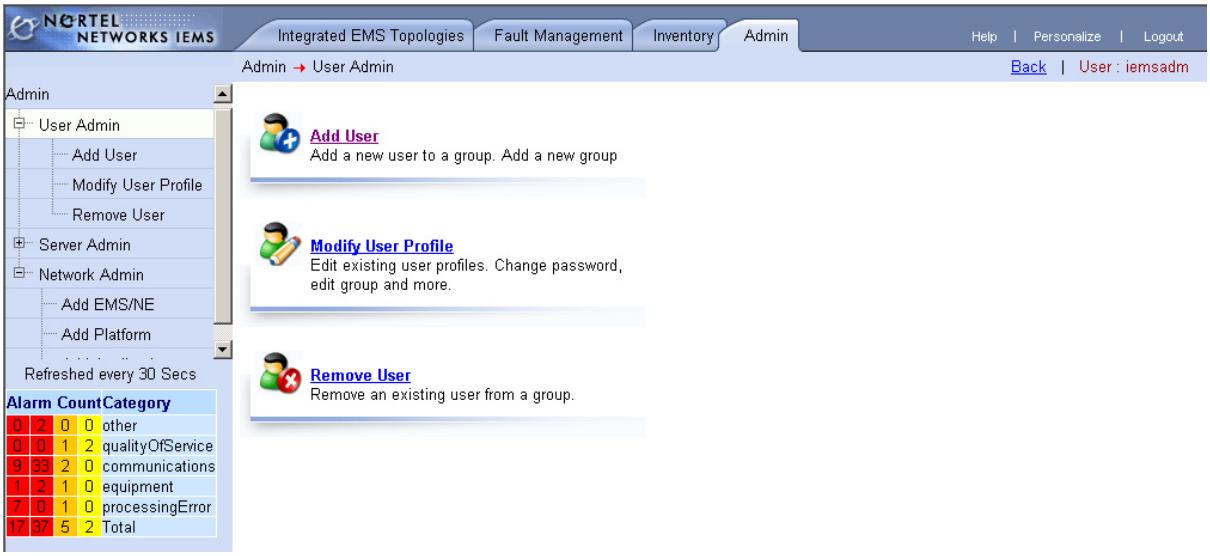


4 Fill in the General Information screen. Refer to the table below.

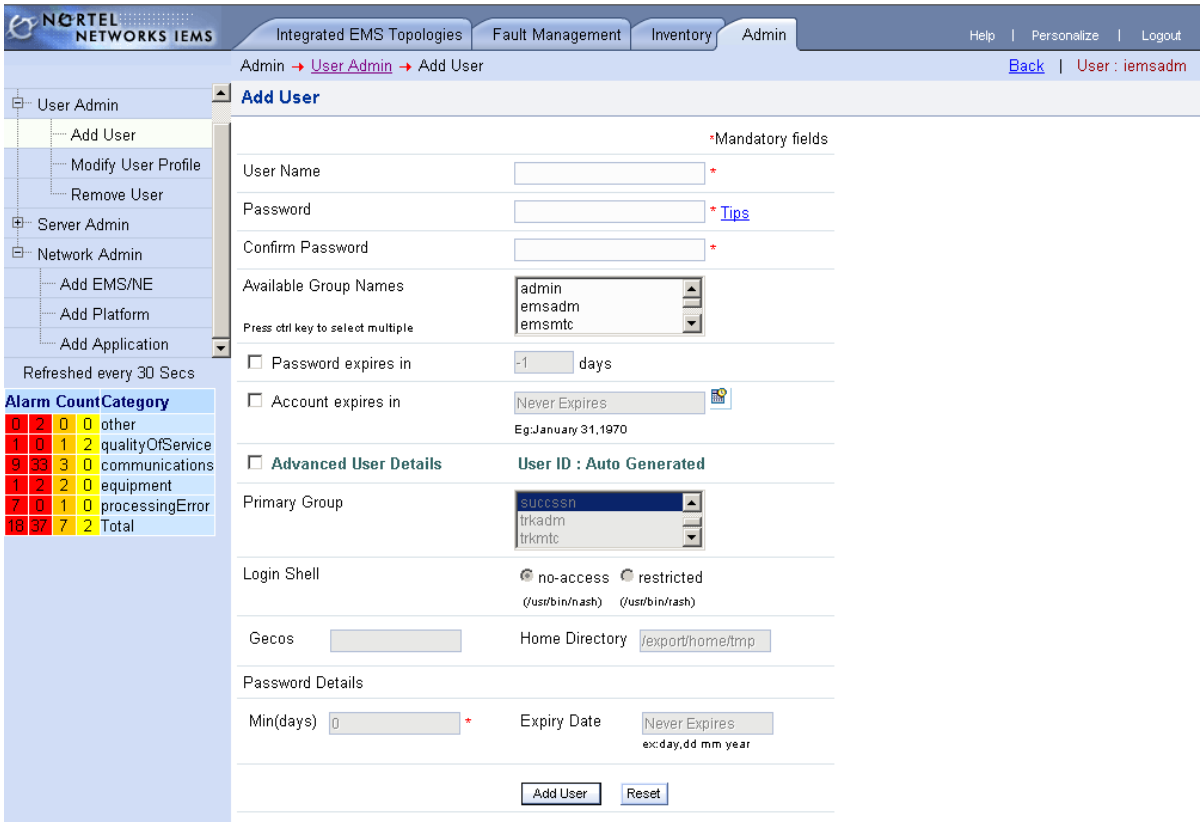
General Information Field	Description
Name	Enter a name for the APS you are adding.
Time Zone	Select your time zone from the pull down list. This is the time offset from Greenwich Mean Time (GMT). The pull down choice list contains regions and city names as well as GMT offset times.
Display Name	Enter a display name for the APS you are adding
Type	Select *EMS* from the pull down list.
Device Type	Select *APS Mgr* from the pull down list.
Device Version	Select the correct version of the APS from the pull down list. Allowable choices are 6.2, 7.0, and 8.0.
Platform	Select the appropriate platform from the pull down list. If it does not belong to any platform, select the the default value *None*.

5 Click on the *Add EMS* button at the bottom of the screen to add the APS manager.

6 Select *User Admin* on the left side of the screen.



7 Select *Add User*.



8 Complete the top portion of this screen to add a user to the *mgcmtc* group for this APS.

a Enter the user name.

b Enter a password.

c Confirm the password by typing it in the *Confirm Password* box.

d Select *mgcmtc* from the *Available Group Names* list.

e Click on the *Add User* button at the bottom of the screen.

