CS 2000 Core Manager Security and Administration

This document describes the administration and security features and operating procedures for the core manager.

What's new in CS 2000 Core Manager Security and Administration in SN09

Features changes

The following feature-related changes have been made in the documentation:

- The SDM to support SAML NSS switch client feature required the addition of the following procedures:
  - Checking the configuration of the security services
  - Migrating core manager user accounts to IEMS
  - Selecting the server for authentication services
  - Deleting IEMS user entries from /etc/passwd after upgrade to SN09

Other changes

There are no other changes in this release.

Logging in to the CS 2000 Core Manager

Purpose

Use this procedure in a standalone system to log in to the CS 2000 Core Manager.

Prerequisites

You must be a user authorized to perform actions associated with the procedure.

For information on how to display actions a user is authorized to perform or how to display information about a user or role group, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Displaying actions a user is authorized to perform	15
Displaying information about a user or role group	20

Application

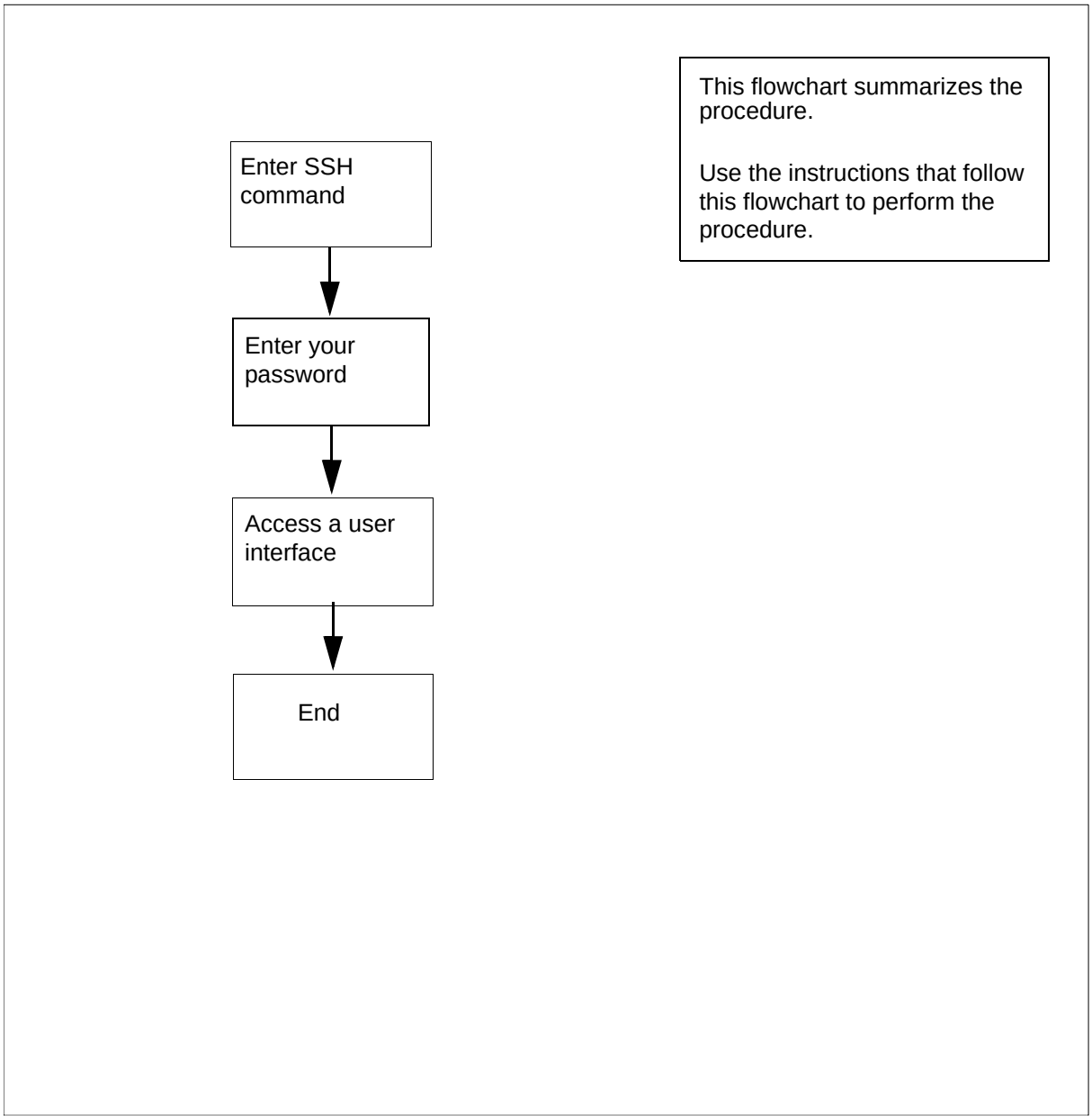
It is recommended that you log in to the CS 2000 Core Manger through SSH (secure shell) using a password.

For a complete description of login methods, refer to CS 2000 Core Manager Basics, NN10018-111.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

Summary of Logging in to the CS 2000 Core Manager



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Logging in to the CS 2000 Core Manager

At the local or remote VT100 console

1 Log in to the CS 2000 Core Manager using one of the following commands for SSH access:

ssh <userID>@<IPaddress | hostname>

or

ssh -l <userID> <IPaddress | hostname>

where

<userID>
is your userID

<IPaddress>
is the IP address of the CS 2000 Core Manager

<hostname>
is the host name for the CS 2000 Core Manager

Example response:

```
Don_secu's Password:
```

2 Enter your password.

Example response:

```
(put example here)
```

3 Access a user interface, for example, access the maintenance interface:

sdmmtc

Example response:

```
(put example here)
```

4 Exit the maintenance interface:

quit all

5 You have completed this procedure.

Adding or removing a user to or from a role group

Purpose

Use this procedure in a standalone system to add or remove a user to or from a role group.

Prerequisites

You must be a user authorized to perform security-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

Role groups allow you to group individual users according to the task each user has to complete. When you assign groups according to the authorization level for a task, you increase the security of your system. For example, if a user performs backup tasks only, you can add the user to the emsadm role group instead of making the user a root user.

The following table lists the standard actions for each role group in a standalone system.

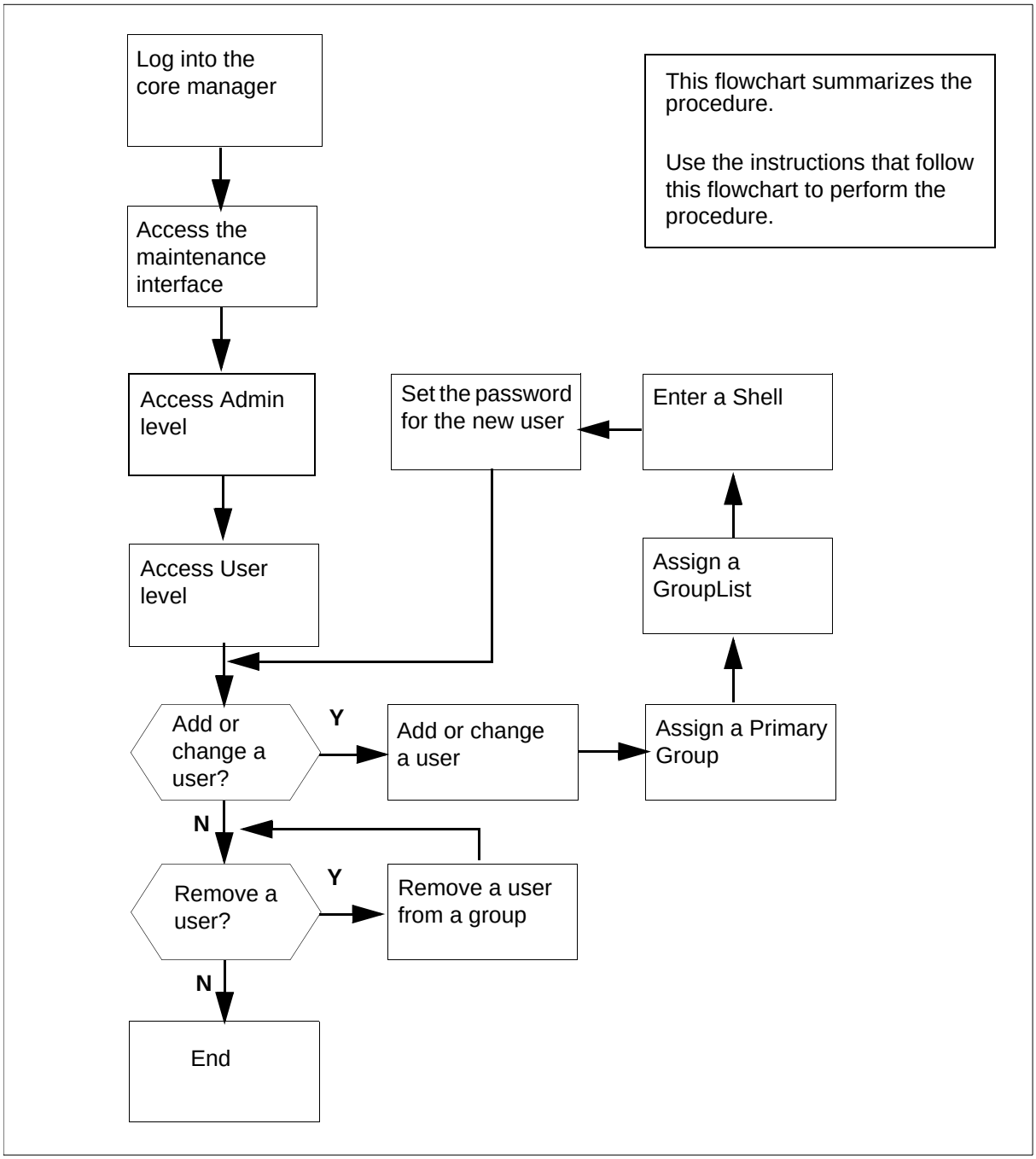
Standard actions for each role group

Role Group	Standard Action
root (user)	all actions
emsadm	fault-view, fault-manage, fault-admin, accounting-admin, config-view, config-manage, config-admin, accounting-view, accounting-manage, accounting-admin, performance-view, performance-manage, performance-admin
secadm	security-view, security-manage, security-admin
maint	fault-view, fault-manage, config-view, config-manage, accounting-view, accounting-manage, performance-view, performance-manage
passthru	
Gr740Oss	performance-manage

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

Summary of Adding or removing a user to or from a role group



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Adding or removing a user to or from a role group

At the local or remote VT100 console

1. Log into the core manager as a user authorized to perform security-admin actions.
2. Access the maintenance interface:

   sdmmtc
3. Access the Admin level:

   admin
4. Access the User level:

   user

   Example response:

```
    SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
    ISTb  ISTb   .C   ISTb  ISTb     Host: wcar8e9
     M                 M                  Fault Tolerant
User
 0 Quit
 2             Role Group      Users
 3 PassThru    maint           maint, fred, ty
 4             secadm          cal, peter
 5             emsadm          task1, task2
 6
 7
 8                     Role Groups: 1 to 3 of 3
 9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help
18 Refresh
  cal
Time  12:54  >
```

If you want to	Do
add a user to a role group	step 5
change the role group, shell, or password of a user	step 13
remove a user from a role group	step 21

5 Add a user to a role group:

add *<userID>*

where

<userID>
is the userID of the new user

Example response:

```
Add User - Primary Group
Enter the new Primary Group for TaskA : [maint]
```

6 Enter the new Primary Group:

<primary group>

where

<primary group>
is maint, secadm, or emsadm

Example response:

```
Add User - Group List
Enter the Group List for TaskA : [maint}
```

If you want to	Do
add the user to another group	step 7
continue to the next prompt	press enter and go to step 8

7 To assign another role group to the user, enter another group:

<group>

where

<group>
is maint, secadm, or emsadm

Note: You can assign more than one group at a time by separating the groups by a comma or by a blank space as shown below.

<group1>,<group2>

or

<group1> <group2>

Example response:

```
Add User - Shell
Enter the new Shell for TaskA : [rash]
```

8 Enter the new Shell:

<shell>

where

<shell>
is rash or fash (nash should not be used)

for secadm and emsadm groups, use fash (full shell)

for maint group, use rash (restricted shell)

Example response:

```
Add User - Change Password?
Do you wish to change the password?
Please confirm for user TaskA
("YES", "Y", "NO", or "N"):
```

9 Confirm that you want to change the password:

Y

Example response:

```
Add User - Change Password
Changing password for TaskA
TaskA's New password:
```

10 Enter the password for the new user, and press the Enter key.

The password must be at minimum a six-character string containing at least one alphabetic character, and at least one

numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

Example response:

```
Add User - Change Password
Enter the new password again
```

11 Enter the password again.

Example response:

```
Add User - Change Password
Press [Enter] to continue...
```

12 Press enter to continue.

Example response:

```
Add TaskA - Command complete.
```

If you	Do
want to add another user	step 5
want to change the role group, shell, or password of a user	step 13
do not want to add another user	step 23

13 Change the role group, shell, or password of a user:

`change <userID>`

where

<userID>
is the userID of an existing user

Example response:

```
Change User - Primary Group
Enter the new Primary Group for TaskA : [maint]
```

14 Enter the new Primary Group:

`<primary group>`

where

<primary group>
is maint, secadm, or emsadm

Example response:

```
Change User - GroupList
Enter the GroupList for TaskA : [maint}
```

If you want to	Do
add the user to another group	step 15
continue to the next prompt	press enter and go to step 16

15 To assign another role group to the user, enter another Group:

<group>

where

<group>
is maint, secadm, or emsadm

Note: You can assign more than one group at a time by separating the groups by a comma or by a blank space as shown below.

<group1>,<group2>

or

<group1> <group2>

Example response:

```
Change User - Shell
Enter the new Shell for TaskA : [rash]
```

16 Enter the new Shell:

<shell>

where

<shell>
is rash or fash (nash should not be used)

for secadm and emsadm groups, use fash (full shell)

for maint group, use rash (restricted shell)

Example response:

```
Change User - Change Password?
Do you wish to change the password?
Please confirm for user TaskA
("YES", "Y", "NO", or "N"):
```

17 Confirm that you want to change the password:

Y

Example response:

```
Change User - Change Password
Changing password for TaskA
TaskA's New password:
```

18 Enter the password for the new user, and press the Enter key.

The password must be at minimum a six-character string containing at least one alphabetic character, and at least one numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

Example response:

```
Change User - Change Password
Enter the new password again
```

19 Enter the password again.

Example response:

```
Change User - Change Password
Press [Enter] to continue...
```

20 Press enter to continue.

Example response:

```
Add TaskA - Command complete.
```

If you	Do
want to make another change to the role group	step 13
do not want to make another change to the role group	step 23

21 Remove a user:

`delete <userID>`

where

<userID>
is the userID of the user

Example response:

Are you sure you want to delete this user?

Do you wish to proceed?

Please confirm ("YES", "Y", "NO", or "N"):

Caution: A user should not be deleted if the user has login sessions currently active. Deleting a user does not terminate any of the user's currently-active login sessions and could, therefore, potentially result in security issues.

To determine which users have currently-active login sessions, enter the following command on the command line:

who

Example response:

```
root    pts/1    Apr 25 13:13    (47.110.112.44)
lsec    pts/2    Apr 25 14:55    (47.110.114.170)
.
.
```

To determine whether a specific user has currently-active login sessions, enter the following command on the command line:

who | grep <userID>

where

<userID>
is the userID of the user

If the user has currently-active login sessions, the system will display only the information about the user's login sessions.

22 In response to the prompt, either confirm that you do want to delete the user or that you don't want to delete the user:

Y <or> N

Example response when the deletion has been confirmed:

```
Delete TaskA - Command complete.
```

If you	Do
want to delete another user	step 21
do not want to delete another user	step 23

23 Exit the maintenance interface:

quit all

24 You have completed this procedure.

Displaying actions a user is authorized to perform

Purpose

Use this procedure in a standalone system to display the actions a user in a particular role group is authorized to perform.

Prerequisites

You must be a user authorized to perform security-view actions.

For information on how to log in to the core manager or how to display other information about a user or role group, review the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the core manager	2
Displaying information about a user or role group	20

Application

Role groups allow you to group individual users according to the task each user has to complete. The following table lists the standard actions for each role group in a standalone system.

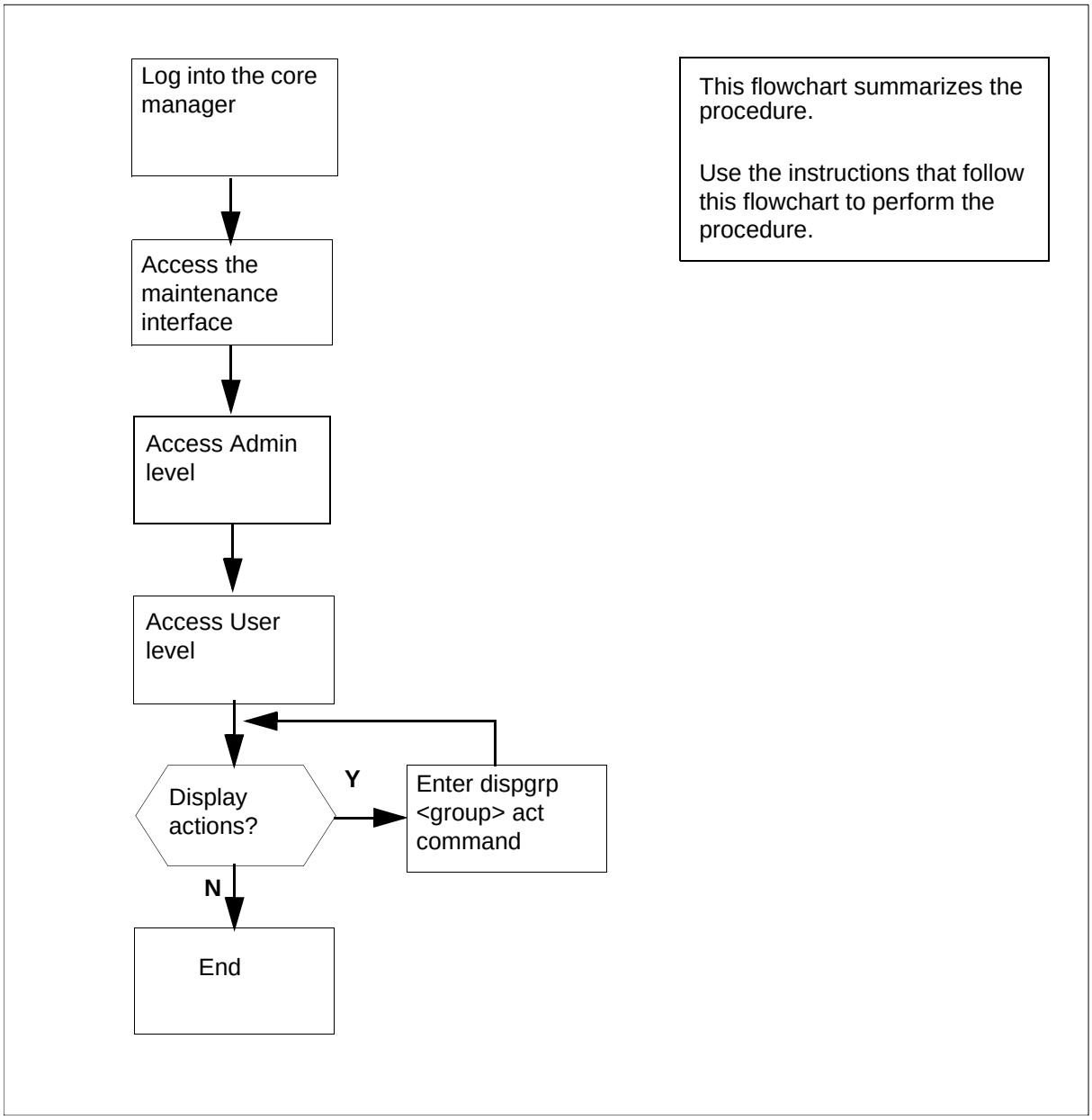
Standard actions for each role group

Role Group	Standard Action
root (user)	all actions
emsadm	fault-view, fault-manage, fault-admin, accounting-admin, config-view, config-manage, config-admin, accounting-view, accounting-manage, accounting-admin, performance-view, performance-manage, performance-admin
secadm	security-view, security-manage, security-admin
maint	fault-view, fault-manage, config-view, config-manage, accounting-view, accounting-manage, performance-view, performance-manage
passthru	
Gr740Oss	performance-manage

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

Summary of Displaying actions a user is authorized to perform



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Displaying actions a user is authorized to perform

At the local or remote VT100 console

1. Log into the core manager as a user authorized to perform security-view actions.
2. Access the maintenance interface:

   sdmmtc
3. Access the Admin level:

   admin
4. Access the User level:

   user

   Example response:

```
    SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
    ISTb  ISTb   .C   ISTb  ISTb     Host: wcar8e9
     M                  M                  Fault Tolerant
User
 0 Quit
 2              Role Group      Users
 3 PassThru     maint           maint, fred, ty
 4              secadm          cal, peter
 5              emsadm          task1, task2
 6
 7
 8                      Role Groups: 1 to 3 of 3
 9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help
18 Refresh
  cal
Time  12:54  >
```

5 Display actions a user in a particular role group is authorized to perform:

dispgrpr <group> act

where

<group>
is maint, secadm, or emsadm

Example response:

```
Authorized actions for secadm
security-admin
security-manage
security-view
```

6 Exit the maintenance interface:

quit all

7 You have completed this procedure.

Displaying information about a user or role group

Purpose

Use this procedure in a standalone system to display information about a user or role group.

In this procedure you can display the following information about users and groups:

- a list of users in a role group
- a list of all role groups and users
- shell, location, and group associated with a user
- a list of all users and role groups

Prerequisites

You must be a user authorized to perform security-view actions.

For information on how to log in to the CS 2000 Core Manager or how to add or remove a user, review the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	20

Application

Role groups allow you to group individual users according to the task each user has to complete. The following table lists the standard actions for each role group in a standalone system.

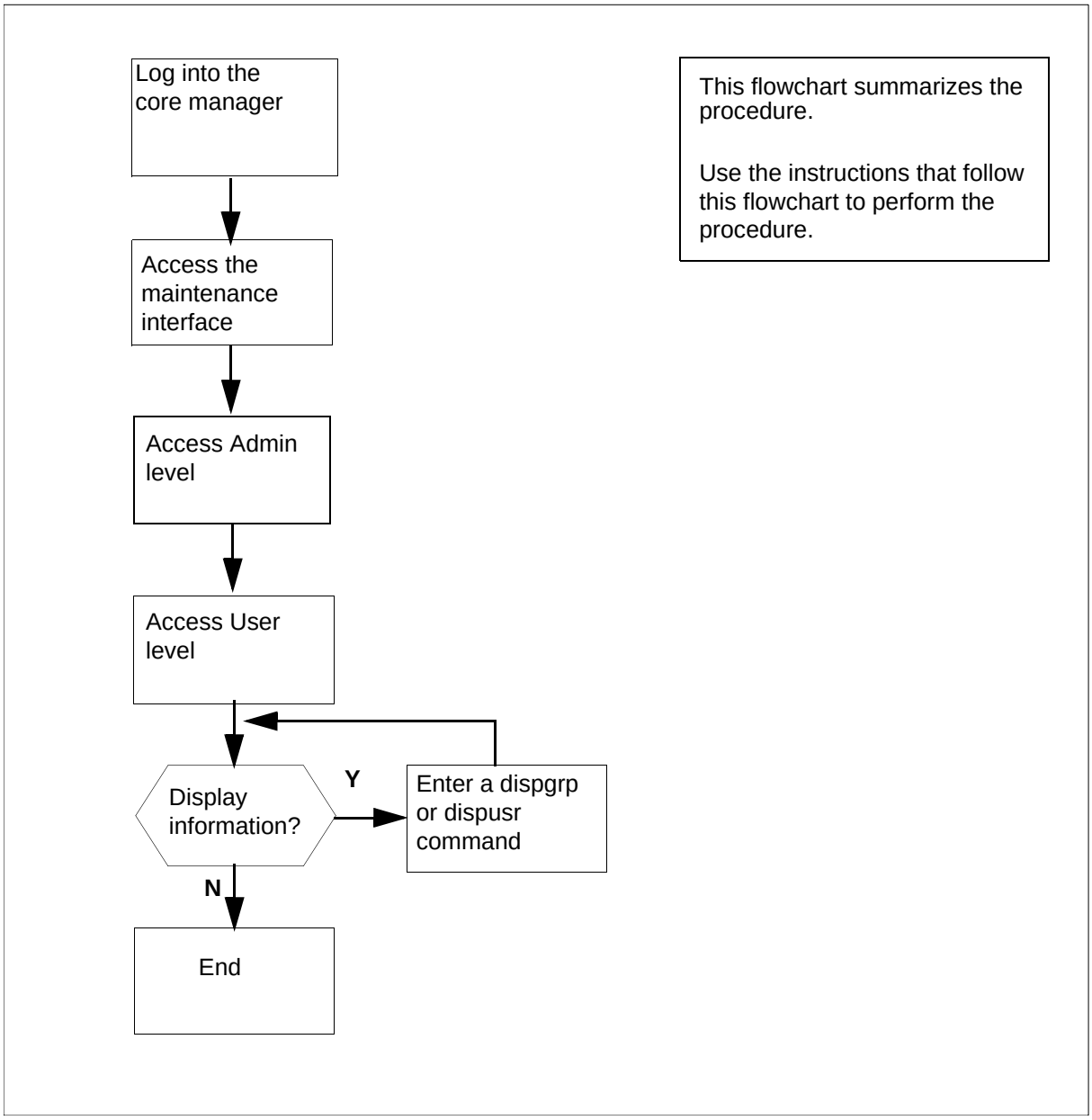
Standard actions for each role group

Role Group	Standard Action
root (user)	all actions
emsadm	fault-view, fault-manage, fault-admin, accounting-admin, config-view, config-manage, config-admin, accounting-view, accounting-manage, accounting-admin, performance-view, performance-manage, performance-admin,
secadm	security-view, security-manage, security-admin
maint	fault-view, fault-manage, config-view, config-manage, accounting-view, accounting-manage, performance-view, performance-manage
passthru	
Gr740Oss	performance-manage

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

Summary of Displaying information about a user or role group



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Displaying information about a user or role group

At the local or remote VT100 console

1 Log into the core manager as a user authorized to perform security-view actions.

2 Access the maintenance interface:

sdmmtc

3 Access the Admin level:

admin

4 Access the User level:

> user

Example response:

```
    SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
    ISTb  ISTb   .C   ISTb  ISTb     Host: wcar8e9
     M                  M                  Fault Tolerant
User
 0 Quit
 2              Role Group      Users
 3 PassThru     maint           maint, fred, ty
 4              secadm          cal, peter
 5              emsadm          task1, task2
 6
 7
 8                      Role Groups: 1 to 3 of 3
 9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help
18 Refresh
  cal
Time  12:54  >
```

If you want to	Do
display a list of users in a role group	step 5
display a list of all role groups and users	step 7
display information about a user	step 9
display a list of all users and role groups	step 11
exit	step 12

5 Display a list of users in a particular role group:

`dispgrp <group>`

where

***<group>* is maint, secadm, or emsadm**

Example response:

```
emsadm Users
1 task1
2 task2
```

6 Go to step 12.

7 Display a list of all role groups and users:

`dispgrp`

Example response:

```
Role Group        Users
1 maint            maint, fred, ty1
2 secadm           cal, peter
3 emsadm           task1, task2
           Role Groups: 1 to 3 of 3
```

8 Go to step 12.

9 Display information about a particular user:

`dispusr <userID>`

where

***<userID>* is the userID of the new user**

Example response:

```
pgrp     emsadm
groups   emsadm
home     /home/task1
shell    /bin/fash
```

10 Go to step 12.

11 Display a list of all users and groups:

dispusr

Example response:

```
User                Groups
maint               maint
bob                 emsadmm
jo                  secadm
fred                secadm, emsadm
sue                 maint, secadm, emsadm
```

12 Exit the maintenance interface:

quit all

13 You have completed this procedure.

Checking the configuration of the security services

Purpose

Use this procedure to check the configuration of the security services.

Prerequisites

You must be a user authorized to perform security-view actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Procedure

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Checking the configuration of the security services

At the local or remote VT100 console

1 Log into the core manager as a user authorized to perform security-view actions.

2 Access the maintenance interface:

```
sdmmtc
```

3 Access the Admin level:

```
admin
```

4 Access the Security Services:

```
secuconf
```

Example response:

```
    SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
    ISTb  ISTb   .C   ISTb  ISTb     Host: wcar8e9
     M                 M                  Fault Tolerant
SecuConf
 0 Quit
 2 Add          1 Authentication Naming Service: LOCAL
 3 Change
 4 Delete       2 Authentication PAM Stack: LOCAL
 5
 6 Next         3 Remote Security Log Destination: -
 7 Prev
 8              4 Remote Audit Log Destination: -
 9 List
10 Step
11
12 Up
13 Down
14
15
16
17 Help
18 Refresh
  alex
Time  12:54  >
```

Note: For this release, LOCAL is the default.

5 You have completed this procedure. To configure security services, refer to the following procedures:

Security services procedures

Procedure	Page
Migrating local user accounts to IEMS	28
Selecting the server for authentication services	42

Migrating core manager user accounts to IEMS

Purpose

Use this procedure to migrate core manager local user accounts to the external security server, Integrated Element Management Server (IEMS).

Prerequisites

Before you can migrate local user accounts to the IEMS, the following tasks must be completed.

- The "Authentication Naming Service" must be set to SAML and the "Authentication PAM Stack" must be set to the IEMS.
- The PAM Radius module and the Radius Group Module must be installed.
- The IEMS centralized security server must be available and configured, and it must be selected as the authentication server

Logging in to the CS 2000 Core Manager

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

Logging into the Core and Billing Manager 850

You must log in as the root user.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedures

Local core manager user accounts can be migrated to the IEMS secure server either manually or through the exportLocalUser program. The

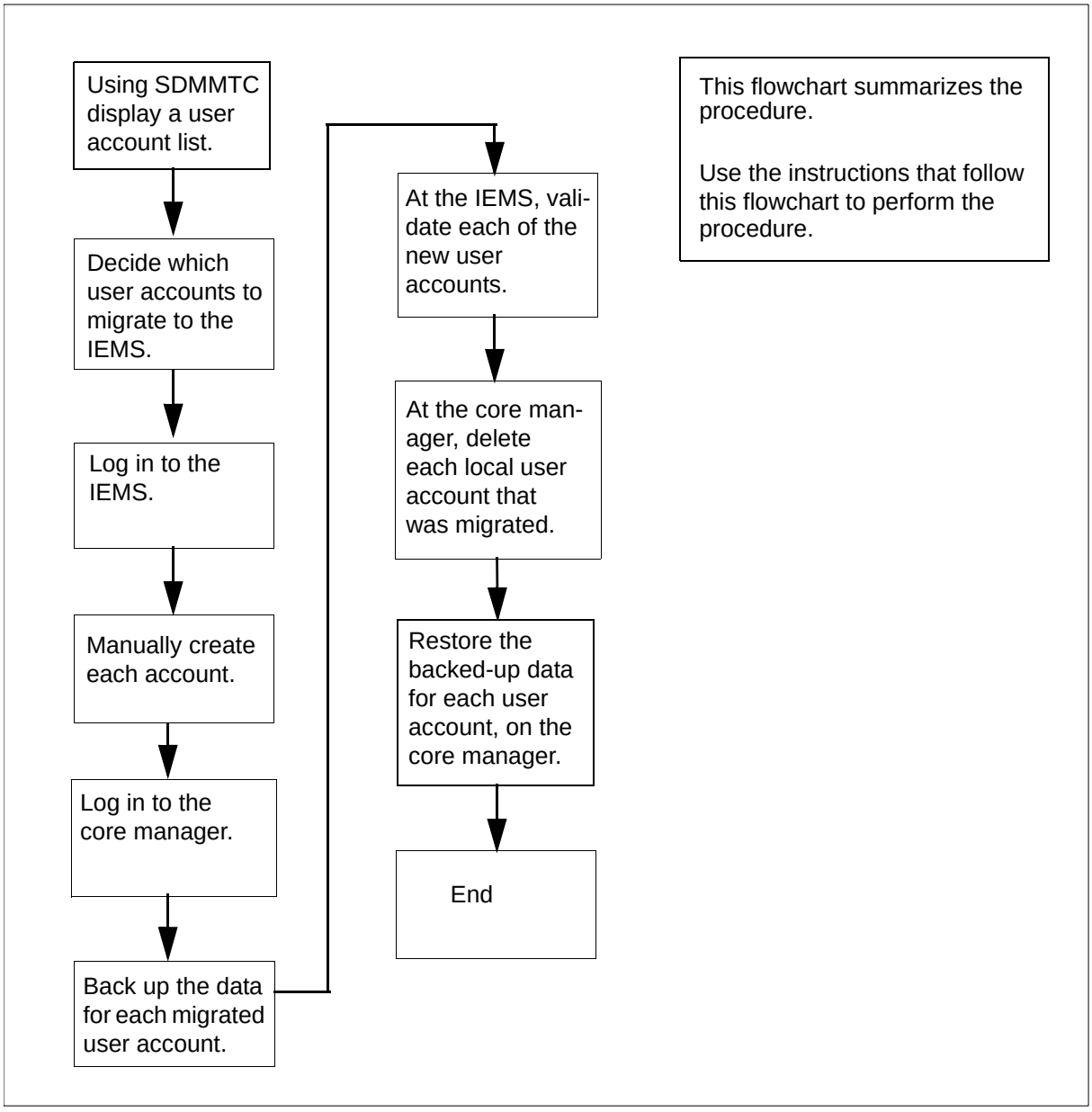
manual migration method requires that you migrate each user account one-at-a-time on the IEMS. The exportLocalUser program, in contrast, enables you to migrate multiple user accounts efficiently, in a single session. The following table shows the procedures used to perform these two methods of user account migration to the IEMS.

Procedures for migrating core manager user accounts to the IEMS
Migrating users to the IEMS manually on page 30 Migrating user accounts to the IEMS using exportLocalUser on page 32

Migrating users to the IEMS manually

The following flowchart provides a high-level overview of the procedure. Use the instructions in the step-action procedure that follows this flowchart to perform the task.

Migrating local core manager user accounts to the IEMS manually



Migrating users to the IEMS manually

At the IEMS security server

1 Obtain a list of users to migrate to the IEMS by performing Obtaining a list of users to migrate to the IEMS on page 36

2 For each user account that you want to migrate, manually create the account on the IEMS security server. Refer to the IEMS OUFCAPS documentation for procedures.

3 Back up the local core manager user accounts that you have created versions of on the IEMS, using the procedure Backing up user accounts on the core manager on page 37

4 Remove the local user accounts on the core manager, using procedure Removing user accounts from the core manager on page 39

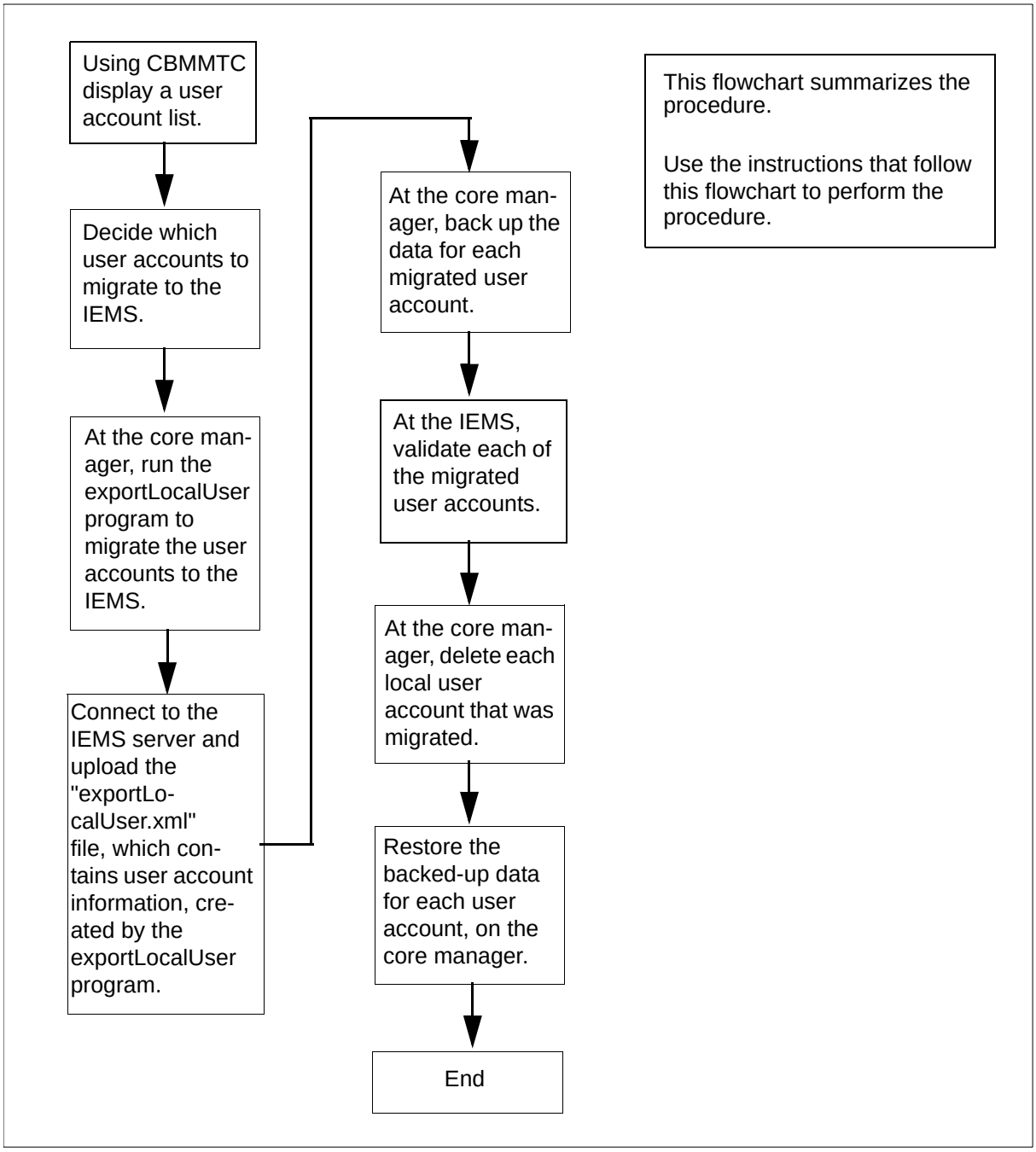
5 Restore the data you backed up in step 3 for each of the user accounts you migrated to the IEMS, using the procedure Restoring user accounts to the core manager on page 40

6 You have completed this procedure.

Migrating users to the IEMS using exportLocalUser

The following flowchart provides a high-level overview of the procedure. Use the instructions in the step-action procedure that follows this flowchart to perform the task.

Migrating local core manager user accounts to the IEMS using exportLocalUser



Migrating user accounts to the IEMS using exportLocalUser

At the core manager

1 Obtain a list of users to migrate to the IEMS by performing Obtaining a list of users to migrate to the IEMS on page 36

2 When the exportLocalUser program runs, it creates two files, "exportLocalUser.xml" and "exportLocalUser.txt". Change directory to the directory that will contain these two files:

```
cd <directory path>
```

where

<directory path>
is the full path of the directory that will contain the two files generated by the exportLocalUser program

3 Verify that the two files, "exportLocalUser.xml" and "exportLocalUser.txt" are not already present in the directory:

```
ls -IRa
```

4 Run the "exportLocalUser" program:

```
exportLocalUser <directory path> <IEMS server domain name>
```

where

<directory path>
is the location of the user accounts to migrate

<IEMS server domain name>
is the domain name of the IEMS server to which the user accounts will be migrated. For example: ca.nortel.com

Example system response:

```
Start scanning local users for migration ...
Local user: user_id_1 has been added to the list
of
   users for migration
   user_id_1 will be a member of IEMS
group:emsadm
Local user: user_id_2 has been added to the list
of
   users for migration
   user_id_2 will be a member of IEMS
group:emsmtc

Scanning local users for user migration to IEMS
is completed
Files: /home/root/exportLocalUser.xml and
/home/root/exportLocalUser.txt are created.

/home/root/exportLocalUser.xml should be sent
to IEMS -
It will be needed by IEMS bulk import script to
import these local users.

/home/root/exportLocalUser.txt contains the
list of local users for migration -
These users should be deleted from this system
when they are migrated to IEMS successfully.

Script executed successfully.
```

5 When the system indicates that the program was successfully executed, display the "exportLocalUser.txt" file:

`cat /<directory_path>/exportLocalUser.txt`

The file contains a list of the users you are migrating to the IEMS.

Example
The following users should be deleted from the local system when the users are migrated to IEMS successfully:

user_id_1
user_id_2

---End of list---

Using this list, you should verify that all of the users you are migrating to the IEMS are listed. If any user is not shown in this

list, migrate the user at a different time using the procedure Migrating users to the IEMS manually on page 30

Record this list of users for reference later on in this procedure.

6 Connect to the IEMS server as the root user and prepare to transfer the newly-created .xml file for users being migrated.

Example
The following example shows the commands that would be used for secure file transfer:

```
sftp <IP address>
```

where

<IP address>
is the IP address of the IEMS server to which the .xml file will be sent.

