UAS Security and Administration

UAS security and administration activities include changing system passwords, checking system configuration, backing up the database, and monitoring APS database activity. Password changes and system configuration checks are performed only on an as-needed basis. Backing up the database and monitoring database activity are performed on a regular basis.

The tools and utilities used to perform UAS and APS security and administration tasks are described in the section, Tools and utilities on page 1. The procedures and tasks that enable you to perform UAS and APS security and administration tasks are grouped by application and are listed in tables shown in the section, Security management procedures on page 1.

Tools and utilities

The UAS security and administration procedures are performed either through the Universal Audio Server Manager, a command line interface, or through a Windows interface.

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

Procedure and page	Interface or Tool used
Changing the APS GUI password on page 4	APS GUI
Logging in to the APS GUI on page 6	APS GUI
Logging out of the APS GUI on page 9	APS GUI

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

UAS device-related security and administration procedures

Procedure and page	Interface or Tool used
Changing the CS 2000 Management Tools server IP address on page 11	LCI GUI
Checking the UAS software configuration on page 15	Command line
Backing up UAS configuration files on page 16	Command line
Configuring security events for auditing on page 19	Windows desktop interface
Changing the UAS IP/Hostname configuration on page 20	UAS Manager
Using NetMeeting with the UAS on page 28	NetMeeting

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 or Tool used
Listing APS patches and release information on page 10	APS GUI
Downloading the Java runtime environment plug-in on page 29	APS GUI
Running the APS command line interface on page 31	APS CLI
Displaying APS mounted file systems on page 32	Command line
Changing the APS IP/Hostname configuration on page 33	Command line
Monitoring nightly cleanup on page 34	Command line
Monitoring audio provisioning activity on page 35	Command line
Checking APS provisioning activity on page 40	Command line
Checking the APS Oracle database on page 42	Command line
Verifying that the APS CD drive is mounted on page 45	Command line

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

Procedure and page	Interface or Tool used
Set APS security on page 47	Command line
Setting the APS administrator (UNIX) password on page 48	Command line
Restarting the SNMP agent on page 49	Command line
Verifying that the Web server is running on page 51	Command line
Listing APS software load packages on page 53	Command line
Changing the APS Oracle account password on page 54	Command line

Changing the APS GUI password

This procedure enables you to change the password of a user currently logged into the APS GUI. To perform this procedure, you must have a valid user ID and password.

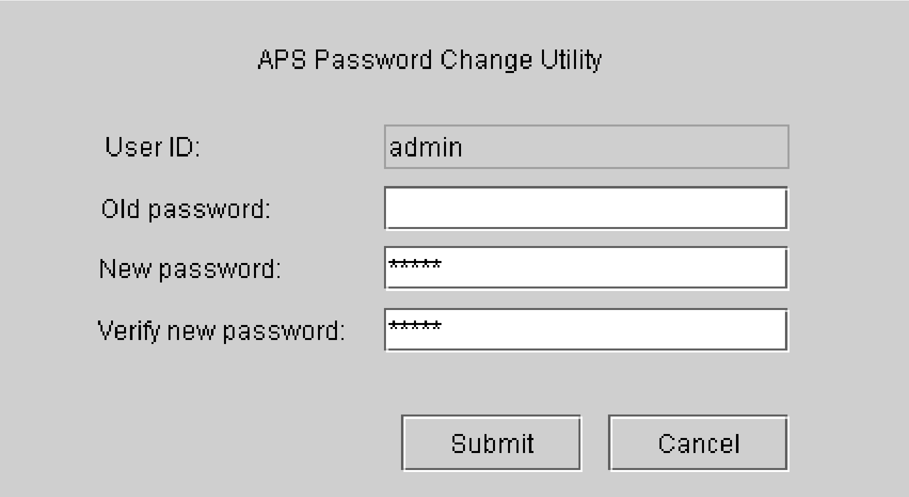
Changing the APS GUI password

At the APS user menu

1 Click Change Password.

The APS Password Change Utility screen opens.

APS Password Change Utility Screen



User ID: admin

Old password:

New password: *****

Verify new password: *****

2 Enter the existing password in the Old password field.

3 Enter the new password in the New password field.

> ***Note:*** The new password must be alphanumeric and 4–8 characters long. The password is also case-sensitive.