9 Repeat step 8 to add a user to the *mgcadm* group for this APS.

10 You have completed this procedure.

Updating the feature key on a Media Server 2000

Overview

The Media Server 2010 and Media Server 2020 have feature keys that enable features and control the quantity of feature resources on the devices. There is one feature key associated with each Trunk Pack Module (TPM) contained in the device. The Media Server 2010 contains one or two TPMs (depending on your configuration), while the Media Server 2020 contains only one TPM.

This procedure describes how to locate the serial number(s), backup the existing feature key(s), and change the feature key(s) associated with a Media Server 2010 or Media Server 2020 TPM. It also contains an abort procedure for reverting back to the original feature key.

Locating the TPM Serial Number

To locate the TPM serial number

1 Open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

2 Enter the IP address of an MS 2000 Series node in the web-browser address field.

3 In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

The main menu buttons located on the left side of the main screen become activated.

4 Select *Status & Diagnostics* from the left side panel.

5

If	Do
the Media Server is using an SN07 software release (4.4)	Select *Versions* from the top panel
the Media Server is using an SN08 software release (4.6)	Select *Device Information* from the top panel

6 Locate and record the serial number.

Backing up the feature keys

To backup existing feature keys

1 Open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

2 Enter the IP address of an MS 2000 Series node in the web-browser address field.

3 In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

The main menu buttons located on the left side of the main screen become activated.

4 Select *Software Update* from the left side panel.

5

If	Do
the Media Server is using an SN07 software release (4.4)	Select *License* from the top panel
the Media Server is using an SN08 software release (4.6)	Select *Software Upgrade Key* from the top panel

6 Select the text in the *Current Key* window.

7 Select *Copy* from the Edit menu of the browser window.

8 Open a new text file.

9 Select *Paste* from the Edit menu of text file window.

10 Save the text file using a convenient file name.

Updating the feature key

To update the feature key

1 Ensure you have a feature key text file with one or more lines of the following format.

```
S/N<serial number of TPM> = <long feature key>
```

Example
S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj ...

Note: One serial number in the text file should match the serial number of the target device.

2 Open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

3 Enter the IP address of an MS 2000 Series node in the web-browser address field.

4 In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

The main menu buttons located on the left side of the main screen become activated.

5 Select *Software Update* from the left side panel.

6

If	Do
the Media Server is using an SN07 software release (4.4)	Select *License* from the top panel
the Media Server is using an SN08 software release (4.6)	Select *Software Upgrade Key* from the top panel

7 Scroll to the bottom and click on the "*Browse*" button.

8 Locate the Feature Key text file and click the "*Open*" button.

9 Click on the "*Send File*" button.

The feature key file is downloaded to the TPM.

The TPM software searches the feature key file for its serial number.

When serial number is found, the TPM software validates the associated feature key, burns the new key into the TPM memory, and performs a reset.

10 After the reset completes (usually 1-2 minutes) reconnect to the target device.

11 Validate the new key by scrolling through the *Key features* panel on the feature key page and verifying the presence of the appropriate features.

Reverting to the original feature key

To revert back to the original feature key

1 Open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

2 Enter the IP address of an MS 2000 Series node in the web-browser address field.

3 In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

The main menu buttons located on the left side of the main screen become activated.

4 Select “Software Update” from the left side panel.

5

If	Do
the Media Server is using an SN07 software release (4.4)	Select *License* from the top panel
the Media Server is using an SN08 software release (4.6)	Select *Software Upgrade Key* from the top panel

6 Locate and open the text file created in the Backing up the feature keys section above.

7 Select the key text.

8 Select *Copy* from the Edit menu.

9 Return to the browser window and position the cursor in the *New Key* window.

10 Select *Paste* from the browser Edit menu.

11 Click on the *Add Key* button.

The TPM software validates the associated feature key, burns the new key into the TPM memory, and performs a reset.

12 After the reset completes (usually 1-2 minutes) reconnect to the target device.

13 Validate the new key by scrolling through the *Key features* panel on the feature key page and verifying the presence of the appropriate features.

Logging in to the APS GUI

This procedure is used for logging in to the APS GUI either to establish a new session, to re-establish a session that has timed out, or to log in to a standby CS 2000 Management Tool to which operation has been redirected.

The APS GUIs are web-based applications. When you launch your web browser to the APS URL, the login page is displayed. While the login page is being downloaded as a JAVA applet, a check is made for the presence of the appropriate JAVA run-time plug-in. If your desktop does not have this plug-in, the CS 2000 Management Tool downloads and installs it if you are operating from a Windows platform.

The recommended client machine for performing APS activities is a Windows 95, 98, ME, XP, NT, or 2000 PC with a minimum of 64 MByte (or greater) of memory, running Netscape 4.7 or Internet Explorer 5.0. Due to the size of the APS application and its memory requirements, it is recommended that no other Windows applications be running at the same time as the APS application.

To log in to the APS GUI, you must have a valid user ID and password and your user account must be active.

Logging in to the APS GUI

At your Web browser screen

1 Type in the following address: https://*<host name or IP address of the APS>*:8443/aps/

Press the Enter key on the keyboard.

The APS login screen opens.

a Enter your user ID and password.

If	Do
you want to submit the user ID and password	step 2
you want to cancel the login operation	step 6