7 Upload the "exportLocalUser.xml" directory to the home directory:

```
put exportLocalUser.xml
```

8 At the IEMS, bulk import the "exportLocalUser.xml" directory:

```
/opt/nortel/applications/security/current_core
/bin/is_bulk_import.sh -uidNumberAssignment
50000:99999 exportLocalUser.xml
```

Example system response:

```
Please enter the amAdmin password: ***********
addUser -- Successfully added user user_id_1
addUser -- Successfully added user user_id_2
addUserRoleAssoc -- Successfully assigned user
uid=user_id_1,ou=People,o=ca.nortel.com to role
cn=emsmtc,o=ca.nortel.com
addUserRoleAssoc -- Successfully assigned user
uid=user_id_2,ou=People,o=ca.nortel.com to role
cn=emsadm,o=ca.nortel.com
NOTE: Operation succeeded.
```

Note: In this example, the first sentence is a request for the "amAdmin" password. This is the SAML server password.

You should record this log for future reference.

9 Close the connection to the IEMS.

10 At the core manager, retrieve the list of user accounts that you recorded in step 5. Back up these user accounts using the procedure Backing up user accounts on the core manager on page 37

11 At the IEMS, you will need to confirm that each of the users that you migrated can log into the core manager from the IEMS.

12 After you have confirmed in step 11 that all of the user accounts that you migrated to the IEMS are valid, at the core manager remove the local user accounts, using procedure Removing user accounts from the core manager on page 39

13 Restore the data you backed up in step 10 for each of the user accounts you migrated to the IEMS, using the procedure Restoring user accounts to the core manager on page 40

14 Remove the "exportLocalUser.txt" and "exportLocalUser.xml" files created by the exportLocalUser program during the migration:

```
cd <directory path>
```

where

<directory path>
is the full path of the directory containing the two files generated by the exportLocalUser program in step 2

```
ls -l
```

In the display, verify that the two files to be removed are present, and then remove both files:

```
rm  exportLocalUser.txt exportLocalUser.xml
```

15 You have completed this procedure.

Obtaining a list of users to migrate to the IEMS

Obtaining a list of users to migrate to the IEMS

At the local or remote VT100 console

1 Log in to the core manager. See Prerequisites on page 28.

2 This procedure can be performed on either version of core manager: the CS 2000 Core Manager (which runs on a Motorola hardware platform) or the Core and Billing Manager 850 (which runs on a Sun Netra240 hardware platform). Therefore, use the following table to determine your next step,

which accesses the appropriate maintenance interface for your core manager.

If	Do
you are migrating CS 2000 Core Manager user accounts	step 3
you are migrating Core and Billing Manager 850 user accounts	step 4

3 Access the maintenance interface:

```
sdmmtc
```

a Access the User level:

```
User
```

b Obtain a list of users to migrate:

```
dispusr
```

c Exit from the maintenance interface:

```
quit all
```

d Go to step 5

4 Access the maintenance interface on the active CBM 850 HA unit:

```
cbmmtc
```

a Access the Admin level:

```
Admin
```

b Obtain a list of users to migrate:

```
user
```

c Exit from the maintenance interface:

```
quit all
```

5 You have completed this procedure.

Backing up user accounts on the core manager

Backing up user accounts on the core manager

At the local or remote VT100 console

1 If you are not already logged on to the core manager, log in. See Prerequisites on page 28.

2 Back up the data for each user account that you want to migrate:

mkdir /data/tmp

cp -rp ~<userID> /data/tmp

where

<userID>
is the userID of the user account

3 Check to make sure that the user is backed up:

ls -lRa /data/tmp/<userID>

where

<userID>
is the userID of the user account

Example response when userID is sdmuser1:

```
total 32
dr-x------ 3 sdmuser1 maint   512 Dec 21 15:30 .
drwx------ 3 root     system  512 Dec 21 15:24 ..
-r-------- 1 sdmuser1 maint  1142 Dec 14 18:09 .profile
drwx------ 2 sdmuser1 maint   512 Dec 21 15:30 .ssh
/data/tmp/sdmuser1/.ssh:
total 32
drwx------ 2 sdmuser1 maint   512 Dec 21 15:30 .
dr-x------ 3 sdmuser1 maint   512 Dec 21 15:30 ..
-rw-r--r-- 1 sdmuser1 maint   223 Dec 21 15:30 known_hosts
-rw------- 1 sdmuser1 maint  1024 Dec 21 15:30 prng_seed
```

4 Use the following table to determine your next step.

If you want to	Do
back up another user account	step 2
you have completed backing up user accounts	You have completed this procedure. Return to the step in the procedure you were performing that referred you to this procedure, either step 3 in Migrating users to the IEMS manually or step 10 in Migrating user accounts to the IEMS using exportLocalUser

Removing user accounts from the core manager

At the local or remote VT100 console

1 If you are not already logged on to the core manager, log in. See Prerequisites on page 28.

2 This procedure can be performed on either version of core manager: the CS 2000 Core Manager (which runs on a Motorola hardware platform) or the Core and Billing Manager 850 (which runs on a Sun Netra240 hardware platform). Therefore, use the following table to determine your next step, which accesses the appropriate maintenance interface for your core manager.

If	Do
you are migrating CS 2000 Core Manager user accounts	step 3
you are migrating Core and Billing Manager 850 user accounts	step 4

3 Access the maintenance interface:

`sdmmtc`

a Access the User level:

`user`

b Go to step 5

4 Access the maintenance interface on the active CBM 850 HA unit:

`cbmmtc`

a Access the Admin level

`Admin`

b Access the User level:

`user`

5 Remove a user:

`delete <userID>`

where

<userID>
is the userID of the user

Example response:

```
Are you sure you want to delete this user?
Do you wish to proceed?

Please confirm ("YES", "Y", "NO", or "N")
```

6 Confirm:

y

Example response:

```
Delete sdmuser1 - Command complete.
```

7 Use the following table to determine your next step.

If you want to	Do
remove another user	step 5
exit from the interface	step 8

8 Exit the maintenance interface:

quit all

9 You have completed this procedure.

Restoring user accounts to the core manager

Restoring user accounts to the core manager

At the local or remote VT100 console

1 If you are not already logged on to the core manager, log in. See Prerequisites on page 28.

2 Restore the data you backed up for each of the user accounts you migrated to the IEMS:

cp -rp /data/tmp/<user_account> /export/home

chown -R <user_account>:<SuccessionGroup> /export/home/<user_account>

Note: The command above is entered on a single line.

ls -la /export/home/<user_account>

where

<user_account>
is a user account that you migrated to the IEMS

<SuccessionGroup>
is "succssn", which represents the user account on the IEMS

Note: Step 2 must be repeated for each of the user accounts that were backed up.

3 After you have completed restoring the backed-up files to the core manager, remove the temporary backed-up files you created:

```
ls -l /data/tmp
```

The system will display the backed-up user accounts you created earlier. Using this listing, delete each of the backed-up user accounts:

```
rm -rf /data/tmp/<user_account>
```

where

<user_account>
is a user account you backed up earlier in this procedure

Note: This command must be performed for each of the backed-up user accounts you created.

```
ls -l /data/tmp
```

Verify that the backed-up user accounts are no longer present.

4 You have completed this procedure.

Selecting the server for authentication services

Purpose

Use this procedure to select the server for authentication services.

Prerequisites

You must be a user authorized to perform security-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN 10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN 10170-611

Before you can select an IEMS server, the following tasks must be completed.

- The IEMS centralized security server must be available and configured.
- The PAM Radius module and the Radius Group Module must be installed

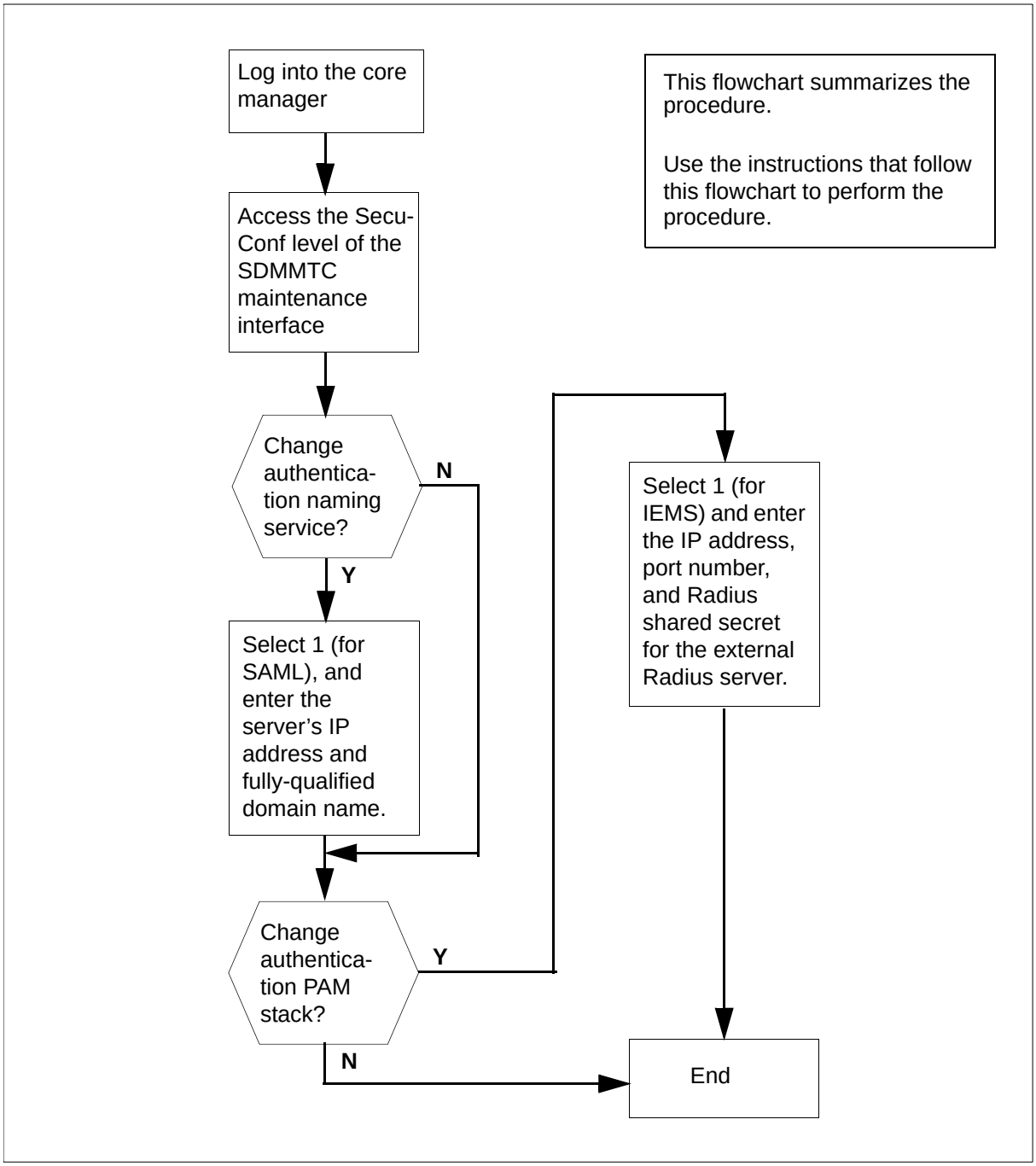
CAUTION

The software node load version of the IEMS server must be equal or greater than (more recent) than the CS 2000 Core Manager node load.

Procedure

The following flowchart provides a high-level overview of the procedure. Use the instructions in the step-action procedure that follows this flowchart to perform the task.

Summary of selecting the server for authentication services



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Selecting the server for authentication services

At the local or remote VT100 console

1. Log into the core manager as a user authorized to perform security-admin actions.
2. Access the maintenance interface:

   sdmmtc
3. Access the Admin level:

   admin
4. Access the SecuConf level:

   secuconf

   Example response:

```
    SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
    ISTb  ISTb   .C   ISTb  ISTb     Host: wcar8e9
     M                  M                  Fault Tolerant
SecuConf
 0 Quit
 2              1 Authentication Naming Service: LOCAL
 3
 4              2 Authentication PAM Stack: LOCAL
 5
 6              3 Remote Security Log Destination: -
 7
 8              4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
18 Refresh
  alex
Time  12:54  >
```

5 Use the following table to determine your next step.

If	Do
you wish to change only Authentication Naming Service	Perform steps 6 through 11 and then go to step 19
you wish to change only the authentication PAM stack	Start at step 12
you wish to change both Authentication Naming Service and authentication PAM stack	Start at step 6

6 Change the authentication naming service:

change <task>

where

<task>
is 1

Example response:

```
Change Authentication Naming Service

Please choose one of the following available
option(s) on the system. More option(s) will be
available if the corresponding fileset(s)
is(are) applied. (1)SAML (2)LOCAL:
```

7 Choose a server:

<server>

where

<server>
is 1 (for SAML)

Example response:

```
Change Authentication Naming Service - SAML

Enter the IP address of the SAML Server:
```

8 Enter the IP address:

<IP address>

where

<IP address>
is IP address of the SAML server

Example response:

```
Change Authentication Naming Service - SAML

Enter the Fully Qualified Domain Name of the
SAML Server:
```

9 Enter the domain name:

<fully qualified domain name>

where

<fully qualified domain name>
is a fully qualified domain name, such as iems-server8.ca.nortel.com

Example response:

```
Change Authentication Naming Service - SAML

Enter the system account password of the SAML
Server:
```

10 Enter the system account password:

Example response:

```
Change Authentication Naming Service - SAML

The SAML Server to be configured:
  IP address: <IP address>
  Fully Qualified Domain Name: <domain name>

Do you wish to proceed?

Please confirm ("YES", "Y", "NO", or "N")
```

11 Confirm:

y

12 Change the authentication PAM stack:

change <task>

where

<task>
is 2

Example response:

```
Change Authentication PAM Stack

Please choose one of the following available
option(s) on the system. More option(s) will be
available if the corresponding fileset(s)
is(are) applied. (1)IEMS (2)LOCAL:
```

13 Choose a server:

<server>

where

<server>
is 1 (for IEMS)

Example response:

```
Change Authentication PAM Stack - IEMS

Enter the IP Address of the External Radius
Server:
```

14 Enter the IP address:

<IP address>

where

<IP address>
is IP address of the external Radius server

Example response:

```
Change Authentication PAM Stack - IEMS

Do you want to enter the port number instead of
using default?

Please confirm ("YES","Y","NO",or"N"):
```

15 Confirm:

y

Note: Although "y" is shown as the response to enter, most users will use the default port, and will enter "n" as the response.

Example response:

```
Change Authentication PAM Stack - IEMS

Enter the Port Number of the External Radius
Server:
```

16 Enter the port number:

<port>

where

<port>
is the port number of the external Radius server

Example response:

```
Change Authentication PAM Stack - IEMS

Enter the Radius Shared Secret:
```

17 Enter the Radius shared secret:

`<secret>`

where

<secret>
is the Radius shared secret

Example response:

```
Change Authentication PAM Stack - IEMS

The Radius Server to be configured
   IP address:10.10.10.10
   Port number:1234

Do you wish to proceed?:
Please confirm ("YES","Y","NO",or"N"):
```

18 Confirm:

y

19 Exit the maintenance interface:

`quit all`

20 You have completed this procedure.

Deleting IEMS user entries from /etc/passwd after upgrade to SN09

Purpose

Use this procedure to delete IEMS user entries from the /etc/passwd file after a core manager with IEMS as the central server has been upgraded from release SN08 to SN09.

Prerequisites

When this procedure should be performed

This procedure should be performed after a core manager with IEMS as the central server has been upgraded from release SN08 to SN09.

Note: Before this procedure is performed, ensure that the naming service has been changed from LOCAL to SAML. For a procedure to change the naming service, see "Selecting the server for authentication services" in NN10170-611, CS 2000 Core Manager Security and Administration.

What core managers the procedure applies to

This procedure applies only to core managers that use the IEMS as the central server. Before starting this procedure, ensure that the core manager uses IEMS as a central server.

Logging in to the CS 2000 Core Manager

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedures

Deleting IEMS user entries from /etc/passwd after upgrade to SN09

At the core manager

1 Log in to the core manager as a user authorized for security-admin or security-manage. For additional information, see Prerequisites on page 49.

2 Delete one IEMS user entry, or all IEMS user entries, from the /etc/passwd file:

```
deleteIEMSLocalEntry <ALL or [user]>
```

where

ALL
indicates all IEMS user entries in the file are to be deleted

[user]
is the login name of the IEMS user that is to be deleted from the file

3 You have completed this procedure.

Forwarding audit and security logs to a remote host

Purpose

Use this procedure to forward the audit and security logs to a remote host.

Prerequisites

You must be a user authorized to perform security-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

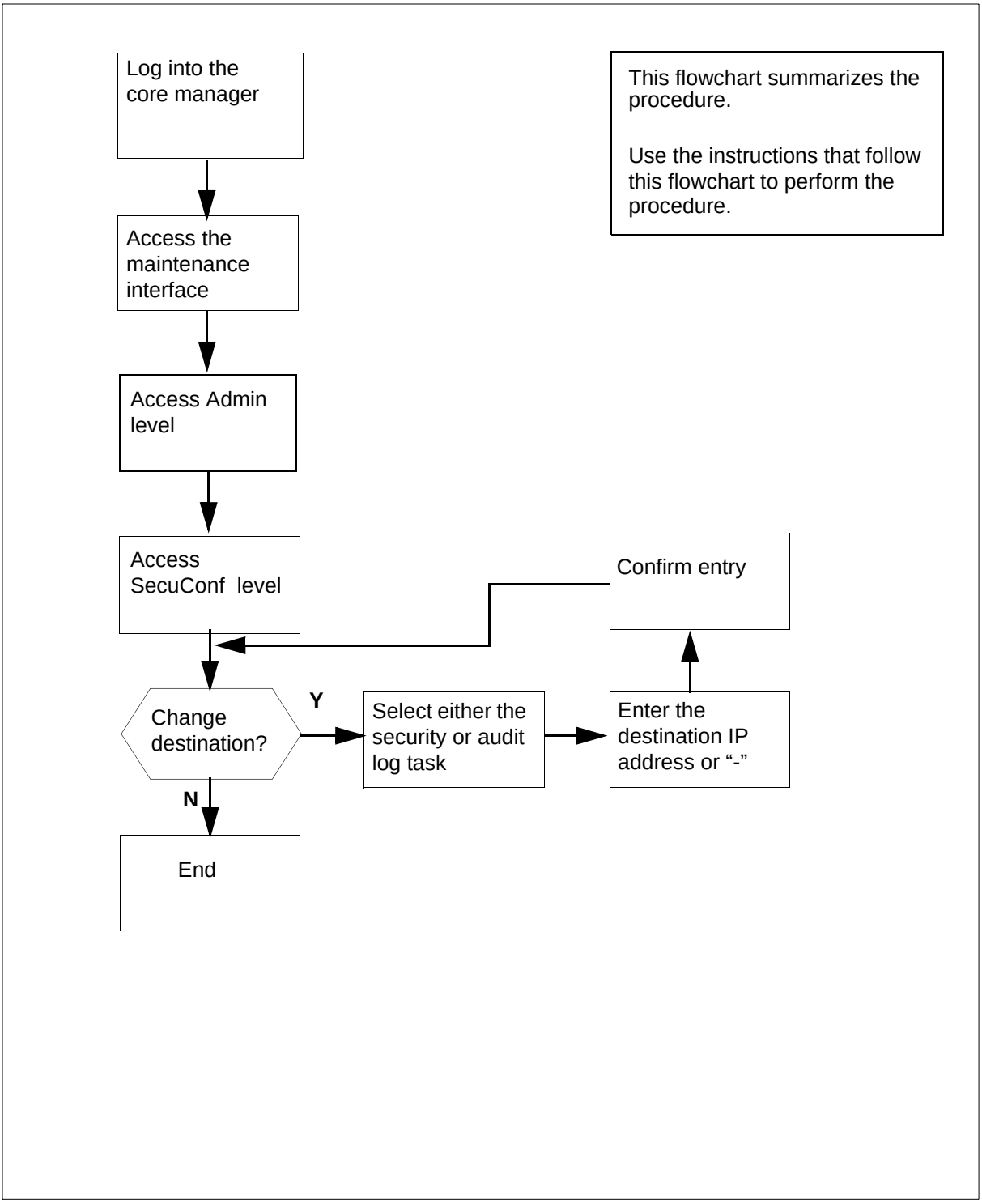
Security and audit log files are rotated daily and are kept for one week. You can forward the files to a remote host through the CS 2000 Core Manager at the SecuConf level.

A security log file is created whenever there is a change to a file. A regular configuration change is recorded in an auditlog file. An abnormal change or changes to security related files are recorded in a securitylog file. For an overview of the security log files, refer to CS 2000 Core Manager Basics, NN10018-111.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

Summary of Forwarding audit and security logs to a remote host



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Forwarding audit and security logs to a remote host

At the local or remote VT100 console

1. Log into the core manager as a user authorized to perform security-admin actions.
2. Access the maintenance interface:

   `sdmmtc`
3. Access the Admin level:

   `admin`
4. Access the SecuConf level:

   `secuconf`

   Example response:

```
    SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
    ISTb  ISTb   .C   ISTb  ISTb     Host: wcar8e9
     M                 M                  Fault Tolerant
SecuConf
 0 Quit
 2              1 Authentication Naming Service: LOCAL
 3
 4              2 Authentication PAM Stack: LOCAL
 5
 6              3 Remote Security Log Destination: -
 7
 8              4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
18 Refresh
  alex
Time  12:54  >
```

5 Change the log destination:

`change <task>`

where

<task>
is either 3 or 4

Enter 3 to change the remote security log destination.
Enter 4 to change the remote audit log destination.

Example response:

```
Change Remote Security Log Destination

The IP address is the destination where the logs
will be forwarded to. Please enter "-" to
indicate unconfiguring the log destination

Enter the new IP Address or -:
```

If you want to	Do
configure the log destination	step 6
unconfigure a previously set destination	step 9

6 Configure the log destination:

`<IPaddress>`

where

<IPaddress>
is the IP address for the log destination

Example response:

```
Change Remote Security Log Destination

The new IP address for the log destination:
47.135.213.56

Proceed with these values?

Enter Y to confirm, N to reject, or E to edit:
```

7 Proceed with the change:

`y`

The destination IP address appears beside the Remote Log Destination list.

Example response:

```
1 Authentication Naming Service: LOCAL
2 Authentication PAM Stack: LOCAL
3 Remote Security Log Destination: 10.10.10.10
4 Remote Audit Log Destination: -
```

8 Go to step 11.

9 Unconfigure a previously set destination:

-

Example response:

```
Change Remote Security Log Destination
The new IP address for the log destination:
-
Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:
```

10 Proceed with the change:

y

A dash appears beside the Remote Log Destination list

Example response:

```
1 Authentication Naming Service: LOCAL
2 Authentication PAM Stack: LOCAL
3 Remote Security Log Destination: -
4 Remote Audit Log Destination: -
```

11 Exit the maintenance interface:

quit all

12 You have completed this procedure.

Creating an administration account

Purpose

Use this procedure to create an administration account.

Application

CAUTION
Possible failure when using sdm_admin account
When you have established your new cell, you must always create an sdm_admin account immediately.

For an existing cell, you can create one or more sdm_admin accounts for the client workstations.Tasks can only be performed successfully by a valid sdm_admin account.

ATTENTION
Do not use the sdm_admin account to configure DCE on a DCE client machine.

Use the cell_admin account to configure or re-configure DCE in a normal DCE client machine except core manager

The default account name is sdm_admin. You can use the sdm_admin account to perform DCE administration activities related to the core manager. The sdm_admin account only has some of the privileges of a cell_admin account.

Use an sdm_admin account for core manager administration routine tasks:

- separate the core manager administration tasks from the DCE administration tasks
- prevent a general core manager operator from damaging or deleting the DCE system-wide data

The sdm_admin account can perform the following procedures:

- configure a core manager in a DCE cell
- remove a core manager from a DCE cell
- create a DCE user

- delete a DCE user
- configure a core manager application server
- remove a core manager application server
- manage the extended registry attributes (ERA) of an application
- set access permission for secure file transfer (SFT)
- optionally, perform like a DCE user account
- optionally, move a core manager from a DCE cell previously configured by a different sdm_admin account

The sdm_admin account cannot:

- delete a DCE user previously created by a cell_admin account
- configure a DCE cell
- assign or reassign a new DCE server

The cell_admin account has the same access privileges as the sdm_admin account. Refer to the corresponding sections when using the sdm_admin or cell_admin accounts to perform any procedure.

Note: The cell_admin account cannot start client applications.

The following conditions must be met before you can create an sdm_admin account:

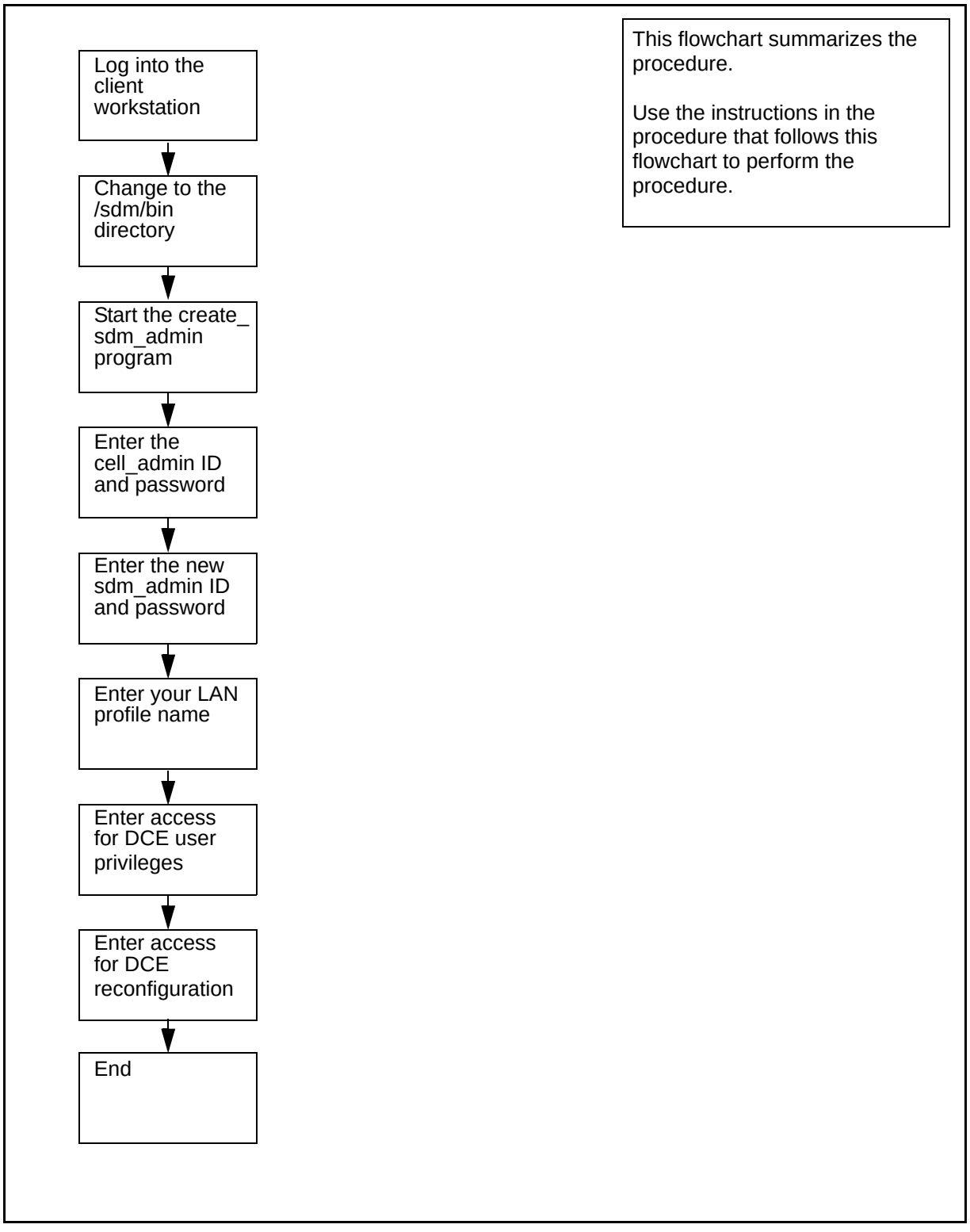
- you must have configured the DCE cell, and at least one remote client machine as the DCE client within the cell
- the DCE cell has cell_admin privileges

Note: You need to perform this procedure once only within your DCE cell.

Procedure

The following flowchart provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the procedure.

Summary of creating an administration account



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Creating an administration account

At the remote client workstation

1 Access the bin directory:

```
cd /sdm/bin
```

2 Create an sdm_admin account:

```
/create_sdm_admin
```

3 Enter the DCE cell_admin user name.

Note: If you do not enter a user ID, the system uses the default value.

4 Enter the DCE cell_admin password.

5 Enter the sdm_admin user name that you want to create.

If you do not specify a user name, the system enters sdm_admin as the default name.

6 Enter the password for the sdm_admin account you entered in step 5.

7 Re-enter the password for the sdm_admin account.

8 Enter the name of your LAN profile used to create your DCE cell.

Note: Use the same LAN profile name as the one you used to create your DCE cell. If you use a different LAN profile name, the creation of the admin user account fails. If you do not specify a LAN profile, the system enters lan_profile as the default value

Example *response:*

```
Do you wish to provide sdm_admin with
“sdm-users” group privileges. (y/n):
```

If you	Do
want the sdm_admin user to have DCE user privileges	enter y, press the Enter key, and continue
do not want the sdm_admin user to have DCE user privileges	enter n, press the Enter key, and go to step 9

Example response:

```
Do you wish to provide sdm_admin with “config”
group privileges. (y/n):
```

If you	Do
want the sdm_admin user to be able to reconfigure the core manager configured by another sdm_admin user	enter y, press the Enter key
do not want the sdm_admin user to be able to reconfigure the core manager that is configured by another sdm_admin user	enter n, press the Enter key

Example response:

```
Creating principal “sdm_admin”...

Adding “sdm_admin” as a member of the
“sdm-admin” organization...

Adding “sdm_admin” as a member of the
“sdm-admin” group...

Creating account for “sdm_admin”...

Adding “sdm_admin” as a member of the
“sdm-users” organization...

Adding “sdm_admin” as a member of the
“sdm-users” group...

Setting “sdm-admin” ACLs for AIX mkdce and rmdce
routine...

Setting “sdm-admin” ACLs for add_sdm_server
script...

Setting “sdm-admin” ACLs for pre-existing SDM
server principals...

Setting “sdm-admin” ACLs for all other DCE
script objects...

Setting “sdm-admin” ACL for SDM servers that use
ERA...

Setting “sdm-admin” ACL for the SDM ETA
server...

Adding “sdm_admin” as a member of the “config”
security group...
```

```
The SDM administrator user ID “sdm_admin” has
been created.
```

9 You have completed this procedure.

Creating ATA user accounts

Purpose

Use this procedure to create an ATA user account.

Application

To install the ATA client application, you must first create the generic ATA user account. Use the following table to determine which procedure to use to create the ATA user account based upon the workstation platform.

Procedures for creating an ATA user account

Platform	Procedure
Hewlett-Packard 700/800 series workstations running the HP-UX 10.20 operating system or higher	Creating the ATA user account with SAM on HP-UX 10.20 on page 62
Sun SPARC workstations running the Solaris 2.6 operating system or higher	Creating the ATA user account with Admintool on Solaris 2.7, 2.8, 2.9 and higher on page 63
IBM RS6000 (AIX 4.3.3) workstations running the AIX 4.1 operating system or higher	Creating the ATA user account with the System Maintenance Interface on the IBM RS6000 on page 64

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Creating the ATA user account with SAM on HP-UX 10.20

At the client workstation

1. Log into the client workstation as the root user.
2. Start the System Administration Manager (SAM):

   ```
   sam &
   ```

   The SAM window appears.
3. Double click the Accounts for Users and Groups icon.

   The Accounts for Users and Groups window appears.
4. Double click the Local Users icon.

   A list of user accounts appears in the list box of the window.

5 From the Actions menu in the Accounts for Users and Groups window, select the Add... menu item.

The Add a user account window appears.

6 In the Login name text box, enter

`ata`

7 Change the startup program to read:

`/sdm/bin/ata`

8 Click the Set Password Options button.

A window for setting password options appears.

9 Select the No restrictions (Normal Behavior) item, and click OK.

10 Click the OK button in the Add a user account window.

The Set user password window appears prompting for a password.

11 Click the OK button without setting a password.

A confirmation window appears.

12 Click the Yes button and the user ata is added to the system.

13 You have completed the procedure. You must proceed to the section "Managing ETA extended registry attributes on page 279 after setting up your workstations.

Creating the ATA user account with Admintool on Solaris 2.7, 2.8, 2.9 and higher

At the client workstation

1 Log into the client workstation as the root user.

2 Start the Admintool:

`admintool`

The Admintool: Users window appears.

3 Select Add from the edit menu.

The Admintool: Add User window appears.

4 In the User Name box, enter

`ata`

5 Select Other from the login shell pop-up menu.

6 In the default login shell text box that appears to the right of the login shell pop-up menu, enter

`/sdm/bin/ata`

7 Select the No password -- setuid only for password option.

8 Select the Create home dir radio button.

9 In the Path text box, enter

`/users/ata`

10 Click the Apply button to add the new user to the system.

11 Click the OK button to close the Admintool:Add User window.

12 Exit the Admintool application.

13 Add an entry to the .rhosts file in the ata directory:

`cat >> .rhosts`

14 Enter a hostname and a user name, separated by a space.

15 Press Ctrl-D to close the file.

16 Change permissions of the .rhosts file to be readable only:

`chmod 644 rhosts`

17 You have completed the procedure. You must proceed to the section Managing ETA extended registry attributes on page 279 after setting up your workstations.

Creating the ATA user account with the System Maintenance Interface on the IBM RS6000

At the client workstation

1 Log into the client workstation as the root user.

2 Start the administration tool:

`smit mkuser`

The Add User window appears.

3 Select Add. from the edit menu.

The Admintool: Add User window appears.

4 In the User Name field, enter

`ata`

5 In the HOME Directory field, enter

`/users/ata`

6 In the Initial PROGRAM field, enter

`/sdm/bin/ata`

7 Exit smit by pressing Esc-0, or press the F10 key.

8 Access the ata user home directory:

`cd /users/ata`

9 Create a .rhosts file:

`cat > .rhosts`

10 Enter a host name and user name separated by a space.

11 Press Ctrl-D to close the .rhosts file.

12 Change the permissions of the .rhosts file:

`chmod 644 .rhosts`

13 Access the smit password screen:

`smit passwd`

14 In the user name field, enter

`ata`

15 Leave the password field blank, and press the Enter key to confirm the ata new blank password.

16 Press the Enter key again to confirm a blank password for the ata account.

17 Exit smit by pressing Esc-0, or the F10 key.

18 Log in to the client machine as the ATA user (leave the password box empty and press the Enter key when prompted)

19 Confirm the blank password when prompted by pressing the Enter key.

20 You have completed this procedure.

Creating system image backup tapes (S-tapes) manually

Purpose

Use this procedure to create a system backup image manually.

Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

Create a system image backup tape (S-tape) manually.

Note: If you want to schedule automatic system image backups, refer to SDM Security and Administration document.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- core manager software

Prerequisites

ATTENTION
This procedure must be performed a trained AIX system administrator authorized to perform config-manage actions.

ATTENTION
All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If not, an error message is displayed.

ATTENTION
If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

ATTENTION
The files under the /data file system are temporary files only, and are excluded from system image backup.

Perform a system image backup after the following events:

- initial installation and commissioning of the core manager
- changes to the configuration of disks or logical volumes
- installation of a new version of core manager platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 minutes to complete, depending on the size of your file systems.

Recommended tapes

To complete this procedure, use one of the digital audio tape (DAT) drive tapes approved by Nortel.

The brands approved by Nortel are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

The tape lengths approved by Nortel are:

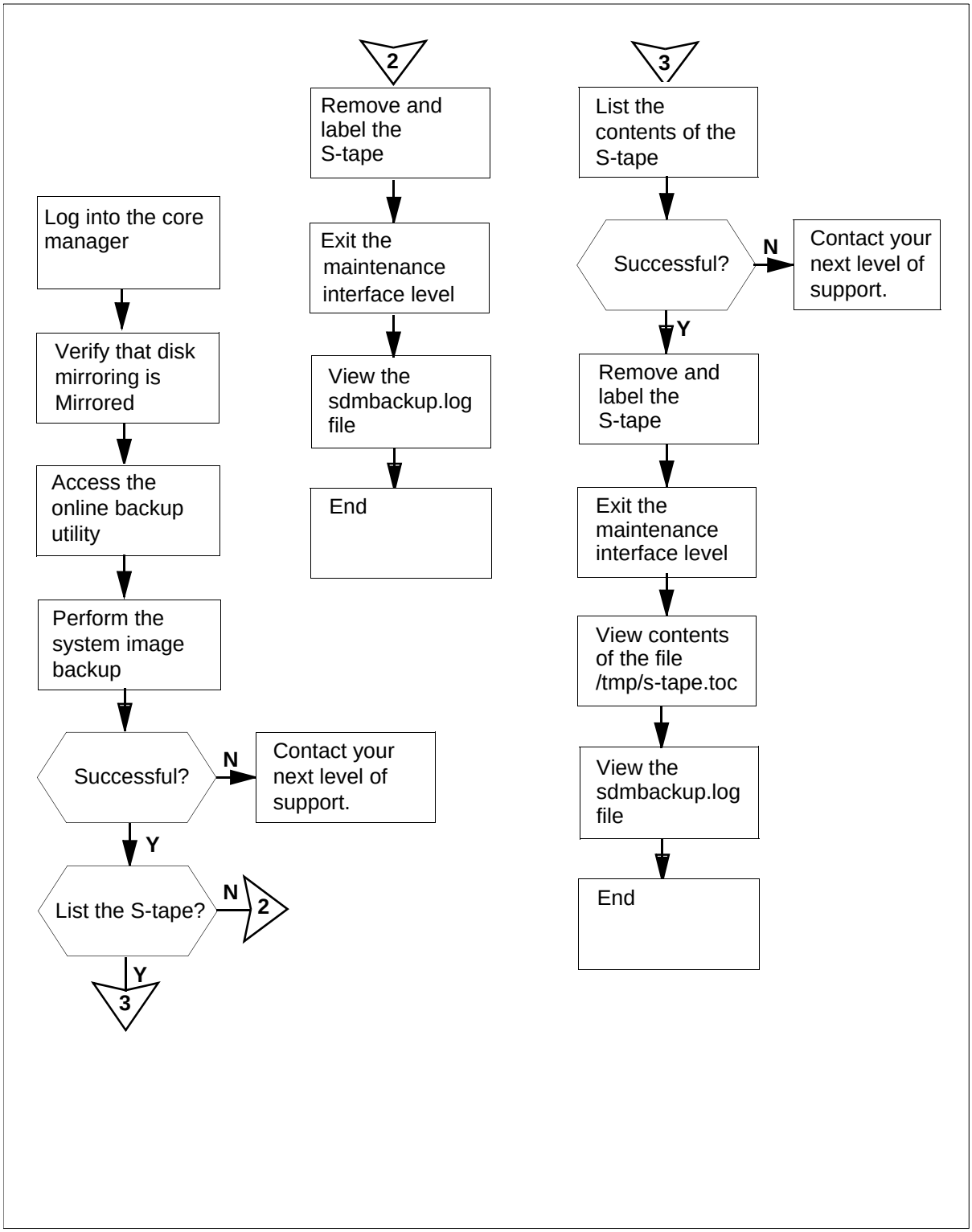
- 90-meter (90M)
- 125-meter (125M)
- 120-meter (120M)

The 125M tape is approved for UMFIOs only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the procedure.

Summary of creating system image backup tapes (S-tapes)



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Creating system image backup tapes (S-tapes)

At the local VT100 console

1 Log into the core manager as a user authorized to perform config-manage actions.

2 Access the maintenance interface:

sdmmtc

3

CAUTION
System mirroring must be MIRRORED
You cannot perform this procedure until disk mirroring of all volume groups is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

Access the storage menu level:

`storage`

Example response:

```
Volume Group                Status
Free(MB)
rootvg                    Mirrored              608


Logical Volume   Location     Size(MB)
%full/threshold 1 /          rootvg    20
25/ 80
2 /usr           rootvg      192              85/ 90
3 /var           rootvg      64               11/ 80
4 /tmp           rootvg      24                6/ 90
5 /home          rootvg      300               4/ 70
```

```
6 /sdm          rootvg     300            44/ 90
Logical volumes showing: 1 to 6 of 6
```

If the disks	Do
are “Mirrored”	step 4
are not “Mirrored”	contact next level of support

4 Access the administration (Admin) menu level of the RMI:

admin

5 Access the System Image Backup and Restore Menu:

backup

Example response:

```
Currently there is a backup running on
bnode73.Please execute yours later.
Exiting . . .
```

Note: If another operator attempts to use the Backup and Restore utility when it is in use, an error message is displayed.

6 From the System Image Backup and Restore Menu, select Create a System Image on Tape (S-tape):

2

After you select option 2, you are prompted to select the tape drive.