4 Reenter the new password in the Verify new password field.

If	Do
you want to submit the password change	step 5
you want to cancel the password change	step 7

5 Click Submit.

The Change Password Result window opens.

6 Click OK. Go to step 8.

7 Click Cancel.

8 You have completed this procedure.

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 APS server 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 APS server 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:

http://*<host name or IP address of the APS>*:8080/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
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 on page 29

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.

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, NN10095-511, entitled “UAS 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: http://<*host name or IP address of the APS*>:8080/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, click the "Go back one page," or equivalent, button located on the tool bar of the Web browser screen.

4 You have completed this procedure.

Changing the CS 2000 Management Tools server IP address

This procedure enables you to change the IP address of the host assigned to receive SNMP traps.

Changing the CS 2000 Management Tools server IP address

At the Network Element Status panel of the Universal Audio Server Manager

1 In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2 In the pull-down list in the box labeled, “Please select,” select Maintenance.

3 In the Maintenance Tree pane, select “Node”.

4 Click the node entry that displays in the table shown in the Node States pane.

5 Lock the node by clicking the “Lock Graceful” button located at the bottom of the Node States pane.

At the Windows desktop interface

6 Stop the UAS applications by performing the following steps:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net stop pmgrdaemon** on the command line

e press Enter

7 To stop the EMANATE master agent, perform the following steps:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **snmpdm -stop** on the command line

e press Enter

8 Launch the Local Configuration Interface GUI by performing the following steps:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **lci** on the command line

e press Enter

> ***Note:*** The first letter in the lci command is an "l", as in "local."

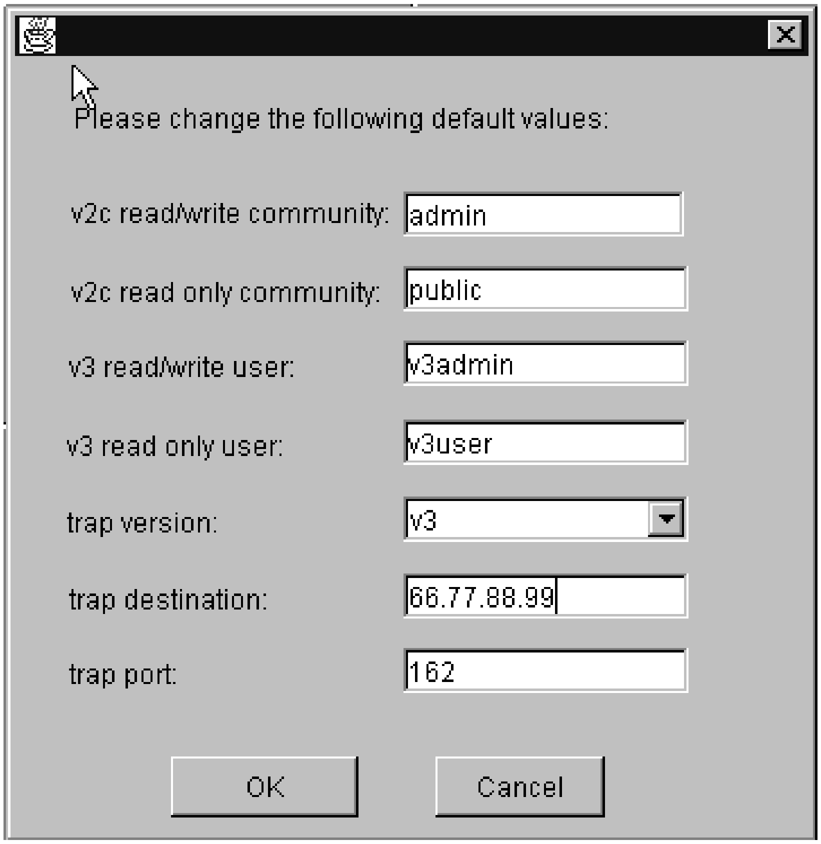
The main Local Configuration Interface GUI screen displays.

9 Select the "node" folder in the Network Element Tree pane.

10 Click the "Reconfigure SNMP" button, located at the bottom of the Local Configuration Interface GUI screen.

The Local Configuration Interface GUI SNMP screen displays.

