UAS Security and Administration

UAS administration and security activities include changing system passwords, checking system configuration, and backing up the database. 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.

Note: For Audio Provisioning Server (APS) related administration and security activities refer to the *Media Server 2000 Series Administration and Security* document.

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 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	LCI GUI
Checking the UAS software configuration	Command line
Backing up UAS configuration files	Command line
Configuring security events for auditing	Windows desktop interface
Changing the UAS IP/Hostname configuration	UAS Manager
Using NetMeeting with the UAS	NetMeeting

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.”

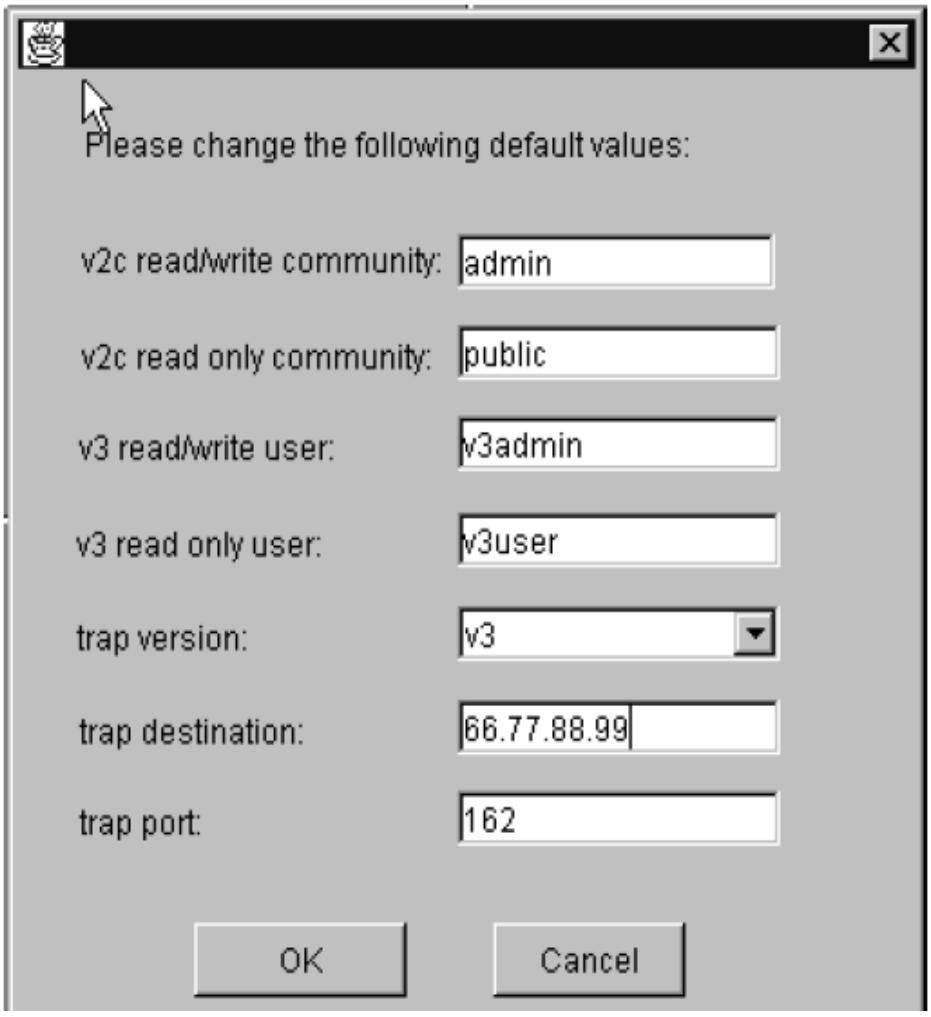
The main Local Configuration Interface GUI screen displays.

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



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 user**

  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.