Example response:

```
Select the tape drive you wish to use:

Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main Chassis-Slot
2
Enter 2 for tape drive DAT1 in Main Chassis-Slot
13
( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

7 Select the tape drive to use:

<n>

where

<n>
is the option (1 or 2) for the tape drive you wish to use

Note: If your system includes SBA, and you wish to use tape drive DAT1 (option 2), the following message is displayed:

Example response:

```
You have selected DAT 1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.

If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing
records will not be lost during the backup
restore operation.

Do you wish to continue with DAT 1? ( y | n )
```

If you	Do
wish to continue using DAT1	enter **y** press the Enter key
do not wish to use DAT1	enter **n** press the Enter key

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

After you select the tape drive, you are prompted to insert a tape in the drive you have selected.

Example response:

```
Please insert a 4mm DAT tape into the tape drive
DAT0.

Caution:
This action will overwrite the content on the
inserted tape.Do you want to proceed? ( y | n )
==>
```

At the core manager

8

CAUTION
System image backup tape
Creating a system image overwrites the contents of the inserted tape. Ensure that you are using the correct tape before starting the system image backup. If your system includes SBA and you are using DAT1, ensure that the tape drive does not contain an SBA tape.

Ensure that the appropriate core manger tape drive contains a 4-mm digital audio tape (DAT) either 90 m or 120 m long. This tape will be designated as the system image backup tape (S-tape).

Note: For the complete list of approved tapes, refer to the Recommended tapes on page 67.

At the local console

9 When you are certain you are using the correct tape, enter:

y

10 Read the system message to determine if there is enough room on the temporary directory for the system image backup to proceed.

Note: If there is not enough room on the temporary directory, an error message appears.

Example response:

```
Rewinding the tape...

    The /tmp directory is not big enough.
    Trying to expand /tmp by 6600KB...

Failed to expand the /tmp directory because
there isn't enough free disk space left on the
rootvg.

Please erase some files under /tmp directory to
create at least 6600KB for the full system image
backup.
```

```
Enter any key and return to exit ==>
```

If there is	Do
enough disk space	step 14
not enough disk space	step 11

11 Erase enough files from the temporary directory to create the required amount of disk space specified in the error message:

rm -rf /tmp/<filenames>

Note: If you have trouble erasing files from the temporary directory to free up disk space, contact the personnel responsible for your next level of support.

12 Execute the system image backup again.

The system image backup begins.

Example response:

```
Rewinding the tape...

Starting the system image backup on bnode73.

The backup takes a minimum of 10 minutes,
depending on the size of your file systems.

When the backup is complete, you will be asked
to remove the tape from the tape drive.

System image backup is in progress ...
```

Note: This backup process takes approximately 10 minutes to complete, depending on the amount of data stored on the disk.

13 Read the system message.

If the backup	Do
is successfully completed	step 14
fails	contact your next level of support

14 The system informs you if the backup is successful. When the backup is complete, the system prompts you to remove the tape and label it as an S-tape.

Example response:

```
The tape backup started on Wed Oct 16 08:21:15
EDT 1997
completed successfully on Wed Oct 16 08:37:37
EDT 1997.
The log for this session has been added to
“/var/adm/sdmbackup.log”.

Please remove the backup tape from the tape
drive.
Label the tape as shown below and store it in a
safe place.
       System Image Tape (S-tape)
       The Machine Node Id: bnode73
       Date: Wed Oct 16 08:37:37 EDT 1997

Eject the S-tape from the tape drive? ( y | n )
==>
```

15 Determine if you wish to eject the S-tape. Enter

- **y** to eject the tape, or
- **n** if you do not wish to eject the tape, and wish to list its contents.

If you	Do
you wish to list the S-tape	step 28
protect and label the tape	step 16

If you eject the tape, the screen displays “Tape ejected.” below the information displayed in step 14. You are then prompted to return to the System Image Backup and Restore Main Menu.

Response:

```
Tape ejected.

    Would you like to return to the previous
menu? ( y | n)
```

16 Place the write-protected tab of the S-tape in the open position, to prevent accidental erasure.

17 When you are ready for the system to return to the System Image Backup and Restore Main Menu, enter

y

18 Determine if the backup is successful.

The system informs you if the system image backup is successful, as shown in the response in step 14. You may also wish to view the /var/adm/sdmbackup.log file or list the files on the S-tape.

If	Do
you wish to view the /var/adm/sdmbackup.log file	step 19
you wish to list the S-tape	step 28
the backup is successful	step 36
the backup fails	contact your next level of support

19 Exit the System Image Backup and Restore Main Menu:

0

20 Exit the RMI:

quit all

21 Access the sdmbackup.log file:

cd /var/adm

22 Scroll through the file:

more sdmbackup.log

This screen informs you that the system image backup was completed successfully.

Example response:

```
bosboot:  Boot image is 5881 512 byte blocks.
0+1 records in.
1+0 records out.

Backing up the system...
.....................................................
............
0512 038 mksysb: Backup Completed Successfully.

The S-tape backup started on Wed Oct 16 09:24:07
EDT 1997
completed successfully on Wed Oct 16 09:36:03
EDT 1997
```

23 Determine if you wish to list the S-tape.

If you	Do
wish to list the S-tape	step 24
do not wish to list the S-tape	step 40

24 Return to the login directory:

cd

25 Access the RMI:

sdmmtc

26 Access the administration (Admin) menu level of the RMI:

admin

27 Access the System Image Backup and Restore Menu:

backup

28 From the System Image Backup and Restore Menu, select List Contents of the System Image Tape (S-tape):

3

29 After you select option 3, you are prompted to select the tape drive.

Example response:

```
Select a tape drive you wish to use:

       Enter 0 to return to previous menu
       Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
       Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
      ( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

30 Select the tape drive:

<n>

where

<n>
is the number (1 or 2) for the tape drive you wish to use

Example response:

```
You have selected DAT 1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.

If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing
records will not be lost during the backup
restore operation.

Do you wish to continue with DAT 1? ( y | n )
```

If you do not wish to use DAT1, the system prompts you to return to the System Image Backup and Restore Menu.

If you wish to	Enter
continue using DAT1	**y**
not continue	**n**

Note: If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

31 After you select the tape drive, you are prompted to insert the S-tape into the tape drive that you selected in step 30.

Example response:

```
Please insert your System Image Backup tape
(S-tape) into the tape drive DAT0 and allow at
least 5 minutes to complete the listing.

A log file will be saved in /tmp/s-tape.toc

Are you ready to proceed? ( y | n )
```

At the core manager

32 Insert the S-tape into the tape drive.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

At the local VT100 terminal

33 When you are ready to continue this procedure, enter:

y

34 The contents of the S-tape are displayed. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

Example response:

```
Would you like to return to the previous menu?
( y | n )
```

35 Return to the System Image Backup and Restore Menu:

y

At the core manager

36 If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive.

37 Label the tape according to your office practices, and store it in a safe location.

38 If you ejected an SBA tape, reinsert the tape.

At the local VT100 terminal

39 Exit the System Image Backup and Restore Menu,:

0

Note: If you wish to exit the RMI, enter QUIT ALL.

40 You have completed this procedure.

Scheduling system image backups

Purpose

Use this procedure to schedule automatic system image backups.

Note 1: If you want to create a system image backup tape (S-tape) manually, refer to procedure “Creating system image backup tapes (S-tapes) manually” in the Administration and Security section.

Note 2: If a Backup Failed alarm exist, the next scheduled backup will not start. You must clear the alarm using procedure “Clearing a system image backup Required or Failed alarm” in the Fault Management section.

Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

ATTENTION
This procedure must be performed by a trained AIX system administrator authorized to perform config-manage actions.

ATTENTION
All volume groups on the core manager must be fully mirrored (Mirrored) before performing the backup. If you attempt to perform the backup when disk mirroring is not Mirrored, an error message will be displayed.

ATTENTION
If your system includes the SuperNode Billing Application (SBA), use tape drive DAT0 to perform the backup.

ATTENTION
The files under the /data file system are excluded from system image backup. The files under the /data file system are temporary files that do not require backing up.

ATTENTION
You must also schedule regular cleaning of the digital audio tape (DAT) drive in an NTRX50FQ I/O controller module. Clean the tape drive heads after each 25th system backup. For cleaning instructions refer to the “Cleaning the DAT drive” procedure in the Fault Management document.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- core manager software

Nortel recommends that you perform a system image backup after the following:

- initial installation and commissioning of the core manager
- changes to the configuration of disks or logical volumes
- installation of a new version of core manager platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 min. to complete, depending on the size of your file systems.

When scheduling the backup, the tool prompts for five different parameter values:

- minute
- hour
- day of the month
- month of the year
- day of the week

The "day of the month" and "day of the week" fields are distinct.

The specification of days can be made by two fields (day of the month and day of the week). If you specify both as a list of elements, both are adhered to. For example, in the following entry:

0 0 1,15 * 1

the backup runs on the first and fifteenth days of each month, as well as every Monday. To specify days by only one field, the other field must contain an asterisk (*).

Recommended tapes

Use one of the digital audio tape (DAT) drive tapes approved by Nortel.

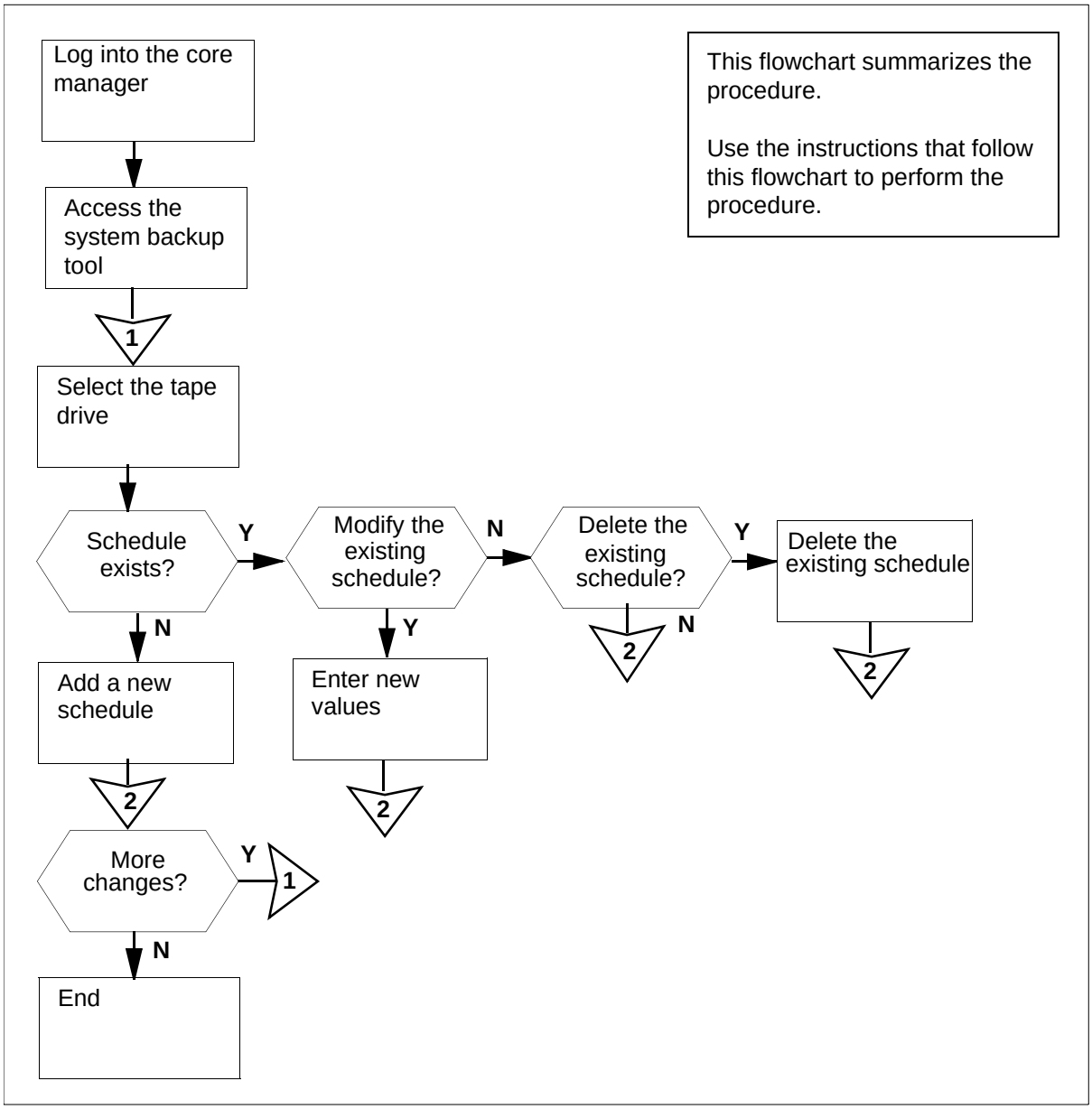
The brands approved by Nortel are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

The tape lengths approved by Nortel are: 90-meter (90M), 120-meter (120M), or 125-meter (125M). The 125M tape is approved for UMFIOs only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of scheduling system image backups



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Scheduling system image backups

At the local VT100 console

1 Log into the core manager as a user authorized to perform config-manage actions.

2 Access the system backup tool:

sysbkup

Example response:

```
0. Exit
1. Help
2. Backup & Restore System image
3. Alarm Configure


Please enter your selection (0 to 3) ?
==>
```

3 Access the System Image Backup and Restore Menu:

2

Example response:

```
0. Exit
1. Previous Menu
2. Create a System Image on Tape (S-tape)
3. List Contents of the System Image Tape
(S-tape)
4. Restore Files from the System Image Tape
(S-tape)
5. Schedule Backup

Please enter your selection (0 to 5) ? ==>
```

4 Access the Schedule Backup Configure Menu:

5

Example response:

```
0. Exit
1. Previous Menu
2. Schedule Dat 0
3. Schedule Dat 1
4. List Backup Schedules

Please enter your selection (0 to 4) ? ==>
```

5 Use the following table to determine your next step.

If you wish to	Do
view the current schedules	step 6
add, delete, or modify a schedule	step 7

6 Select the List Backup Schedules option:

4

Example response:

```
DAT0
----
         Min    : *
         Hrs    : *
         Date   : *
         Month  : *
         Day    : *
DAT1
----
         Min    : *
         Hrs    : *
         Date   : *
         Month  : *
         Day    : *
```

Note 1: Overlapping backup schedules can be created when fields are set to overlap. For example, when the date of the month and the day of the week are both assigned scheduled backup events, the schedules can overlap.

Note 2: If there are no scheduled backups configured, the system displays the following message:

```
There is no Scheduled backup entry
Press Enter to continue...
```

Press the Enter key. The system returns to the Schedule Backup Configure Menu.

7 Select the tape drive that you want to use for the scheduled backup:

<x>

where

<x>
is the number (2 or 3) for the tape drive you wish to use

Note: If your system includes SBA, Nortel recommends that you use tape drive DAT0 (enter 2).

8 Use the following table to determine your next step.

If the response is:	Do
`There is no schedule for DAT<#>, Add new schedule [y/n] ==>`	step 9
`The existing schedule for DAT<#> is ..... Please Enter Your Selection: Modify [1] Disable [2] Exit [0] -->`	step 12

9 To add a new schedule, enter **`y`**.

If the selected tape drive is	Do
Dat 1 (option 3)	step 10
Dat 0 (option 2)	step 11

10 The system displays the following message:

```
You have selected DAT1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.

If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing
records will not be lost during the backup
restore operation.
```

```
Do you wish to continue with DAT 1? ( y | n )
 ==>
```

If the response is:	Do
If you wish to continue scheduling for DAT1	enter **y** continue with step 11
If you do not wish to use DAT1	enter **n** The system returns to the Schedule Backup Configure Menu. Go back to step 7 to continue the procedure.

11 The system displays the following Scheduling Backup screen and prompts you to enter the value for the first parameter (Minute).

```
                    Scheduling Backup

minute (0-59 or '*')
hour (0-23 or '*')
day of the month (1-31 or '*')
month of the year (1-12 or '*')
day of the week (0-6 with 0=Sunday or '*')

Note:
Each pattern can be either an asterisk '*',
meaning all legal values, or a list of elements
separated by commas. An element is either a
number in the ranges, or two numbers in the
range separated by a hyphen (meaning all
inclusive range).

Minute [ 0-59 | * | abort ] :
```

Enter a value (from the range displayed) for each parameter, and press the Enter key after each entered value.

After you enter the last value (day of the week), the system returns to the Schedule Backup Configure Menu.

Go to step 13 to continue the procedure.

12 Determine if existing schedules to be modified or deleted.

If you want to	Do
modify the existing schedule	substep a
delete the existing schedule	substep b

a Enter **1**, and go back to step 11

b Enter **2**.

Example response:

```
Continue with deleting Schedule for DAT<#>
[y/n] ==>
```

c Confirm the command: **y**.

Example response:

```
Deleted successfully
Press Enter to Continue...
```

Press the Enter key again.

Note: If you want to cancel your delete operation, enter **n** and press the Enter key. When prompted, press the Enter key again.

13 If you want to make more changes to your schedules, go back to step 4. Otherwise, continue with step 14.

14 Exit the system backup tool:

0

15 You have completed the procedure.

Starting an SCFT client session

Application

Use this procedure to start an SSH Core File transfer (SCFT) session.

You must perform this procedure either from the client workstation running UNIX or Linux with SSH commands or from the client workstation running UNIX or Linux with the CMFT script installed.

> ***Note:*** To install the CMFT script, use the procedure "Installing the CMFT on a client workstation" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

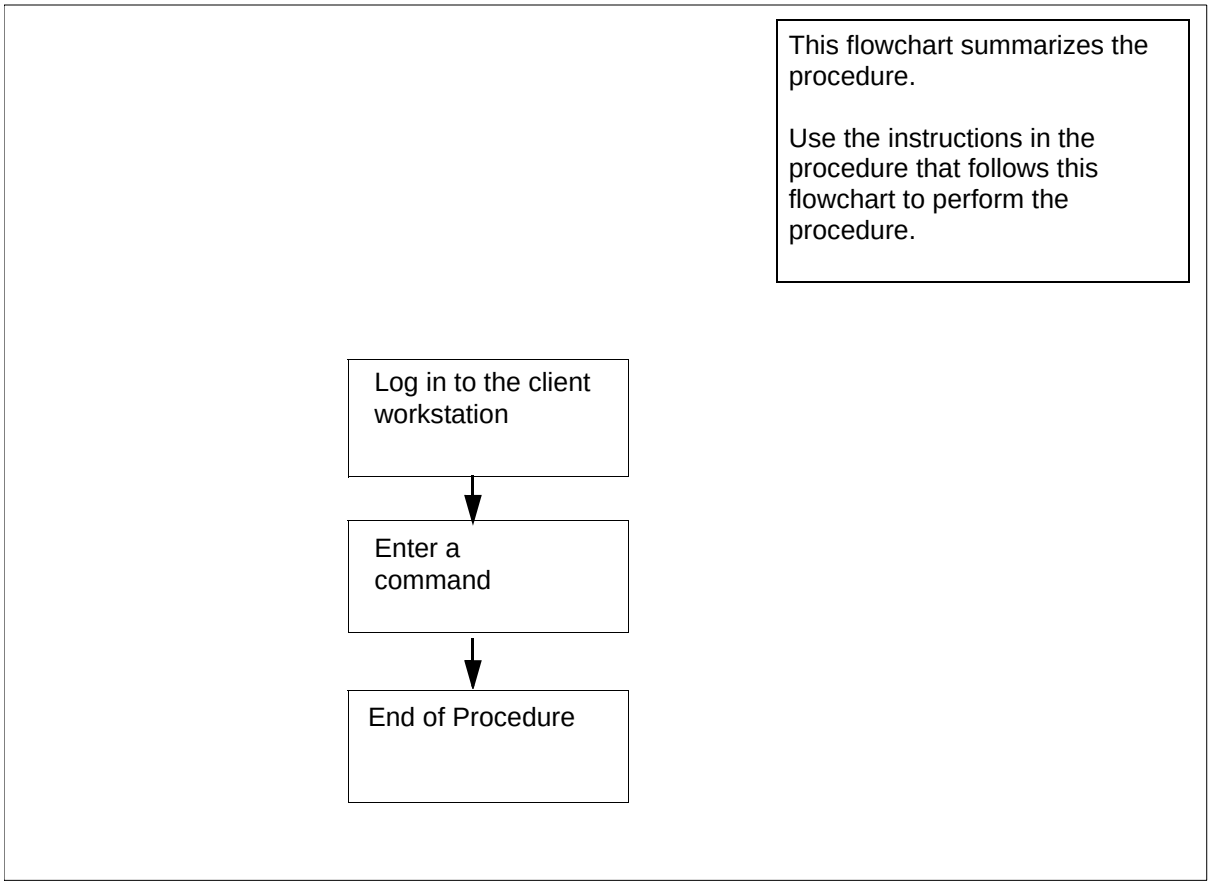
Nortel recommends that all component level security management connections to the core be made using SCFT.

You must have root user privileges on the core module to perform this procedure.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of starting an SCFT client session



Starting an SCFT client session

At the client workstation

1 Enter a command. Refer to the following procedures in this document:

- Displaying help for SCFT on page 102
- Listing volumes on Core using SCFT on page 107
- Removing a file from Core using SCFT on page 99
- Transferring files from Core using SCFT on page 91
- Transferring files to Core using SCFT on page 95

2 You have completed this procedure.

Transferring files from Core using SCFT

Purpose

Use this procedure to transfer files from the Core using SSH Core File transfer (SCFT).

Prerequisites

You must perform this procedure either from the client workstation running UNIX or Linux with SSH commands or from the client workstation running UNIX or Linux with the CMFT script installed.

Note: To install the CMFT script, use the procedure "Installing the CMFT on a client workstation" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

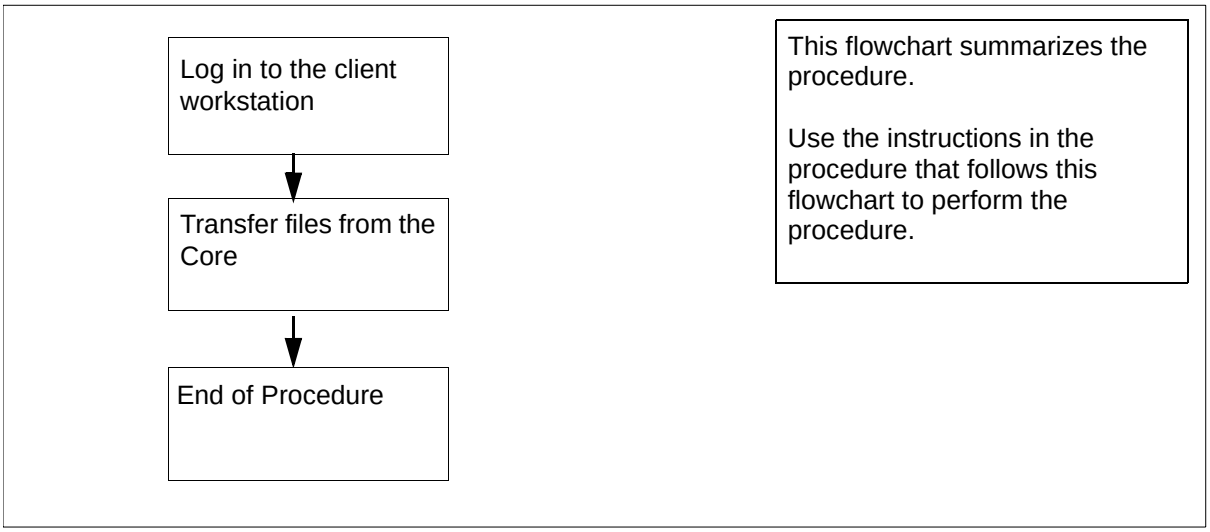
You must have root user privileges on the core module to perform this procedure.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of transferring files from core using SCFT



Transferring files from core using SCFT

At the client workstation

1 Choose the command type:

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Transfer files from a specific volume on the core:

```
ssh <user>@<host> "scft <-b|-a>  -s <reclen> -g
/<volume>/<corefile>" > <localfile>
```

where

<user>
is the user name you are using to log on to the core manager

<host>
is the name or IP address of the core manager

<-b|-a>
is used with get or put to specify the transfer format

- **-b**
  to specify binary format
- **-a**
  to specify ASCII format

<reclen>
is the length of the records in the file being transferred

<volume>
is the name of the core manager volume on the core from which the file to be downloaded is located.

<corefile>
is the full name (including the directory path) of the core manager file on the core from which the copy originates.

<localfile>
is the name of the local file the copy is going to including the directory path

Note: For passthru users, the full path for the "scft" command, "/bin/scft", must be entered instead of only "scft".

Example entry:

```
ssh root@host1 "scft -b -s 1024 -g /sfdev/file1"
> /localdir/localfile
```

Example response:

```
Opened Connection to Core
Command complete
```

3 You have completed this part of the procedure.

4 Transfer files from a specific volume on the core:

```
cmft <-b|-a> -s <reclen> <user>@<host>:
/<volume>/<corefile> <localfile>
```

where

<user>
is the user name you are using to log on to the core manager

<host>
is the name or IP address of the workstation

<-b|-a>
is used with get or put to specify the transfer format

- **-b**
  to specify binary format
- **-a**
  to specify ASCII format

<reclen>
is the length of the records in the file being transferred

<volume>
is the name of the volume on the core

<corefile>
is the name of the core file the copy is coming from including the directory path

<localfile>
is the name of the local file the copy is going to including the directory path

Example entry:

```
cmft root@host1:/sfdev/file1/localdir
/localfile
```

Example response:

```
Opened Connection to Core
Command complete
```

5 You have completed this procedure.

Transferring files to Core using SCFT

Purpose

Use this procedure to transfer files to the Core using SSH Core File transfer (SCFT).

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform security-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

You must perform this procedure either from the client workstation running UNIX or Linux with SSH commands or from the client workstation running UNIX or Linux with the CMFT script installed.

Note: To install the CMFT script, use the procedure "Installing the CMFT on a client workstation" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

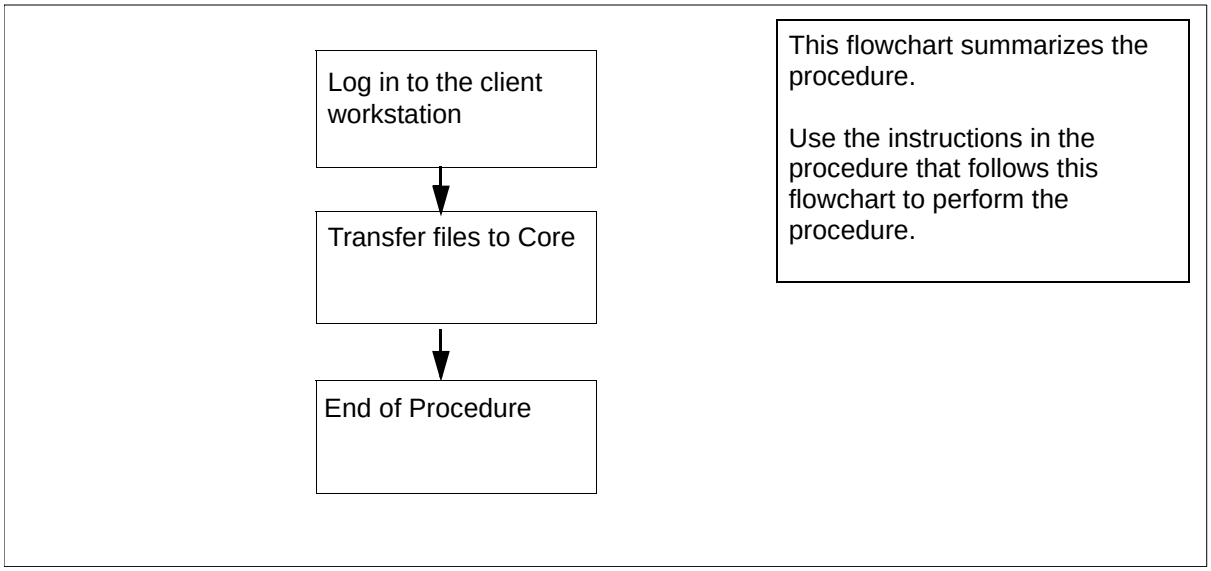
Logging on to the Core and Billing Manager

You must have the root user ID and password to log into the server.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of transferring files to core using SCFT



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Transferring files to core using SCFT

At the client workstation

1 Select the command type.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Transfer files to a specific volume on the core:

```
ssh <user>@<host> "scft <-b|-a> -s <reclen> -p
/<volume>/<corefile>" < <localfile>
```

where

<user>
is the user name you are using to log on to the core manager

<host>
is the name or IP address of the core manager

<-b|-a>
is used with get or put to specify the transfer format

- **-b**
  to specify binary format
- **-a**
  to specify ASCII format

<reclen>
is the length of the records in the file being transferred

<volume>
is the name of the volume on the core manager

<corefile>
is the name and the directory path of the core file the copy is going to

<localfile>
is the name and the directory path of the local file the copy is coming from

Note: For passthru users, the full path for the "scft" command, "/bin/scft", must be entered instead of only "scft".

Example entry:

```
ssh alex@host1 "scft -b -s 1024 -p /sfdev/file1"
< /localdir/localfile
```

Example response:

```
Opened Connection to Core
Command complete
```

3 Go to step 5.

4 Transfer files to a specific volume on the core:

```
cmft <-b|-a> < -s reclen> <localfile>
<user>@<host>:/<volume>/<corefile>
```

where

<-b|-a>
is used with get or put to specify the transfer format

- **-b**
  to specify binary format
- **-a**
  to specify ASCII format

<reclen>
is the length of the records in the file being transferred

<localfile>
is the name of the local file the copy is coming from including the directory path

<user>
the user name you are using to log on to the core manager

<host>
the name or IP address of the core manager

<volume>
is the name of the volume on the core manager

<corefile>
is the name and directory path of the Core file the copy is going to

Example entry:

```
cmft /localdir/localfile alex@host1:/sfdev
/file1
```

Example response:

```
Opened Connection to Core
Command complete
```

5 You have completed this procedure.

Removing a file from Core using SCFT

Purpose

Use this procedure to remove a file from the Core using SSH Core File transfer (SCFT).

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform security-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

You must perform this procedure either from the client workstation running UNIX or Linux with SSH commands or from the client workstation running UNIX or Linux with the CMFT script installed.

Note: To install the CMFT script, use the procedure "Installing the CMFT on a client workstation" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

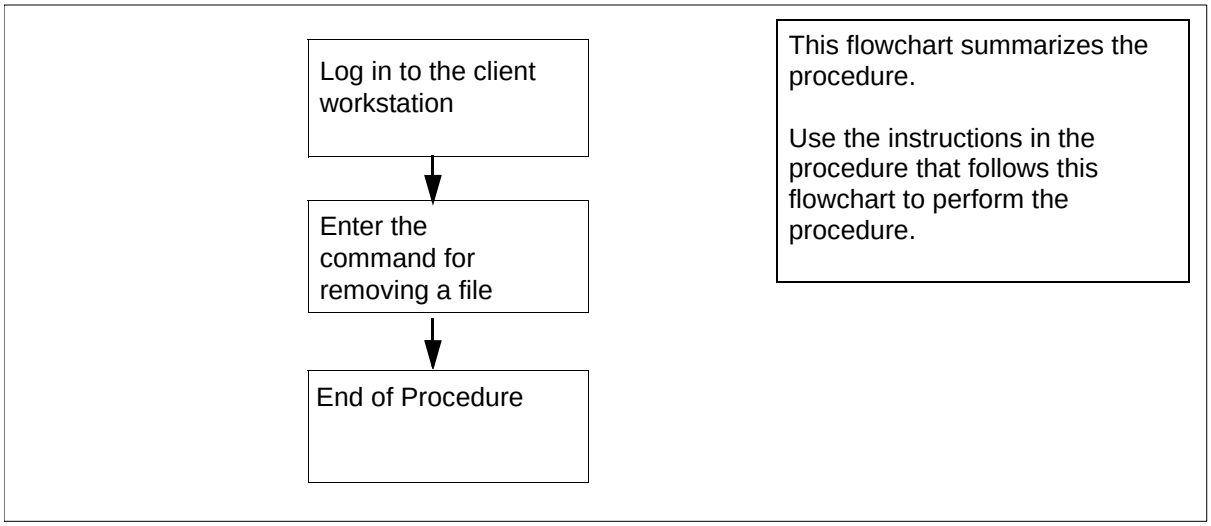
Logging on to the Core and Billing Manager

You must have the root user ID and password to log into the server.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of removing a file from core using SCFT



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Removing a file from core using SCFT

At the client workstation

1 Select the command type.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Remove a file in a specific volume on the core:

```
ssh <user>@<host>"scft -r /<volume>/
<filename>"
```

where

<user>
is the user name you are using to log on to the core manager

<host>
is the name or IP address of the core manager

<volume>
is the name of the volume on the core

<filename>
is the name of the core file being removed including the directory path

Note: For passthru users, the full path for the "scft" command, "/bin/scft", must be entered instead of only "scft".

Example response:

```
Opened Connection to Core
Command complete
```

3 Go to step 5.

4 Remove a file in a specific volume on the core:

`cmft -r <user>@<host>:/<volume>/<filename>`

where

<user>
is the user name you are using to log on to the core manger

<host>
is the name or IP address of the core manger

<volume>
is the name of the volume on the core

<filename>
is the name of the core file being removed including the directory path

Example response:

```
Opened Connection to Core

Command complete
```

5 You have completed this procedure.

Displaying help for SCFT

Purpose

Use this procedure to display help during an SSH Core File transfer (SCFT) session.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform security-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

You must perform this procedure either from the client workstation running UNIX or Linux with SSH commands or from the client workstation running UNIX or Linux with the CMFT script installed.

Note: To install the CMFT script, use the procedure "Installing the CMFT on a client workstation" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

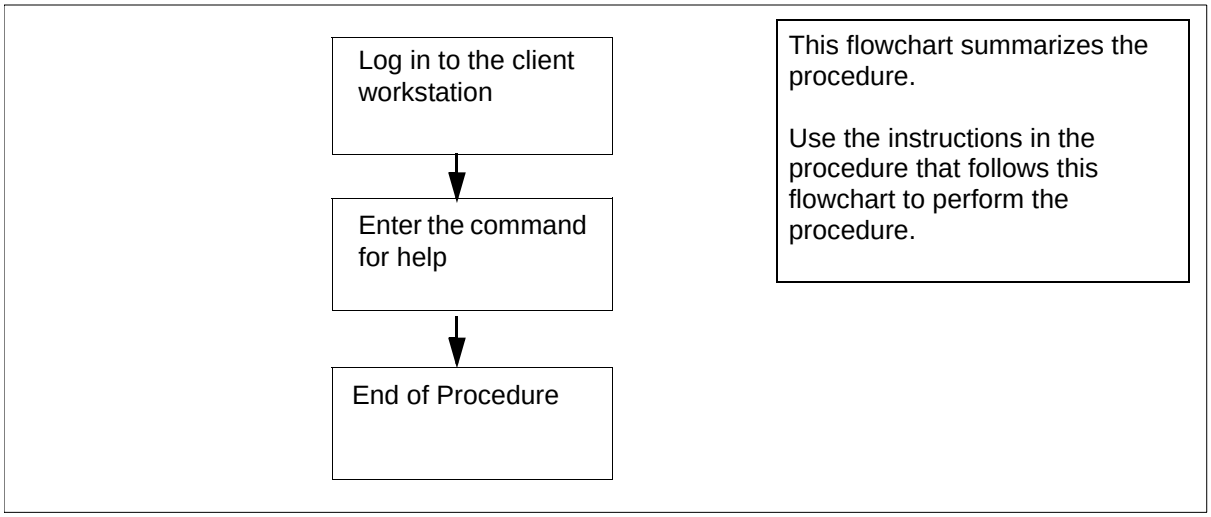
Logging on to the Core and Billing Manager

You must have the root user ID and password to log into the server.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of displaying help for SCFT



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Displaying help for SCFT

At the client workstation

1 Select the command type.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Display help text:.

```
ssh <user>@<host> "scft -h"
```

where

<user>
the user name you are using to log on to the core manager

<host>
the name or IP address of the core manager

Note: For passthru users, the full path for the "scft" command, "/bin/scft", must be entered instead of only "scft".

Example response:

```
Command complete


SCFT Help:

<-n hostname><-a><-b><-s record length>
<-p filename><-h><-l volume><-g filename>
<-r filename>

-n: Hostname of Core
-b: Binary Transfer
-a: Ascii Transfer
-s: Specify the record length to be used for the
file being transferred
-p: Put a file on the Core
-h: Help
-l: List the directory on the Core
-g: Get a file from the Core
-r: Remove a file on the Core
```

3 Go to step 5.

4 Display help text:.

`cmft - h`

Example response:

```
 To transfer a file
cmft  [-b|-a][-s <int>] [[[user@host:]vol]file1
[[[user@]host:]vol]file2

 To list a volume on the Core
cmft  -l [user@]host:<vol>

 To remove a file from the CBM
cmft  -r [[[user@]host:]vol]file1
```

```
 For this help information
cmft -h
  -l  -- To list a volume on the Core
  -r  -- To remove a file from the Core
  -h  -- To get this help information
  -s  -- To set the record length for the file
being transferred
  -b  -- Use with a get or put to specify binary
format
  -a  -- Use with a file transfer to specify
ASCII format
       NOTE:  one or the other can be used not
both.  Default is binary

 int  -- An integer representing the record
size.
 user -- the user name you wish to log on to the
CBM with.
     This is optional. If not entered the userid
you are executing this script with will be used.
          eg.   root

 host --  the name or ip address of the cbm you
wish to log on to.
          eg.   ##.###.###.## or HOSTNAME

 file1 -- name of the file the copy is coming
from including directory path
 file2 -- name of the file the copy is going to
including directory path
      NOTE: Only one of the files can have the
host name present.
             This would be the file that is or
will be on the CBM.
       NOTE: the local files can also have an
extension
            Allowable extensions are .bin[##],
.txt[##], $df and $patch
          .txt is Ascii with a specified record
length
             .bin is Binary with a specified
record length
          $df and $patch are Binary with record
length of 128
```

```
 vol  -- the name of the volume on the SDM, you
wish to list or
          '/' to list all volume

 examples:
   To put a binary file with record length 1024
from local file /bin/data1 to core file
/volume/data:
          cmft -b -s 1024 /bin/data1
root@HOSTNAME:/volume/data1

   To get a file from the core file /volume/data
to a local file data:
          cmft root@HOSTNAME:/volume/data1
/bin/data1

    To list the volume names on the core:
          cmft -l root@HOSTNAME:/

    To list the files in the sfdev volume:
          cmft -l root@HOSTNAME:/sfdev
```

5 You have completed this procedure.

Listing volumes on Core using SCFT

Purpose

Use this procedure to list volumes on the Core during SSH Core File transfer (SCFT) session.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform security-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

You must perform this procedure either from the client workstation running UNIX or Linux with SSH commands or from the client workstation running UNIX or Linux with the CMFT script installed.

Note: To install the CMFT script, use the procedure "Installing the CMFT on a client workstation" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

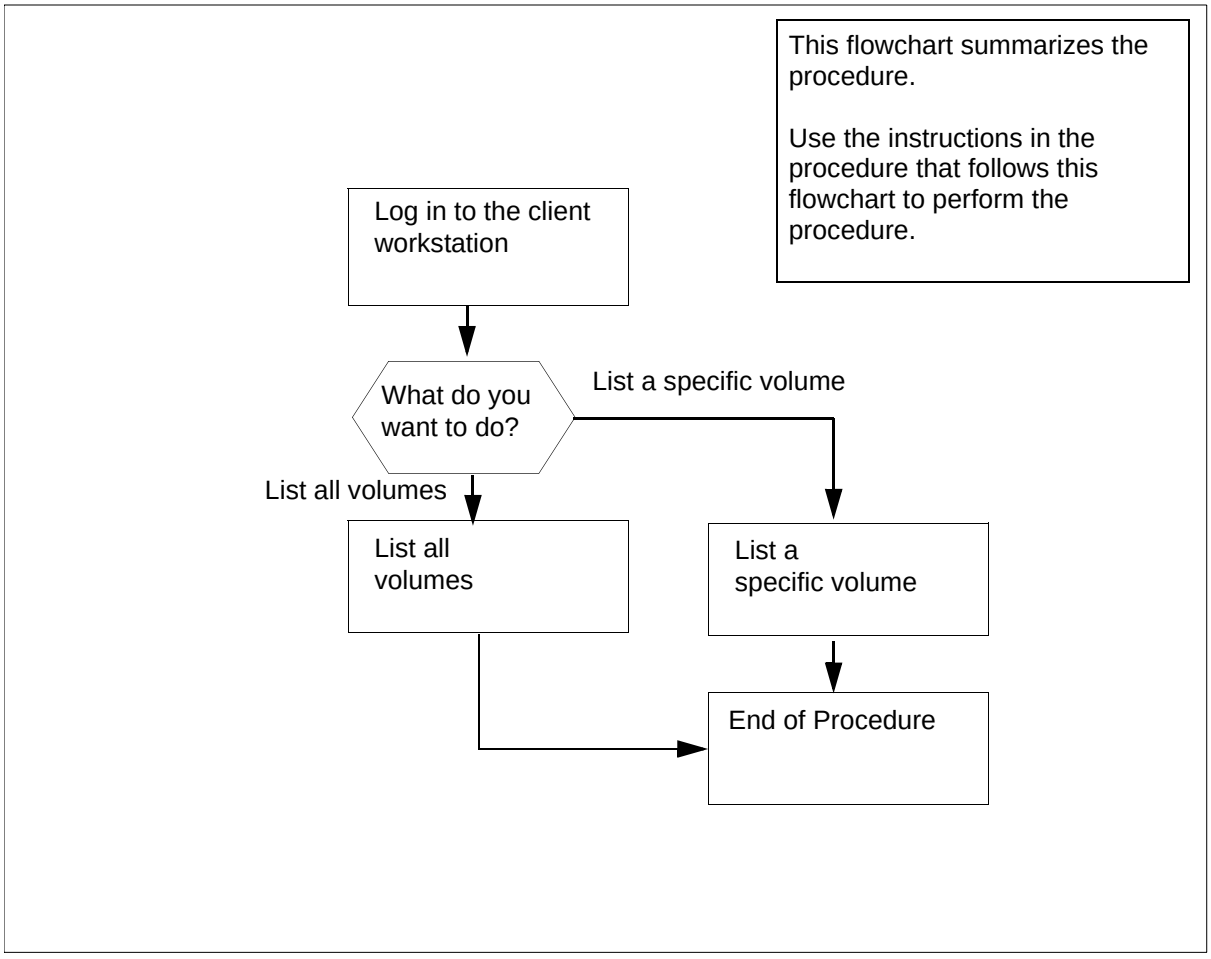
Logging on to the Core and Billing Manager

You must have the root user ID and password to log into the server.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of listing volumes on Core using SCFT



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Listing volumes on Core using SCFT

At the client workstation

1 Go to the next step depending on the type of command you use.

If you use	Do
ssh commands	step 2
cmft commands	step 6

2 List all or specific volumes.

If you want to	Do
list all volumes	step 3
list a specific volume	step 4

3 List all volumes on the Core:

ssh <user>@<host>"scft -1 /"

where

<user>
the user name you are using to log on to the core manager

<host>
the name or IP address of the core manager

Note: For passthru users, the full path for the "scft" command, "/bin/scft", must be entered instead of only "scft".