Local Configuration Interface GUI SNMP screen



Please change the following default values:

v2c read/write community: admin

v2c read only community: public

v3 read/write user: v3admin

v3 read only user: v3user

trap version: v3

trap destination: 66.77.88.99

trap port: 162

a Enter the new IP address in the "trap destination" field in the screen.

b Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step c
you do not want to save the information	step f

c Click OK.

d Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

e Go to step 11.

f Click Cancel.

The “trap destination” entry in the screen fields revert to the existing value.

11 Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting “Exit”.

12 Start the EMANATE master agent, by performing the following steps:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net start snmpdm** on the command line

e press Enter

13 Start the UAS applications by performing the following steps:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net start pmgrdaemon** on the command line

e press Enter

At the Network Element Status panel of the Universal Audio Server Manager

14 In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

15 In the pull-down list in the box labeled, “Please select,” select Maintenance.

16 In the Maintenance Tree pane, select “Node”.

17 Click the node entry that displays in the table shown in the Node States pane.

18 Unlock the node by clicking the “Unlock” button located at the bottom of the Node States pane.

19 You have completed this procedure.

Checking the UAS software configuration

The UAS ConfigMgr utility runs at the time of each program manager restart. The utility performs pending configuration changes and checks the UAS software configuration. The UAS ConfigMgr utility can also be invoked manually, using the following procedure, to validate the UAS configuration.

Checking the UAS software configuration

At the system console (Windows desktop interface)

1 Open a command line by performing the following steps:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

2 Type **configmgr -v** on the command line and press Enter.

A series of messages displays indicating whether the software configuration is correct.

3 You have completed this procedure.

Backing up UAS configuration files

All configuration data supporting the operation of the UAS is stored in configuration files. The configuration files include:

- uas.conf - containing configuration parameters that support the function of the UAS, including CG6000C card settings, Call Agent definition, APS hostname definition, network element settings, and conferencing service state definition
- ugw.conf - containing trunk configuration information for PRI Solutions
- snmpd.cnf - containing parameters that support the SNMP function, including management station address, SNMP user names, community names, and trap version
- hosts - containing parameters that support the function of the APS, including APS hostname and IP address
- atmhard.con - containing ATM bearer interface settings that link a local port ATM address to a particular ATM interface port
- atmconn.con - containing ATM bearer connections settings that provide the UAS with a remote gateway's name and ATM address
- mainsa.conf - containing Main Subagent program settings specifying the kinds of error and log messages to be sent to the management station
- atmSvcProfile.con - containing data on Switched Virtual Channel (SVC) traffic parameters associated with AAL2 SVCs
- atmhardloop.con - containing information associated with the loopback of SVCs

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server. This procedure enables you to set up automatic backup to a remote server.

Backing up UAS configuration files

At the Windows desktop interface

1 This step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server.

- **a** Open a command interface by performing the following steps:
  - **i** select **Start -> Run**
  - **ii** type **cmd** in the window that displays
  - **iii** press Enter
- **b** Open a telnet session to the remote UNIX server and log in as the Root user. Then enter:

```
cd /;mkdir /opt;chmod 777 opt

cd /opt;

mkdir uas;chmod 777 uas

cd uas;

mkdir uas_conf_backup;chmod 777
uas_conf_backup

cd /

cd /opt/uas/uas_conf_backup
```

- **c** Configure NFS to share the “/opt/uas” filesystem and start the NFS server:

```
echo “share -F nfs /opt/uas” >>
/etc/dfs/dfstab
```

> ***Note:*** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

- **d** Create a user login called “Administrator” that does not require a password:

```
/usr/sbin/useradd -d
/export/home/Administrator -g 1 -s /bin/ksh
-m -u 1002 Administrator 2> /dev/null

passwd -d Administrator 2> /dev/null
```

2 At the local system console, enter the IP address of the remote server in the “Backup Storage IP” field of the Local Configuration Interface GUI screen, using the procedure “Modifying

configuration parameters through the Local Configuration Interface GUI" in the document, NN10095-511, entitled "UAS Configuration Management."

3 You have completed this procedure.

Configuring security events for auditing

The UAS install program enables security auditing on the UAS, but does not configure the events. Thus, you must manually configure the events for auditing using the procedure below.

Configuring security events for auditing

At the system console (Windows desktop interface)

1 Open the Local Security Settings dialog window by performing the following:

- **a** Select **Start -> Programs -> Administrative Tools -> Local Security Policy**

2 On the tree panel of the Local Security Settings dialog window (located on the left side of the window), double-click Local Policies.