2 Click OK.

If	Do
your user ID is a member of only one program group	step 3

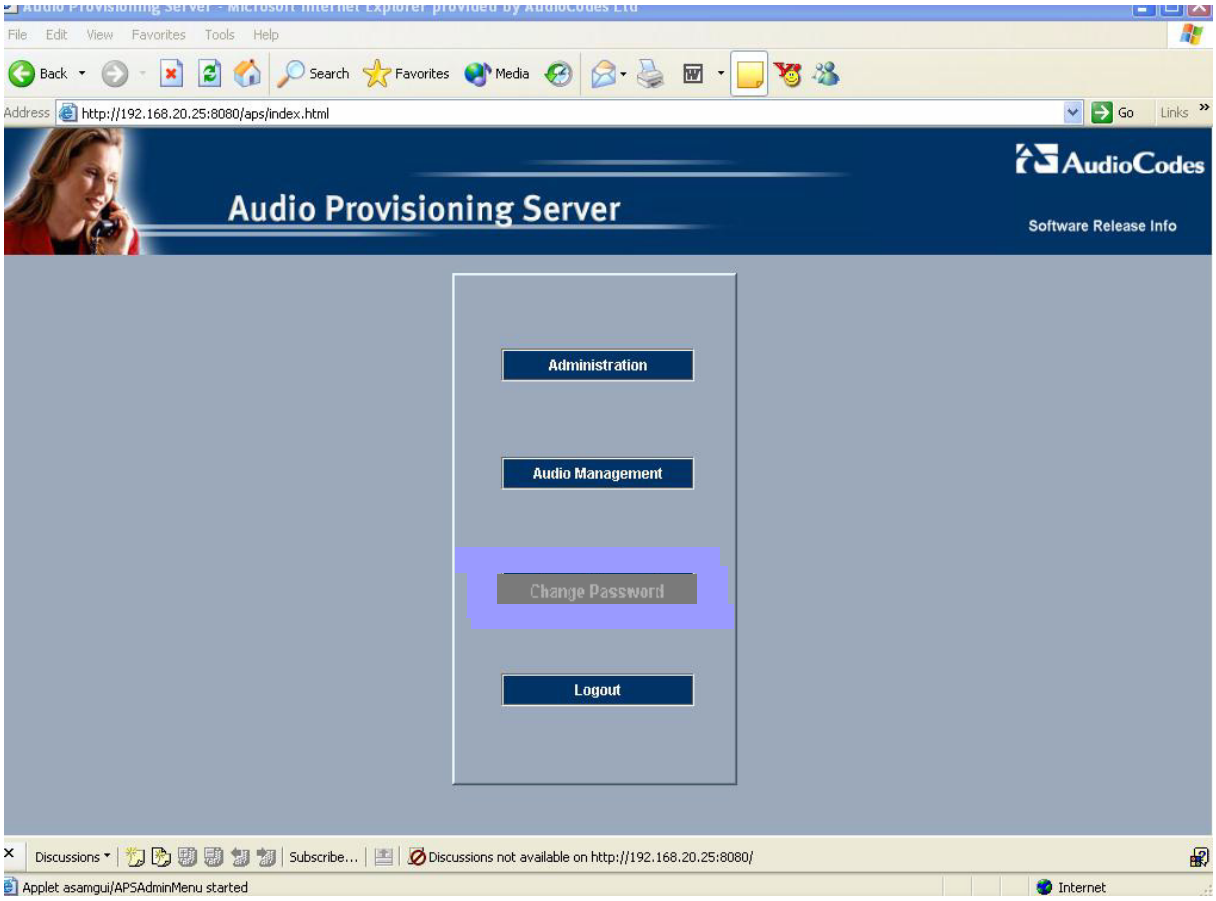
If	Do
your user ID is a member of more than one program group	step 4
your user ID is not a member of a program group	step 5
you want to cancel the login operation	step 6
access is denied because your user account is not active	step 7
you entered an invalid user ID or password	step 8
you do not have the Java runtime environment plug-in	Procedure Downloading the Java runtime environment plug-in

3 The APS main menu screen opens.

Note 1: The administration and audio management functions you are allowed to perform are based on the administration and audio management permissions allowed for your user ID.

Note 2: When your user ID is associated with only one program group, you are restricted to the administration and audio management functions allowed for that program group.

APS main menu screen



a Go to step 9.

4 Select the active program group from the pull-down list.

Note: The program group you select determines the audio data that you will have access to when you use the APS Audio Management Tool.

a Click OK.

The APS main menu screen opens.

b Go to step 9.

5 Click OK in the Missing Program Group window.

The APS main menu screen opens.

Note: When your user ID is not associated with a program group, you do not have access to any audio data. If your user ID has administration permission, you are still able, however, to perform administration functions that do not involve audio

data, using the APS Administration Tool, and to perform the following two functions using the APS Audio Management Tool:

- upload files (File Upload button on the APS Audio Management Tool menu tool bar)
- distribute audio packages (Distribute Packages button on the APS Audio Management Tool menu tool bar.

a Go to step 9.

6 Click the Cancel button. Go to step 9.

7 An *un-authorized user* message displays. Activate the user ID (for instructions, refer to the procedure *Editing user profiles* in the document, NN10340-511, *Media Server 2000 Series Configuration Management*), and then attempt to log in again.

8 Attempt to log in again or contact your next level of support for assistance.

9 You have completed this procedure.

Logging out of the APS GUI

This procedure enables you to log out of an established APS GUI session.

Logging out of the APS GUI

At the APS Administration Tool or APS Audio Management Tool screen

1 Close any dialog boxes that are open.

2 Click the Exit button.

The APS main menu screen opens.

3 Click Logout.

4 You have completed this procedure.

Listing APS patches and release information

This procedure enables you to list the current APS release and patches installed on the CS 2000 Management Tools server. For additional information about this server, refer to your solution's Basics document.

Listing APS patches and releases

At your Web browser screen

1 Type in the following address: https://*<host name or IP address of the APS>*:8443/aps/

Press the Enter key on the keyboard.

The APS login screen opens.

2 On the Audio Provisioning Server title banner, click the Software Release *x* statement below the Nortel Networks logo located on the right side of the banner.

An Audio Provisioning Server Software Load Information screen displays, showing the current time and date, Sun operation system version, APS-specific packages installed on the Call Server, all application packages installed on the Call Server, and SSPFS load information.

3 To return to the APS login screen, close the Web browser screen.

4 You have completed this procedure.

Downloading the Java runtime environment plug-in

This procedure enables you to download the appropriate Java Runtime Environment (JRE) plug-in for your operating system.

The correct version of the JRE plug-in software, a product of Sun Microsystems, Inc., is required to run the APS software in a web browser. The JRE plug-in software allows enterprise web managers to direct Java applets and JavaBeans components on their intranet web pages to run.

The recommended JRE plug-in needed to run the APS software in the Windows environment is JRE 1.4.2. To select and download this plug-in, address your browser (either Internet Explorer or Netscape) to: http://*<IP Address of APS Machine>*:8080/aps/PluginDownload.html

> ***Note:*** Different versions of the JRE can coexist on the same Windows machine. When the APS software is loaded, your browser detects the correct JRE 1.4.2 software version. On the Sun Solaris platform, however, only one version of the Java plug-in can be resident on a single machine. If you are using the Sun Solaris platform, and if the appropriate JRE plug-in is not installed on your machine, your browser detects and reports to you the need for installing the correct Java plug-in. Note that you must normally be logged in as the root user in order to install the Java plug-in.

Downloading the Java runtime environment plug-in

At the APS Welcome screen

1 After you click Login, the Plug-in Download page opens. Read the information on the page to download the plug-in for your operating system.