Example response:

```
SFDEV
S01DIMAGE
S00DIMAGE1
S00DAMA
S01DPMLOADS
S01DPERM
S01DDLOG
S01DTEMP

Command complete
```

If you	Do
want to list a specific volume	step 4
do not want to list a specific volume	you have completed this procedure

4 List a specific volume on the Core:

ssh <user>@<host>"scft -1 /<volume>"

where

<user>
the user name you are using to log on to the core manager

<host>
the name or IP address of the core manager

<volume>
is the name of the volume on the core manager

Note: For passthru users, the full path for the "scft" command, "/bin/scft", must be entered instead of only "scft".

Example response:

```
LOGIN STDFAULT
IOC$
MSCDINV$
CMSHELF$
EADASOM$DATAFILL
NNASST$
OFCENG
VRDATA$
OM CONFIG
OFCOPT
OFCVAR
OFCSTD
NNASST
DATASIZE
OMKEYORD$INFO$FILE
PML

Command complete
```

5 You have completed this procedure.

If you want to	Do
list all volumes	step 6
list a specific volume	step 7

6 List all volumes on the Core:

`cmft -l <user>@<host>:/`

where

<user>
the user name you are using to log on to the core manager

<host>
the name or IP address of the core manager

Example response:

```
SFDEV
S01DIMAGE
S00DIMAGE1
S00DAMA
S01DPMLOADS
S01DPERM
S01DDLOG
S01DTEMP

Command complete
```

If you	Do
want to list a specific volume	step 7
do not want to list a specific volume	you have completed this procedure

7 List a specific volume on the Core:

`cmft -l <user>@<host>:/<volume>`

and pressing the Enter key.

where

<user>
the user name you are using to log on to the core manager

<host>
the name or IP address of the core manager

<volume>
is the name of the volume on the core manager

Example response:

```
LOGIN STDFAULT
IOC$
MSCDINV$
CMSHELF$
EADASOM$DATAFILL
NNASST$
OFCENG
VRDATA$
OM CONFIG
OFCOPT
OFCVAR
OFCSTD
```

```
NNASST
DATASIZE
OMKEYORD$INFO$FILE
PML

Command complete
```

8 You have completed this procedure.

Creating a DCE user

Purpose

Use this procedure to create a DCE user account for a user who runs core manager graphical user interface (GUI) client programs.

Prerequisites

ATTENTION
You must be a trained Distributed Computing Environment (DCE) system administrator to perform this procedure.

ATTENTION
Use either the master administration account (cell_admin) or a DCE sub administrator account (sdm_admin) to perform this procedure.

Application

You cannot use the sdm_admin account to delete a DCE user created by a cell_admin account. The cell_admin account can delete any DCE users created by either a cell_admin or an sdm_admin account.

The create_dce_user command creates a new DCE user and makes the user a member of a specified group.

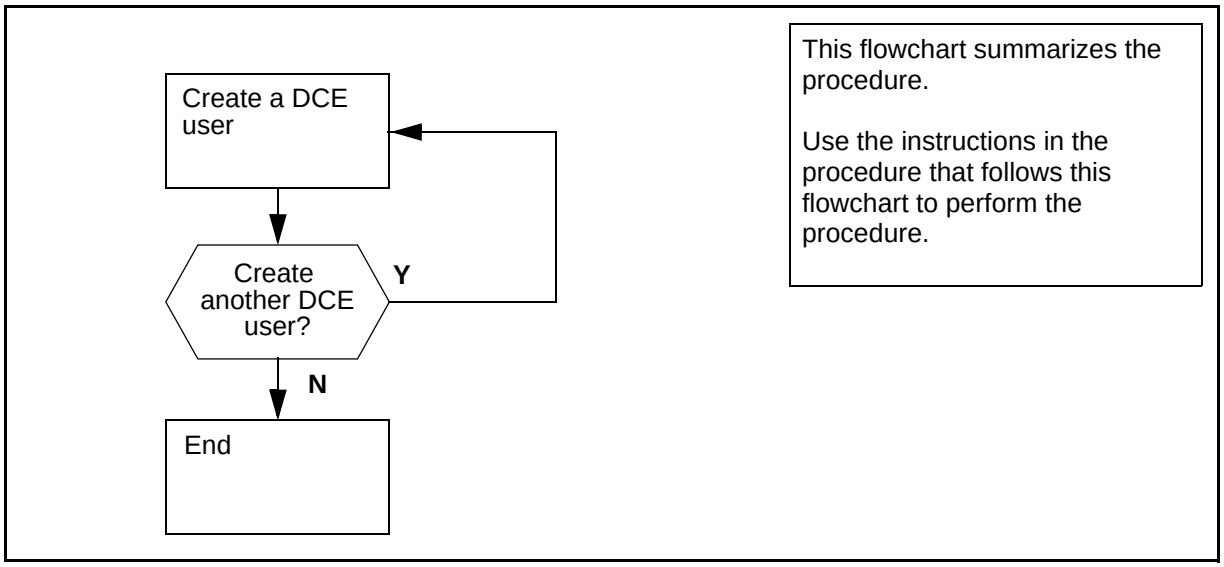
Note: You must use the cell_admin account to create groups.

You can use these groups for access control purposes to categorize users with similar job functions.You only need a DCE account to run a core manager GUI program. There can be some exceptions for specific core manager applications. For any exceptions, refer to the *OSF DCE Command Reference* document that is provided with the application.

Procedure

The following flowchart provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the procedure.

Summary of creating a DCE user account



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Creating a DCE user

At the client workstation

1 Create a DCE user:

```
/sdm/bin/create_dce_user
```

Note: When running the create_dce_user script, place the new dce user ONLY into the sdm-users group.

2 Enter the DCE administrator user ID.

Note: If you do not enter a user name, the system enters sdm_admin as the default value.

3 Enter the DCE administrator password.

4 Enter the new DCE user ID.

5 Enter a password for the new DCE user ID.

6 Re-enter the password.

Example response:

```
Full name of the person associated with “ops_1”
```

7 Enter the full name of the person associated with the new user ID.

8 Enter the user group for the new DCE user.

Note: If you do not enter a user group, the system enters sdm-users as the default value.

Example response:

```
Creating principal “ops_1”...

Adding “ops_1” as a member of the “sdm-users”
organization...

Adding “ops_1” as a member of the “sdm-users”
group...

Creating account for “j_smith”...

Setting “ops_1” ACL for SDM server to use
ERAs...

Setting “ops_1” ACL for the SDM ETA server...

The DCE user ID “ops_1” has been created.
```

9 You have completed this procedure.

Connecting to the Core with ATA

Purpose

Use the following procedure to use the ASCII Terminal Application (ATA) to connect to the Core.

Prerequisites

This procedure requires the following information:

- access to the ATA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the Core to access

Application

ATA provides two methods to connect to the Core:

- ATA client (Using the ATA client to connect to the Core on page 116)
- command line arguments (Using command line arguments to connect to the Core on page 117)

Procedure

Perform the following steps to complete this procedure.

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Using the ATA client to connect to the Core

At your workstation

1 Log into the application client machine.

2 Change the directory to the sdm/bin directory:

```
cd /sdm/bin
```

3 Start the ATA application:

```
ata
```

The system prompts for a DCE principal name.

4 Enter your DCE userid.

The system prompts for a password.

5 Enter your DCE password.

The ATA application starts and the prompt changes to `ata>`.

6 List the CLLI of the available switches:

`list`

ATA displays a list of CLLI names.

7 Locate the CLLI of the switch with the Core to access.

8 Access the Core:

`open <switch_CLLI> cm`

where

<switch_CLLI> is the CLLI of the switch with the Core you want to access

Example input:

`ata> open RLGHNC01ECB cm`

ATA connects to the Core

Note: *Once connected to the core and if you loose your connection, the core drops your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.*

9 Close the session with the Core before you quit ATA.

`logout`

10 Quit ATA:

`quit`

11 You have completed this part of the procedure.

Using command line arguments to connect to the Core

At your workstation

1 Log into the application client machine.

2 Start the ATA application and list the CLLI of the available switches:

`/sdm/bin/ata -list`

The system prompts for a DCE principal name.

3 Enter your DCE userid.

The system prompts for a password.

4 Enter your DCE password.

A list of CLLI names is displayed.

5 Locate the CLLI of the switch with the Core to access.

6 Connect to the Core:

`/sdm/bin/ata -clli <switch_CLLI> -session CM`

where

<switch_CLLI> is the CLLI of the switch with the Core you want to access

Example of input:

`> /sdm/bin/ata -clli RLGHNC01ECB -session CM`

The system prompts for a DCE principal name.

7 Enter your DCE userid.

The system prompts for a password.

8 Enter your DCE password.

ATA connects to the Core.

Note: *Once connected to the core and if you loose your connection, the core drops your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.*

9 Close the session with the Core before you quit ATA.**logout**

10 Quit ATA:
quit

11 You have completed the procedure.

Connecting to the Core with ETA

Purpose

Use the following procedure to use Enhanced Terminal Application (ETA) to access the Core.

Prerequisites

This procedure requires the following information:

- access to the ETA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the Core to access

Procedure

Perform the following steps to complete this procedure.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

At your workstation

1 Log into the application client machine.

2 Go to the directory with the ETA application client:

```
cd /sdm/bin
```

3 Start the ETA application client:

```
./eta
```

The system displays a copyright window.

4

> **ATTENTION**
> If the system displays a window with an error message and a Trace Back button, a serious software error may have occurred. Ask your system administrator to click the Track Back button, record the response for analysis, and click the OK button to continue. If necessary, contact Nortel Networks for assistance.

Wait 10 seconds.

ETA displays the DCE Login window.

Note: If you do not want to log in, click the **Abort** button. The system returns to the UNIX prompt.

5 Log in to DCE.

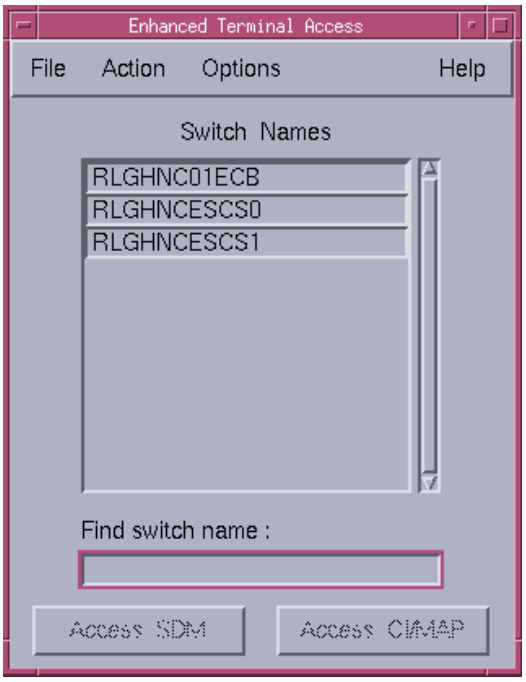
6 Enter your DCE userid in the field **Principal name**.

7 Enter your DCE password in the field **Password**.

8 Click the **OK** button.

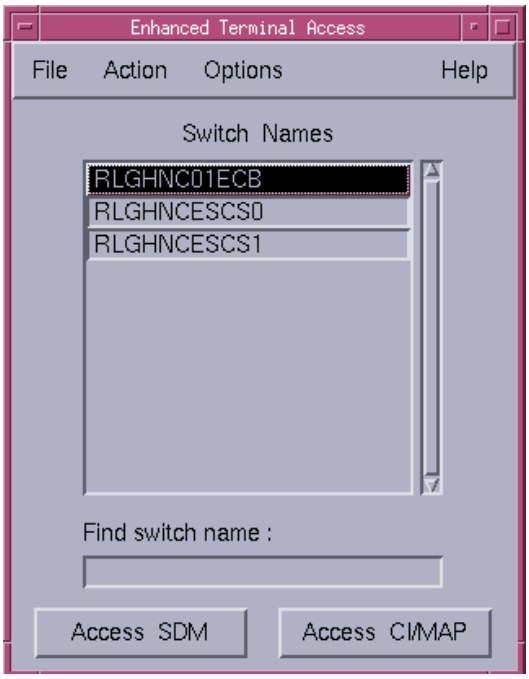
ETA displays a list of available CLLI.

Example of an ETA window:



9 Select the CLLI of the switch with the Core you want to access. If necessary, use the scroll bar on the right side of the list.

Example of an ETA window:



10 Access the Core by clicking the **Access CI/MAP** button.

ETA connects to the Core and displays a CI prompt.

> ***Note:*** *Once connected to the core, if you lose your connection, the core drops your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.*

11 Close all CI/MAP sessions before you quit ETA. To close the CI/MAP session with the Core, logout at the CI prompt:

```
logout
```

12 To quit ETA, select **Exit** from the **File** menu in the main ETA window

13 You have completed this procedure.

Connecting to the core manager with ATA

Purpose

Use the following procedure to connect to the core manager using the ASCII Terminal Application (ATA) application.

Prerequisites

This procedure requires the following information:

- access to the ATA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the core manager you want to access

Application

ATA provides two methods to connect to the core manager.

- ATA client (Using the ATA client to connect to the core manager on page 122)
- command line arguments (Using command line arguments to connect to the core manager on page 124)

Note: Connecting to the core manager and then connecting to the Core is not recommended. Connect to the Core as a pass-thru user instead.

Procedure

Perform the following steps to complete this procedure.

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Using the ATA client to connect to the core manager

At your workstation

1 Log into the application client machine.

2 Change the directory to the sdm/bin directory:

cd /sdm/bin

3 Start the ATA application:

ata

The system prompts for a DCE principal name.

4 Enter your DCE userid.

The system prompts for a password.

5 Enter your DCE password.

The ATA application starts and the prompt changes to `ata>`.

6 List the CLLIs of the available switches:

list

ATA displays a list of CLLI names.

7 Locate the CLLI of the switch with the core manager you want to access.

8 Access the core manager:

open <switch_CLLI> sdm

where

<switch_CLLI> is the CLLI of the switch with the core manager you want to access

Example input:

`ata>` **open RLGHNC01ECB sdm**

ATA connects to the core manager.

Example response:

```
There is 1 local login.
There are 3 ETA logins to the SDM.
There is 1 ETA logins to the CM.

Current SDM status:
SDM     CON     512     NET      APPL     SYS     HW
  .       .      ..       .        .        .       .
                 ..

maint:
```

Note: Once connected to the core, if you lose your connection, the core will drop your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

9 Close the SDM session before you quit ATA. To close the SDM session, logout at the prompt:

`logout`

10 To quit ATA, enter:

`quit`

11 You have completed this part of the procedure.

Using command line arguments to connect to the core manager

At your workstation

1 Log into the application client machine.

2 Start the ATA application and list the CLLIs of the available switches:

/sdm/bin/ata -list

The system prompts for a DCE principal name.

3 Enter your DCE userid.

The system prompts for a password.

4 Enter your DCE password.

ATA displays a list of CLLI names.

5 Locate the CLLI of the switch with the core manager you want to access.

6 Access the core manager:

/sdm/bin/ata -clli <switch_CLLI> -session SDM

where

<switch_CLLI> is the CLLI of the switch with the core manager you want to access

Example input:

/sdm/bin/ata -clli RLGHNC01ECB -session SDM

The system prompts for a DCE principal name.

7 Enter your DCE userid.

The system prompts for a password.

8 Enter your DCE password.

ATA connects to the core manager.

Example response:

```
There is 1 local login.
There are 3 ETA logins to the SDM.
There is 1 ETA logins to the CM.

Current SDM status:
SDM     CON     512     NET      APPL     SYS     HW
  .       .      ..       .        .        .       .
                 ..

maint:
```

Note: Once connected to the core, if you loose your connection, the core will drop your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

9 Close the SDM session before you quit ATA. To close the SDM session, exit at the prompt:

`exit`

10 To quit ATA, quit at the prompt:

quit

11 You have completed the procedure.

Connecting to the core manager with ETA

Purpose

Use the following procedure to use Enhanced Terminal Application (ETA) to connect to the core manager.

Note: Connecting to the core manger and then connecting to the Core is not recommended. Connect to the Core as a pass-thru user instead.

Prerequisites

This procedure requires the following information:

- access to the ETA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the core manager you want to access

Procedure

Perform the following steps to complete this procedure.

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

At your workstation

1 Log into the application client machine.

2 Go to the directory with the ETA application client:

cd /sdm/bin

3 Start the ETA application client:

/eta

The system displays a copyright window.

4

ATTENTION

If the system displays a window with an error message and a Trace Back button, a serious software error may have occurred. Ask your system administrator to click the Track Back button, record the response for analysis, and click the OK button to continue. If necessary, contact Nortel Networks for assistance.

Wait 10 seconds.

ETA displays the DCE Login window.

Note: If you do not want to log in, click the Abort button. The system returns to the UNIX prompt.

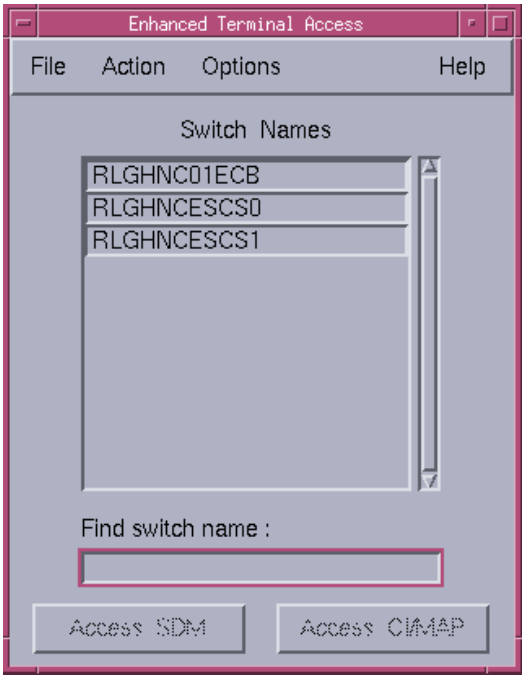
5 Enter your DCE userid in the field **Principal name**.

6 Enter your DCE password in the field **Password.**

7 Click the **OK** button.

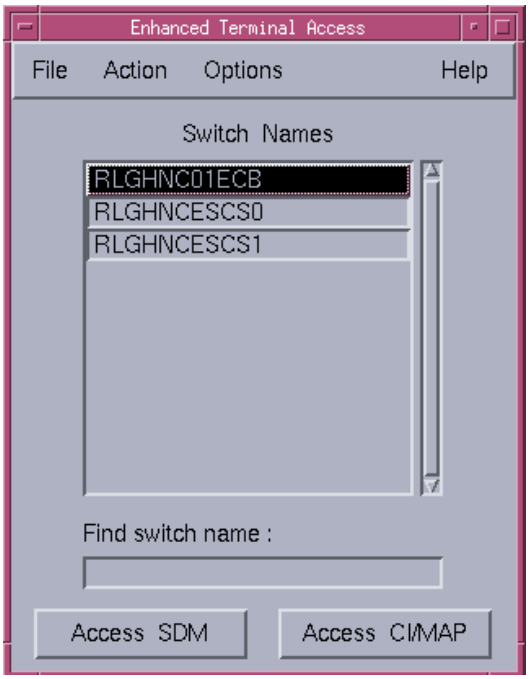
ETA displays a list of available CLLI.

Example of an ETA window:



8 Select the CLLI of the switch with the core manager you want to access. If necessary, use the scroll bar on the right side of the list.

Example of an ETA window:



9 Access the core manager by clicking the **Access SDM** button.

ETA connects to the core manager.

Example response:

```
There is 1 local login.
There are 3 ETA logins to the SDM.
There is 1 ETA logins to the CM.

Current SDM status:
SDM     CON     512     NET      APPL     SYS     HW
  .       .      ..       .        .        .       .
                 ..

maint:
```

Note: Once connected to the core, if you lose your connection, the core will drop your login session within five seconds. If your login id is not released by the core after that time, then login to the core with another userid and manually end the original login session.

10 Close all SDM sessions before you quit ETA. To close an SDM session, exit at the command prompt:

exit

11 To quit ETA, select Exit from the File menu in the main ETA window.

12 You have completed the procedure.

Connecting to the core manager with SDMRLOGIN

Purpose

SDMRLOGIN is a non-menu command available at any level of the maintenance and administration position (MAP). SDMRLOGIN creates a telnet session from Core to the CS 2000 Core Manager. SDMRLOGIN is used to access CS 2000 Core Manager nodes that are either in service (InSv) or in-service trouble (ISTb).

An SDMRLOGIN session accesses a restricted shell on the CS 2000 Core Manager, which provides a limited set of commands. When you type **help** within an SDMRLOGIN session, a list of available commands displays. The following table lists some of the commands available during an SDMRLOGIN session.

Note: SDMRLOGIN commands are case-sensitive.

Commands available during an SDMRLOGIN session

Command	Function
AFTAdd (see Note 1)	Adds a new AFT session
AFTAddfile (see Note 1)	Adds a file to an AFT session transfer list
AFTAlarm (see Note 1)	Queries or cancels AFT session alarms
AFTChange (see Note 1)	Changes the value of retry attempts for an AFT session
AFTDelete (see Note 1)	Deletes an AFT session
AFTList (see Note 1)	Lists configuration information about AFT sessions
AFTListfile (see Note 1)	Lists processed files for a stream
AFTQuery (see Note 1)	Queries and displays data about an AFT session
AFTRsetfile (see Note 1)	Resets the state of a file for an AFT session
AFTSetfile (see Note 1)	Sets override file or deletes a file from a list
AFTStart (see Note 1)	Starts an existing AFT session
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Commands available during an SDMRLOGIN session

Command	Function
AFTStop (see Note 1)	Stops an existing AFT session
amadump (see Note 2)	Displays record information contained in a billing file
awk	Pattern-directed scaling and processing language
bsyapp	Busies an application
closec (see Note 2)	Closes currently open billing file or files for each stream
CONFSTRM.act (see Note 2)	Activates a filtered stream
CONFSTRM.add (see Note 2)	Adds a configured billing stream
CONFSTRM.change (see Note 2)	Changes an existing billing stream configuration
CONFSTRM.deact (see Note 2)	Deactivates a filtered stream
CONFSTRM.delete (see Note 2)	Deletes an existing billing stream configuration
CONFSTRM.list (see Note 2)	Lists configuration of a single billing stream or all billing streams
CONFSTRM.start (see Note 2)	Resumes receiving records on a filtered stream
CONFSTRM.stop (see Note 2)	Stops receiving records on a filtered stream
CONFSTRM.update (see Note 2)	Updates the criteria of a filtered stream
cut	Cuts out (extracts) selected fields of each line of a file
dispal (see Note 2)	Displays current billing alarms
displogs (see Note 2)	Displays billing logs not acknowledged by the Core
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Commands available during an SDMRLOGIN session

Command	Function
grep	Searches a file for a pattern
help	Displays generic help information
java	Java Runtime Environment
listfile (see Note 2)	Lists stored billing file or files for each stream
locate	Queries hardware module information
logout	Logs the user out of the CS 2000 Core Manager
logquery	Initiates the logquery tool to browse DMS logs
ls	Lists contents of the CS 2000 Core Manager remote login directory
mib (see Note 2)	Gets or sets MIB objects for billing
offlapp	Offlines an application
ping	Sends ICMP ECHO_REQUEST packets to network hosts
ps	Reports process status
query (see Note 2)	Queries SBA billing stream status
readtape.sh (see Note 2)	File used by TAPE.send; should not be called directly
rtsapp	Returns an application to service
SCHEDULE.add (see Note 2)	Adds a tuple to the schedule
SCHEDULE.change (see Note 2)	Changes an existing tuple in the schedule
SCHEDULE.delete (see Note 2)	Deletes a tuple or tuples from the schedule
SCHEDULE.list (see Note 2)	Lists a tuple or tuples in the schedule
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Commands available during an SDMRLOGIN session

Command	Function
SCHEDULE.RTBAdd (see Note 2)	Adds Real-Time Billing (RTB) to a stream
SCHEDULE.RTBBsy (see Note 2)	Busies RTB for a stream
SCHEDULE.RTBChange (see Note 2)	Changes the RTB configuration for a stream
SCHEDULE.RTBConfQuery (see Note 2)	Queries the RTB configured destinations
SCHEDULE.RTBDelete (see Note 2)	Deletes RTB from a stream
SCHEDULE.RTBIptest (see Note 2)	Tests the IP address used by RTB for a stream
SCHEDULE.RTBOffl (see Note 2)	Offlines RTB for a stream
SCHEDULE.RTBQuery (see Note 2)	Queries the state of RTB for a stream
SCHEDULE.RTBRts (see Note 2)	Returns RTB to service for a stream
sendfile	Sends billing file or files for each stream to downstream DPMS
TAPE.list (see Note 2)	Lists the billing files written to a digital audio tape (DAT)
TAPE.send (see Note 2)	Sends (FTP) billing files from a DAT
TAPE.write (see Note 2)	Writes billing files to a DAT
who_is_on	Displays the users logged in to the CS 2000 Core Manager

Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT).

Note 2: Applies only to SBA.

Use the following procedure to access the core manager from the Core with the SDMRLOGIN command.

Note: Connecting to the core manager in order to connect to the Core is not recommended. Connect to the Core as a passthru user instead.

Prerequisites

This procedure requires the following information:

- core manager userid
- core manager password

Note: SDMRLOGIN is supported only on DS-512 connected core managers.

Procedure

Perform the following steps to complete this procedure.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

At the MAPCI

1 Start an SDMRLOGIN session.

sdmrlogin

The Core starts a telnet session to the core manager and prompts for a login.

2 Enter your core manager userid.

The screen prompts for a password.

3 Enter your core manager password.

The Core connects to the core manager.

- The screen displays login history information
- The prompt changes to SDM>.

Note: Once connected to the core, if you lose your connection, the core drops your login session within five seconds. If your login id is not released by the core, then login to the core with another userid and manually end the original login session.

4 Quit the SDMRLOGIN session and return to the MAPCI level where you began this procedure.

logout

5 You have completed this procedure.

Example

The following figure shows an example of an **SDMRLOGIN** session.

```
>sdmrlogin
SDM IP address is 47.245.8.70

SDM Remote Logins command in progress. Please wait...

telnet (brtppycf1)
AIX Version 4
(C) Copyrights by IBM and by others 19982, 1994.
login:
>maint
Password:
>
************************************************************
**
**
**               This is a private database.
**          All activity is subject to monitoring.
**      Any UNAUTHORIZED access or use is PROHIBITED.
**
**
**
************************************************************
Last unsuccessful login: Wed Jul 2 11:02:26 EDT 1997 o
Last login: Thu Jul 3 12:05:35 EDT 1997 on /dev/pts/2
SDM>
```

Troubleshooting SDMRLOGIN errors

The following errors can occur during an SDMRLOGIN session.

- The CS 2000 Core Manager is not in the InSv or ISTb state. Put the CS 2000 Core Manager in the InSv state, and re-enter the SDMRLogin command.
- A telnet session cannot be established between the CM and the CS 2000 Core Manager.

- The terminal that you are using for the remote login does not suppress the echoing of password entries. You can either continue or exit the remote login session.
- The terminal that you are using for the remote login is being used to output DMS logs. You can either continue or exit the remote login session.

Connecting to another node as a passthru user

Purpose

Use following procedures to connect to another node using the core manager as a passthru user. The following types of connections are supported:

- Telnet to a node logically behind the core manger
- File Transfer Protocol (FTP) to the Core
- Secure Core File Transfer (SCFT) to the Core

A passthru connection occurs through the core manager. A passthru connection does not allow you to perform operations on the core manager.

Prerequisites

This procedure requires the following information and applications:

- Passthru userid and password

  Note: FTP access to the Core requires a password.

- Userid and password of destination node

  Note: FTP access to the Core does not require a destination userid and password.

- Secure File Transfer (SFT) installed on the core manager if you wish to FTP to the Core.

Procedures

Connecting to another node using telnet

At the workstation

1 Telnet to the core manager, and log in using your passthru user ID and password (if prompted).

A telnet connection is established to the destination node.

2 At the prompt, enter your user ID and password to log in to the destination node.

3 You have completed this part of the procedure.

Connecting to the Core using FTP

At the workstation

1 FTP to the core manager, and log in using your passthru user ID and password.

The prompt changes to `ftp>`

2 Connect to the Core:

ftp> **site cm**

Note: Once connected to the core, if you lose your connection, the core drops your login session within five seconds. If your login id is not released by the core, then login to the core with another userid and manually end the original login session.

3 You have completed the procedure.

Connecting to the Core using SCFT

At the workstation

1 Enter a command.

Note: Once SCFT is installed, you have a choice of several commands, which are listed in Starting an SCFT client session.

2 You have completed the procedure.

Adding CM userIDs and passwords for ETA and ATA clients

Purpose

Use the following procedure to add ERA values for CM userIDs and passwords.

Application

ATTENTION
To complete this procedure, the DCE userids must have been configured. Refer to procedure Creating a DCE user on page 113 in this document.

You must configure CM userIDs and passwords and add them to a list of ERA values for each ETA client principal account. When the ATA or ETA client requests a MAP/CI session, the ETA server obtains the client CM userID and password ERA values, and uses them to log in to the switch for the client.

Procedure

Adding CM userIDs and passwords

At the client workstation

1 Log into the client workstation.

2 Log into DCE using the administrator userID:

`dce_login <DCE_admin_user>`

where

<DCE_admin_user>
is the administrator userID

3 Enter your DCE password.

4 Access the bin directory:

`cd /sdm/bin`

5 Add the ERA value for the CM userID and password:

`./add_cm_userid <principal_name> <CM_userID_list> [<CM_password_list>]`

where

<principal_name>
is the DCE userID

<CM_userID_list>
s the CM userIDs

[*<CM_password_list>*]
is all CM passwords (optional)

Note 1: A CM userID can appear more than once.

Note 2: The CM password list is optional. If you do not provide this information, the add_cm_userid command automatically assigns * for each password. The password can then be changed through the ATA or ETA client (refer to procedure “Changing CM passwords from the ETA client” and “Changing CM passwords from the ATA client” in this document). If you provide this information, align each CM userID and password so that the first password corresponds to the first userID.

Example
./add_cm_userid ops_1 “admin cmap5 cmap8” “a_pwd pwd_5 pwd_8“

Three CM user accounts are created for the ATA or ETA client ops_1. The password for the admin userID is a_pwd; for the cmap5 userID, pwd_5; for the cmap8 userID, pwd_8.

Example
./add_cm_userid ops_1 “admin admin admin” “a_pwd pwd_5 pwd_8”

The CM admin userID has three different passwords (pwd_1, pwd_2 and pwd_3). Each password is used to access different switches.

6 You have completed this procedure.

You can proceed to the procedure Adding core manager userIDs and passwords for ETA and ATA clients on page 148 if you want to allow users access to the core manager using the ETA application.

Adding disks and creating a logical volume in datavg

Purpose

Use this procedure to add disks and create logical volumes in datavg.

Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

Use this procedure to

- add disks to the data volume group (datavg)
- create a new logical volume in the datavg

Note: The maximum number of datavg disks that can be provisioned on a core manager is 11 pairs.

ATTENTION
This procedure must be performed by a trained Advanced Interactive Executive (AIX) system administrator authorized to perform config-manage actions.

ATTENTION
Perform this procedure after your system has been installed with the required I/O controller modules installed, in pairs, in the main or I/O expansion chassis. If you have not installed the required modules, refer to the procedure “Adding I/O controller Modules” in the SDM Upgrades document.

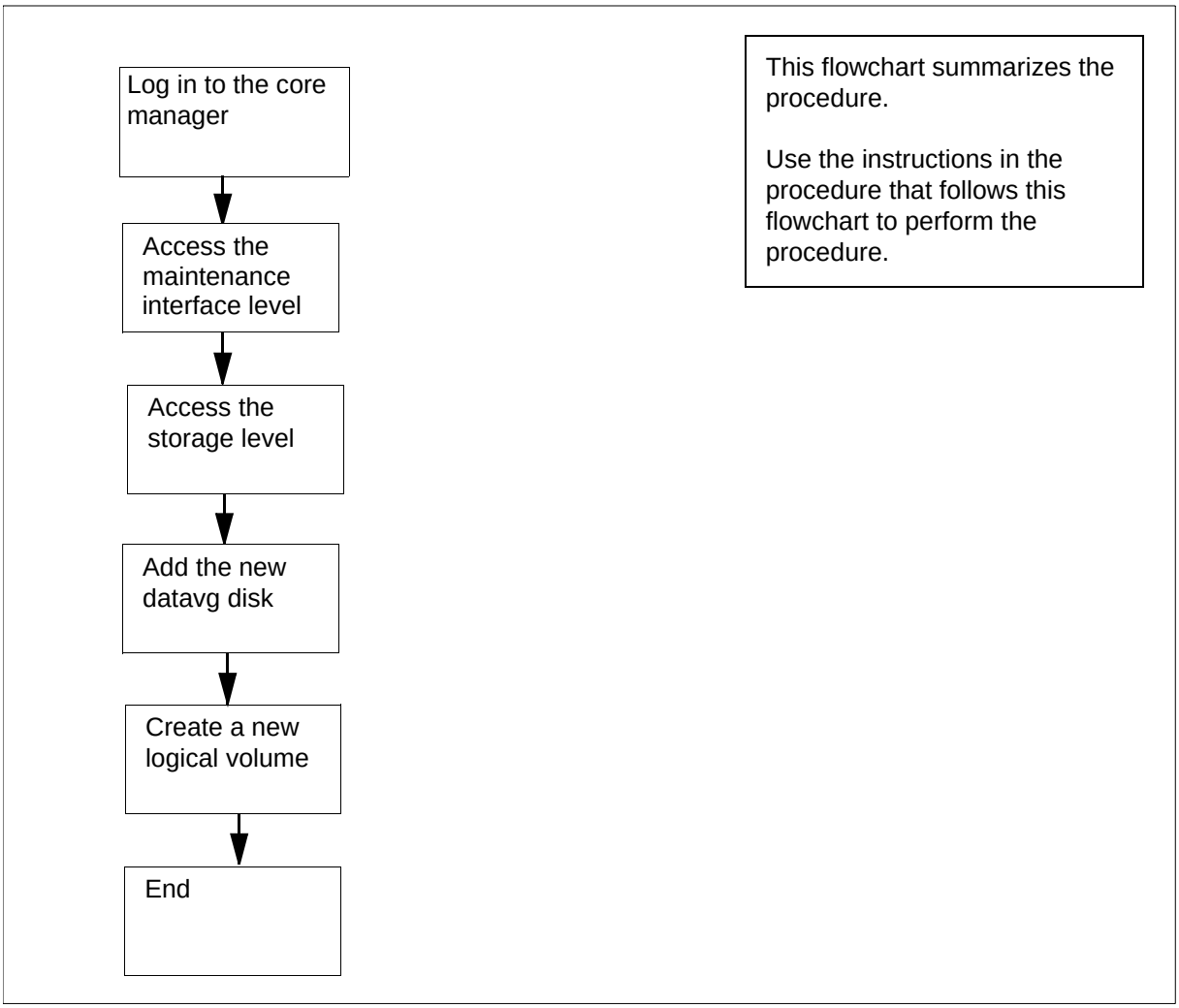
If you have a root volume group (rootvg) system, and you want to add datavg to your system, use the procedure “Migrating from a rootvg system to a rootvg/datavg system” in the SDM Upgrades document.

ATTENTION
The logical volume management feature allows you to create no more than 32 logical volumes.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the procedure.

Summary of adding disks and creating a logical volume in datavg



Adding disks and creating a logical volume in datavg

At the local VT100 console

1 Log in to the core manager as a user authorized to perform config-manage actions.

2 Access the maintenance interface:

```
# sdmmtc
```

3 Access the storage menu level:

```
> storage
```

Example response:

```
Volume Group            Status            Free
(MB)   rootvg              mirrored
608
datavg                mirrored             7872

Logical Volume   Location
1 /            rootvg     20             25/ 80
2 /usr         rootvg     192            85/ 90
3 /var         rootvg                    11/ 80
4 /tmp         rootvg     24              6/ 90
5 /home        rootvg     300             4/ 70
6 /sdm         rootvg     300            44/ 90
7 /data        datavg     300           20/ 80
Logical volumes showing: 1 to 7 of 7
```

Note: The example response shows part of the information displayed at the storage level.

4 Determine your next step with regards to I/O modules.

If you have	Do
added an Input/Output (I/O) module and you want to add the module to the datavg before you create your logical volume	step 5
not added an I/O module and you have enough free disk space for the logical volume that you want to create	step 6

5 Add a new disk:

> add vg

Example response:

```
The following disks will be added to the system:

Datavg is currently being created...
```

The system informs you when the disk has been added successfully.

Example response:

```
All disks were successfully added.

Command complete.
```

Note 1: This step automatically adds the new disks to the datavg.

Note 2: An error message is displayed if the disks are not added successfully. If this occurs, contact the personnel responsible for the next level of support.

6 Create the new logical volume:

> add lv <xxx> <Mbyte>

where

<xxx>
is the new logical volume name

<Mbyte>
is the size of the logical volume in Mbyte

Example response:

```
Creating Volume XXX ...
Volume Successfully Created...
Volume was created...
Command complete
```

7 You have completed this procedure.

Adding or removing passthru users

Purpose

Use the following procedure to add or remove one or more passthru users. You can change the information for an existing passthru user using the Change command.

Application

A passthru user is a core manager user ID that is used to connect to a node that is logically behind the core manager in a network, such as the CM or XA-Core. A passthru user cannot perform any functions on the core manager itself.

ATTENTION
For the *current release*, there is *no limit* to the number of telnet sessions allowed for maintenance and passthru users. For previous releases, a total of 16 telnet sessions is allowed.

You can configure a passthru user ID with or without a password. However, a password is required to transfer or retrieve files to or from a node using FTP. The Secure File Transfer (SFT) application must be installed on the core manager to use FTP with a passthru user ID. SFT must be configured in either Normal FTP access mode or Secure and Normal FTP access mode. Refer to the following SFT procedures:

- “Installing the SFT server software”
- “Configuring the SFT server application software”
- “Transferring and retrieving files using SFT”

Note 1: The Distributed Computing Environment (DCE) is not required for SFT, but it can add more security to the file transfer environment.

Note 2: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Adding or removing passthru users

At the core manager

1 Log into the core manager as a user authorized to perform security-admin actions.

2 Access the passthru level:

```
sdmmtc passthru
```

3 Create or delete a passthru user.

If you want to	Do
add a passthru user	step 4
delete a passthru user	step 13

4 Add a passthru user:

add

5 When prompted, enter the user name for the new user (for example, cmusr).

6 When prompted, enter the real name for the passthru user (for example, CM passthru).

7 When prompted, type the telnet command arguments for the passthru user.

Note: The telnet command arguments can be the hostname or the IP address of the destination node. If you are adding a user ID that is used to connect to the CM or XA-Core, the telnet command arguments must be cm.

8 When prompted, indicate whether a password is required.

Note: A password is required for user IDs that is used to connect to the CM or XA-Core using FTP.

9 When prompted, confirm the data you entered:

y

If you indicated a password	Do
is required	step 10
is not required	step 12

10 When prompted to set the initial password, enter a password.

11 When prompted, re-enter the password to confirm it.

Note: The user who accesses the core manager for the first time using this new passthru user ID, is first prompted for the initial password and then prompted to change it.