3 Double-click one of the policy groupings in the listing that displays below **Local Policies** in the tree panel.

4 For each of the policies that then display in the right panel, perform the following:

- **a** Double-click the policy.

  The Local Security Policy Setting dialog window displays.

- **b** Check the “Success” or “Failure” boxes according to the desired settings.

- **c** Click OK.

5 If desired, double-click another policy grouping that displays below **Local Policies** in the tree panel and perform step 4.

6 When you have completed changing the Local Security Settings, close the Local Security Settings dialog window.

7 You have completed this procedure.

Changing the UAS IP/Hostname configuration

This procedure enables you to change the IP address and hostname configuration of the UAS, after the UAS has been installed. In the procedure, the name “domain D” denotes the domain for which the IP address is being changed; “domain D1” denotes the mate domain of the D domain.

Changing the UAS IP/Hostname configuration

At the Network Elements pane of the Universal Audio Server Manager main screen

1 Determine whether you are changing a UAS host name.

If	Do
you are changing a UAS host name	step 2
you are not changing a UAS host name	step 3

2 Perform the procedure, “Configuring the SNMP trap destination” in the document, NN10095-511, entitled “UAS Configuration Management,” to display trap destinations associated with the D domain. Record this trap destination information for use later in this procedure.

3 Using the APS Administration GUI procedure “Disabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” disable audio provisioning for domain D.

4 Using the procedure “Changing the Admin state” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state both for domain D and for domain D1 to “lock graceful.”

After you change the administrative state for each domain, the domain informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to the domain.

5 Using the procedure ”Deleting a UAS or APS from the network topology” in the document, NN10095-511, entitled “UAS Configuration Management,” delete the domain D UAS from the Universal Audio Server Manager network topology.

At the Windows desktop interface, connected to domain D

6 Stop any applications that are running on domain D by performing the following steps:

a Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

At the Windows desktop interface, connected to domain D1

7 Stop any applications that are running on domain D1 by performing the following steps:

a Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

At the Windows desktop interface, connected to domain D

8 Determine whether you are changing the IP address.

If	Do
you are changing the IP address	step 9
you are not changing the IP address	step 14

9 Disassociate the UAS from the Gateway Controller by performing the procedure, “Disassociating a gateway from a Gateway Controller” in the Gateway Controller document, NN10205-511, entitled “GWC Configuration Management.”

10 Using the Notepad tool, edit the host file of domain D and change the IP address associated with domain D, by performing the following steps:

a `select` **`Start -> Run`**

b Enter the following on a single line:

```
Notepad c:\winnt\system32\drivers\etc\hosts
```

c Change the IP address that appears in the following line in the format shown:

```
<IP address> local_sc
```

where <IP address> is the IP address of domain D

d Save the file and close the Notepad window.

At the Windows desktop interface, connected to domain D1

11 Using the Notepad tool, edit the host file of domain D1 and change the IP address associated with domain D, by performing the following steps:

a `select` **`Start -> Run`**

b Enter the following on a single line:

```
Notepad c:\winnt\system32\drivers\etc\hosts
```

c Change the IP address that appears in the following line in the format shown:

```
<IP address> mate_sc
```

where <IP address> is the IP address of domain D

d Save the file and close the Notepad window.

At the Windows desktop interface, connected to domain D

12 Change the IP address for domain D by performing the following steps:

a On the domain D desktop, right-click the “My Network Places” icon and select Properties from the drop-down menu.

The Network and Dial-up Connections window displays.

b In the Network and Dial-up Connections window, right-click Local Area Connection 3 and select Properties from the drop-down menu.

The Local Area Connection 3 Properties window displays.

c In the Local Area Connection 3 Properties window, scroll to Internet Protocol and double-click Internet Protocol (TCP/IP).

The Internet Protocol TCP/IP Properties window displays.

d In the Internet Protocol TCP/IP Properties window, select “Use the following IP addresses” and fill in all fields with the addresses previously obtained from the system administrator, and then click OK.

- **e** In the Local Area Connection 3 Properties window, click OK.
- **f** You may see the prompt, “This connection has empty primary WINS address - do you want to continue?” If this prompt displays, click Yes.
- **g** Close the Network and Dial-up Connection window.