2 Select your platform.

3 Click Download.

4 Download the plug-in to a directory of your choice.

If	Do
you are running Netscape Navigator	step 5
you are running Internet Explorer	step 7

5 Click Close X.

6 Double-click the JRE file in the specified directory.

7 Follow the instructions in the JRE setup screen.

8 Exit from the web browser and restart the operating system.

9 Log in to the APS GUI. Refer to the procedure Logging in to the APS GUI for instructions.

10 You have completed this procedure.

Running the APS command line interface

The APS command line interface is a tool that enables you to perform basic APS-related maintenance tasks. Through the tool, you can perform the following tasks.

- query APS-related data bases
- perform audio provisioner maintenance activities
- restart APS-related CS 2000 Management Tool processes
- list the software loaded on your APS
- query and perform database backups and restorations
- manipulate the APS SNMP Agent, view APS log files
- view information about backed-up files for MS 2000 Series nodes

The tool can be accessed when you are logged as the root user.

Running the APS command line interface

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in to the system as the root user.

2 Run the APS command line interface tool by entering the following command.

```
apscli
```

The APS Command Line Interface main menu displays.

3 In response to the prompt that displays, enter the number of the task that you wish to perform.

4 You have completed this procedure.

Displaying APS mounted file systems

This procedure enables you to view a complete directory structure, including the root directory (/) and all directories and files contained within the root directory, in order to determine whether any file systems are approaching maximum capacity.

Displaying APS mounted file systems

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the root user by entering the following command.

```
su - root
```

3 Enter the following command.

```
df -k
```

The output of this command consists of a single line of information for each specified file system. Each line of information includes a file system name (filesystem), the total space allocated in the file system (kbytes), the amount of space allocated to existing files (used), the amount of space available for the creation of new files by unprivileged users (avail), the percentage of normally-available space that is currently allocated to all files on the file system (capacity), and the device on which the file system is mounted (mounted on).

It is important to note file systems that are approaching maximum capacity (90% or more). For a procedure used to increase (grow) the size of a file system, see your solution's Configuration Management document.

4 You have completed this procedure

Changing the APS IP/Hostname configuration

This procedure enables you to change the IP address and hostname configuration of the APS, after the APS has been installed.

Changing the APS IP/Hostname configuration

In a telnet connection to the CS 2000 Management Tools server

1. Open an xterm window and log in using the *maint* login and password.
2. Become the root user by entering the following command.

   `su root`
3. Enter the following command.

   `cli`

   The system displays a Command Line Interface command menu.
4. In response to the select prompt, enter **2** (Configuration).

   The system displays a Configuration command menu.
5. In response to the select prompt, enter **3** (IP Configuration).

   The system displays an IP Configuration command menu.
6. In response to the select prompt, enter **3** (Change system hostname, IP address, or router).

   A series of prompts display, asking you for the hostname, IP address, and router IP address. Enter the appropriate information in response to each prompt.
7. Enter the following command to reboot the server.

   `shutdown -i 6 -y`
8. After the reboot has completed, log into the system as the root user and enter the following command.

   `aps_cli.sh`

   The system displays the messages, *local_parms.sh is set up - Successfully set up site specific information.* If you do not see this message displayed, contact your next level of support.
9. You have completed this procedure.

Monitoring nightly cleanup

Every night, during off-peak service hours, the *nightly_cleanup.sh* script runs automatically. The script cleans files that are known to fill up file systems, before damage can be done to your APS system. Specifically, the script cleans the following files.

- /var/adm/wtmpx (2000 lines of this file are retained)
- /var/adm/sulog (2000 lines of this file are retained)
- provisioner audit files (retains logs of the last known successful provisioning)
- provisioner logs (3 days worth are retained)

Two days worth of output and error files are stored in the /APS_spool directory. Review these files to ensure that the cleanup process is being performed successfully.

Monitoring audio provisioning activity

The script programs in the procedure below create reports that enable you to monitor the audio provisioning activity that you have performed.

Note: All of the reports generated below can also be created through a special APS command line interface tool. For a procedure containing instructions for running the tool, see Running the APS command line interface.

Monitoring audio provisioning activity

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the root user by entering the following command.

```
su - root
```

3 Change directory to the scripts directory by entering the following command.

```
cd /usr/ntdb/uas/scripts
```

4 Determine the report you wish to create.

If	Do
you wish to display information about segments that you have provisioned	step 5
you wish to display information about export packages that you have provisioned	step 6
you wish to display information about program groups that you have provisioned	step 7
you wish to display information about segments you have provisioned that are not associated with a program group	step 8
you wish to determine that free disk space to be used during audio provisioning is available	step 12
you wish to display users for which administration information was changed	step 10

If	Do
you wish to display a list of all nodes define in the APS database	step 11
you wish to display data about all of the nodes in the APS database	step 12
you wish to display a list of configuration parameters for your APS system	step 13

5 To display information about the segments that have provisioned in the database, enter the following command.

```
audio_added.sh <start date> <end date>
```

Note: The date parameters must be entered in the format, *dd-mmm-yy* (the *mmm* variable consists of the first three letters of the name of the month, for example 16-JUL-02).

A list of segment IDs and the data and time at which the segments they represent were last modified, in the date and time range that you specified, displays.

a Either return to step 4 and create a different report or go to step 14.

6 To display information about the export packages that you have provisioned, enter the following command.

```
packages_report.sh <start date> <end date>
```

Note: The date parameters must be entered in the format, *dd-mmm-yy* (the *mmm* variable consists of the first three letters of the name of the month, for example 16-JUL-02).

A list of export package IDs, the creator of each of the packages they represent, and the date and time at which the packages were created, within the date and time range that you specified, displays.

a Either return to step 4 and create a different report or go to step 14.

7 To display information about the program groups that you have either added or deleted, enter the following command.

```
prg_grp_report.sh <start date> <end date>
```

Note: The date parameters must be entered in the format, *dd-mmm-yy* (the *mmm* variable consists of the first three letters of the name of the month, for example 16-JUL-02).

For each program group you have either added or deleted, the following information displays.

Status

Program Group name

Provision Set it is associated with

ID of the users it is associated with

Date of the last modification

a Either return to step 4 and create a different report or go to step 14.

8 To display information about segments that are not associated with a program group, enter the following command.

`segment_no_prg_grp.sh`

A list of segment IDs that are not associated with any program groups, displays.

a Either return to step 4 and create a different report or go to step 14.

9 To display the amount of free disk space available for audio provisioning, enter the following command.

`freespace.sh`

A listing of each table-space and disk-space, and the number of free bytes and blocks within each, displays.

Note: Although this data can require a more detailed review to determine system health, by looking for free-space values at or near zero you can determine whether system maintenance is required. If system maintenance is required, contact your Oracle database administrator.

a Either return to step 4 and create a different report or go to step 14.