12 Add another user or finish this procedure.

If you	Do
want to add another user	step 4
do not want to add another user	you have completed this procedure

13 To delete the passthru user:

`delete <username>`

where

<username>
is the user ID of the user you want to delete

14 When prompted, confirm you want to delete the user:

y

15 Use the following table to determine your next step.

If you	Do
want to delete another user	step 13
do not want to delete another user	you have completed this procedure

Adding core manager userIDs and passwords for ETA and ATA clients

Purpose

Use this procedure to set an ERA value for a core manager userID.

Prerequisites

ATTENTION

To complete this procedure, you must have created the DCE principals for the ETA and ATA users. Refer to procedure Creating a DCE user on page 113 in the Security and Administration section.

Application

You must set an ERA value for the core manager userID of the ETA client using the add_sdm_userid command.

When an ATA or ETA client initiates a core manager session, the ETA server obtains the ERA value for the core manager userID of that client. The value is used to start a core manager session.

Procedure

Adding userIDs for the ATA and ETA client

At the client workstation

1. Log into the client workstation.
2. Log into DCE using the administrator userID:

   > dce_login <*DCE_admin_user*>

   where

   <DCE_admin_user>
   is your administrator userID
3. Enter your DCE password.
4. Access the bin directory:

   > cd /sdm/bin

5 Add the ERA value for the userID:

```
> ./add_sdm_userid <principal_name>
<sdm_userid>
```

where

<principal_name>
is the DCE userID you wish to set ERA values for

<sdm_userid>
is the userID you wish to have

6 You have completed this procedure.

Assigning the master server for DCE

Purpose

Use this procedure to assign the DEC master server.

Prerequisites

ATTENTION
This procedure can affect the DCE cell. You must be a Distributed Computing Environment (DCE) system administrator to perform this procedure. Perform this procedure with caution.

Application

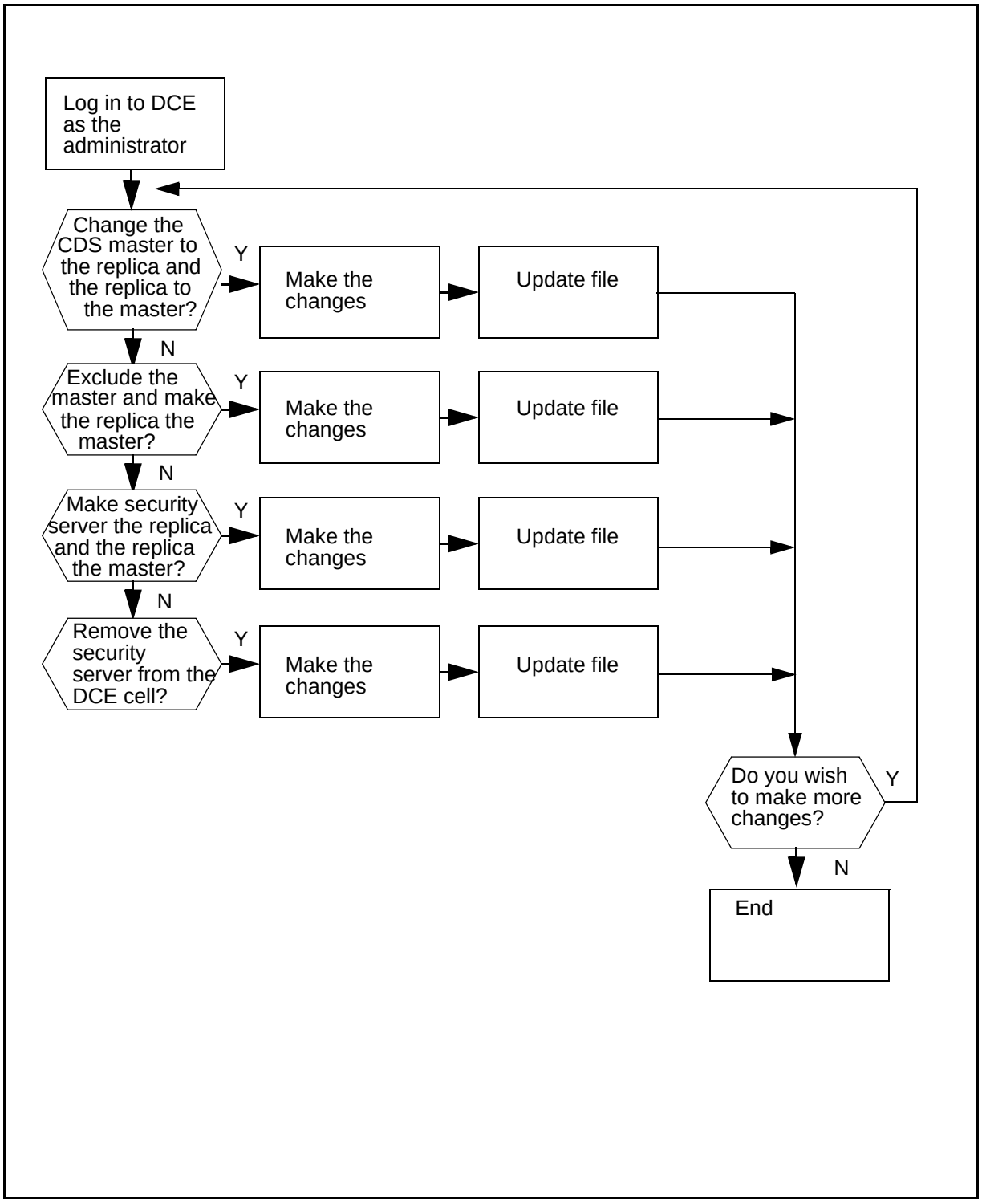
Use this procedure to perform the following items:

- assign a new master CDS clearinghouse
- exclude a replica CDS clearinghouse
- assign a new master security server
- remove a replica security server

Procedure

The flowchart that follows provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the procedure.

Summary of assigning the master server for DCE



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Assigning the master server for DCE

At the local or remote VT100 console

1 Login to the DCE cell as an administrator:

dce_login <principal_name>

where

<principal_name>
is the user ID of the administrator.

2 Determine which DCE re-mastering script to run.

If you are	Do
assigning a new master CDS clearinghouse	step 3
excluding a replica CDS clearinghouse	step 7
assigning a new master security server	step 10
removing a replica security server	step 13
not making any changes	step 16

3 Assign a new master CDS clearinghouse:

/sdm/bin/remaster_cds_server master <new_master_hostname> replica <replica_hostname_list>

where

<new_master_hostname>
is the host name of the master server.

<replica_hostname_list>
is the list of hostnames for replica servers that remain in the CDS replica clearinghouse set.

4 Confirm the request:

yes

After you confirm your request, the system displays the following response:

```
Remastering CDS server...
   Remastering/.:...
   Remastering/.:...
```

5 Update the cds_cache.wan file:

.sdm/bin/update_cds_cache_wan

6 Return to step 2 to determine your next step.

7 Exclude a list of replica CDS clearinghouses:

/sdm/bin/remaster_cds_server master <master_host_name> replica <replica_hostname_list> exclude <exclude_replica_hostname_list>

where

<master_hostname>
is the host name of the new master server.

<replica_hostname_list>
is the list of host names for replica servers.

<exclude_replica_hostname_list>
is the list of host names of replica servers you want to exclude from the CDS replica clearinghouse set.

8 Update the cds_cache.wan file:

/sdm/bin/update_cds_cache_wan

9 Return to step 2 to determine your next step.

10 Assign the new master security server:

/sdm/bin/remaster_sec_server <new_master_server_hostname>

where

<new_master_server_hostname>
is the hostname of the new DCE master security server.

11 Update the cds_cache.wan file:

/sdm/bin/update_pe_site

12 Return to step 2 to determine your next step.

13 Remove the replica security server:

/sdm/bin/remove_sec_server_data <replica_security_server_hostname>

where

<replica_security_server_hostname>
is the hostname of the replica security server you want to remove from the DCE cell.

14 Update the cds_cache.wan file:

/sdm/bin/update_pe_site

15 Return to step 2 to determine your next step.

16 You have completed this procedure.

Removing ERA values for CM userIDs and passwords

Purpose

Use the following procedure to remove ERA values for CM userIDs and passwords.

Application

The remove_cm_userid command removes ERA values for CM userIDs and passwords.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Removing ERA values for CM userIDs and passwords

At the client workstation

1 Log into the client workstation.

2 Log into DCE using the administrator userID:

dce_login <DCE_admin_user>

where

<DCE_admin_user>
is the administrator userID

3 Enter your DCE password.

4 Change to the bin directory:

cd /sdm/bin

5 Remove the ERA value for the CM userID and password:

/remove_cm_userid <principal_name>

where

<principal_name>
is the CM userID for the ERA value to remove

6 You have completed this procedure.

Removing DCE port restrictions

Purpose

Use the following procedure to return the core manager to the system default values.

Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

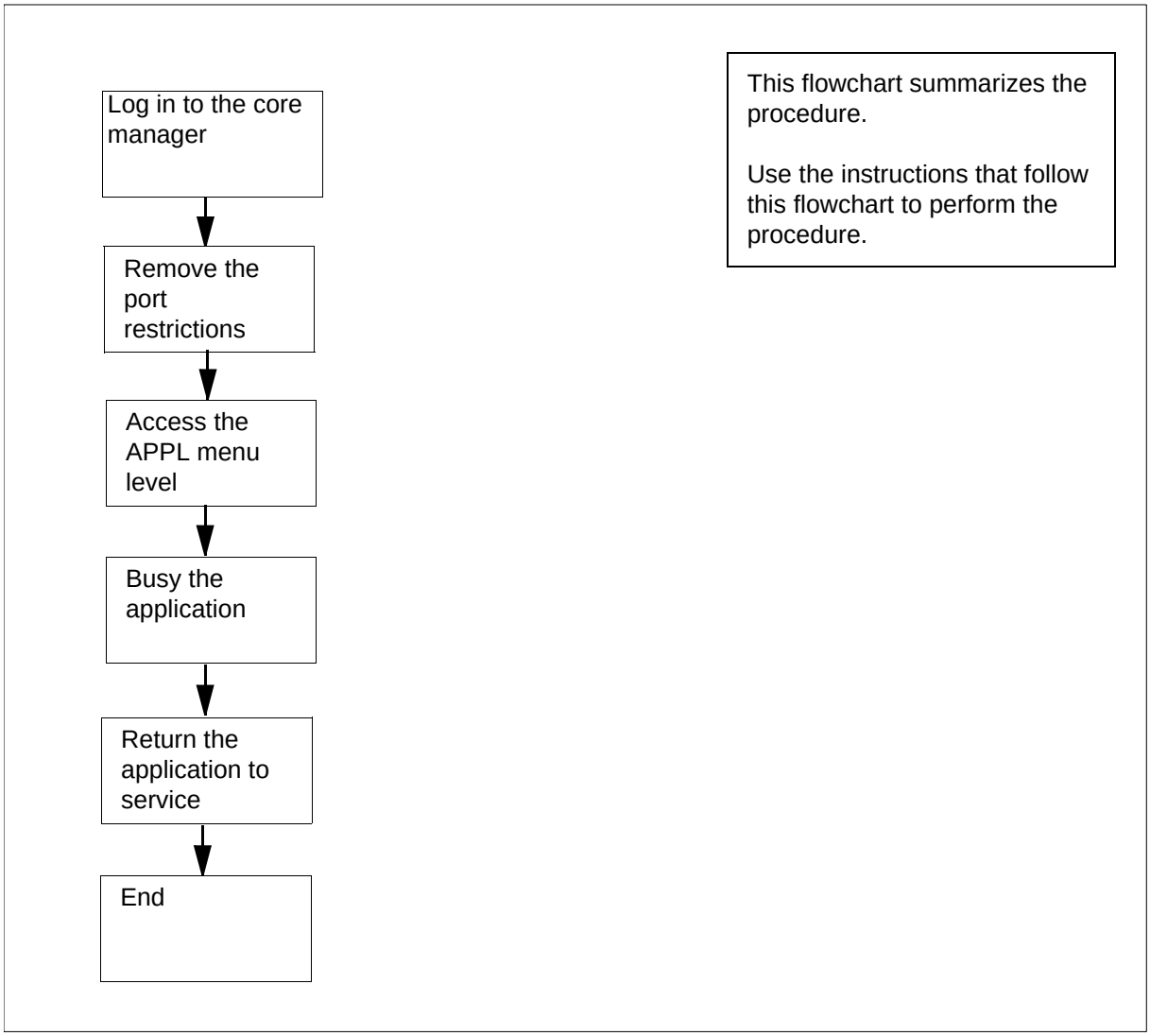
ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator who knows DCE administration procedures.

DCE ports are randomly assigned when you complete this procedure. You must log in as the root user to perform this procedure.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of removing DCE port restrictions



Removing DCE port restrictions

At the client workstation

1 Log in to the core manager as a user authorized to perform config-manage actions.

2 Restrict the ports to a core manager-defined range:

 # restrict_dce_ports unrestricted

Example response:

```
DCE servers port range restrictions have been
removed.
```

3 Access the maintenance interface:

 # sdmmtc

4 Access the NET level:

> net

5 Wait for DCE to go to InSv. This may take several minutes.

Example response:

```
DCE State:  .
```

6 Access the application (appl) level:

> appl

Example response:

```
#
Application                                State
1 Table Access Service                       .
2 OM Access Service                          .
3 Log Delivery Service                       .
4 Secure File Transfer                       .
5 Enhanced Terminal Access                   .
6 Exception Reporting                           .
```

7 Determine the key number for the application (shown under the header “#”).

8 Manually busy the application software:

> bsy <n>

where

<n>
is the application number to busy

Example response:

```
The application is in service.
This command will cause a service interruption.
Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, or “N”):
```

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

9 Confirm the Busy command:

> y

After you confirm the Bsy command, the following is displayed:

```
Application Bsy - Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappears. The word “initiated” also changes to “submitted”:

```
Application Bsy - Command submitted.
```

10 Return the application to service:

> rts <n>

where

<n>
is the number next to the application you busied previously

Example response:

```
Application RTS - Command initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application RTS - Command submitted.
```

11 You have completed this procedure.

Removing the ERA value for the userID

Purpose

Use the following procedure to remove the ERA value for the userID.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Removing the ERA value for the userID

At the client workstation

1 Log into the client workstation.

2 Log into DCE using the administrator userID:

dce_login <DCE_admin_user>

where

<DCE_admin_user>
is the administrator userID

3 Enter your DCE password.

4 Access the bin directory:

cd /sdm/bin

5 Remove the ERA value for the userID:

./remove_sdm_userid <principal_name>

where

<principal_name>
is the userID for the ERA value you are removing

6 You have completed this procedure.

Restricting DCE ports to a predefined range

Purpose

Use the following procedure to restrict the ports to a range that is predefined by the core manager software.

Prerequisites

You must have root user privileges to perform this procedure.

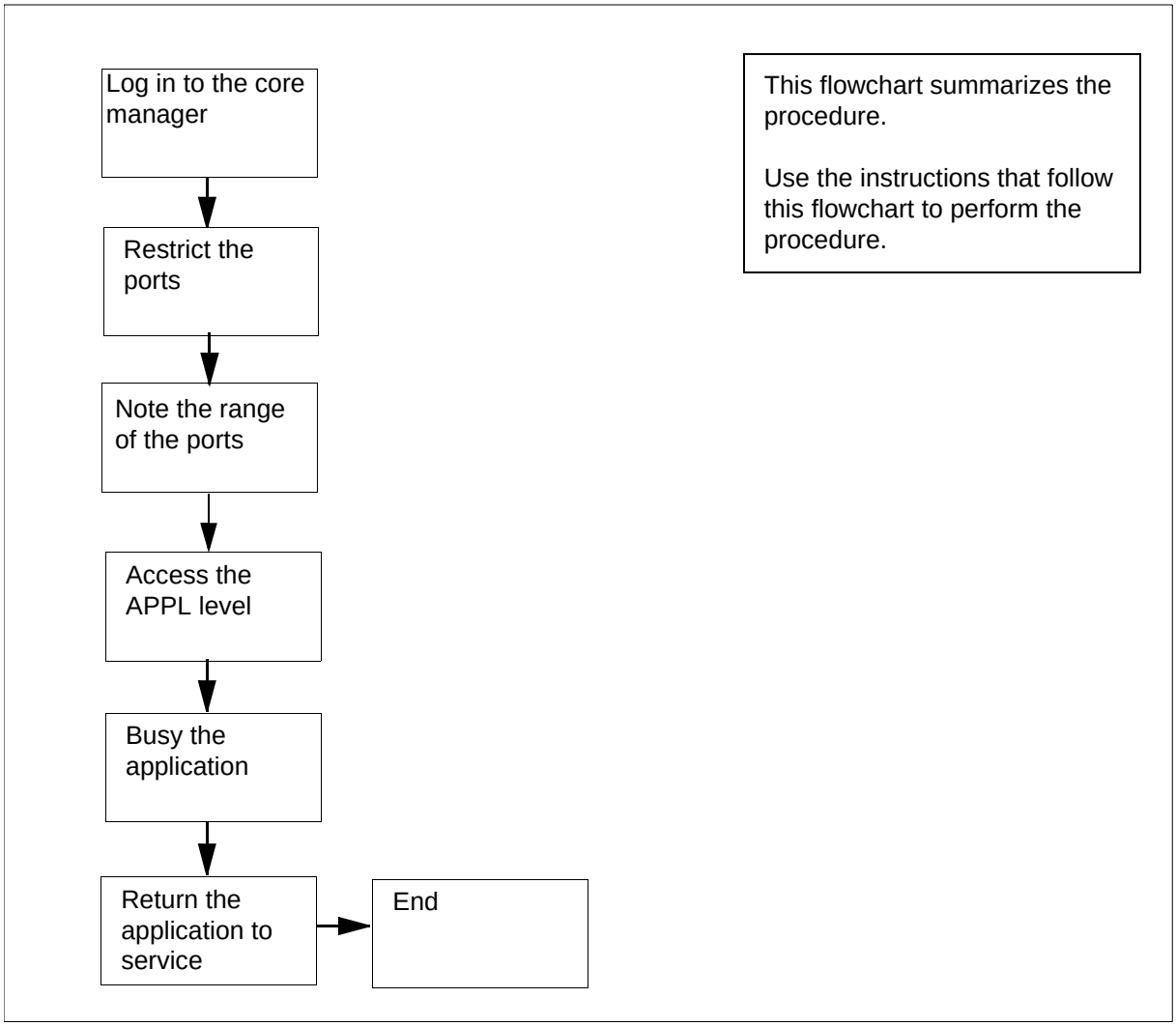
ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator.

The range of ports must be compatible with other core manager applications.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of restricting DCE ports to a predefined range



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Restricting DCE ports to a predefined range

At the client workstation

1 Log in to the core manager as the root user.

2 Restrict the ports to a core manager-defined range:

restrict_dce_ports system_defined

Response:

```
The following port ranges have been configured
   TCP: 4500-4540    UDP: 4500-4540
Killing and restarting SDM's DCE daemons for the
change to take effect...
Stopping DCE daemons:
killing dced

Please run sdmmtce tool:
under the Mtc/LAN level: wait for DCE state to
change to InSv.
under the MTC/Appl level: BSY and then RTS any
application that uses DCE.
```

3 Record the range of ports that are displayed Use these values for the firewall configuration.

4 Access the maintenance interface:

sdmmtc

5 Access the NET menu level:

net

6 Wait for DCE to go to InSv. This may take several minutes.

Example response:

```
DCE State:    .
```

7 Access the application (Appl) level:

appl

Example response:

```
# Application                          State
1 Table Access Service                   .
2 OM Access Service                      .
3 Log Delivery Service                   .
4 Secure File Transfer                   .
5 Enhanced Terminal Access               .
6 Exception Reporting                    .
```

8 Determine the key number for the application (shown under the header "#").

9 Busy the application software:

bsy <app_no>

where

<app_no>
is the number next to the application to busy

Example response:

```
The application is in service.
This command will cause a service interruption.
Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, or “N”):
```

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

10 Confirm the Busy command:

y

After you confirm the Bsy command, the following is displayed:

```
Application Bsy- Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application Bsy - Command submitted.
```

11 Return the application to service:

rts <num>

where

<num>
is the number next to the application you previously busied

Example response:

```
Application RTS - Command initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application RTS - Command submitted.
```

12 You have completed this procedure.

Restricting DCE ports to a specific range

Purpose

Use the following procedure to restrict the ports to a specific range.

Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

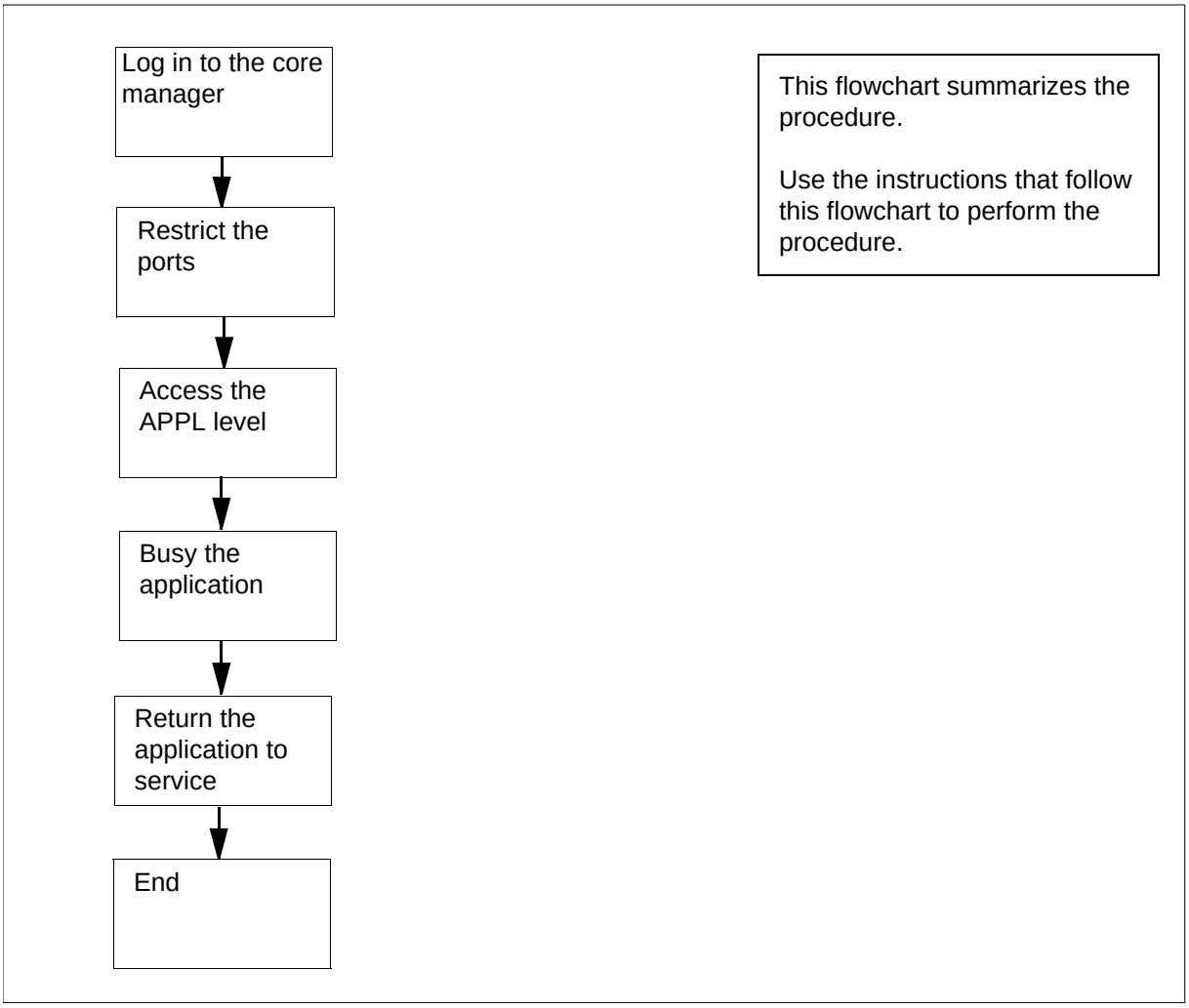
ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator.

You must have root user privileges to perform this procedure.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of restricting DCE ports to a specific range



Restricting DCE ports to specific range

At the client workstation

1 Log in to the core manager as a user authorized to perform config-manage actions.

2 Restrict the ports to a core manager-defined range:

 # restrict_dce_ports tcp <start_TCP>:<end_TCP> udp <start_UDP>:<end_UDP>

where

<start_TCP>
is the start of the range for TCP ports (must be greater than 1024)

<end_TCP>
is the end of the range for TCP ports (must be less than 32 000)

<start_UDP>
is the start of the range for universal datagram protocol (UDP) ports (must be greater than 1024)

<end_UDP>
is the end of the range for UDP ports (must be less than 32 000)

Example response:

```
The following port ranges have been configured
      TCP: 3000-3050        UDP: 3000-3050
```

3 Access the maintenance interface:

 # sdmmtc

4 Access the NET level:

> net

5 Wait for DCE to go to InSv. This can take several minutes.

Example response:

```
DCE State:     .
```

6 Access the application (APPL) level:

> appl

Example response:

```
# Application                              State
1 Table Access Service                       .
2 OM Access Service                          .
3 Log Delivery Service                       .
4 Secure File Transfer                       .
5 Enhanced Terminal Access                   .
6 Exception Reporting                           .
```

7 Determine the key number for the application (shown under the header “#”).

8 Busy the application software:

> bsy <app_no>

where

<app_no>
is the number next to the application to busy

Example response:

```
The application is in service.
This command will cause a service interruption.
Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, or “N”):
```

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

9 Confirm the Busy command:

> y

10 After you confirm the Bsy command, the following is displayed:

```
Application Bsy - Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application Bsy - Command submitted.
```

11 Return the application to service:

> rts <app_no>

where

<app_no>
is the number next to the application you busied previously

Example response:

```
Application RTS - Command initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application RTS - Command submitted.
```

12 You have completed this procedure.

Setting SFT access permissions

Purpose

Use the following procedure to set the SFT access permissions for an SFT client.

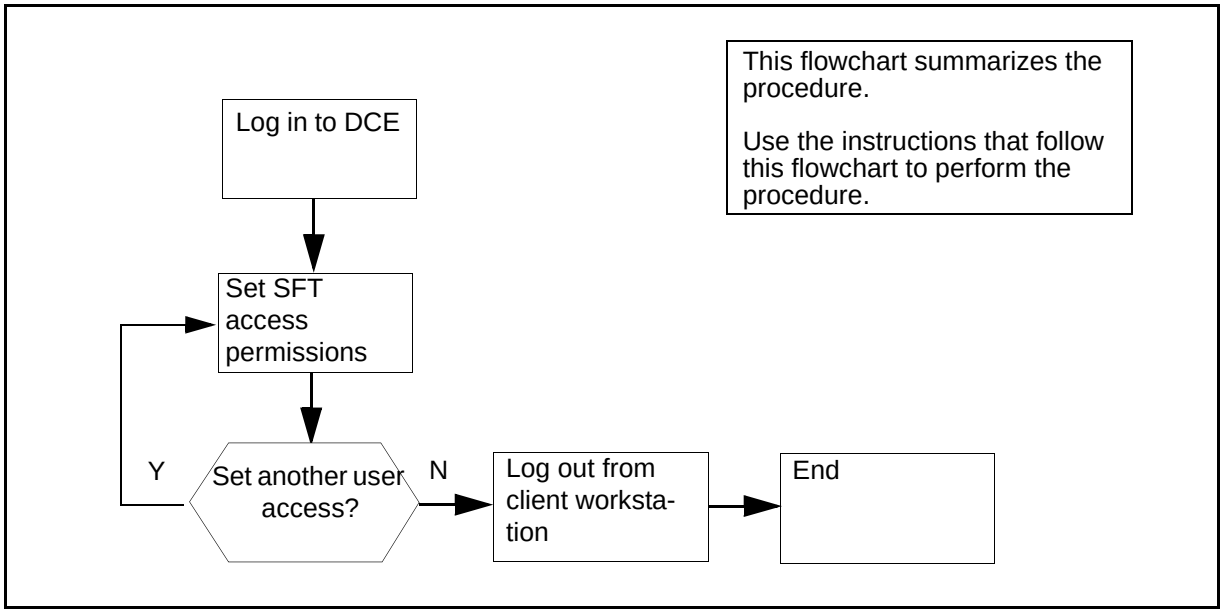
Application

The default permission for the SFT user is none. If you do not perform this procedure, the user does not have access to SFT

Procedure

The following flowchart summarizes the procedure. To complete the procedure, perform the procedures that follow the flowchart.

Summary of setting the SFT access permission



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Setting the SFT access permissions

At a UNIX prompt on the client workstation:

1 Log in to DCE as the DCE administrator:

dce_login <admin_name>

where

<admin_name>
is the userID for the administrator account

2 Enter the administrator password.

3 Access the /sdm/bin directory:

cd /sdm/bin

4 Set the SFT client access permissions for the user:

/set_sft_access <DCE_principal> <SFT_permission>

where

<DCE_principal>
is the DCE userID whose access permissions you are changing.

<SFT_permission>
is the access permission level for the user. Values are as follows:

- none (access is not permitted to the SFT services - default value)
- sdm_only (access is permitted to the core manager)
- dm_cm (access is permitted to both the core manager and the CM)

5 Repeat step 4 to set SFT access for another user.

6 Log out from the client workstation:

exit

7 You have completed this procedure.

Setting the time zone, or the date and time

Purpose

Use this procedure to set the time zone, or the date and time on the core manager.

Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

ATTENTION
This procedure must be performed only by UNIX system administration personnel authorized to perform config-manage actions.

ATTENTION
The time zone, date and time on the core manager cannot be changed when DCE is operational. The core manager must also be in ManB or OffL state to change the time zone, date and time.

Application

Once you have entered the new time zone, or the date and time, the values are recalculated from the system clock and displayed on the screen to confirm the change.

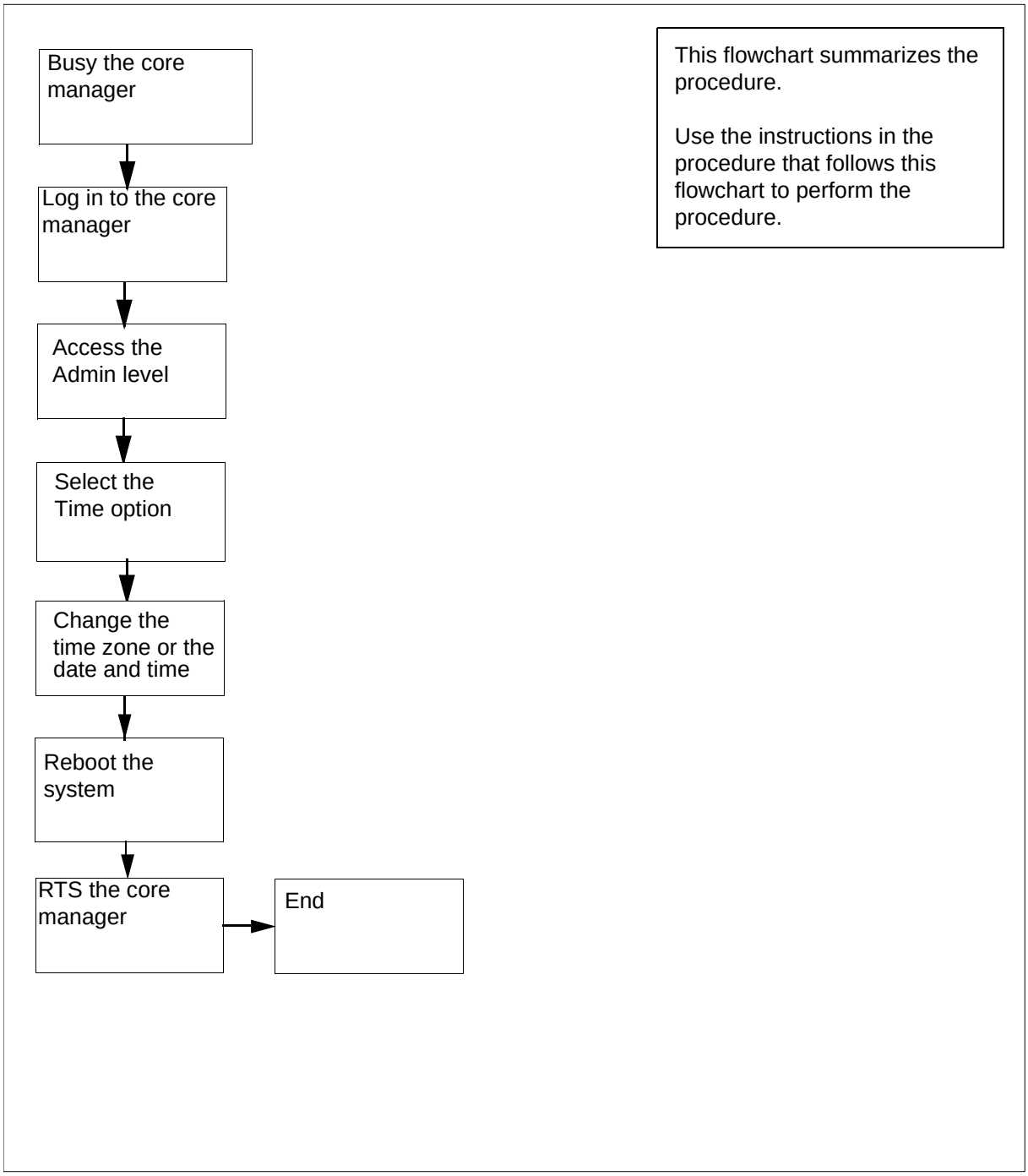
You must reboot the core manager after changing the time zone, or the date and time for the changes to take effect.

Note: The time zone, date and time cannot be changed together. You must complete the procedure once for setting or changing the time zone and again for setting or changing the date and time.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of setting the time zone, or the date and time



Setting the time zone, or the date and time

At the MAP display

1 Access the core manager from the APPL level of the MAP display:

```
> mapci;mtc;appl
```

If the core manager node state is	Do
in service (InSv)	step 3
anything else	step 2

2 A fault exists on the core manager, or another core manager maintenance activity is already in progress. Clear the fault or complete the maintenance activity, as required.

Clear the faults by checking for core manager-related alarms under the APPL header of the MAP display alarm banner, and use the appropriate alarm clearing procedure in the Fault Management document to clear the fault before continuing this procedure.

3

CAUTION
Loss of service
Manually busying the core manager shuts down all applications without warning to the application users.

Busy the core manager:

```
> bsy
```

Example response:

```
SDM is in service.
This command will cause a service interruption.
Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

4 Confirm the Bsy command:

```
> y
```

Example response:

```
SDM Bsy initiated.
SDM Bsy completed.
```

At the local or remote VT100 terminal

5 Log into the core manager as a user authorized to perform config-manage actions.

If you are configuring	Do
date and time	step 10
time zone	step 6

6 Configure the time zone:

```
# sdmconfig
```

7 Select the date and time zone:

```
> 2
```

8 Refer to the procedure Recommissioning date and time zone to configure the time zone. Return to this procedure after configuring the time zone.

9 Proceed to step 19.

10 Access the maintenance interface level:

```
# sdmmtc
```

11 Access the administration (Admin) level:

```
> admin
```

12 Select Time:

```
> time
```

13 Confirm you want to proceed with the procedure:

```
> y
```

14 The Change / Show Day and Time screen appears. Use the up and down arrows to move the cursor to a date or time entry you want to change. Repeat until you modify all the entries you want to change. Press the Enter key.

The Command Status screen appears. The command status is shown as “running” while the system processes the changes. The command status changes to “OK” when processing completes. The date, time and time zone appear.

15 Exit the command status screen by pressing the F10 key. You can also press the ESC key and the number 0 key to exit the screen.

At the SDM level of the MAP display

16 Reboot the core manager:

```
> rebootsdm
```

Example response:

```
Communication with the SDM will be down for
approximately 10 minutes.

Do you wish to proceed?

Please confirm (“YES”, “Y”, “NO”, or “N”):
```

17 Confirm that you want to proceed:

```
> y
```

Example response:

```
SDM 0 ManB                          Links_00S: .
/ RebootSDM in progress
SDM 0 RebootSDM initiated.
```

Note: The command response indicates that the command has been successfully received by the core manager. The maintenance flag, “Reboot SDM in progress” is displayed until the core manager recovers from the reboot.

18 When the maintenance flag message disappears, continue with step 19.

19 Return the core manager to service:

```
> rts
```

Example response:

```
SDM InSv                             Links_00S:  .
SDM RTS initiated.
SDM RTS completed.
```

Note: If there are no other faults on the system, then the core manager applications automatically return to service immediately following the completion of the reboot.

20 You have completed this procedure.

Starting an FTP client

Purpose

Use this procedure to start an FTP client.

Application

Use the SFT client for secure FTP connections. Standard FTP userIDs and passwords are not encrypted when they are passed across the network.

SFT and FTP clients can both access the CM FTP server by using the command SITE CM. You can use standard FTP commands with some exceptions.

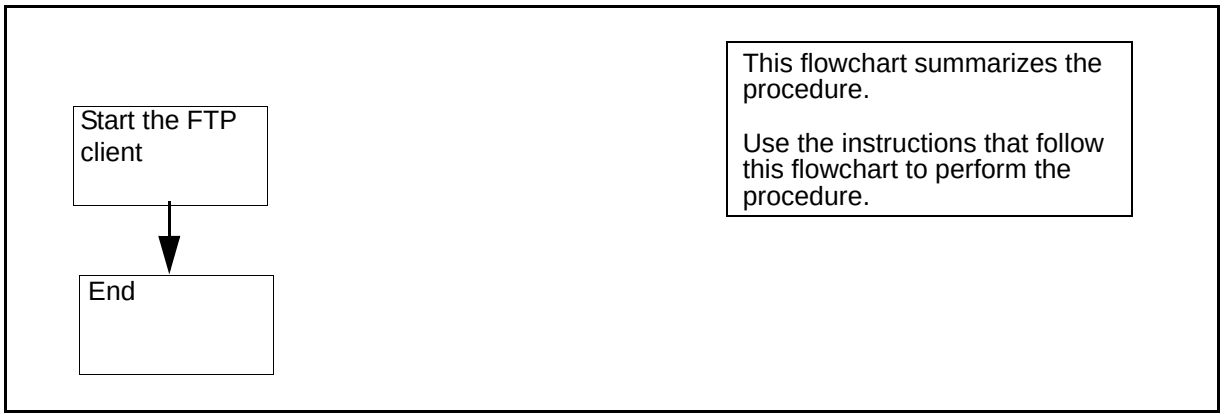
The limits to standard FTP commands when accessing the CM FTP server are as follows.

- the user command is intercepted and disallowed by the SFT server. A user does not have to log in manually.
- the mkdir and rmdir commands are not supported by the CM FTP server. The CM file system contains volumes only. It does not support directory hierarchies within the volume.
- files transferred to SFDEV are owned by the user $$SYS$$.
- SFT performs a clean-up routine after the SFT application is returned to service.
  If you attempt to use the SITE CM command immediately after the RTS command is issued, you may experience a delay of about 20 seconds before access to the CM is given.
- file names and volume names are case sensitive. Volume names are always in uppercase, for example, S01DVOL1. File names are usually in uppercase.

Procedure

To complete the procedure for starting an FTP client, perform the procedure that follows the flowchart.

Summary of starting an FTP client



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Starting an FTP client

At a UNIX prompt:

1 Start the FTP client workstation:

ftp <address>

where

<address>
is the IP address, or the DNS address of the FTP server.

Note: The location of the FTP client varies.