13 Determine whether you are changing a UAS host name.

If	Do
you are changing a UAS host name	step 14
you are not changing a UAS host name	step 21

At the Windows desktop interface, connected to domain D1

14 Perform the following steps:

- **a** open a command window by selecting **Start -> Run**
- **b** type **cmd** in the window that displays
- **c** press Enter
- **d** type **del c:\globalserver\etc\ems\alarms.txt** on the command line
- **e** press Enter

At the Windows desktop interface, connected to domain D

15 Perform the following steps:

- **a** open a command window by selecting **Start -> Run**
- **b** type **cmd** in the window that displays
- **c** press Enter
- **d** type **del c:\globalserver\etc\ems\alarms.txt** on the command line
- **e** press Enter

16 Change the name of domain D by performing the following steps:

- **a** Double-click My Computer
- **b** Select Properties in the drop-down menu that displays.

c In the System Properties window that displays, select the Network Identification tab.

d In the window that displays, click Properties.

The Identification changes window displays.

e In the “Computer name” field, enter the new host name.

f Click OK.

g In response to the request to reboot, click OK.

h After the reboot has completed, stop any applications that are running on domain D by performing the following steps:

i Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

ii Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

17 Stop the snmp master agent by performing the following steps:

a open a command window by selecting **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net stop snmpdm** on the command line

e press Enter

18 Launch the Local Configuration Interface GUI by performing the following step:

a open a command window by selecting **Start -> Run**

b type **lci** in the window that displays

Note: The first letter in the lci command is an “l”, as in “local.”

c click OK or press Enter

The Local Configuration Interface GUI screen displays.

d select the “node” folder in the Network Element Tree pane

19 At the LCI GUI screen, click the “Reconfigure SNMP” button, located at the bottom of the Local Configuration Interface GUI screen.

The Local Configuration Interface GUI SNMP screen displays.

a Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write use**r

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP trap version used by the SNMP-based management station for handling trap events.

- **trap destination**

  This is the destination IP address associated with the remote SNMP management station.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

Note: The LCI GUI updates the hostname in the SNMP master agent configuration file, even though the hostname is not shown among the fields that you datafill.

b At the bottom of the screen, click OK.

c Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

20 Start the snmp master agent by performing the following steps:

a open a command window by selecting **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net start snmpdm** on the command line

e press Enter

21 Restart domain D application processes by performing the following steps:

- **a** Access the “Services” window as follows:

  Start -> Programs -> Administrative Tools -> Services

- **b** Right-click PMGRdaemon service and select Start.

If	Do
you are changing the IP address	step 22
you are not changing the IP address	step 23

22 Associate the UAS with the Gateway Controller by performing the procedure, “Associating a media gateway with a Gateway Controller” in the Gateway Controller document, NN10205-511, entitled, “GWC Configuration Management.” When you associate the UAS with the Gateway Controller, ensure that the signal protocol type, MEGACO/H.248 is specified.

At the Windows desktop interface, connected to domain D1

23 Restart domain D1 application processes by performing the following steps:

- **a** Access the “Services” window as follows:

  Start -> Programs -> Administrative Tools -> Services

- **b** Right-click PMGRdaemon service and select Start.

At the Network Elements pane of the Universal Audio Server Manager main screen

24 Using the procedure “Adding a UAS or APS to the network topology” in the document, NN10095-511, entitled “UAS Configuration Management,” add the UAS domain D to the Universal Audio Server Manager network topology.

25 After the network element has restarted (that is, the network element appears in the Network Elements pane), set the administrative state for both domain D and domain D1 to “unlocked” by performing the procedure “Changing the Admin state” in the document, NN10073-911, entitled “UAS Fault Management”.

Each UAS domain informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the domain.

If	Do
you are changing a UAS host name	step 26
you are not changing a UAS host name	step 27

26 Perform the procedure, “Configuring the SNMP trap destination” in the document, NN10095-511, entitled “UAS Configuration Management,” using the information that you recorded in step 2.

27 Associate the APS with this UAS node (domain D) at the node’s new address and/or with its new name, by performing the following steps:

- **a** Perform the procedure “Deleting a UAS node” in the document, NN10095-511, entitled “UAS Configuration Management,” to disassociate domain D from the APS.
- **b** Perform the procedure “Creating a UAS node” in the document, NN10095-511, entitled “UAS Configuration Management” to re-associate domain D with the APS, at domain D’s new IP address and/or with its new name.