10 To display the users for which administrative information was changed, enter the following command.

`users_modified.sh`

A listing for each user modified, including the status of the modification, who made the modification, and the date on which the modification was made, displays.

a Either return to step 4 and create a different report or go to step 14.

11 To display a list of all MS 2000 Series nodes defined in the APS database, enter the following command.

`list_uas_nodes.sh`

A listing of the nodes and their associated IP addresses defined in the APS database, displays.

a Either return to step 4 and create a different report or go to step 14.

12 To display provisioning data for all MS 2000 Series nodes defined in the APS database, enter the following command.

```
list_uas_nodes.sh -all
```

A listing of the nodes displays, which includes for each node the node's name and IP address, provision sets associated with the node, whether the node is enabled for provisioning (under column E in the listing, 1 = yes, 2 = no) and the date the node was last updated with new audio.

a Either return to step 4 and create a different report or go to step 14.

13 To display a list of your APS system's configured parameters, enter the following command:

```
list_sys_parms.sh
```

A listing of the system parameters displays. The parameters include the following.

- response timer (UAS_RESPONSE_TIMER) (This parameter can be changed through the APS Administration GUI.)
- maximum number of physical segment versions (UAS_MAX_PHYS_SEG_VER) (This parameter can be changed through the APS Administration GUI.)
- maximum number of package versions (UAS_MAX_PKG_VER) (This parameter can be changed through the APS Administration GUI.)
- maximum segment depth (MAX_SEG_DEPTH) (This parameter can be changed through the APS Administration GUI.)
- user audio file path (UAS_USER_AUDIO_FILEPATH)
- IPS database provisioning file path (IPS_PROV_PATH)
- maximum number of language versions (UAS_MAX_LANG_VERS) (This parameter can be changed through the APS Administration GUI.)
- maximum number of users (UAS_MAX_USERS)
- maximum number of program groups (UAS_MAX_PROGRAM_GROUPS)

- maximum number of provision sets (UAS_MAX_PROVISION_SETS)
- maximum number of UAS nodes (UAS_MAX_NODES)

a Either return to step 4 and create a different report or go to step 14.

14 You have completed this procedure.

Checking APS provisioning activity

This procedure enables you to check the provisioning activity in your MS 2000 Series system. This helps you ensure that the audio you have created using the APS GUIs has actually been provisioned to an MS 2000 Series node.

Checking APS provisioning activity

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the root user by entering the following command.

```
su - root
```

3 Display the provisioner log file content by entering the following command.

```
more /PROV_data/provisioner.log
```

Examine the file content display and look for entries like those described below, pertaining to the audio file distribution you have just performed, to ensure that all of the audio files have been successfully provisioned in the MS 2000 Series node.

Each time a provisioner process runs, an entry is appended to the log for the related CS 2000 Management Tool, in the format shown below.

PROVISIONER START on <*hostname*> at <*date*> [PID: <*pid*>]
<*single provision or full provision information*>

Each time a provisioner process exits, an entry is also appended to the log for the related CS 2000 Management Tool, in the format shown below.

PROVISIONER END on <*hostname*> at <*date*> [PID: <*pid*>]
<*single provision or full provision information*>

During normal operation, progress messages are entered in the provisioner logs. For example, when a provisioner creates transaction files for a node, the following entries are made in the related provisioner log.

Attempting to provision node <*node name*> from host <*hostname*> at
<*date*>. [PID: <*pid*>]

Attempting to transfer files for node <*node name*> from <*hostname*>
at <*date*>. [PID: <*pid*>]

Last prov date updated for node <*node name*> on host <*hostname*> at
<*date*>. [PID: <*pid*>]

If a provisioner process exits abnormally, an entry is appended to the log for the related CS 2000 Management Tool, in the format shown below.

PROVISIONER STOP on <*hostname*> at <*date*> because <*fault*
***information*> [PID: <*pid*>] <*single provision or full provision information*>**

If an abnormal exit occurs, indicating that provisioning did not succeed, contact your Nortel Networks service representative.

4 You have completed this procedure.

Checking the APS Oracle database

This procedure enables you to check the status of the Oracle database.

Checking the APS Oracle database

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the root user by entering the following command.

```
su - root
```

3 Perform the following steps to verify that you can connect to the Oracle database:

a Enter the following command to verify that you can connect to the Oracle database.

```
sql
```

b At the prompt, enter the following command.

```
select count(*) from tab;
```

A number other than zero displays.

c Enter the following command to disconnect from the Oracle database.

```
sql > quit
```

d If you are unable to connect to the database, ensure that your database is on-line by entering the following command.

```
look ora
```

A listing of Oracle processes displays.

4 Enter the following command to check the status of the database:

```
/opt/servman/bin/servman query -status -g
DATABASE -v
```

A status report like the following displays.

Connecting to
(DESCRIPTION=(ADDRESS-(PROTOCOL=TCP))HOST=<*ip address*> (PORT=<*port #*>)))
STATUS OF THE LISTENER
Alias LISTENER
Version TNSLL+SNR for Solaris: Version 8.1.7.0.0
Start Date <*date and time*>
Uptime <*days; hours; minutes; seconds*>
Trace Level off
Security off
SNMP off
Listener Parameter File
/opt/oracle/product/8.1.7/network/admin/listener.ora
Listener Log File
/opt/oracle/product/8.1.7/network/log/listener.log

```
Services Summary ...
   PSLExtProc has 1 service handler
  pfs has 1 service handler
  pfs has 1 service handler
The command completed successfully.
oracle  694  1  0  14:07:59  ?   0:00 ora_pmon_pfs
oracle  696  1  0  14:07:59  ?   0:00 ora_dbw0_pfs
oracle  698  1  0  14:07:59  ?   0:00 ora_lgwr_pfs
oracle  700  1  0  14:07:59  ?   0:00 ora_ckpt_pfs
oracle  702  1  0  14:07:59  ?   0:00 ora_smon_pfs
oracle  704  1  0  14:07:59  ?   0:00 ora_reco_pfs
oracle  70 6 1  0  14:07:59  ?   0:00 ora_snp0_pfs
oracle  708  1  0  14:07:59  ?   0:00 ora_arc0_pfs
```

If	Do
you saw information like this display	step 8
you did not see information like this display	step 5

5 Start the Oracle database by entering the following commands.

`/opt/servman/bin/servstart DATABASE`

6 Kill the CS 2000 Management Tool process and let the server restart automatically, by entering the following command.

`/opt/uas/aps/scripts/killDbServer.sh`

A message eventually displays indicating that the server is restarting.