2 For additional instructions on FTP client usage, refer to the documentation for the client application.

3 You have completed this procedure.

Transferring files as a passthru user using FTPProxy

Application

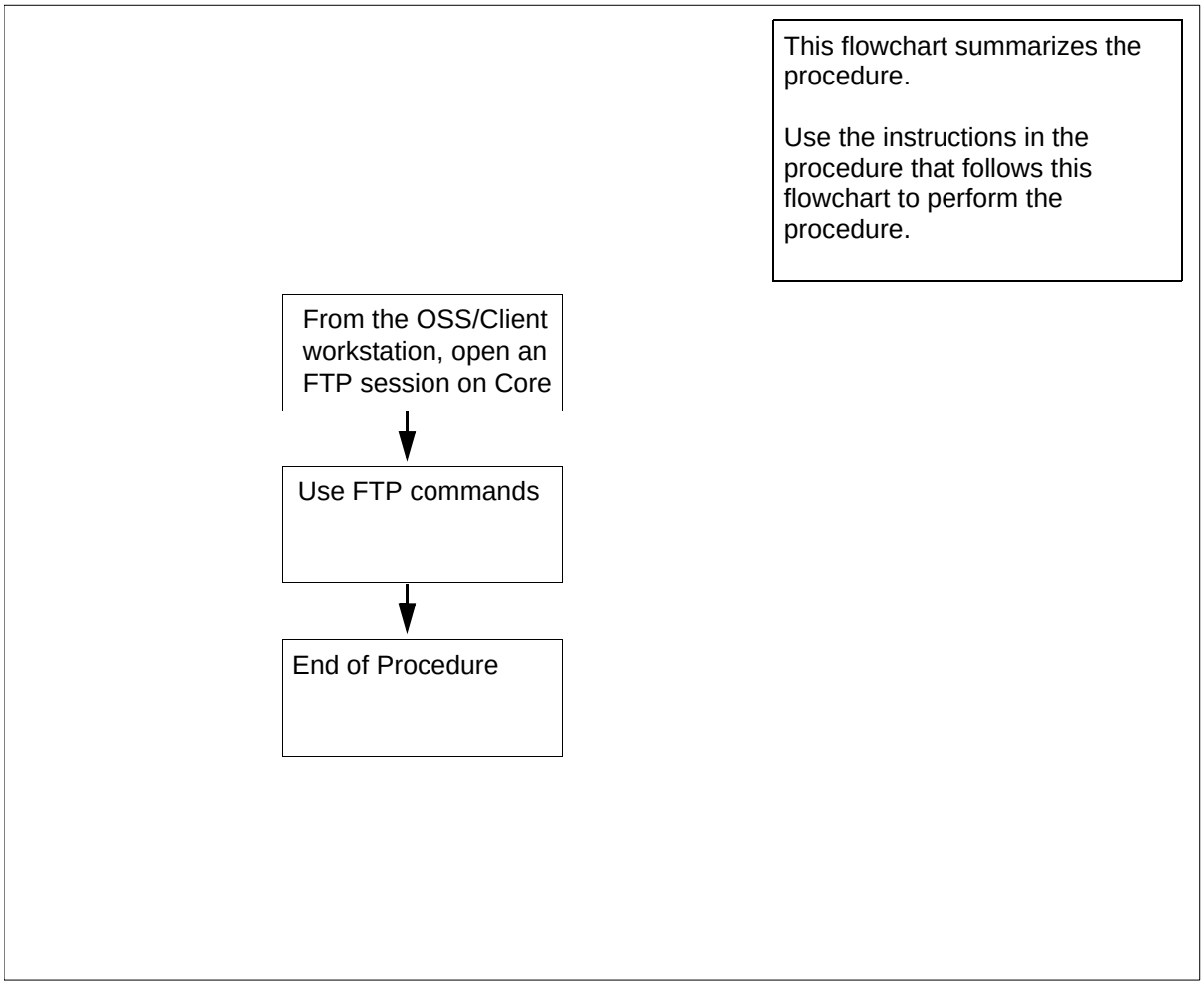
Use this procedure to transfer files between the OSS machine and the Core using the FTPProxy application. Use this procedure if you have passthru user privileges.

If you have core user privileges (mgcadm, mgcrw, mgcsprov, mgcmtce,and mgcro), refer to Transferring files as a passthru user using FTPProxy on page 178 in this document.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of transferring files as a passthru user using FTPProxy



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Transferring files as a passthru user using FTPProxy

At the OSS/Client workstation

1 Open an FTP session.

a Log in to the core manager by typing

```
ftp <IP address>
```

and pressing the Enter key.

where

<IP address>
is the IP address of the core manager.

b At the prompt, enter your userID.

c At the prompt, enter you password.

The FTPProxy application authenticates your userID and password and logs you in to the Core.

2 Use the commands in the table to transfer files.

If you want to	At the ftp> prompt, type the following command and press the enter key
transfer files in ASCII mode	ascii
transfer files in Binary mode	bin
get a file from the Core	get < filename on Core >
put a file to the Core from the OSS/client machine	put <filename on client machine>
list files on the Core - type	ls
- or type	dir
view the current directory on the core	pwd
log out of the ftp session	bye

3 You have completed this procedure.

Transferring files as a core user using FTPProxy

Application

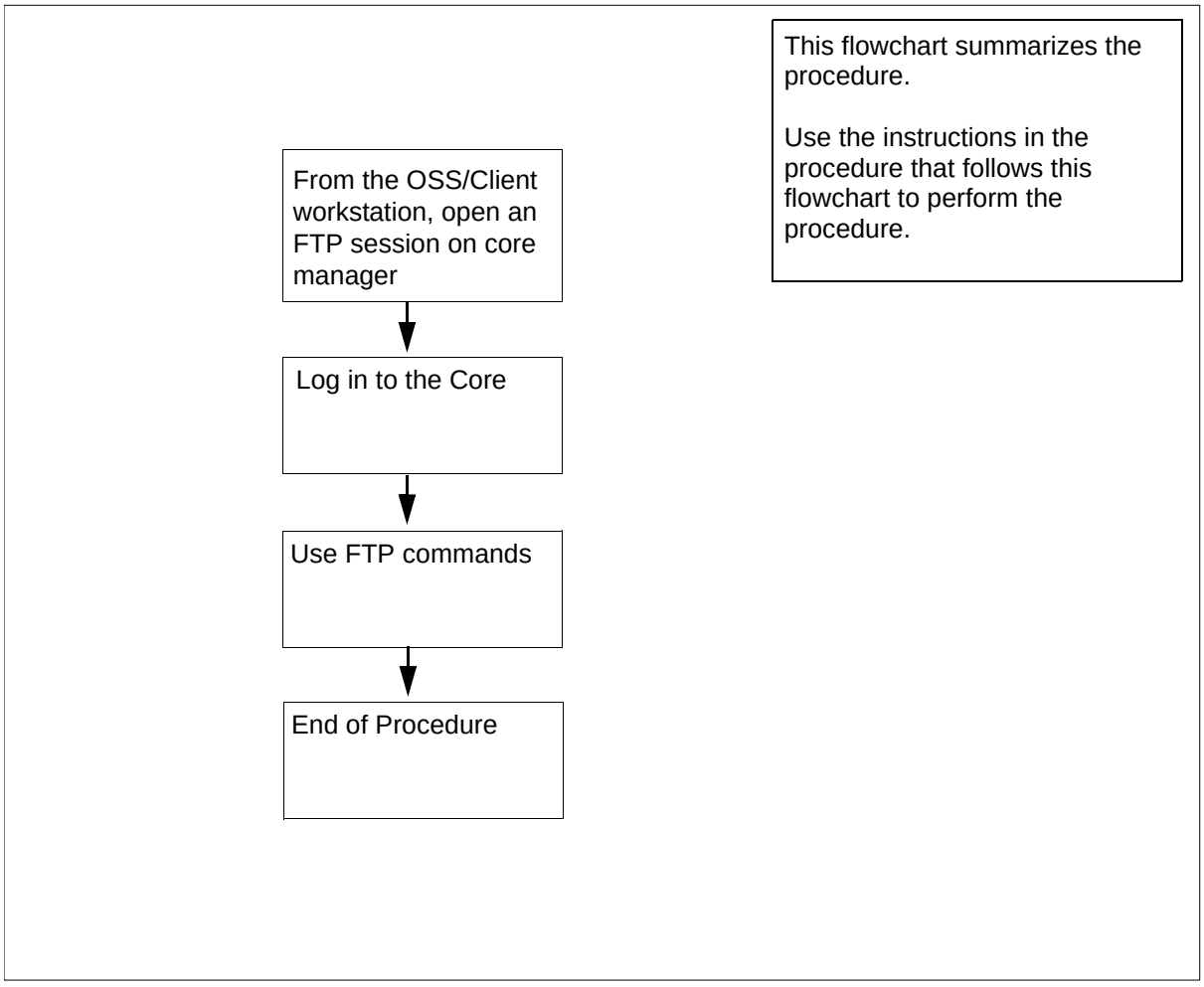
Use this procedure to transfer files between the OSS machine and the Core using the FTPProxy application. Use this procedure if you have core user privileges. Core user privileges include mgcadm, mgcrw, mgcsprov, mgcmtce,and mgcro.

If you have passthru user privileges, refer to Transferring files as a passthru user using FTPProxy on page 178 in this document.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of transferring files as a core user using FTPProxy



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Transferring files as a core user using FTPProxy

At the OSS/Client workstation

1 Log in to the core manager.

a Open an FTP session by typing

`ftp <IP address>`

and pressing the Enter key.

where

<IP address>
is the IP address of the core manager.

b At the prompt, enter your userID.

c At the prompt, enter you password.

The FTPProxy application authenticates your userID and password and logs you in to the core manager.

2 At the ftp> prompt, log in to the Core by typing

`ftp>` **`site cm`**

and pressing the Enter key.

The command logs you in to the Core.

3 Use the commands in the table to transfer files.

If you want to	At the ftp> prompt, type the following command and press the enter key
transfer files in ASCII mode	ascii
transfer files in Binary mode	bin
get a file from the Core	get < filename on Core >
put a file to the Core from the OSS/client machine	put <filename on client machine >
list files on the Core - type	ls
- or type	dir

If you want to	At the ftp> prompt, type the following command and press the enter key
view the current directory on the core	pwd
log out of the ftp session	bye

4 You have completed this procedure.

Starting an SFT session

Purpose

The following procedure describes how to start an SFT session in secure access.

Prerequisites

Ensure you have correctly defined the DCE principal names.

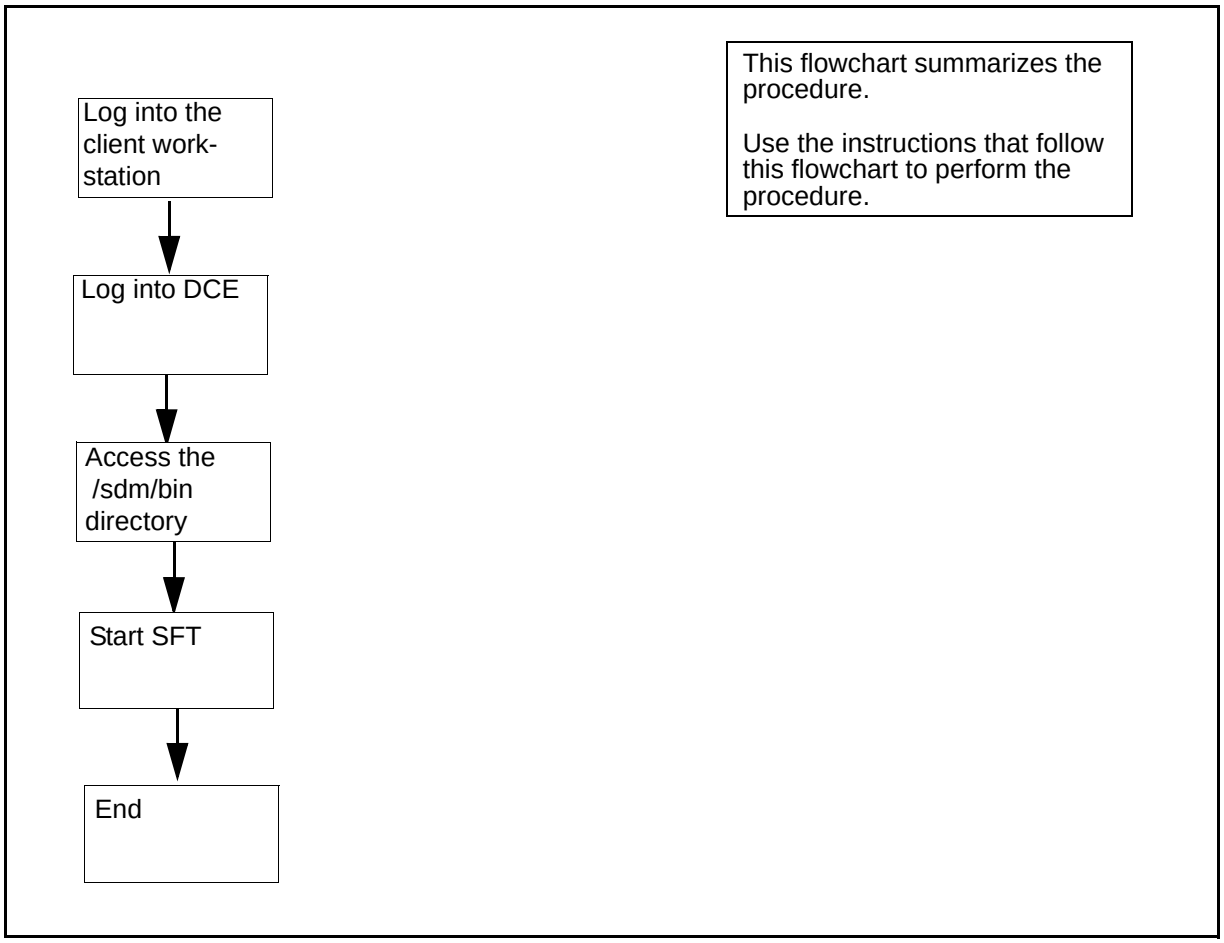
You must have a DCE account, and password to use SFT. If you do not have a DCE account, your DCE administrator can create one for you.

Application

Information is provided to enable the SFT client to access either the core manager, or the computing module (CM) for the purpose of doing file transfers.

Note: If you are using anonymous or normal FTP access, refer to the procedure, Starting an FTP client on page 176 in this document.

Summary of starting an SFT session



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Starting an SFT session

At the client workstation:

1 Log into the SFT client workstation.

2 Log into DCE:

dce_login

Example response:

```
Enter Principal Name:
```

3 Enter your DCE user ID.

Example response:

```
Enter Password:
```

4 Enter your DCE password.

5 Change to the bin directory:

cd /sdm/bin

6 Determine the CM CLLI.

If you	Do
know the value for the CM CLLI	step 7
do not know the value for the CM CLLI	step 9

7 Start the SFT application:

./sft <CLLI>

where

<CLLI>
is the CM CLLI, for example FCC11

Example response:

```
220 FCC11 SFTPD Server (Version 9.0.21.0 Jan
27 1998) ready.
```

8 Go to step 11

9 List the CM CLLIs for all core manager nodes in the same DCE cell as your SFT client workstation:

./sft clist

Example response:

```
FCC11 ottwaonye6a
```

10 Start the SFT application:

sft> open <CLLI>

where

<CLLI>
is the CM CLLI, for example FCC11

Example response:

```
220 FCC11 SFTPD Server (Version 9.0.21.0 Jan
27 1998) ready.
```

11 Transfer files to or from the CM, or to or from the core manager as follows.

- Transfer files to or from the CM:

  ```
  sft> site cm
  ```

- Transfer files to or from the core manager:

  ```
  sft> site sdm
  ```

12 Repeat step 11 as required.

Note: You can toggle between the CM and core manager at any time.

13 You have completed this procedure.

Transferring and retrieving files using SFT

Purpose

Use this procedure to transfer and retrieve files using SFT.

Application

The following sections describe the procedures to transfer and retrieve files using SFT:

- Transferring a file to a core manager directory on page 187
- Retrieving a file from a core manager directory on page 190
- Transferring a CM file to a CS 2000 volume on page 192
- Retrieving a CM file from a CS 2000 volume on page 196
- Retrieving an active DIRP file on page 198
- Discontinuing a file transfer on page 199

The following procedures are referenced in this procedure:

- Starting an SFT session on page 183
- Starting an FTP client on page 176

Transferring a file to a core manager directory

Use this procedure to transfer a file from the client workstation to a core manager directory. The file can be in either binary or ASCII format. You must know the format of the file to complete this procedure.

To transfer a file from the client workstation to a core manager directory, the system uses the file extension and sets the correct transfer type. The system recognizes the following file extensions:

- .patch
- .xref

- .bin(<n>)

  where

  <n>
  is the logical record length to transfer a file to the core manager for a binary file type.

- .txt(<n>)

  where

  <n>
  is the logical record length to transfer a file to the core manager for an ASCII file type.

Note: If you are transferring files to or from the core manager, the system recognizes the same file extensions as above, and sets the correct logical record length.

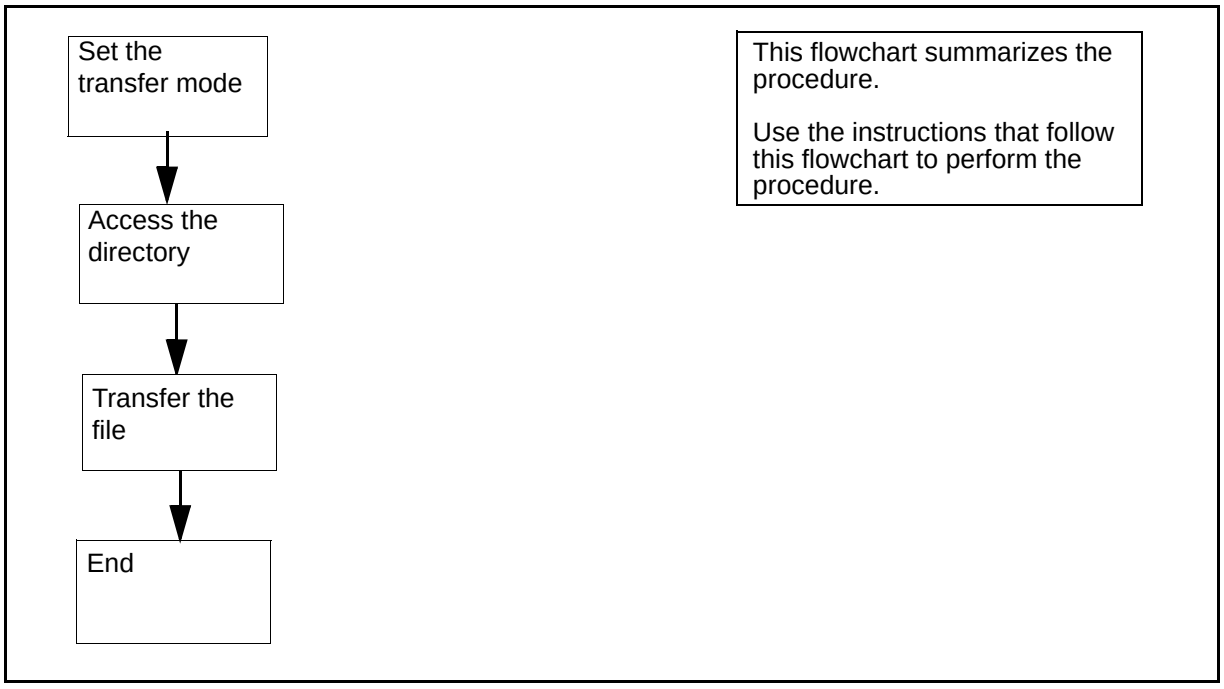
If the system does not know the transfer type, the transfer type is not changed and remains as the last specified transfer type. In this instance, the following warning message is displayed as the first sentence of the response:

Unrecognized File Type. Using Current Transfer Type.

This procedure assumes you have already started an SFT session in DCE mode including a “site sdm” command. If you have not done so, refer to procedures Starting an SFT session on page 183 or Starting an FTP client on page 176 in this document. This procedure also assumes that you have set your current local working directory to be the directory containing the file.

To transfer and retrieve files using SFT, perform the procedure that follows the flowchart.

Summary of transferring a file to a core manager directory



Transferring a file to a core manager directory

At the SFT prompt:

1 Set the transfer mode:

sft> <transfer_mode>

where

<transfer_mode>
is either binary or ASCII

2 Change to the core manager directory:

sft> cd <directory_name>

where

<directory_name>
is the name of the core manager directory

3 Transfer the file to the core manager directory:

sft> put *<file_name>*

where

<file_name>
is the name of the file.

4 You have completed this part of the procedure.

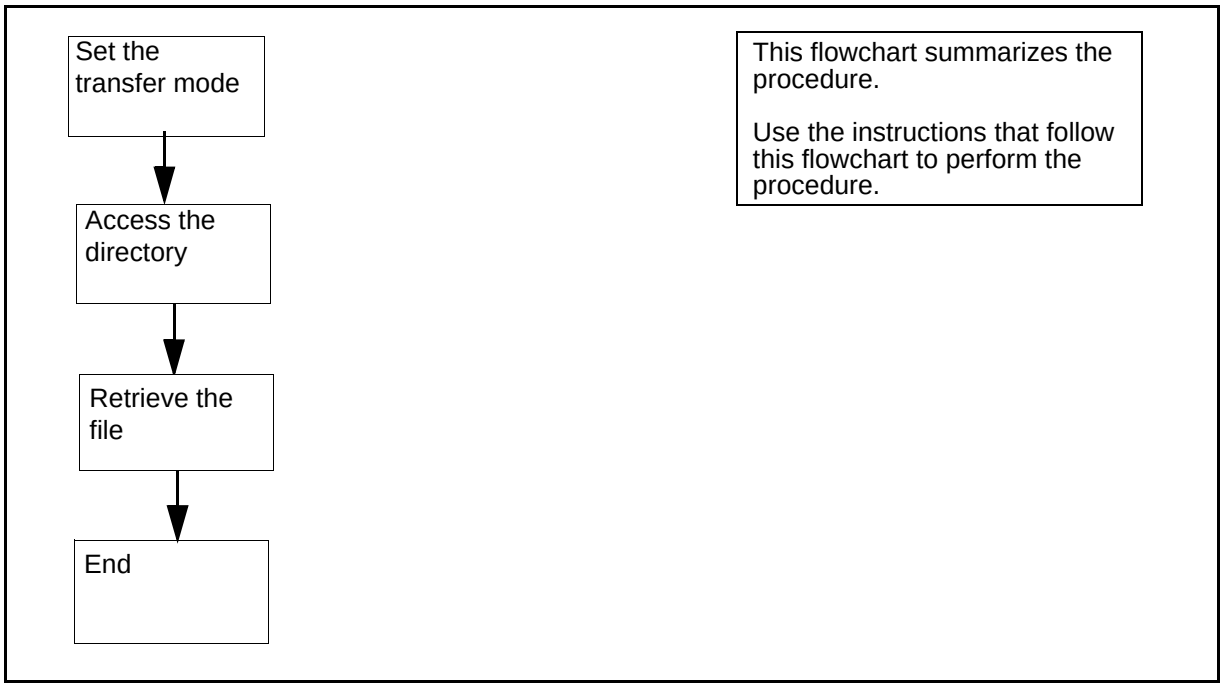
Retrieving a file from a core manager directory

Use this procedure to retrieve a file from a core manager directory to the client workstation. The file can be in either binary or ASCII format. You must know the format of the file to complete this procedure.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures, Starting an SFT session on page 183, or Starting an FTP client on page 176. This procedure also assumes that you have set your current local working directory to be the directory that is to receive the file.

To retrieve a file from the core manager directory, perform the step-action procedure that follows the flowchart.

Summary of retrieving a file from a core manager directory



Retrieving a file from a core manager directory

At an SFT prompt:

1 Set the transfer mode:

sft> <transfer_mode>

where

<transfer_mode>
is either binary or ASCII

2 Access the core manager directory:

sft> cd <directory_name>

where:

<directory_name>
is the name of the core manager directory

3 Retrieve the file from the core manager directory:

sft> get <file_name>

where:

<file_name>
is the name of the file.

4 You have completed this part of the procedure.

Transferring a CM file to a CS 2000 volume

Use this procedure to transfer a CM file from the client workstation to a volume group on the Communication Server 2000. The file can be in either binary or ascii format. You must know the format of the file to complete this procedure.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures Starting an SFT session on page 183 or Starting an FTP client on page 176. This procedure also assumes that you have set your local working directory to be the directory that is to receive the file.

Record lengths and formats for CM files

To transfer a CM file to a CS 2000 volume, you must know the record length of the file. Use this information in the CM File Formats table below.

Table CM File Formats provides a sample of formats for selected CM files for reference purposes. It is not a complete list. Formats can vary.

CM File Formats

File	Fixed or variable length record	Transfer mode	Record length
Image files	Fixed	binary	1020
Patches	Fixed	binary	128
SMDR	Fixed	binary	2048
EDRAM	Fixed	binary	44
SOC	Variable	ASCII	
Translations	Variable	ASCII	

Record lengths and formats for peripheral module (PM) files

You must know the record length of the file to transfer a PM file to a CS 2000 volume.

You can determine the record length for a peripheral module (PM) file by its file extension.

The following example shows a typical LCM file format.

LCM file: lcm ##**aa.**bin **nn**

where

is the XPM stream number of the load

aa is the version of the load

nn is the file extension number

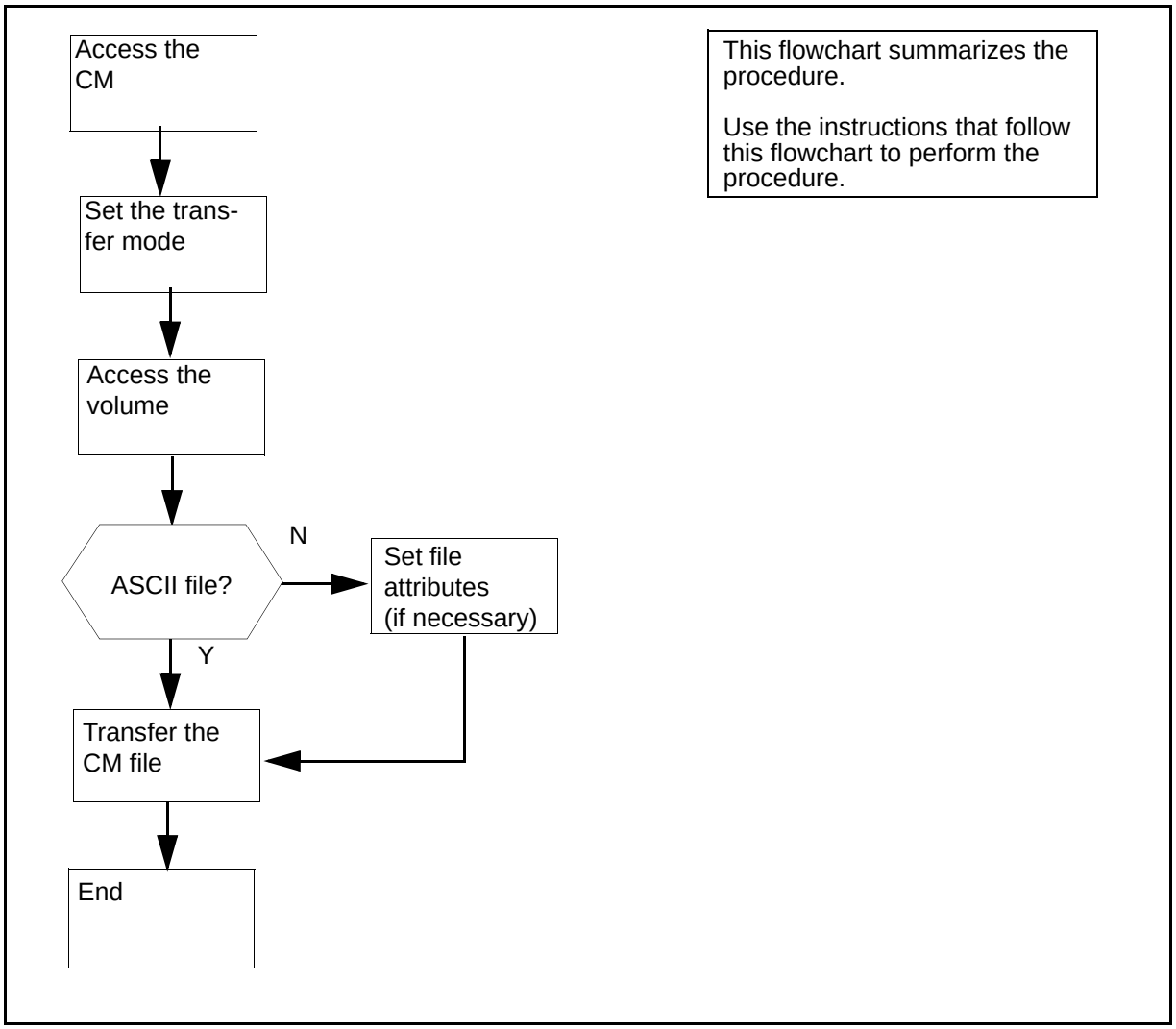
The table PM file extensions describes typical PM file extensions.

PM file extensions

File extension	Type of image	Fixed- or variable-length record	Transfer mode	Record length
.bin1024	non-system	fixed-length	binary	1024
.txt55	non-system	variable-length	ASCII	55
.bin1020	system	fixed-length	binary	1020

To transfer a CM file to a DMS volume, perform the procedure that follows the flowchart.

Summary of transferring a CM file to a CS 2000 volume



Transferring a CM file to a CS 2000 volume

At an SFT prompt:

1 Go to the CS 2000 volume:

sft> cd /<volume_name>

where

<volume_name>
is the name of the CS 2000 volume.

Note: Specify CS 2000 volume names in uppercase characters.

2 Set the transfer mode:

sft> <transfer_mode>

where

transfer_mode
is either binary or ASCII.

3 Use the following table to determine your next step.

If you want to transfer	Do
an ASCII file	step 6
a binary file	step 4

4 Enter the file characteristics or attributes, if necessary.

You must enter the file characteristics if:

- the suffix of the transfer file does not match the pattern ".bin###" (where ### indicates the record length a value between 1 and 32767), or
- the file is a patch file

If you do not need to enter the file characteristics or attributes, proceed to step 6.

5 Set the record length of the file:

sft> site lrecl <Record_length>

where

<Record_length>
is the record length of the file

Note: See table CM File Formats for a format list of various CM file types.

6 Transfer the CM to the CS 2000 volume:

sft> put <file_name>

where

<file_name>
is the name of the CM file

7 You have completed this procedure.

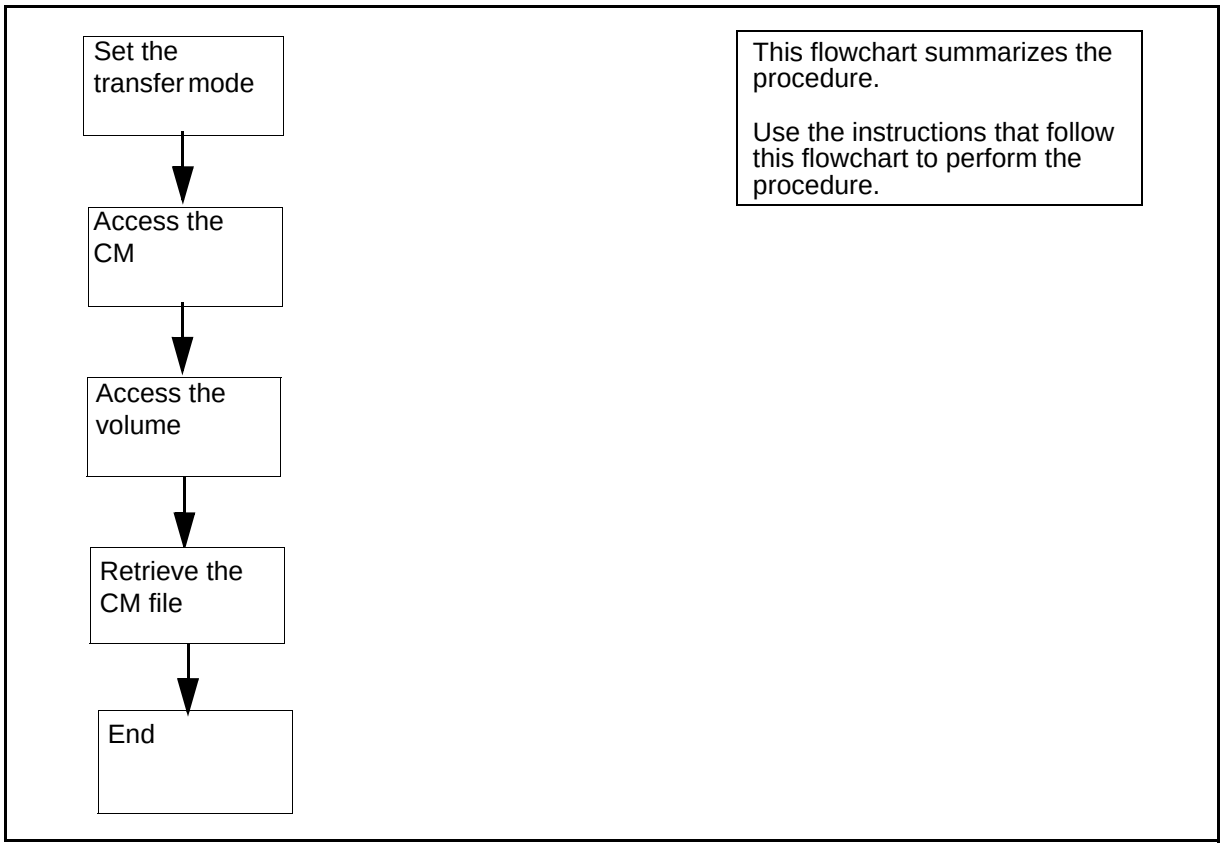
Retrieving a CM file from a CS 2000 volume

Use this procedure to retrieve a CM file from a CS 2000 volume and transfer it to the client workstation. The file can be in either binary or ASCII format. You must know the format of the file to complete this procedure.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures, Starting an SFT session on page 183 or Starting an FTP client on page 176. This procedure also assumes that you have set your current local working directory to be the directory that is to receive the file.

To complete the procedure for retrieving a CM file from a CS 2000 volume, perform the procedure that follows the flowchart.

Summary of retrieving a CM file from a CS 2000 volume



Retrieving a CM file from a CS 2000 volume

At an SFT prompt:

1 Set the transfer mode:

sft> <transfer_mode>

where

<transfer_mode>
is either binary or ASCII

2 Change to the CS 2000 volume:

sft> cd /<volume_name>

where

<volume_name>
is the name of the CS 2000 volume

Note: Specify CS 2000 volume names in uppercase characters.

3 Retrieve the CM file from the CS 2000 volume:

sft> get <file_name>

where

<file_name>
is the name of the CM file.

4 You have completed this procedure.

Retrieving an active DIRP file

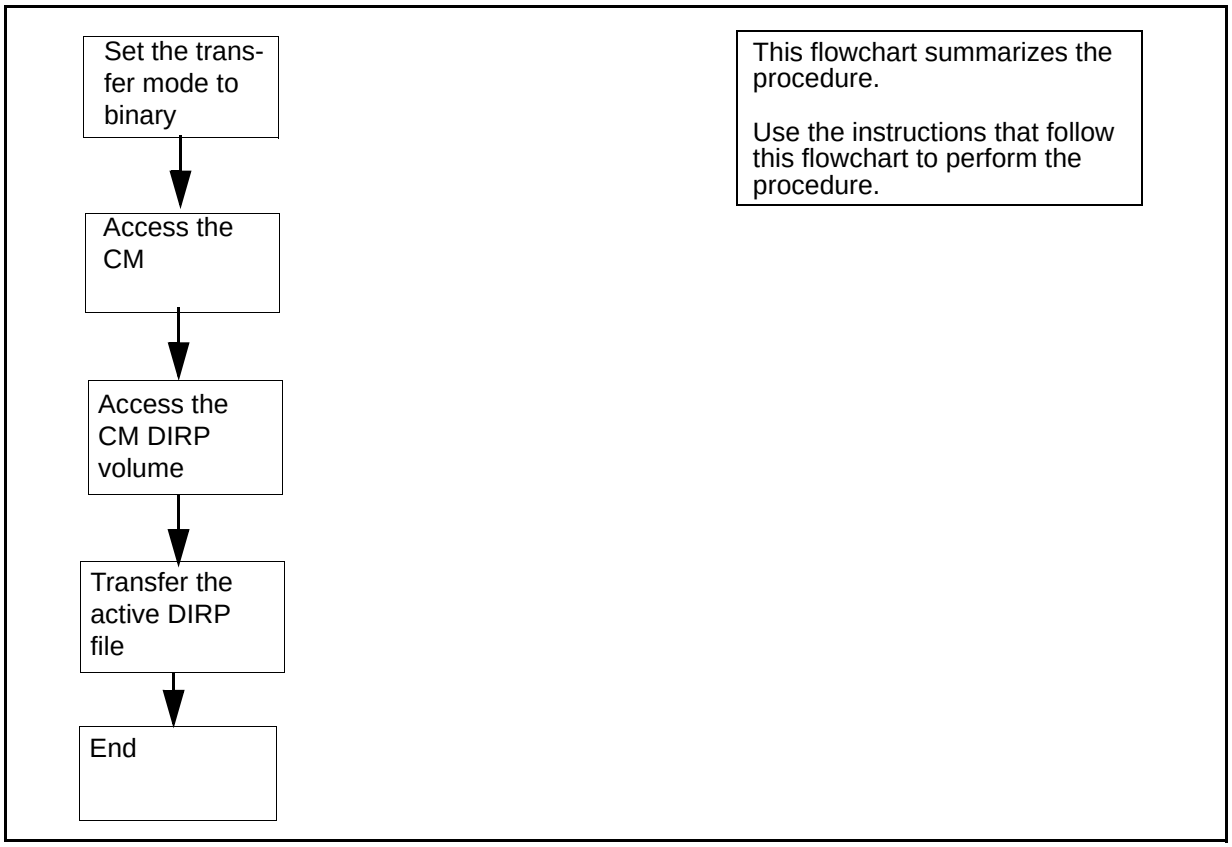
Use the following procedure to retrieve an active DIRP file.

The Device Independent Recording Package (DIRP) is CM software that automatically directs data from the various administrative and maintenance facilities on the Communication Server 2000 to the appropriate recording devices.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures, Starting an SFT session on page 183 or Starting an FTP client on page 176. This procedure also assumes that you have set your current local working directory to be the directory that is to receive the file.

To complete the procedure for retrieving an active DIRP file, perform the procedure that follows the flowchart.

Summary of retrieving an active DIRP file



Retrieving an active DIRP file

At an SFT prompt

1 Set the transfer mode to binary:

sft> binary

2 Access the CM:

sft> site cm

3 Set the file characteristics for a DIRP file:

sft> site getdirp <DIRP_subsystem_number>

where

<DIRP_subsystem_number>
is the DIRP subsystem number

Note: For automatic message accounting (AMA), the DIRP subsystem number is 0.

4 Go to the core manager volume group:

sft> cd /<DIRP_volume>

where

<DIRP_volume>
is the name of the DIRP volume

Note: Specify the core manager volume names in uppercase characters.

5 Retrieve the DIRP file:

sft> get <active_DIRP_file_name>

where

<active_DIRP_file_name>
is the name of the active DIRP file

6 You have completed this procedure.

Discontinuing a file transfer

Discontinue file transfers by entering the interrupt key sequence (<CTRL> C). Set the interrupt key sequence by using the STTY command. When you enter the interrupt key sequence, SFT terminates and closes all open sessions.

Changing the system time zone and daylight savings time parameters

Purpose

Use this procedure to change the time zone and daylight savings time parameters on the core manager.

Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

Application

It is recommended that you perform this procedure at the same time you are performing an upgrade while the core manager is in split mode, or out of service (non-split mode). If you choose to do so, follow the steps under Changing the system time zone and daylight savings time parameters on page 203 in this procedure.

If you decide to perform this procedure independently of an upgrade, it is recommended that you use the split-mode process instead of the non-split mode process, which takes the core manager out of service for approximately 20 minutes.

- To use the split mode process, first follow the steps under Splitting the system on page 201 and then follow the steps under Changing the system time zone and daylight savings time parameters on page 203 in this procedure.
- To use the non-split mode process, first follow the steps under Busying the core manager on page 202 and then follow the steps under Changing the system time zone and daylight savings time parameters on page 203 in this procedure.

Splitting the system

At the VT100 console connected to SP0

1 Log on to the core manager as a user authorized to perform config-admin actions.

2 Access the split-mode screen:

 # sdmmtc split

3 Begin the split-mode process:

> start

4 When prompted, confirm that you want to perform an upgrade:

> y

The system performs some checks.

5 Determine if errors were found.

If the system	Do
detects errors	go to the appropriate procedure to correct the errors, and perform this procedure again
does not detect errors	step 6

6 When prompted, select the first option on the list, Software upgrade:

> 1

7 When prompted, confirm that you want to proceed:

> y

8 Wait until the system split is 100% complete (minimum of 20 minutes), as indicated by the following message on the SP0 console.

20 min.+

```
Split: [100%] Completed
Configure: [User] Waiting for user input
```

Note: You do not have a connection available to the inactive console until the system is 100% split. Once the system is split, each VT100 console display reports, in the upper-right corner, the domain that it is connected to. For example, SP0 reports

```
Active Domain 0
```

At the VT100 console SP1 (inactive)

9 Wait until the FX-Bug prompt appears on the SP1 (inactive) console before you proceed to step 10.

10 At the FX-Bug prompt, manually reboot domain 1:

FX-Bug> **pboot 6 0**

11 Log into the inactive side (SP1) of the core manager as a user authorized to perform config-admin actions.

The system automatically displays the split-mode screen.

12

7 min.

CAUTION
Possible loss of service
If the core manager begins the system stabilization process, do not attempt to perform any activities on the system until stabilization is complete.

Wait until system stabilization is complete (approximately 7 minutes) before proceeding to step 13.

Note: When the stabilization process begins, the system displays a time estimate for its completion.

13 Proceed to Changing the system time zone and daylight savings time parameters in this procedure.

Busying the core manager

At the MAP display

1 Access the SDM level of the MAP display:

> mapci;mtc;appl;sdm

2 Check that the core manager is in a fault-free state.

- If the core manager is not in a fault-free state, correct all faults and alarms before continuing this procedure. Refer to the Fault Management document for alarm-clearing procedures.
- If you have alarms or faults that you cannot clear, stop and contact your next level of support.