28 Enable audio distribution at the APS for domain D by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management”.

29 You have completed this procedure.

Using NetMeeting with the UAS

NetMeeting is a remote console control application that is intended for use on Universal Audio Server nodes that are not in service. The following procedure enables you initiate a remote control session with a UAS node, using the NetMeeting application.

> ***Note 1:*** Use of this application for configuration, diagnostics, and software installation on an in-service node can have detrimental effects on the call processing capabilities of the UAS. Thus, it is important that you ensure that the UAS has been removed from service prior to initiating a remote control session through NetMeeting.
>
> ***Note 2:*** When a remote control session with a UAS node is initiated, the local terminal loses control of all keyboard and mouse functionality until the session is terminated.

Using NetMeeting with the UAS

At the Windows desktop interface

1 select **Start -> Programs -> Accessories -> Communications -> NetMeeting**

2 In the NetMeeting GUI window that displays, click Place Call, located on the right side of the window.

3 In the Place a Call GUI window that display, enter the IP address of the UAS node you wish to access. Ensure that the “Require security for this call (data only)” checkbox is selected.

4 Click the “call” button.

5 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 1.4.1. 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 should detect and use the correct JRE 1.4.1 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 should detect and report 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 on page 6 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 server 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 UAS 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 APS server

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 APS server

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
```

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, refer to 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:

```
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 on page 31.

Monitoring audio provisioning activity

In a telnet connection to the APS server

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

2 Become the “root” user by entering:

```
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 the number of free bytes and blocks within each, displays.

> ***Note:*** Although this data may require more detailed review to determine system health, by looking for free-space values at or near zero you should be able to 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 UAS 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 UAS 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 of the system parameters displays. The parameters include:

- 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_PROVISIION_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 UAS system. This helps you ensure that the audio you have created using the APS GUIs has actually been provisioned to a UAS.

Checking APS provisioning activity

In a telnet connection to the APS server

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

2 Become the "root" user by entering:

```
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 UAS unit.

Each time a provisioner process runs, an entry is appended to the log for the related APS server, in the format:

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 APS server, in the format:

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 APS server, in the format:

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 APS server

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

2 Become the “root” user by entering:

```
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 should display.

- **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 should display.

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 should display:

```
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 APS server 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 should indicate 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 APS server

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 should 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, “use 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 should show 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 should 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 APS server 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 NN10095-511, entitled, “UAS Configuration Management”), choosing user passwords that 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 Administration and Security 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 APS server by creating a UNIX Administrator password.

Setting the APS administrator (UNIX) password

At the system console (Windows desktop interface)

1 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.

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

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

4 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 on page 31.

Restarting the SNMP agent

In a telnet connection to the APS server

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:

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

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

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:

```
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/APSagentctl 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 should display.

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:

```
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:

Start up Netscape or Internet Explorer.

Enter the URL for the APS GUI in your Web browser: http://*<ip address of the APS>*:8080/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 APS server processes:

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

a Go to step 8.

5 Log in as the “root” user.

6 Enter the IP address of the APS server in the browser address window.

An Application Launch Point page should display.

If	Do
the Application Launch Point page displays	step 8

If	Do
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 APS server. You may, instead, choose to use your web browser to view this information; refer to the procedure, Listing APS patches and releases on page 10.

Listing APS software load packages

In a telnet connection to the APS server

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 to list the installed software packages on the APS server:

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

A list of the installed software packages displays.

4 If you would like a count of all installed application software packages on the APS server, enter the following command:

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

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

5 If you would like 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: http://*<ip address of the APS>*:8080/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 APS server

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

2 If you are unsure whether the password has been changed, obtain the current password by entering the following command:

```
getNTDBpasswd.ksh
```

The system displays the current Oracle account password.

3 Become the "Oracle" user by entering the following command:

```
su - oracle
```

4 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 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.

e Enter the following command to exit from the Oracle user account:

```
exit
```

This causes you to become the "root" user again.

5 Restart the APS processes by entering the following command:

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

A message eventually displays indicating that the server is restarting.

6 Enter the following commands to complete the password change:

```
cd /
. /etc/profile
. ./.profile
```

7 You can now check the password change you have made by entering the following command:

```
getNTDBpasswd.ksh
```

The system displays the current Oracle account password.

8 You have completed this procedure.