7 Enter the following command to check the status.

```
/opt/servman/bin/servman query -status -g
DATABASE -v
```

The display indicates that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with *oracle <pid>*), are running. If the processes are not running, contact your next level of support.

8 You have completed this procedure.

Verifying that the APS CD drive is mounted

This procedure enables you to determine whether the APS CD drive is accessible and that the APS CD is inserted in the drive. This is normal operating condition.

Verifying that the APS CD drive is mounted

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the root user by entering:

```
su - root
```

3 Enter the following command:

```
df -k
```

A status report displays, indicating for each device, capacity measurements. If the CD drive is mounted you will see a */cdrom/ ...* entry.

If	Do
you saw a */cdrom/ ...* entry	step 10
you did not see a */cdrom/ ...* entry	step 4

4 Enter the following command to the display the contents of the */etc/vold.conf* file.

```
cat /etc/vold.conf
```

The contents of the file displays. In the display, look for the command, u*se cdrom drive /dev/rdsk/c*s2 dev_cdrom.so cdrom%d*.

If	Do
the command, *use cdrom drive /dev/rdsk/c*s2 dev_cdrom.so cdrom%d* appears in the file	step 6
the command, *use cdrom drive /dev/rdsk/c*s2 dev_cdrom.so cdrom%d* doesn't appear in the file	step 5

5 Contact your next level of support. You cannot perform this procedure.

6 Enter the following command.

```
ps -fea | grep vold
```

The resulting display shows that the vold (volume manager daemon) process (*usr/sbin/vold*) is running. Record the process ID associated with this process.

7 Enter the following command to stop the volume manager daemon.

```
kill -HUP <process ID of vold process>
```

(The *process ID of vold process* was obtained in step 6.)

The operating system will restart, and then re-read the *vold* process and any changes that have been made to the */etc/vold.conf* file.

8 Enter the following command:

```
df -k
```

A status report displays, indicating for each device, capacity measurements. If the CD drive is mounted you will see a */cdrom/ ...* entry.

If	Do
you saw a "/*cdrom/ ...*" entry	step 10
you did not see a "/*cdrom/ ...*" entry	step 9

9 Reboot the CS 2000 Management Tool by entering the following command:

```
shutdown -i 6 -y
```

10 You have completed this procedure.

Set APS security

There are a number of ways to make access to the APS more secure, including configuring SNMP community read and write community strings to non-default values (see the procedure, *Configuring the SNMP agent* in the document NN10340-511, *Media Server 2000 Series Configuration Management*), choosing user passwords that are different from login IDs or that cannot be easily guessed. Another way to secure APS access is to add a password to the Oracle Listener port, 1521. For procedures used to set and change the Oracle Listener password, refer to your solution's Security and Administration document.

Setting the APS administrator (UNIX) password

The APS software is pre-configured with a UNIX Administrator user without a UNIX Administrator password. This procedure enables you to secure the access to your CS 2000 Management Tool by creating a UNIX Administrator password.

After you have initially set the Administrator password to secure CS 2000 Management Tool access, this procedure enables you to then change the Administrator password, as required.

Setting the APS administrator (UNIX) password

At the system console (Windows desktop interface)

1 Decide whether you are setting the Administrator password for the first time.

If	Do
you are setting the password for the first time	step 2
you are not setting the password for the first time	step 4

2 Log in as the root user.

3 Enter the following command.

```
password Administrator
```

a Go to step 5

4 Log in as Administrator.

Note: The login is case-sensitive and must be entered in the form, Administrator.

The system responds with the message, *Choosing a new password*.

5 In response to the system prompt, enter your new password.

6 In response to the system prompt, re-enter the new password.

7 You have completed this procedure.

Restarting the SNMP agent

This procedure enables you to determine whether the SNMP agent is running and, if it has stopped, to restart it.

Note: The following procedure can also be performed through a special APS command line interface tool. For a procedure containing instructions for running the tool, see Running the APS command line interface.

Restarting the SNMP agent

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the “root” user by entering.

```
su - root
```

3 Verify that the agent is, or was, running by entering the following command.

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

A numeric process id (pid) associated with the agent displays.

If	Do
a process id displays	step 4
a process id doesn’t display	step 5

4 Verify that the process associated with the agent is running by entering the following command.

```
ps -ef | grep nnnnn
```

where *nnnnn* is the process id that was displayed in step3.

If the process is running, a descriptive line of information about the process displays.

If	Do
the process is running	step 8
the process is not running	step 5

5 Enter the following command to start the SNMP agent.

/opt/uas/SnmpAgent/bin/agentctl start

6 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 associated with the agent displays.

If	Do
the process id displays	step 7
the process id doesn't display	repeat steps 5 and 6 one more time and, if the process still doesn't display, contact your next level of support

7 Verify that the process associated with the agent is running by entering the following command.

ps -ef | grep *nnnnn*

where *nnnnn* is the process id that was displayed in step 6.

If	Do
the process is running	step 8
the process is not running	repeat steps 5 through 7 one more time and, if the process is still not running, contact your next level of support

8 You have completed this procedure.

Verifying that the Web server is running

This procedure enables you to determine whether the Web server is running. The Web server enables you to access the APS Administration and Audio Management GUIs.

Verifying that the Web server is running

At your console

1 Start the APS GUI by entering the following command.

`Start up Netscape or Internet Explorer.`

`Enter the URL for the APS GUI in your Web browser: https://<host name or ip address of the APS>:8443/aps/`

If	Do
the APS login screen displays	step 8
the APS login screen does not display	step 2

2 Enter the following URL in your Web browser: http://*<ip address>*

If	Do
Apache Web server page displays	step 3
the Apache Web server page does not display	step 5

3 Log in as the root user.

4 Enter the following command to restart the CS 2000 Management Tool processes.

`/opt/uas/aps/scripts/killDbServer.sh`

Note: The web server and the Java servlet engine will be restarted as a result of this command. CS 2000 Management Tools users are temporarily impacted while the web server restarts.

a Go to step 8.

5 Log in as the root user.

6 Enter the IP address of the CS 2000 Management Tool in the browser address window.

An Application Launch Point page displays.

If	Do
the Application Launch Point page displays	step 8
the Application Launch Point page does not display	step 7

7 Enter the following command to start the Apache server:

```
/opt/servman/bin/servstart WEBSERVICES
```

Messages that indicate the Apache server has started display.

8 You have completed this procedure.

Listing APS software load packages

This procedure enables you to list the installed APS software on an CS 2000 Management Tool. If you choose to use your web browser to view this information; refer to the procedure, Listing APS patches and release information.

Listing APS software load packages

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the *maint* login and password.