3 Busy the core manager:

> bsy

4 Confirm the busy request:

> y

5 Proceed to Changing the system time zone and daylight savings time parameters on page 203 in this procedure.

Changing the system time zone and daylight savings time parameters

At the local VT100 console

1 Log in as root user.

2 Enter the Time Zone level:

 # sdmmtc tz

Example response:

```
  SDM      CON    512     NET     APPL    SYS      HW     CLLI: SNM0
  ManB      .     . .      .      ManB     .       .      Host: wcary2p3
                   . .                                        Fault Tolerant

TimeZone
 0  Quit
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17 Help
 18 Refresh
  root
 Time 18:51  >

Time Zone: Eastern U.S.; Colombia
   EST5EDT (CUT -5)
   Daylight Start: M4.1.0/02:00:00 (Standard)
   End: M10.5.0/02:00:00
   Thu Sep 5, 2002 18:51
```

3 Change the time zone:

> c

Example response:

```
Time Zone: Daylight Savings?
Does this time zone go on Daylight Savings Time?
Please confirm ("YES", "Y", "NO", or "N"):
```

4 Determine if Daylight Savings Time is to be used.

If the time zone	Do
goes into Daylight Savings Time	enter **y**
does not go into Daylight Savings Time	enter **n**

Example response: Screen 1

```
  SDM      CON     512     NET     APPL    SYS      HW     CLLI: SNM0
  ManB      .      . .      .      ManB     .       .      Host: wcary2p3
                   . .                                          Fault Tolerant

TimeZone
 0  Quit
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17 Help
 18 Refresh

Time Zone: Closest Match
Choose the Time Zone which is the closest match to yours:

1. Bering Straits              (BST11BDT)          (CUT -11)
2. Hawaii;Aleutian Islands     (HST10HDT)          (CUT -10)
3. Alaska                      (AST9ADT)           (CUT -9)
4. Pacific U.S.;Yukon          (PST8PDT)           (CUT -8)
5. Mountain U.S.               (MST7MDT)           (CUT -7)
6. Central U.S.;Honduras       (CST6CDT)           (CUT -6)
7. Eastern U.S.;Colombia       (EST5EDT)           (CUT -5)
8. Central Brazil              (AST4ADT)           (CUT -4)
9. Greenland;East Brazil       (GRNLNDST3GRNLNDDT) (CUT -3)
10 Falkland Islands            (FALKST2FALKDT)     (CUT -2)
11.Azores;Cape Verde           (AZOREST1AZOREDT)   (CUT -1)
12 Coordinated Universal Time  (CUT0GDT)           (CUT)
13.United Kingdom              (GMT0BST)           (CUT)
14.Norway, France              (NFT-1DFT)          (CUT +1)
15.South Africa                (USAST-2USADT)      (CUT +2)
16.Finland                     (WET-2WET)          (CUT +2)
  root
 Time 18:54   >MORE...(52%)
```

5 Press the Space Bar to display the next screen:

Example response: Screen 2

```
  SDM      CON    512     NET    APPL    SYS      HW     CLLI: SNM0
  ManB      .     . .      .     ManB     .       .      Host: wcary2p3
                  . .                                        Fault Tolerant

TimeZone
 0  Quit
 2              17. Turkey                      (MEST-3MEDT)       (CUT +3)
 3              18. Saudi Arabia                (SAUST-3SAUDT)     (CUT +3)
 4              19. Gorki;Central Asia;Oman     (WST-4WDT)         (CUT +4)
 5              20. Pakistan                    (PAKST-5PAKDT)     (CUT +5)
 6              21. Tashkent;Central Asia       (TASHST-6TASHDT)   (CUT +6)
 7              22. Thailand                    (THAIST-7THAIDT)   (CUT +7)
 8              23. People's Republic of China  (BEIST-8BEIDT)     (CUT +8)
 9              24. Taiwan                      (TAIST-8TAIDT)     (CUT +8)
 10             25. Western Australia           (WAUST-8WAUDT)     (CUT +8)
 11             26  Japan                       (JST-9JSTDT)       (CUT +9)
 12             27. Korea                       (KORST-9KORDT)     (CUT +9)
 13             28  Eastern Australia           (EET-10EEDT)       (CUT +10)
 14             29. Solomon Islands             (MET-11METDT)      (CUT +11)
 15             30. New Zealand                 (NZST-12NZDT)      (CUT +12)
 16
 17 Help        Enter a number from 1 to 30 to choose the time zone that
 18 Refresh     most closely matches yours. You will have the opportunity
                to customize the time zone if necessary: [7]
  root
 Time 18:54  >
```

6 Select a time zone:

> <n>

where:
<n> is the number of the time zone closest to the one in which you are geographically located.

Example:

The closest time zone to Newfoundland is *Greenland; East Brazil,* or number 9 in the list of time zones.To select the time zone for Newfoundland, enter:

> 9

Example response:

```
Time Zone: Edit this zone?
Selected Zone: Greenland;East Brazil
     GRNLNDST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 18:57


The above shows the values for the time zone that you
have selected. Proceed to set the time zone using the
current values, or edit them and make changes.

Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:
>
```

7 When prompted, confirm, reject, or edit the values.

If you entered	Do
y to confirm the values	you have completed this procedure
n to reject the values	return to step 3
e to edit the values	step 8

8 The system displays the current value of the time zone description, and prompts you enter another value.

Example response:

```
Time Zone: Description
Selected Zone: Greenland;East Brazil
     GRNLNDST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:01

The time zone description should include a few words
such as the name of your city which describes the area
where the time zone is in use.

Enter the description: [Greenland;East Brazil]
>
```

9 Enter the new description for your time zone.

Example:

To enter the value for Newfoundland, enter:

> Newfoundland

Example response:

```
Time Zone: Acronym
Selected Zone: Newfoundland
     GRNLNDST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:15

Enter the acronym associated with this time zone. For
example, the time zone acronym for New York is EST,
which is short for Eastern Standard time

Enter the acronym: [GRNLNDST]
>
```

10 Enter an acronym for your time zone.

Example:

To enter an acronym for Newfoundland Standard Time, enter:

> NST

Example response:

```
Time Zone: Offset from CUT
Selected Zone: Newfoundland
     NST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:19

The offset from CUT (Coordinated Universal Time) is
the number of hours BEFORE CUT for this time zone. For
example, EST in North America is 5 hours before CUT,
while NFT for France and Norway is -1 hours before
CUT. Specify the time in the form HH[:MM[:SS]] where
HH ranges from -12 to 11. Minutes and seconds are
optional.

Enter the offset from CUT: [3]

>
```

11 Enter the time zone offset from CUT (Coordinated Universal Time).

Example:

To set the time zone offset from CUT for Newfoundland, enter:

> 3:30

If the time zone	Do
goes into Daylight Savings Time (you entered **y** in step 4)	step 12
does not go into Daylight Savings Time (you entered **n** in step 4)	step 19

12 The system displays the following response.

Example response:

```
Time Zone: Daylight Savings Acronym
Selected Zone: Newfoundland
     NST3:30GRNLNDDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:21


The daylight savings time acronym is the name
associated with daylight savings for this time zone.
For example, for EST (Eastern Standard Time), the
associated daylight savings acronym is EDT (Eastern
Daylight Time).

Enter the daylight savings acronym: [GRNLNDDT]
>
```

13 Enter the daylight savings acronym for the time zone.

Example:

To set the daylight savings acronym for Newfoundland Daylight Time, enter:

> NDT

Example response:

```
Time Zone: Daylight Savings offset from CUT
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:24


The daylight savings offset from CUT (Coordinated
Universal Time) is the number of hours BEFORE CUT for
daylight savings in this time zone. For example, EDT
in North America is 4 hours before CUT, while DFT for
France and Norway is -2 hours before CUT. The daylight
savings offset is normally 1 hour less that (ahead of)
the standard offset. Specify the time in the form
HH[:MM[:SS]] where HH ranges from -12 to 11. Minutes
and seconds are optional.


Enter the daylight savings offset from CUT: [2]
>
```

14 Enter the daylight savings offset from CUT for the time zone.

Example:

To set the daylight savings offset from CUT for Newfoundland, enter:

> 2:30

Example response:

```
Time Zone: Daylight Savings Start Day
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:27


The daylight savings start day indicates the day of the
year when daylight savings takes effect. The day can
be specified one of two forms: M<month>.<week>.<day>
or J<julianday> where:
  <month> is the month, a number from 1 to 12
  <week> is the week during that month, an number from
         1 to 5,
  <day> is the day of that week, a number from 0 to 6,
         0 indicating Sunday,
  <julianday> is the day of the year, a number from
         1 to 365, leap days are not counted.

Enter the daylight savings start day: [M4.1.0]
>
```

15 Enter the starting day for daylight savings for your time zone.

Example:

Newfoundland changes on the first Sunday of April, which is the current value in the example. To accept a current value, press the Enter key.

Example response:

```
Time Zone: Daylight Savings Start Time
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:30

The daylight savings start time indicates the time on
the daylight saving start day when daylight savings
takes effect. The time is specified in the format
HH[:MM[:SS]] where HH ranges from 00 to 23. Minutes
and seconds are optional.

Enter the daylight savings start time: [02:00:00]
>
```

16 Enter the daylight savings start time for your time zone.

Example:

Newfoundland changes as 02:00:00, which is the value already specified in the example. To accept the current value, press the Enter key.

Example response:

```
Time Zone: Daylight Savings End Day
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:33


The daylight savings end day indicates the day of the
year when daylight savings ends. The day can be
specified in one of two forms:
 M<month>.<week>.<day> or J<julianday> where:
  <month> is the month, a number from 1 to 12,
  <week> is the week during that month, a number
         from 1 to 5
  <day> is the day of that week, a number
         from 0 to 6, 0 indicating Sunday
  <julianday> is the day of the year, a number
         from 1 to 365, leap days are not counted.


Enter the daylight savings end day: [M10.5.0]
>
```

17 Enter the daylight savings end day for your time zone.

Example:

Newfoundland changes on the last Sunday in October, which is the current value in the example. To accept the current value, press the Enter key.

Example response:

```
Time Zone: Daylight Savings End Time
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:36

The daylight savings end time indicates the time on
the daylight saving end when daylight savings ends.
The time is specified in the format HH:[MM[:SS]]
where HH ranges from 00 to 23. Minutes and seconds
are optional.

Enter the daylight savings end time: [02:00:00]
>
```

18 Enter the daylight savings end time for your time zone.

Example:

Newfoundland changes at 02:00:00, which is the default in the example. To accept the current value, press the Enter key.

Example response:

```
Time Zone: Edit this zone?
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:39

The above shows the values for the time zone that you
have selected. Proceed to set the time zone using the
current values, or edit them and make changes.

Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:
>
```

If you want to	Do
confirm the values	enter **y**, and go to step 19
reject the values	enter **n**, and go to step 3
edit the values	enter **e**, and return to step 8

19 The system displays the values for both the current and the commissioned time zones, and a prompt for a system reboot.

Example response:

```
Current Zone: Eastern U.S.: Colombia
     EST5EDT (CUT -5)
     Daylight Start: M4.1.0/02:00:00 (Standard)
              End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:42

Commissioned Zone: Newfoundland
     NSTE:30NDT (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
              End:   M10.5.0/02:00:00
     Thu Sep 5, 2002 19:42

Time Zone: Reboot Required
The commissioned time zone will not take effect until
after the system has been rebooted.

Reboot the system now?
Please confirm: ("YES", "Y", "NO", or "N")

>
```

If you want to	Do
reboot now	enter **y**
reboot later	enter **n**

20 You have completed this procedure.

Using an FTP client

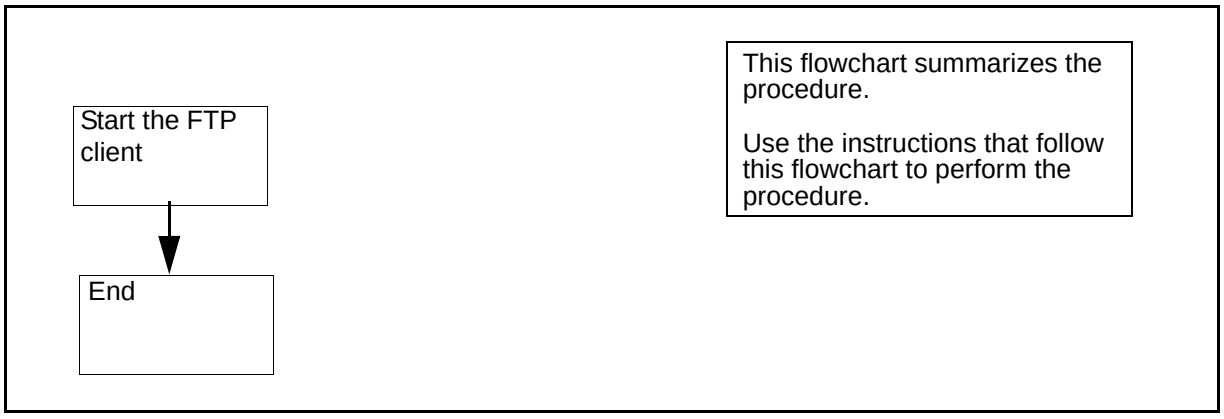
Starting an FTP client

The following procedure describes how to start an FTP client.

Note 1: Nortel recommends that you use the SFT client. FTP userIDs and passwords are passed unencrypted across the network. Standard FTP cannot determine which users are allowed to transfer files to and from the CM.

Note 2: To complete the procedure for starting an FTP client, perform the step-action procedures that follow the flowchart.

Summary of Starting an FTP client



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Starting an FTP client

At a UNIX prompt:

1 Start the FTP client workstation:

```
ftp <address>
```

where

<address>
is the IP address, or the DNS address of the FTP server.

Note: The location of the FTP client varies.

2 You have completed this procedure.

For additional instructions on FTP client usage, refer to the documentation of the client application. For instructions on using CM FTP, refer to section CM FTP server on page 217.

CM FTP server

SFT clients and FTP clients can both access the CM FTP server: SITE CM.You can use standard FTP commands with some exceptions. A list of exceptions follows.

Command limits and restrictions

The following describes limits to standard FTP commands when accessing the CM FTP server.

- The user command is intercepted and disallowed by the SFT server. A user does not have to log in manually.
- The mkdir and rmdir commands are not supported by the CM FTP server. The CM file system only contains volumes. It does not support directory hierarchies within the volume.
- Files transferred to SFDEV are owned by the user $$SYS$$.
- SFT performs a clean-up routine after the SFT application is returned to service. If you attempt to use the SITE CM command immediately after the RTS command is issued, you may experience a delay of about 20 seconds before access to the CM is given.
- File names and volume names are case respective. Volume names are always in uppercase, for example, S01DVOL1. File names are usually in uppercase.

Note: For more information on commands, refer to the commands glossary.

Allowing ATA and ETA to operate across a firewall

Purpose

Use this procedure to allow ATA and ETA to operate across a firewall by controlling the client TCP port.

Application

Special measures must be taken for DCE-based applications when the core manager is separated by a firewall or other filtering device, or from:

- the DCE cell security and cell directory servers (CDS)
- a workstation that runs an ETA client program

The ETA server on the core manager can connect back to the ATA or ETA client, in response to a request to establish a session from the client. It is necessary to control the TCP port that the client uses for the reverse connection.

Restricting ports for incoming connections works in combination with firewalls by implementing a packet-filtering technique. Consult the firewall vendor documentation to determine whether your firewall can be used in this manner.

Procedure

Use the following procedure to restrict the ATA and ETA client reverse connection ports on the client workstation.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Restricting the port range

At the local or remote VT100 console

1 Log into the client workstation as the root user.

2 Change to the ETA directory:

cd /sdm/bin

3 Start the port range configuration script:

/eta_port_range

Example response:

```
 ENHANCED TERMINAL ACCESS PORT RANGE
CONFIGURATION
```

```
This configuration script allows you to control
the ETA Client reverse connection ports on the
client workstation.
The current port restriction range for the ETA
Client is:
Range start: -
  Range end:   -
   (no port restriction range)
Set a new port restriction range by entering two
numbers (and pressing [Enter]) which represent
the start and end of the port restriction range.
To remove the port restriction, type 'None' and
press [Enter]. To quit this program, type
'Quit' and press [Enter].
Port restriction range:
```

4 At the "Port restriction range:" prompt, enter two numeric values separated by a space:

Port restriction range: <a> <b>

where

<a>
is the beginning the range for ports (must be greater than 1024)

<b>
is the end of the range for ports (must be less than 32 000)

Note 1: These values are not range checked. Check that the values range from 1024 to 32000. The lowest value must be entered first.

Note 2: The range size is determined by the maximum number of simultaneous instances of the ETA client program that are expected to run on the machine where the client is installed. This number is the number of ETA client instances, not the number of core manager console sessions or core MAP terminal sessions, because all sessions started by an ETA client instance share the same port number.

5 Exit the program:

quit

6 You have completed this procedure.

Changing a DCE user password

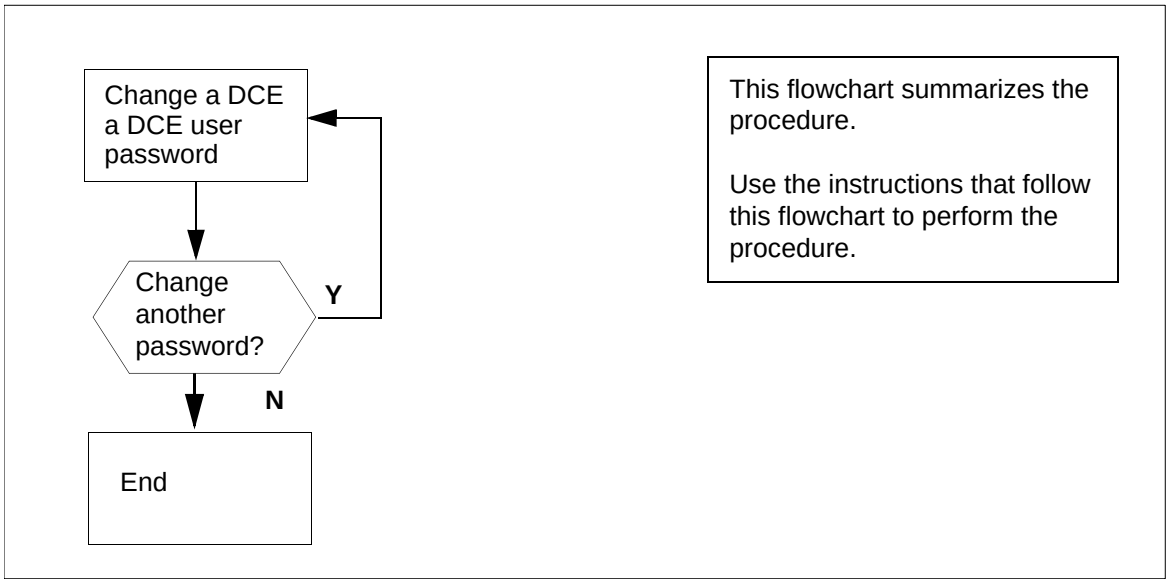
Purpose

Use this procedure to change a DCE user password.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the procedure.

Summary of changing a DCE user password



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Changing a DCE user password

At the core manager client workstation

1 Change a DCE user password:

/sdm/bin/change_dce_password

Example response:

```
DCE user ID:
```

2 Enter the user ID of the user for whom you are changing the password, and press the Enter key.

Example response:

```
Old password:
```

3 Enter the old password.

Example response:

```
New password:
```

4 Enter the new password.

Example response:

```
Re-enter password:
```

5 Re-enter the user password.

Example response:

```
The password for “ops_1” has been changed.
```

6 You have completed this procedure.

Changing a user password on the core manager

Purpose

Use this procedure to change a user password on the core manager, or to set up a temporary password for a new user.

Prerequisites

You must be a user authorized to perform security-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

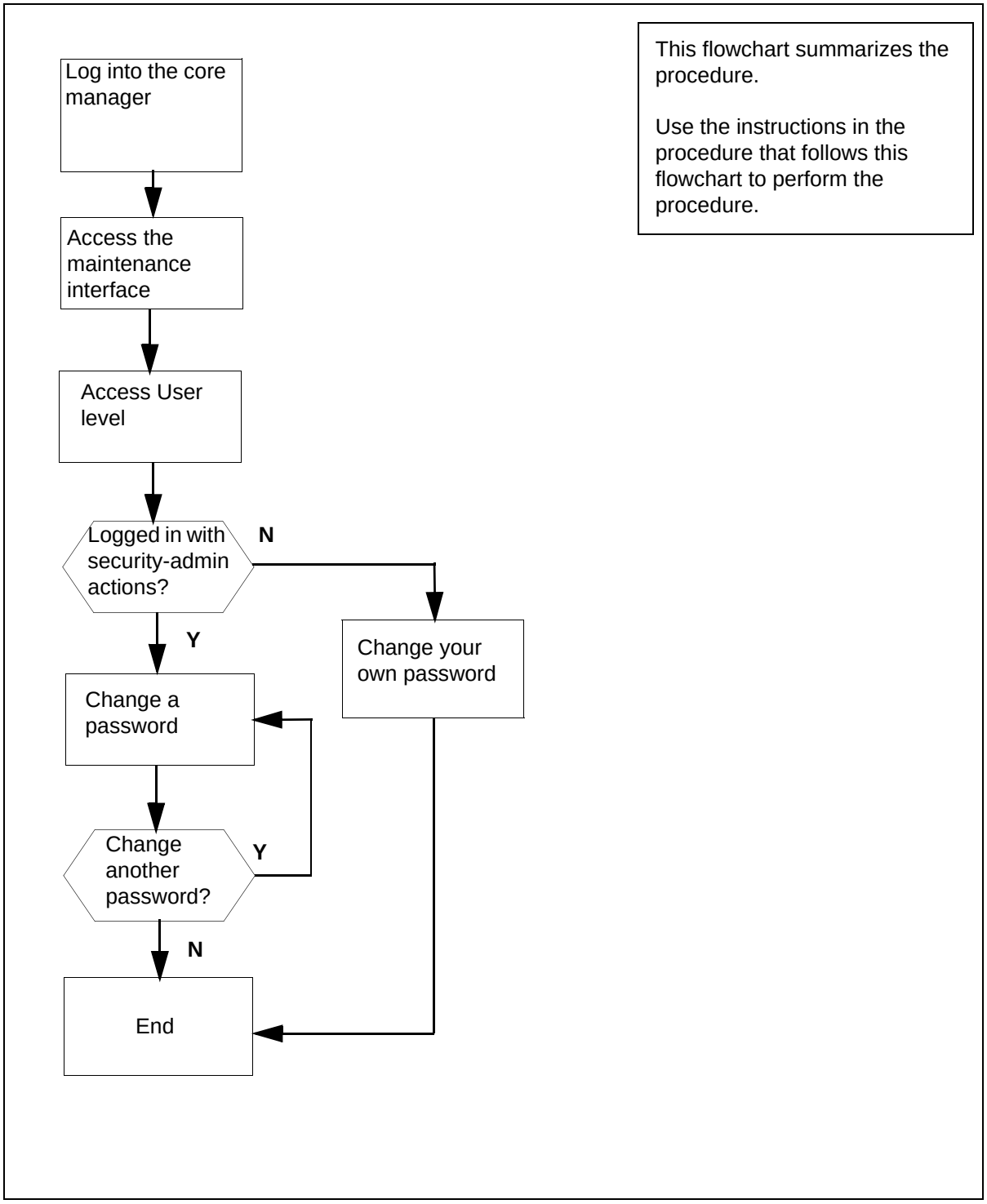
Application

Maintenance class and root users can change their own password. The root user can change the password of any other user class on the system.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the procedure.

Summary of Changing a user password



Changing a user password

At the local or remote VT100 terminal

1 Log in to the core manager as a user authorized to perform security-admin actions.

2 Access the maintenance interface:

 # sdmmtc

3 Display the User screen:

> user

4 Set the appropriate password.

If you are a	Do
maint class user	step 9
root user	step 5

5 Change a user password:

> change <userID>

where

<userID>
is the userID of the user for whom you are changing the password

Note: If no userID is specified, the system attempts to change the password of the root user.

6 When prompted, enter a new password.

Note: The password must be a minimum of six characters, containing at least one alphabetic character, and at least one numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

7 When prompted, re-enter the password.

Note: If the root user changes a maint class user password, the change is temporary. The maint class user is prompted to change their password again at the next login.

8 Press Enter to continue.

If you	Do
want to change another password	step 5

If you	Do
do not want to change another password	step 14

9 Change your password:

> change

10 When prompted, enter your old (current) password.

11 When prompted, enter a new password.

Note: The password must be a minimum of six characters, containing at least one alphabetic character, and at least one numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

12 When prompted, re-enter the new password.

13 Press Enter to continue.

14 Exit the maintenance interface:

> quit all

15 You have completed this procedure.

Changing a passthru user password

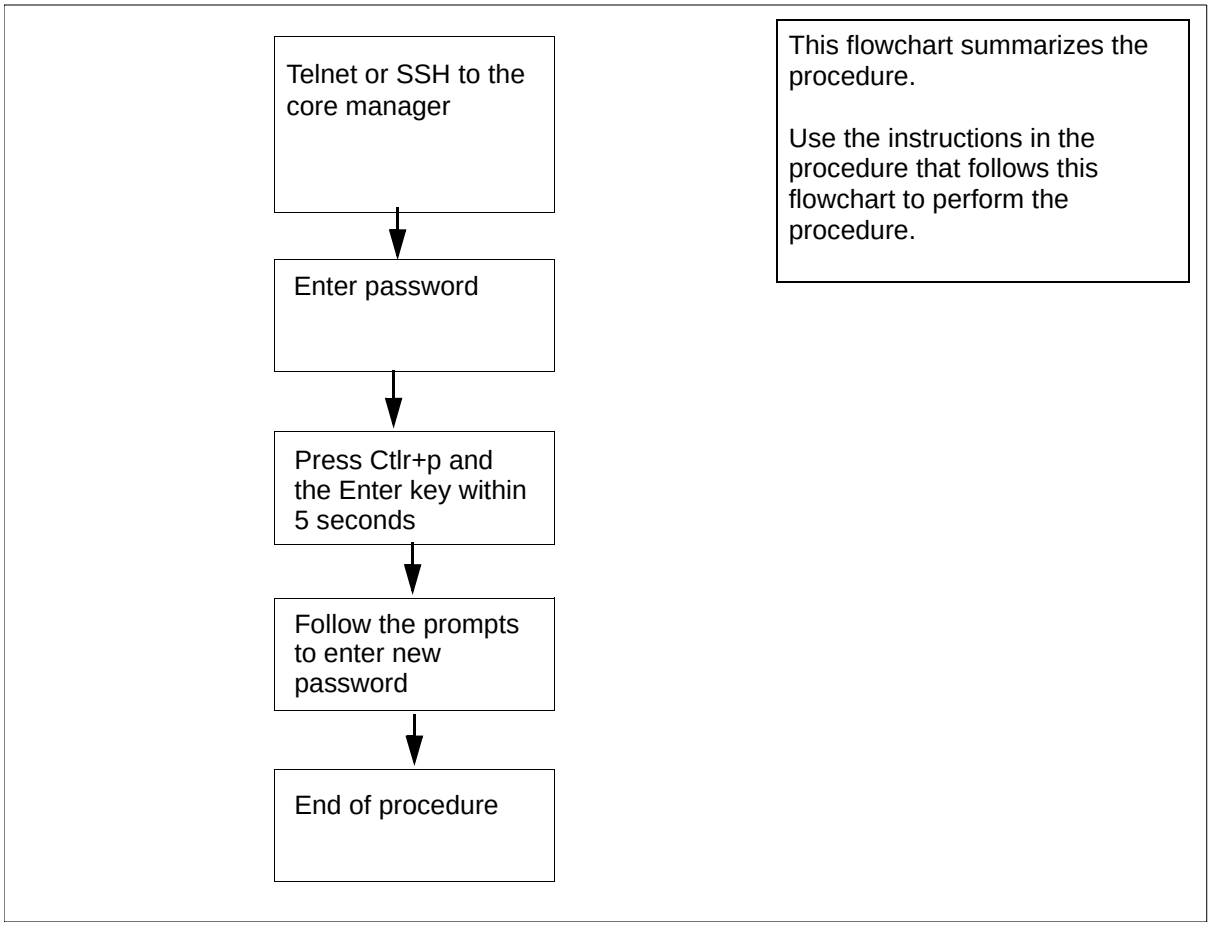
Purpose

Use this procedure to change a password for a passthru user who is configured as "password required".

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of changing a passthru user password



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Changing a passthru user password

At the workstation

1 Log in to the core manager as a passthru user.

If you	Do
use telnet	step 2
use SSH	step 3

2 Telnet to the core manager:

```
telnet <IP address>
```

where

<IP address>
is the IP address of the core manager.

Continue with step 4.

3 Open an SSH session:

```
ssh-l<passthru userID><IP address>
```

where

<IP passthru userID>
is the IP address of the core manager.

4 At the prompt, enter your password.

Note: The following response is only displayed when the passthru user is configured as "password required". Otherwise, the connection is directly forwarded to the Core login prompt.

Example response:

```
This is a passthru user.

Please type "Ctrl+p" and Enter for changing your
password.

type "Enter" or wait for 5 seconds to continue.
```

5 Open the password change session by pressing the Ctrl and p keys at the same time and then pressing the Enter Key.

Note: you must complete this step within 5 seconds or the connection will be forwarded to the Core login prompt.

6 At the prompt, enter the old password.

7 At the prompt, enter the new password.

8 At the prompt, re-enter the new password.

9 You have completed this procedure.

Changing CM passwords from ATA client

Purpose

Use the following procedure to change your CM password in the DCE security database.

Application

Changing CM passwords consists of :

- Changing CM passwords in the DCE security database on page 229 and
- Changing the CM password on the core on page 231

ASCII Terminal Access (ATA) clients can change their own user passwords.

Note 1: You can change the CM password on the core before or immediately after you have changed the CM password in the DCE security database.

Note 2: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Changing CM passwords in the DCE security database

Changing CM passwords in the DCE security database

At the client workstation

1 Log into the client workstation.

2 Log into DCE:

dce_login <DCE_user>

where

<DCE_user>
is the DCE administrator user ID

3 Enter your DCE password.

4 Access the bin directory:

cd /sdm/bin

5 Change the CM password:

./ata -passwd

Example response:

```
This operation will only change your MAP/CI
password in the central database. Make sure you
have the same password for the user ID on the
DMS.

Available MAP/CI User Ids:
   user1 user2 user3 user4
```

Note: You can also change the CM password from the ATA prompt. For example,
ata> passwd

6 When prompted, enter the MAP/CI user ID associated with the password to change.

7 When prompted, enter the old password for the user ID.

8 When prompted, enter the new password for the user ID.

9 When prompted, enter the new password again to confirm.

Example response:

```
Password change successful.

Continue Change Password (y/n):
```

If you	Do
want to change another password	type y, press the Enter key, and repeat steps 6 through 9
do not want to change another password	step 10

10 Exit the password command:

n

11 You have completed this part of the procedure

Changing the CM password on the core

Use the following procedure to change your CM password. You must complete this procedure before or immediately after you change your CM password in the DCE security database.

Changing the CM password on the core

At the ATA prompt:

1 Log in to the core:

ata> <clli name> cm

2 Change the CM password on the core:

password

3 Enter your new password, and press the Enter key.

Example response:

```
Please enter new password again to verify.
```

4 Enter your new password again, and press the Enter key.

Example response:

```
Enter your current password to verify.
```

5 Enter your old (current) password.

A message informs you that the password has been successfully changed, and that it must be changed in 30 days.

6 You have completed this procedure.

Changing CM passwords from ETA client

Purpose

Use this procedure to change your CM password in the DCE security database.

Application

Changing CM passwords consists of:

- Changing CM passwords in the DCE security database and
- Changing the CM password on the core

ETA clients can change their own user passwords at the ETA main window.

Note 1: You can change the CM password on the core before or immediately after you have changed the CM password in the DCE security database.

Note 2: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Changing CM passwords in the DCE security database

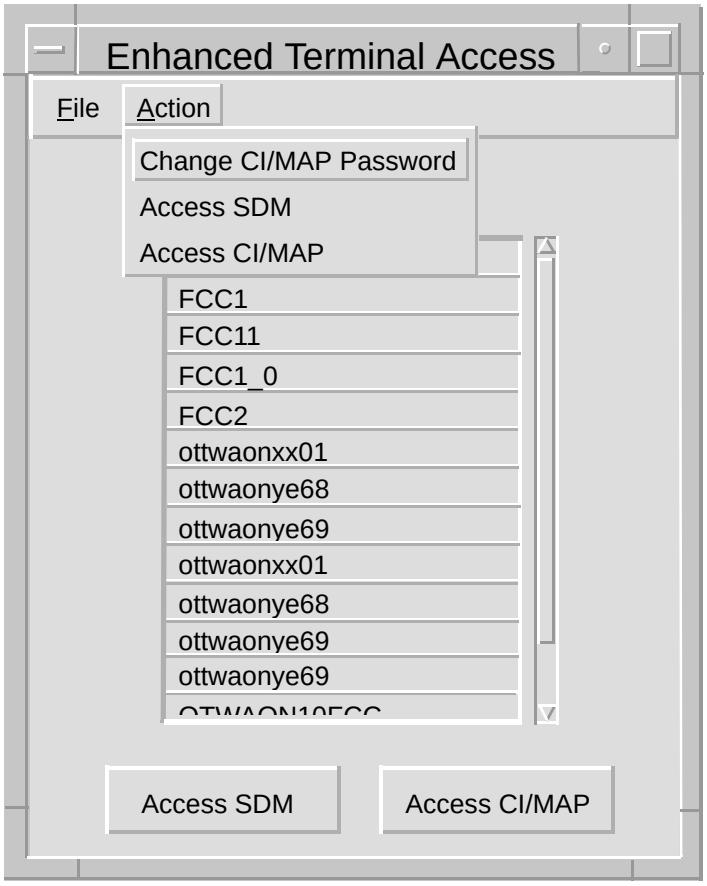
Changing CM passwords in the DCE security database

At the ETA main window

1 Select Change CI/MAP Password from the Action pull-down menu.

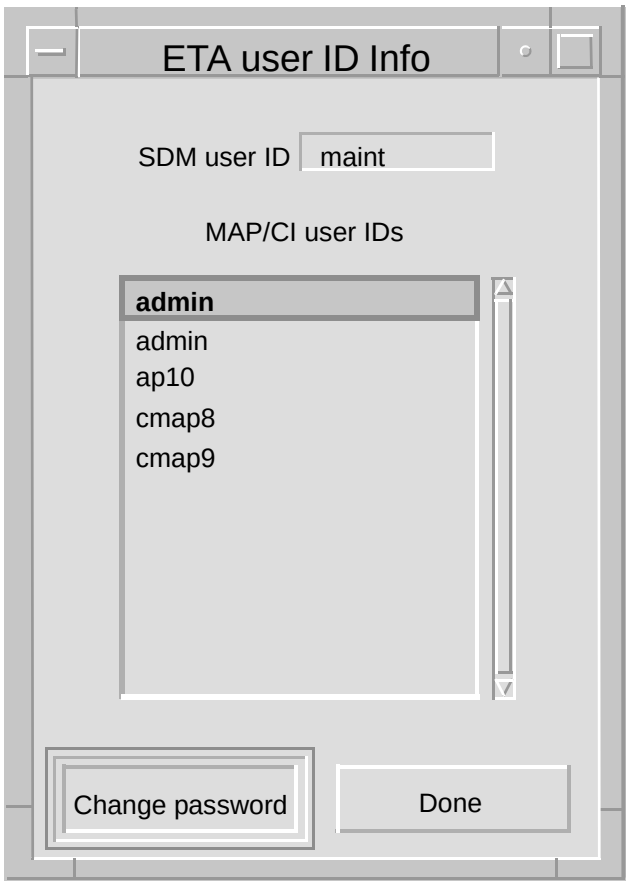
The ETA user ID Info window appears.

ETA window



2 Click on the CM user ID for which you want to change the password.

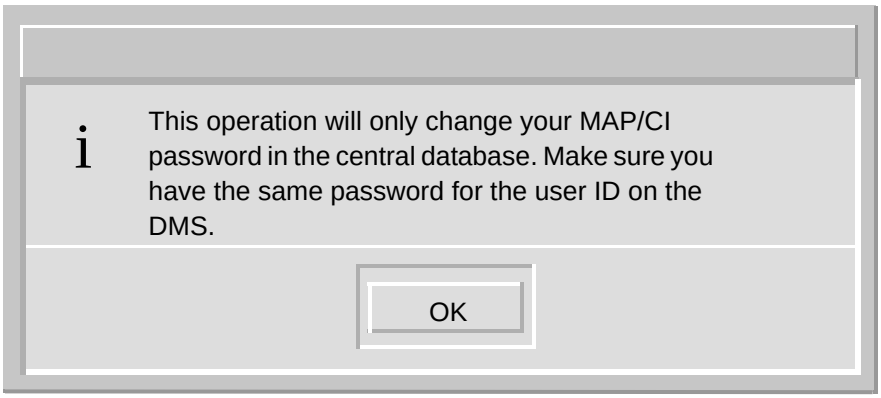
ETA user ID info window



3 Click on Change password button.

A warning message appears.

MAP/CI password change warning message

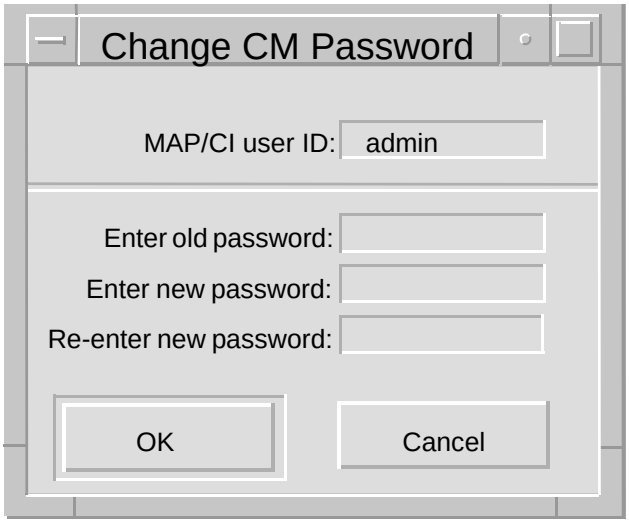


4 Click OK to continue.

Note: The two administration user IDs are used to access different cores. This allows multiple passwords to be used with each CM user ID.

The Change CM Password window appears.

Change CM Password window



5 Enter the old password, the new password, and re-enter the new password. Click the OK button when you are finished.

The Change CM Password window disappears after you click OK.

If you are	Do
changing another password	step 2
finished changing passwords	step 6

6 Click on Done from the ETA User ID Info window.

7 You have completed this procedure.

Changing the CM password on the core

Use the following procedure to change your CM password. You must complete this procedure before or immediately after you change your CM password in the DCE security database.

Under certain conditions, the CM response from a user-entered command and subsequent user keyboard input compete for the display

cursor. The CM output and the user input can be interleaved causing garbled data to appear.

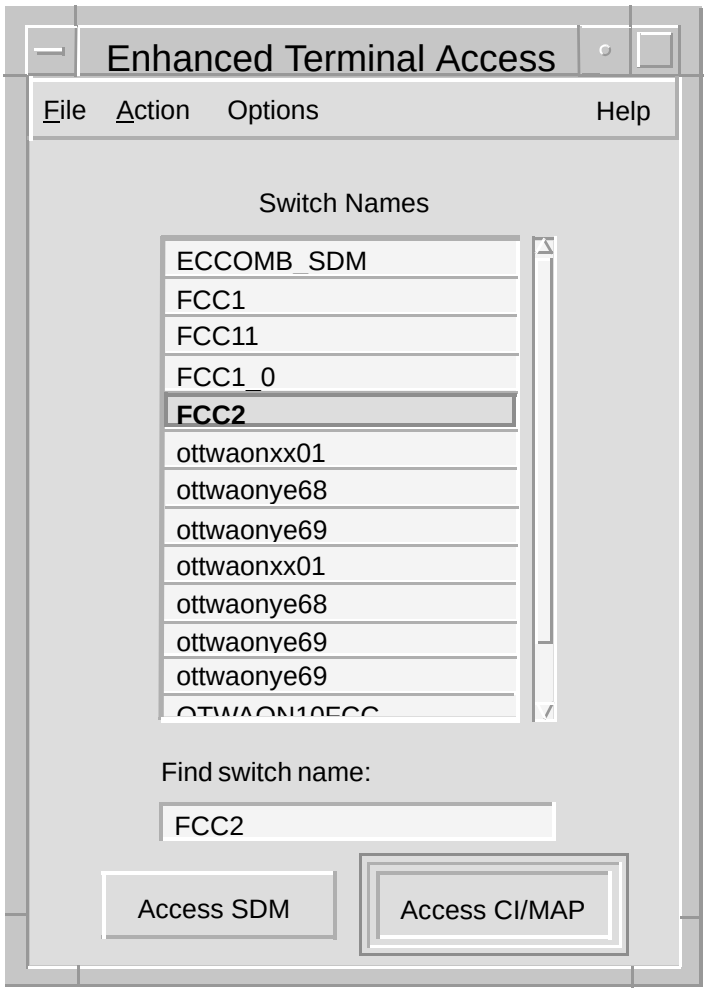
This limitation also exists on the telnet sessions using an Ethernet Interface Unit (EIU). To correct this problem, refresh the screen. This limitation does not corrupt data or user commands on the CM.