2 Become the root user by entering the following command.

```
su - root
```

3 Enter the following command to list the installed software packages on the CS 2000 Management Tool.

```
pkginfo | grep aps | more
```

A list of the installed software packages displays.

4 Too see a count of all installed application software packages on the CS 2000 Management Tool, enter the following command.

```
pkginfo | grep application | wc
```

A count of the installed software packages displays. The number of packages will be at least 37, depending on the number APS bug fixes.

5 To display the APS software load version that is currently using the APS Web server, perform the following steps.

Start up Netscape or Internet Explorer.

Enter the following URL in your Web browser: https://*<host name or ip address of the APS>*:8443/aps/servlet/HelloASAM

A window opens, displaying the current APS software version, a time stamp, and the version of the SUN operating system on which the APS software is running.

6 You have completed this procedure.

Changing the APS Oracle account password

When the APS is installed, a default password is assigned to the Oracle account. This procedure enables you to change the default password, for added system security.

Changing the APS Oracle account password

In a telnet connection to the CS 2000 Management Tool

1 Open an xterm window and log in using the root login and password.

2 When the APS is installed, the Oracle account password is *lionpwd*. If you are unsure whether the password has been changed, obtain the current password by entering the following command.

`/usr/ntdb/uas/scripts/getNTDBpasswd.ksh`

The system displays the current Oracle account password.

3 Perform the following steps to change the Oracle account password.

a Enter the following command to run the script that enables you to change the password.

`/usr/ntdb/uas/scripts/setNTDBpasswd.ksh`

b At the prompt, enter the current APS Oracle account password.

Note: This is either the default password, *lionpwd* or the password that you displayed in step 2.

c At the prompt, enter the new APS Oracle account password.

d At the prompt, reenter the new APS Oracle account password.

The system changes the password in UNIX and in the Oracle database.

4 The following prompt displays.

```
The APS dbserver software should be restarted to
use the new password.

Do you want to do this now? (Y/N)
```

Enter Y to restart the APS dbserver software.

5 You can now check the password change you have made by entering the following command.

```
/usr/ntdb/uas/scripts/getNTDBpasswd.ksh
```

The system displays the current Oracle account password.

6 You have completed this procedure.

Performing a backup of APS audio files into a single tar archive (FTP)

Use this procedure to backup APS audio files into a single tar archive to FTP off of the server for backup.

Prerequisites

This procedure is for sites with a SUN v240 server.

At the APS server

1. Become the root user by entering the following command and then entering the root password when prompted.

   ```
   su - root
   ```

2. Change your working directory to the root file system by typing the following command.

   ```
   $ cd /
   ```

3. Create the tar archive by typing the following command.

   ```
   tar cvf AudioFiles.tar /audio_files
   /user_audio_files /opt/uas/uas_conf_backup
   ```

4. Ftp the *AudioFiles.tar* file off of this server for backup purposes.
5. Perform APS-only database only backup to CD if not already performed.
6. You have completed this procedure.

Performing an APS-only Data Base Backup to Disk and to CD

Use this procedure to back up the APS database to disk and CD.

Prerequisites

This procedure is for sites with a SUN v240 server equipped with a CD-DVD drive that can burn CDs.

At the APS server

1 Become the root user by entering the following command and then entering the root password when prompted.

```
su - root
```

2 Back up the files to the disk on the server by typing the following command.

```
$ ips_export_db.sh -diskonly
```

Note: This command backs up the APS tables to the disk on the server. The directory is /audio_files/aps_db_backup/*.

3

If	Do
you are backing up the APS files to disk	step 9
you are backing up the APS files to CD	step 4

4 Change to the audio_files directory by typing the following command.

```
cd /audio_files
```

5 Ensure that there is a blank CD in the drive.

6 Burn the APS dmp files to CD by typing the following command.

```
/opt/nortel/sspfs/bks/cdwrite aps_db_backup
```

7 Verify the files are on the CD by typing the following command.

```
-rwxrwsrwx 1 root other 54272 May 13 11:11
ips_db_audit.dmp

-rwxrwsrwx 1 root other 4096 May 13 11:11
ips_node_config.dmp

-rwxrwsrwx 1 root other 2048 May 13 11:11
ips_prov_prg_grp.dmp
```

```
-rwxrwsrwx 1 root other 2048 May 13 11:11
ips_prov_set.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
ips_user.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
ips_user_perm_group.dmp

-rwxrwsrwx 1 root other 71 May 13 11:11 README

-rwxrwsrwx 1 root other 4096 May 13 11:11
sys_parms.dmp

. . . . . .

-rwxrwsrwx 1 root other 44032 May 13 11:11
uas_segments.dmp

-rwxrwsrwx 1 root other 6144 May 13 11:11
uas_selector_relation.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_selector_type.dmp

-rwxrwsrwx 1 root other 7168 May 13 11:11
uas_selector_value.dmp

-rwxrwsrwx 1 root other 5120 May 13 11:11
uas_sequences.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_content.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_definition.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_user_perms.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_var_start_seg_id.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_variables.dmp

#
```

8 Back up the APS audio files if not already performed. Refer to procedure *Performing a backup of APS audio files into a single tar archive (FTP)*.

9 You have completed this procedure.

Performing an APS-only Data Base Backup to 4mm DAT

Use this procedure to back up the APS database to a blank 4mm Tape.

Prerequisites

This procedure is for sites with a SUN t1400 server equipped with a 4mm DAT drive.

Note: This procedure is not for sites with a SUN v240 and the CD-DVD drive.

At the APS server

1 Become the root user by entering the following command and then entering the "root" password when prompted.

```
su - root
```

2 Ensure there is a write-enabled 4mm DAT tape in the drive

3 Back up the files to the tape by typing the following command.

```
$ ips_export_db.sh -t /dev/rmt/0
```

4 Verify the files are on the tape by typing the following command and viewing the command output.

```
# tar tvf /dev/rmt/0
-rwxrwsrwx 1 root other 54272 May 13 11:11
ips_db_audit.dmp
-rwxrwsrwx 1 root other 4096 May 13 11:11
ips_node_config.dmp
-rwxrwsrwx 1 root other 2048 May 13 11:11
ips_prov_prg_grp.dmp
-rwxrwsrwx 1 root other 2048 May 13 11:11
ips_prov_set.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
ips_user.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
ips_user_perm_group.dmp
-rwxrwsrwx 1 root other 71 May 13 11:11 README
-rwxrwsrwx 1 root other 4096 May 13 11:11
sys_parms.dmp
. . . . . .
```

```
-rwxrwsrwx 1 root other 44032 May 13 11:11
uas_segments.dmp

-rwxrwsrwx 1 root other 6144 May 13 11:11
uas_selector_relation.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_selector_type.dmp

-rwxrwsrwx 1 root other 7168 May 13 11:11
uas_selector_value.dmp

-rwxrwsrwx 1 root other 5120 May 13 11:11
uas_sequences.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_content.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_definition.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_user_perms.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_var_start_seg_id.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_variables.dmp

#
```

5. Eject the tape and move the tape tab to read-only position. Label the tape and store in a safe place.
6. Backup the APS audio files to tape, if not already performed.
7. You have completed this procedure.

Performing an APS-only Data Base Restore from a 4mm DAT

Use this procedure to restore the APS DB from an APS DB tape backup in a 4mm DAT drive.

Prerequisites

This procedure is for sites with a SUN t1400 server equipped with a 4mm DAT drive.

Note: This procedure is not for sites with a SUN v240 and the CD-DVD drive.

At the APS server

1 Become the root user by entering the following command and then entering the "root" password when prompted.

```
su - root
```

2 Ensure the 4mm DAT tape in the drive is a write-protected.

3 Start the DB restore from the tape by typing the following command.

```
$ ips_export_db.sh -t /dev/rmt/0 -restore
```

This command restores the APS DB from the tape to the following directory.

```
/audio_files/aps_db_backup/*.dmp
```

4 Restore the APS audio files to the file system if not already performed.

5 You have completed this procedure.

Performing an APS-only Database restore from a CD

Use this procedure on a SUN v240 server with a CD drive.

Prerequisites

This procedure is for sites with a SUN v240 and the CD-DVD drive.

Note: This procedure is not for sites with a SUN t1400 server equipped with a 4mm DAT drive.

At the APS server

1 Become the root user by entering the following command and then entering the "root" password when prompted.

```
su - root
```

2 Load the backup CD into the CD drive on the server.

3 Change to the aps backup directory on the server by typing the following command.

```
cd /audio_files/aps_db_backup
```

4 Copy the dmp files on the CD to this directory by typing the following command.

```
$ cp /cdrom/cdrom0/* ./
```

5 Verify the dmp files were copied from CD to the destination directory by typing the following command and then viewing the command output.

```
$ ls -l *
-rwxrwsrwx 1 root other 54272 May 13 11:11
ips_db_audit.dmp
-rwxrwsrwx 1 root other 4096 May 13 11:11
ips_node_config.dmp
-rwxrwsrwx 1 root other 2048 May 13 11:11
ips_prov_prg_grp.dmp
-rwxrwsrwx 1 root other 2048 May 13 11:11
ips_prov_set.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
ips_user.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
ips_user_perm_group.dmp
-rwxrwsrwx 1 root other 71 May 13 11:11 README
```

```
-rwxrwsrwx 1 root other 4096 May 13 11:11
sys_parms.dmp

. . . . . .

-rwxrwsrwx 1 root other 44032 May 13 11:11
uas_segments.dmp

-rwxrwsrwx 1 root other 6144 May 13 11:11
uas_selector_relation.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_selector_type.dmp

-rwxrwsrwx 1 root other 7168 May 13 11:11
uas_selector_value.dmp

-rwxrwsrwx 1 root other 5120 May 13 11:11
uas_sequences.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_content.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_definition.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_user_perms.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_var_start_seg_id.dmp

-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_variables.dmp

#
```

6 Start the DB restore from the disk files by typing the following command.

`$ . ips_export_db.sh -diskonly -restore`

This command restores the APS DB from the disk files to the directory shown below.

`/audio_files/aps_db_backup/*.dmp`

7 Restore the APS audio files to the file system if not already performed.

8 You have completed this procedure.

Performing a restore of APS audio from 4mm DAT

Use this procedure to restore APS audio files from a tape.

Prerequisites

This procedure is for sites with a SUN t1400 server equipped with a 4mm DAT drive.

Note: This procedure is not for sites with a SUN v240 and the CD-DVD drive.

At the APS server

1 Become the root user by entering the following command and then entering the "root" password when prompted.

```
su - root
```

2 Load the APS audio file tape into the drive.

3 Change directory to the root file system by typing the following command.

```
$ cd /
```

4 Restore audio files to the file system by entering the following command.

```
$ tar xvf /dev/rmt/0
```

The file are read from tar and placed on the file systems.

5 Place the Audio files in the following filesystems.

- /audio_files
- /user_audio_files

6 If a corresponding restore of the APS database is needed, locate the backup tape for the APS database and restore the APS DB tables.

7 You have completed this procedure.

Performing a restore of APS audio files from a TAR file

Use this procedure to restore APS audio files from a TAR file.

At the APS server

1 Become the root user by entering the following command and then entering the "root" password when prompted.

```
su - root
```

2 Change directory to where the tar file is located.

```
$ cd /<directory>
```

where <directory> is the absolute path of the directory where the TAR file is located.

3 Restore audio files to the file system by entering the following command.

```
$ tar xvf <tar_file_name>
```

where <tar_file_name> is the name of the TAR file

The files are read from tar and placed on the file systems.

4 Place the Audio files in the following filesystems.

- /audio_files
- /user_audio_files

5 If a corresponding restore of the APS database is needed, locate the APS database backup files and restore the APS DB tables.

6 You have completed this procedure.

Changing the PMGRdaemon password

This procedure enables you to change the Windows Administrator password and the 'Logon' password for the PMGRdaemon service.

> **ATTENTION**
> When changing the administrator password for the machine you must also change the 'Logon' password for the PMGRdaemon service.

At the Windows desktop interface

1. Right click the "My Computer" icon on the desktop.
2. Select "Manage" from the pop-up menu. The Computer Management window opens.
3. Under "System Tools", expand the "Local Users and Groups" folder.
4. Open the "Users" folder.
5. In the right panel of the Computer Management window, right click the "Administrator" icon.
6. Select "Set Password" from the pop-up menu. The Set Password window opens.
7. In the Set Password window, enter the new password in the "New password" dialog box.
8. Enter the new password in the "Confirm password" dialog box.
9. Click "OK". The Set Password window closes.
10. From the Computer Management window, expand the "Services and Applications" folder.
11. Open the "Services" folder.
12. In the right panel of the Computer Management window, right click the "PMGRdaemon service" icon and select "Properties".
13. When the PMGRdaemon Properties dialog box opens, select the logon tab.
14. Make sure the user is set to '.\Administrator'.
15. Enter the new password.
16. Confirm the new password.

Note: You must log off and back on to the system once you change the passwords.

17 Close all windows and log off and back on to the system.

18 You have completed this procedure.