Changing the CM password on the core

At the ETA main window:

1 Select the name of the core.

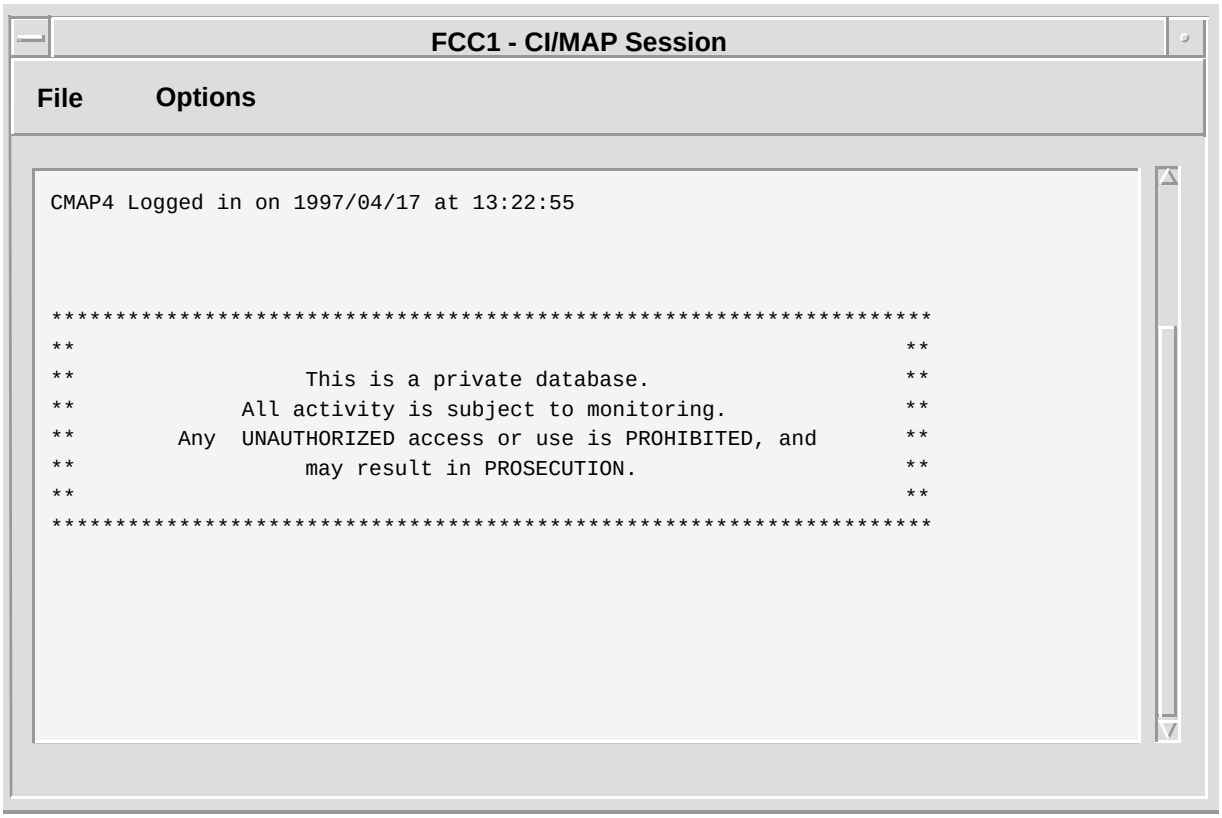
ETA main window



2 Click the Access CI/MAP button.

A CI/MAP session window appears.

Example CI/MAP session window



3 Change the CM password on the core:

password

4 Enter your new password.

Example response:

```
Please enter new password again to verify.
```

5 Enter your new password again.

Example response:

```
Enter your current password to verify.
```

6 Enter your old (current) password.

A message informs you that the password has been successfully changed, and that it must be changed in 30 days.

7 You have completed this procedure.

Changing logical volume thresholds

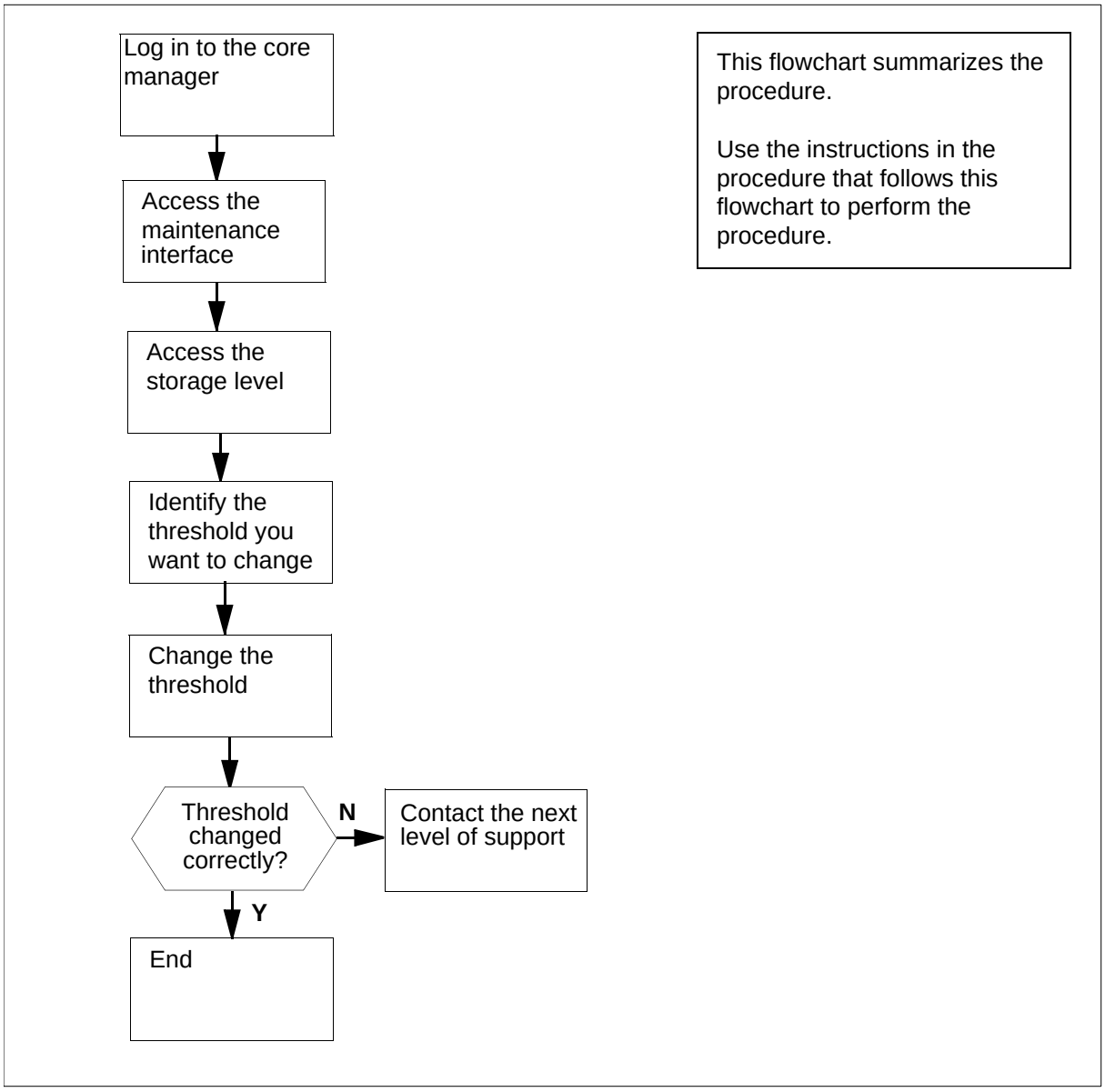
Purpose

Use this procedure to change core manager logical volume thresholds.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of changing logical volume thresholds



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Changing system thresholds

At the local VT100 console

1 Log into the core manager.

2 Access the maintenance interface:

sdmmtc

3 Access the storage level:

storage

Example Response:

```
Volume Group        Status          Free (MB)
rootvg              Mirrored        1932
datavg              Mirrored        7760

Logical Volume  Location   Size(MB)    % full/
threshold
1 /           rootvg     88              25/ 80
2 /usr         rootvg     600             85/ 90
3 /var         rootvg     200             11/ 80
4 /tmp         rootvg     24               6/ 90
5 /home        rootvg     304              4/ 70
6 /sdm         rootvg     504             44/ 90
7 /data        datavg     208              6/ 80
               Logical volumes showing: 1 to 7
of 7
```

4 Identify the logical volume threshold to change. Note the entry number of the logical volume on the left of the storage menu.

5 Change the logical volume threshold:

change <n> <x>

where

<n>
is the entry number of the logical volume for which you want to change the threshold

<x>
is the new threshold value

Example input:

change 5 80

6 Wait 5 seconds. Check to see that the logical volume threshold changed to the value that you entered.

If the logical volume threshold did not change correctly, contact your next level of support.

7 You have completed this procedure.

Changing system thresholds

Purpose

Use this procedure to change core manager system thresholds.

Application

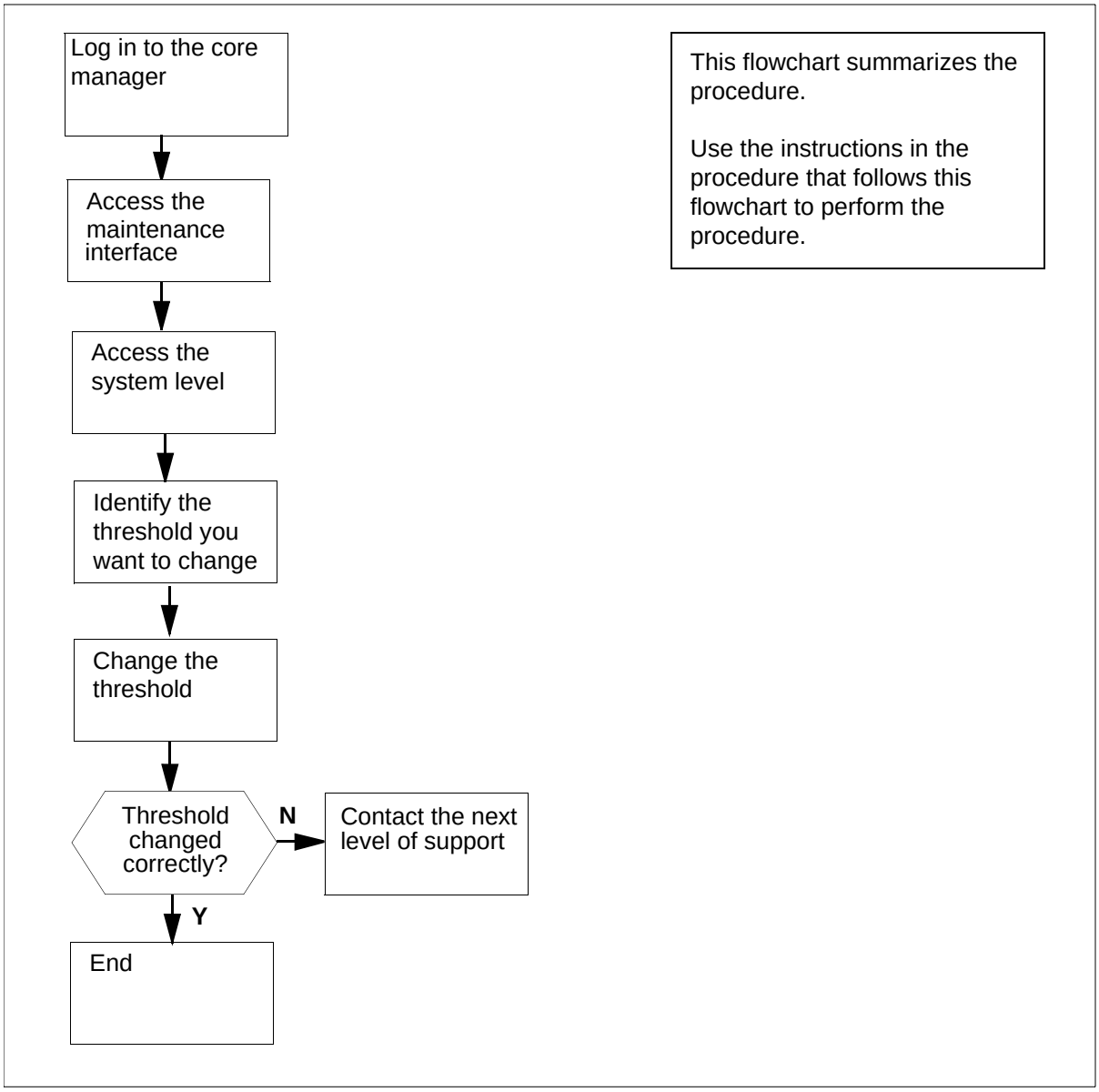
You can change the following core manager system thresholds at the system menu level of the Remote Maintenance Interface (RMI):

- CPU (run queue entries)
- number of Processes
- number of Zombies
- Swap Space (% full)
- number of Swap Queue Entries

Action

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the tasks.

Summary of changing system thresholds



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Changing system thresholds

At the local VT100 console

1 Log into the core manager.

2 Access the maintenance interface:

sdmmtc

3 Access the system (Sys) level:

sys

Example response:

```
SDM Storage State:          .

#
Description                          Current/Thres
hold
1 CPU (run queue entries):                    1/  5
2 Number of Processes:                       63/250
3 Number of Zombies:                          0/  3
4 Swap Space (% full):                       72/ 70*
5 Number of Swap Queue Entries:               0/  2
```

4 Identify the system threshold to change. Record the entry number of the system threshold located on the left System menu. The number is shown under the header #.

In the example in step 3:

- CPU threshold is 1
- Number of Processes threshold is 2
- Number of Zombies is 3
- Swap Space threshold is 4, and
- Number of Swap Queue Entries is 5

The current threshold value is shown in the right column under the header Current/Threshold.

5 Change the system threshold:

change <*n*> <x>

where

<*n*>
is the entry number of the threshold you want to change

<*x*>
is the new threshold value

Example input:

```
> change 4 80
```

6 Wait 5 seconds. Check if the system threshold changed to the value that you entered.

If the system threshold did not change correctly, contact your next level of support.

7 You have completed this procedure.

Recovering the system when root password unknown

Purpose

Use this procedure to change the root user password when it is not known.

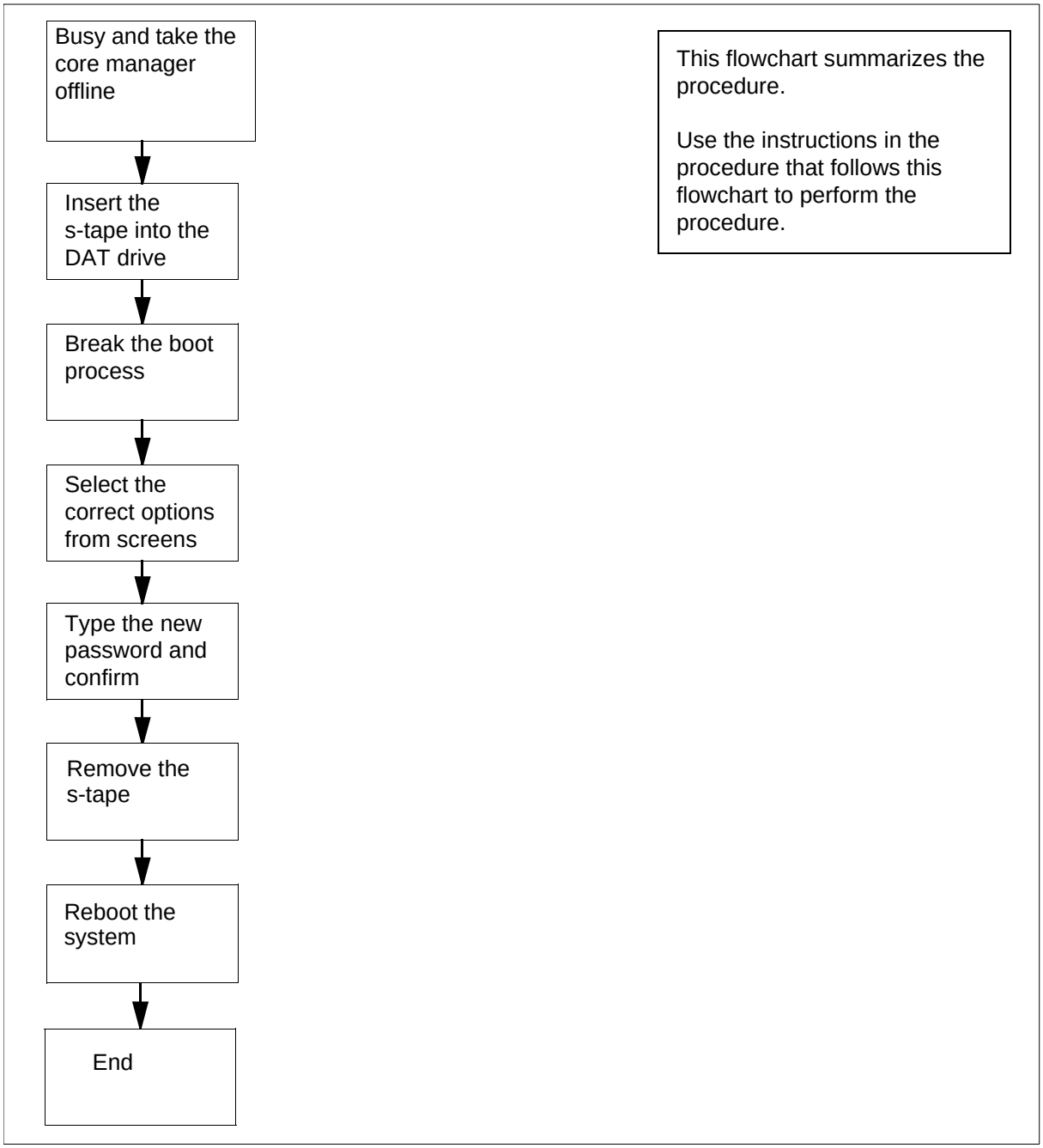
Application

If the ETA application is installed and in service, use the ETA application to open a root user session. Then, use the procedure Changing a user password in this section to change the root password.

Action

The following flowchart summarizes the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the tasks.

Summary for recovering the system when root password unknown



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Recovering the system when root password unknown

At the SDM level of the MAP display

1 Busy the core manager:

bsy

You are prompted to confirm whether you want to busy the core manager.

2 Confirm that you want to busy the core manager:

y

At the core manager

3 Insert the latest system backup tape (s-tape) into DAT drive 0 (slot 2).

Note: Wait until the tape drive is ready (yellow LED is off) before you proceed.

At the SDM level of the MAP display

4 Reboot the core manager:

rebootsdm

At the local console

5 When the system displays COLD Start, press the Break key or the Esc key twice to interrupt the boot process.

6 Reboot the system:

Fx-Bug> pboot 1 50

The system displays progress messages. When they are completed, proceed to the next step.

Note: In case of any boot failures, contact your next level of support.

7 At the “Please define the system console” display, enter:

1

8 At the second interactive screen, select 1 for English.

9 At the “Welcome to base operating system installation and maintenance” display, select 3 to begin the maintenance mode for system recovery.

10 At the Maintenance display, select 1 to access a root volume group.

11 At the Warning display, select 0.

The “Access a Root Volume Group” display lists the volume groups with the disks they contain. Each disk has a name, (for example, hdisk0) and a location code (for example 4056 c1-f2-00-0,0).

12 Enter the number of the volume group whose location code contains the characters c1-f2. Press the Enter key.

Example output:

```
1) Volume Group 002e43cdaa6655f5 contains these
disks:       hdisk1 4056 c1-f4-00-0,0    hdisk2
4056 c1-f4-00-1,0        hdisk3 4056
c1-f4-00-0,0  hdisk4 4056c1-f15-00-1,0
2) Volume Group 002e43cda6d92fc7 contains these
disks:       hdisk0  4056 c1-f2-00-0,0  hdisk3
4056c1-f13-00-0,0
```

13 At the Volume group information display, select 1 to access the volume group and start a UNIX shell.

14 At the UNIX prompt enter:

passwd root

and press the Enter key. The system prompts you for a new root password.

15 Enter the new root password. When prompted, re-enter the new root password.

16 Confirm the password change:

ls -l /etc/passwd

```
Example output:
-rw-r--r--1 root root11539 Jul 912:37
/etc/passwd
```

17 Check that the date and time that are displayed as a result of step 16 are the current date and time.

If the current date and time	Do
are displayed	step 18
are not displayed	contact your next level of support

18 Remove the s-tape.

19 Reboot the system:

shutdown -Fr

When the reboot completes, the login prompt appears. You must then use the new password to log in as the root user.

20 You have completed this procedure.

Recommissioning date and time zone

Purpose

Use this procedure to commission the date, time, and time zone on the core manager.

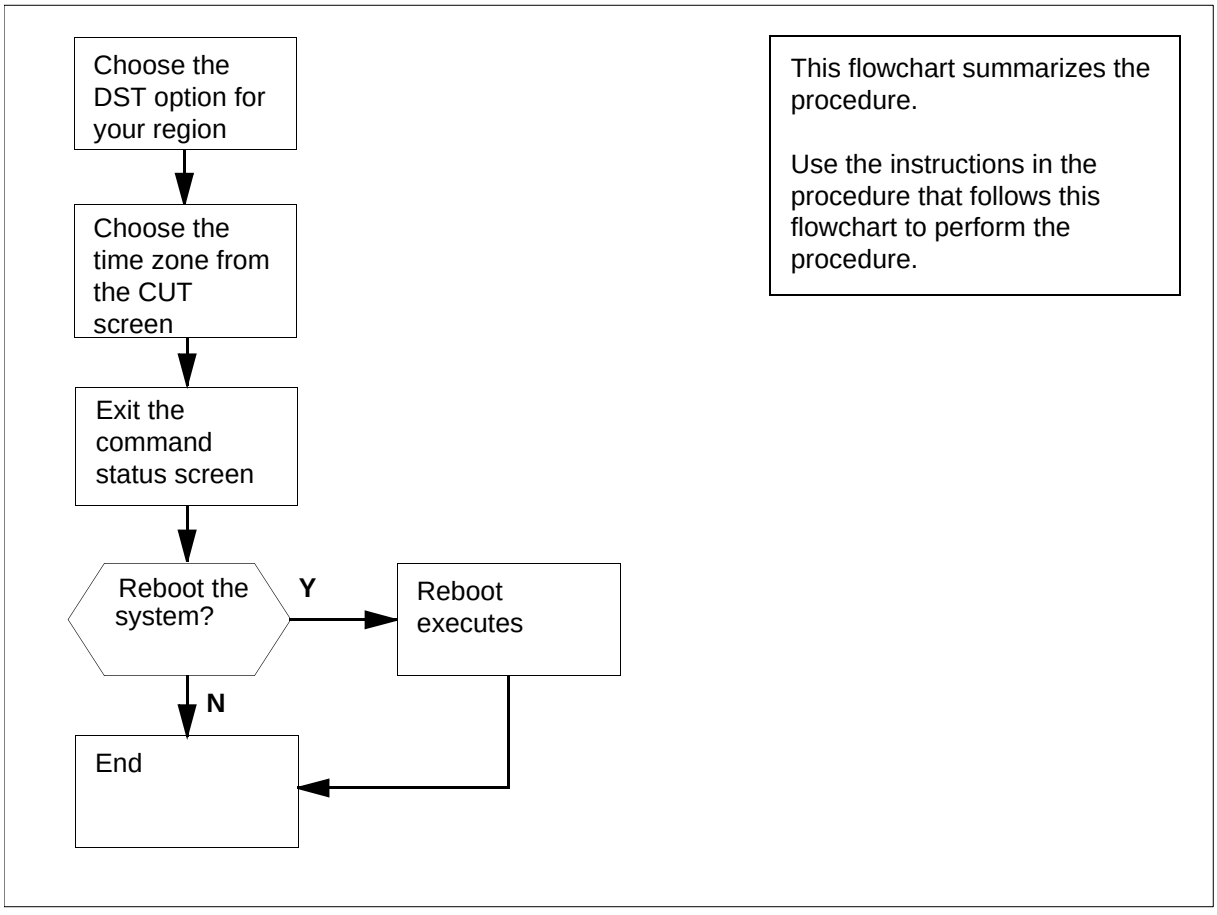
Prerequisites

To recommission the date, time, and time zone, the node state must either be ManB or OffL, and the node must not be DCE synchronized. Refer to the procedure, “Removing a core manager from a DCE” in the Configuration document. This restriction does not apply to initial commissioning.

Procedure

The following flowchart summarizes the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of commissioning miscellaneous items: date, time, and time zone



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Commissioning miscellaneous items: date, time, and time zones

CAUTION
Inability to recommission time zone
To recommission the date, time, and time zone, the node state must either be ManB or OffL, and the node must not be DCE synchronized. With the exception of initial commissioning, you do not have the option of recommissioning the date, time, and time zone if the core manager is not ManB or Offl and if DCE is running and in service.

At the local VT100 console

1 Log in to the core manager.

2 Access the commissioning level:

`sdmconfig`

3 Select the Time and Time Zone option:

2

The system displays the prompt for the date, time, and time zone configuration preview window.

```
SDM COMMISSIONING

DATE, TIME AND TIME ZONE

You will be prompted for time and date
information. Once you have entered the
information, you will need to reboot the SDM for
the changes to take effect.

HIT ENTER TO CONTINUE
```

4 Press the Enter key to continue.

The system displays the Change / Show Date, Time, and Time Zone screen.

5 Use the following table to determine your next step.

If you	Do
follow the daylight saving time conventions for North America	step 8
do not follow the daylight saving time conventions for North America	step 6

Note 1: Under North American conventions, the move from standard time to daylight saving time occurs on the first Sunday of April. On this day, clock time is moved forward one hour at 2:00 a.m. The move from daylight saving time to standard time occurs on the last Sunday of October. On this day, clock time is moved backward one hour at 2:00 a.m.

Note 2: If you do not follow the North American daylight saving time zone conventions, check with appropriate personnel for the dates and times that daylight saving changes occur in your region.

6 Select Change Time Zone Using User Entered Values on the Change / Show Date, Time, and Time Zone screen, and press the Enter key.

The Change Time Zone screen appears.

7 Use the up and down arrow keys to move the cursor and highlight the entries in the entry fields. Change the value in the field after you highlight it. When you finish changing the values in the fields, press the Enter key and go to step 9.

The following table explains each of the value fields in the Change Time Zone window, and their formats.

(Sheet 1 of 3)

Field or subfield	Value	Description
Standard Time ID	Alphabetic characters	Any identifier you wish to use for your region's standard time.
Standard Time Offset from CUT		Identifies the value that must be added to or subtracted from local standard time to equal Coordinated Universal Time (CUT). This field contains the subfields HH:MM:SS, as follows:
[+|-] HH (required)	Range of integers from -12 to +11	Identifies the number of hours in the offset, and whether to add or subtract the offset.
MM (optional)	Numeric between 0 and 59. Always preceded by a colon (:)	Identifies the number of minutes in the offset.
SS (optional)	Numeric from 0 to 59. Always preceded by a colon (:)	Identifies the number of seconds in the offset.
Daylight Saving Time ID	Alphabetic characters	Any identifier you want to use for your region's daylight saving time.
Daylight Saving Time Offset from CUT		Identifies the value that must be added to or subtracted from local daylight time to equal CUT. This field contains the subfields HH:MM:SS (as explained under Standard Time Offset from CUT, preceding.)
Start Daylight Saving Day		Identifies the date on which daylight saving time starts. This field contains the subfields Mmm.ww.dd or Jn, as follows.

(Sheet 2 of 3)

Field or subfield	Value	Description
M	Constant	Indicates that the date is being specified using the mm.ww.dd subfields.
mm	Numeric from 1 to 12	Identifies the month.
ww	Numeric from 1 to 5 (single digit), always preceded by a period (.)	Identifies the number of the week within the month, as follows: • 1 if the date falls on the 1st to the 7th day • 2 if the date falls on the 8th to the 14th day • 3 if the date falls on the 15th to the 21st day • 4 if the date falls on the 22nd to the 28th day • 5 if the date falls on the 29th to the 31st day
dd	Numeric from 0 to 6, always preceded by a period (.)	Identifies the day of the week, as follows: • 0 for Sunday • 1 for Monday • 2 for Tuesday • 3 for Wednesday • 4 for Thursday • 5 for Friday • 6 for Saturday
J	Constant	Indicates that the date string is being specified using a 365-day calendar.
n	Numeric from 1 to 365	Indicates the number of the date in a 365-day calendar year.

(Sheet 3 of 3)

Field or subfield	Value	Description
Start Daylight Saving Time	None	Identifies the time at which Daylight Saving Time starts. This field contains the subfields HH:MM:SS (as explained in Standard Time Offset from CUT, preceding, but without a plus or minus sign on the HH subfield).
Stop Daylight Saving Day	None	Identifies the date on which Daylight Saving Time stops. This field contains the subfields Mmm.ww.dd or Jn (as explained in Start Daylight Saving Day, preceding).
Stop Daylight Saving Time		Identifies the time at which Daylight Saving Time stops. This field contains the subfields HH:MM:SS (as explained in Standard Time Offset from CUT, but without a plus (+) or minus (-) sign on the HH subfield).

8 Select Change Time Zone Using System Defined Values on the Change / Show Date, Time, and Time Zone screen, and press the Enter key.

The Use Daylight Savings Time? screen appears.

9 Use the up and down arrow keys to select an option in response to the question, “Does this time zone go on daylight saving time?” Select “yes” (option 1) if at some time in the year daylight saving time is applied to this time zone. Otherwise, select “no” (option 2). Press the Enter key when you have selected the appropriate response.

The system displays the CUT (Coordinated Universal Time) Time Zone screen.

Each option in the CUT Time Zone screen corresponds to a Greenwich Mean Time (GMT) value, as shown in the following table.

(Sheet 1 of 2)

Name on screen	Text on screen	Offset CUT value on screen	GMT value
CUT0GDT	Coordinated Universal Time	CUT	GMT
GMT0BST	United Kingdom	CUT	GMT
AZOREST1AZOREDT	Azores; Cape Verde	CUT -1	GMT -01:00
FALKST2FALKDT	Falkland Islands	CUT -2	GMT -02:00
GRNLNDST3GRNLNDDT	Greenland; East Brazil	CUT -3	GMT -03:00
AST4ADT	Central Brazil	CUT -4	GMT -04:00
EST5EDT	Eastern U.S.; Columbia	CUT -5	GMT -05:00
CST6CDT	Central U.S.; Honduras	CUT -6	GMT -06:00
MST7MDT	Mountain U.S.	CUT -7	GMT -07:00
PST8PDT	Pacific U.S.; Yukon	CUT -8	GMT -08:00
AST9ADT	Alaska	CUT -9	GMT -09:00
HST10HDT	Hawaii; Aleutian	CUT -10	GMT -10:00
BST11BDT	Bering Straits	CUT -11	GMT -11:00
NZST-12NZDT	New Zealand	CUT +12	GMT +12:00
MET-11METDT	Solomon Islands	CUT +11	GMT +11:00
EET-10EETDT	Eastern Australia	CUT +10	GMT +10:00
JST-9JDT	Japan	CUT +9	GMT +09:00
KORST-9KORDT	Korea	CUT +9	GMT +09:00
WAUST-8WAUDT	Western Australia	CUT +8	GMT+08:00

(Sheet 2 of 2)

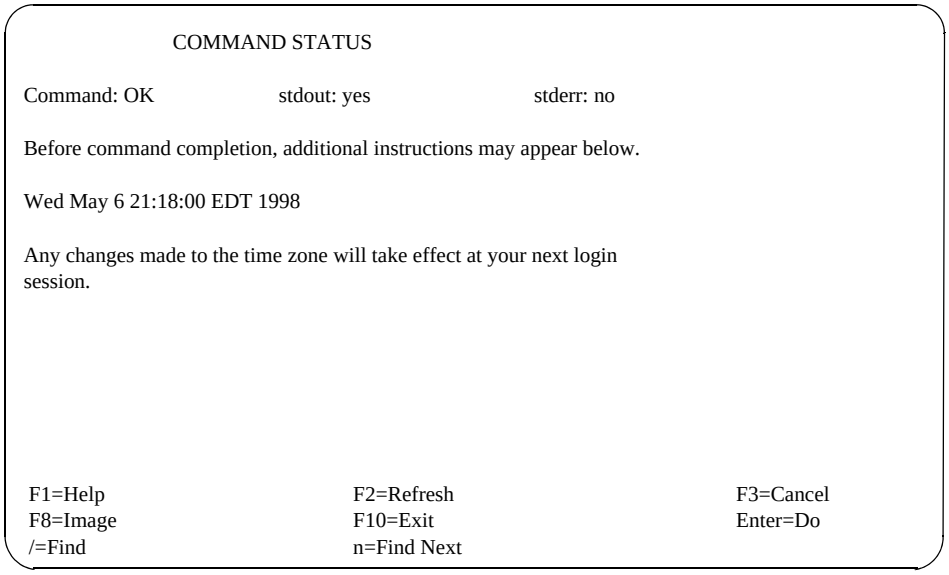
Name on screen	Text on screen	Offset CUT value on screen	GMT value
TAIST-8TAIDT	Taiwan	CUT +8	GMT +08:00
THAIST-7THAIDT	Thailand	CUT +7	GMT +07:00
TASHST-6TASHDT	Tashkent; Central Asia	CUT +6	GMT +06:00
PAKST-5PAKDT	Pakistan	CUT +5	GMT +05:00
WST-4WDT	Gorki, Central Asia; Oman	CUT +4	GMT +04:00
MEST-3MEDT	Turkey	CUT +3	GMT +03:00
SAUST-3SAUDT	Saudi Arabia	CUT +3	GMT +03:00
WET-2WET	Finland	CUT +2	GMT +02:00
USAST-2USADT	South Africa	CUT +2	GMT+ 02:00
NFT-1DFT	Norway; France	CUT +1	GMT +01:00

10 Use the up and down arrow keys to select the time zone you use. Then press the Enter key. The Change Time Zone screen appears.

11 You do not need to change the variables on the Change Time Zone screen. Press the Enter Key.

12 The Command Status screen appears. The command status is shown as “running” while the changes are being processed. The command status changes to “OK” when processing is complete. The date, time, and time zone appear.

Example response:



Note: If the command status changes to “Failed”, repeat this procedure.

13 Exit the Command Status screen by pressing the F10 key, Esc+10, or PF10 keys.

Example response:

```
SDM COMMISSIONING
DATE, TIME AND TIME ZONE

Your time and date information has been entered.
For this information to take effect, you will
need to reboot the SDM.

Do you wish to reboot the SDM now?
Please confirm (“YES”, “Y”, “NO”, or “N”)
```

If you wish to	Do
defer rebooting the core manager	type n and press the Enter key you have completed this procedure
reboot the core manager	step 14

14 Confirm the system reboot:

y

Wait until the reboot completes and the login prompt reappears.

15 You have completed the procedure.

Changing the system date or time

Purpose

Use this procedure to change the system date or time on the core manager.

Prerequisites

Perform this procedure to change the system date or time when the core manager is in operation, and not controlled by a DCE server. Ensure that the core manager is either ManB or OffL.

Application

This procedure does not replace the commissioning procedure Changing the system time zone and daylight savings time parameters on page 200.

ATTENTION

This procedure is for in-operation core managers only. If you are configuring the core manager for the first time, use the procedure Changing the system time zone and daylight savings time parameters on page 200.

ATTENTION

To change the date or time the node state must either be ManB or OffL and the node must not be DCE synchronized. If the node is DCE synchronized, change the time on the DCE server. The DCE server controls the time change for all nodes under its control in the DCE cell.

ATTENTION

This procedure cannot be used to change the date or time while the core manager is in split-mode.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Changing the system date or time

At the local VT100 terminal

1 Log in to the core manager.

2 Access the maintenance interface level:

sdmmtc

3 Access the admin level:

admin

4 Select “Time” from the menu:

9

5 Enter the change command:

change

6 Accept or change the year.

If you want to	Do
accept the specified “Year”	press Enter, and proceed to step 7
change the specified “Year”	edit the value, press Enter, and proceed to step 7

7 Accept or change the month.

If you want to	Do
accept the specified “Month”	press Enter, and proceed to step 8
change the specified “Month”	edit the value, press Enter, and proceed to step 8

8 Accept or change the Day.

If you want to	Do
accept the specified “Day”	press Enter, and proceed to step 9
change the specified “Day”	edit the value, press Enter, and proceed to step 9

9 Accept or change the Hour.

If you want to	Do
accept the specified “Hour”	press Enter, and proceed to step 10
change the specified “Hour”	edit the value, press Enter, and proceed to step 10

10 Accept or change the Minutes.

If you want to	Do
accept the specified “Minutes”	press Enter, and proceed to step 11
change the specified “Minutes”	edit the value, press Enter, and proceed to step 11

11 Accept the new date and time:

y

12 You have completed this procedure.

Stopping and restarting an application

Purpose

Use this procedure to stop and restart applications.

Prerequisites

You must be a user authorized to perform performance-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying actions a user is authorized to perform	15

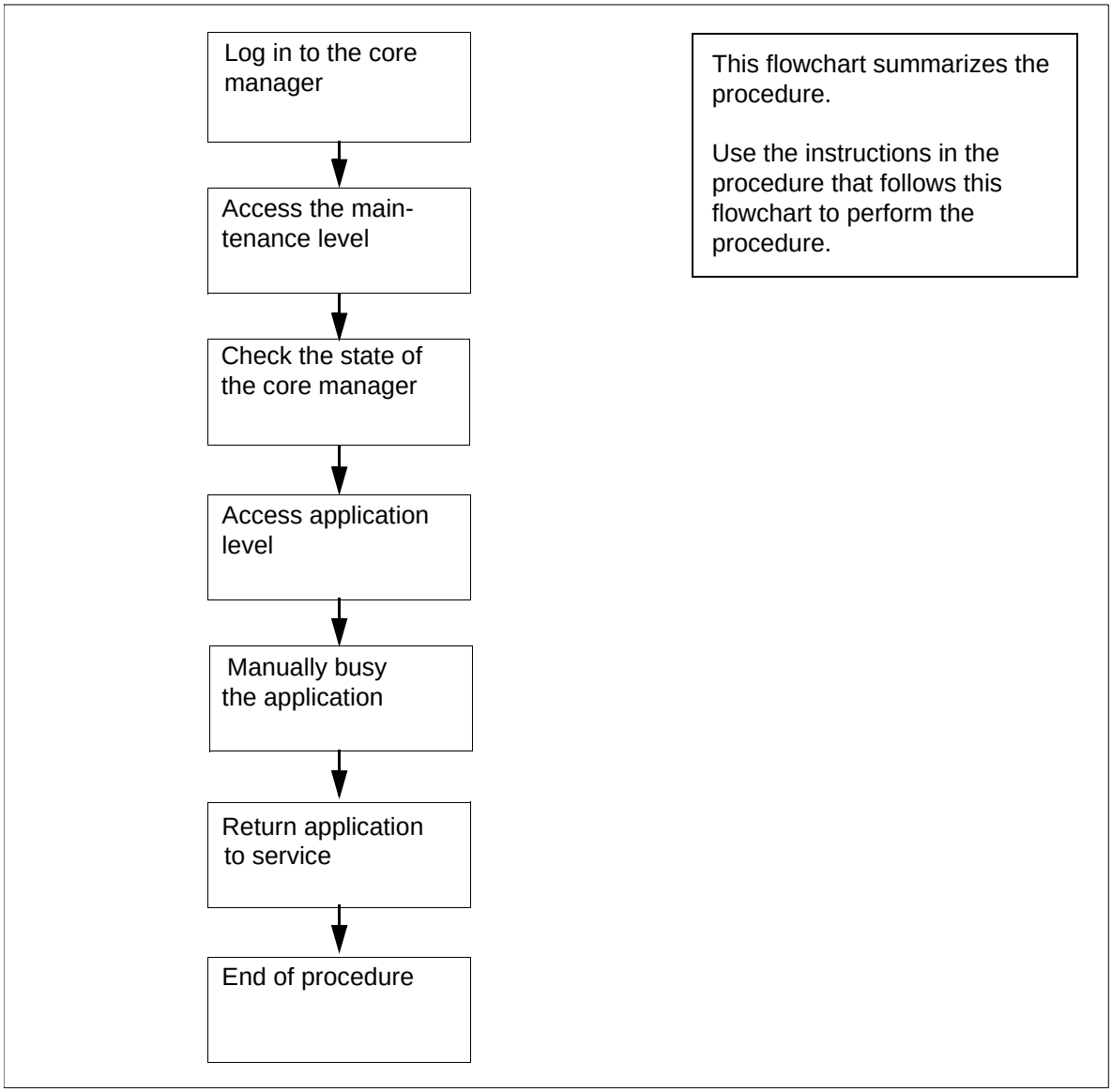
Application

Use this procedure to stop (manually busy) and restart (return to service) core manager software applications.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of stopping and restarting an application



Stopping and restarting an application

At the local or remote VT100 terminal

1 Log in to the core manager as a user authorized to perform performance-admin actions.

2 Access the maintenance interface:

 # sdmmtc

3 Access the application level:

> appl

4 Busy the software application:

> bsy <n>

where

<n>
is the number next to the application to busy

Example response:

```
The application is in service.
This command will cause a service interruption.
Please confirm (“YES”, “Y”, “NO”, or “N”):
```

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

5 Confirm the Busy command:

> y

After you confirm the Bsy command, the following is displayed:

Example response:

```
Application Bsy- Command initiated.Please
wait...

Application Bsy - Command complete.
```

6 Return the application to service:

> rts <n>

where

<n>
is the number next to the application you want to return to service

Example response:

```
Application RTS - Command initiated.
Please wait...

Application RTS - Command complete.
```

7 You have completed this procedure.

Deleting a DCE user

Purpose

Use this procedure to delete a DCE user.

Prerequisites

ATTENTION
You must be a trained Distributed Computing Environment (DCE) system administrator to perform this procedure.

Application

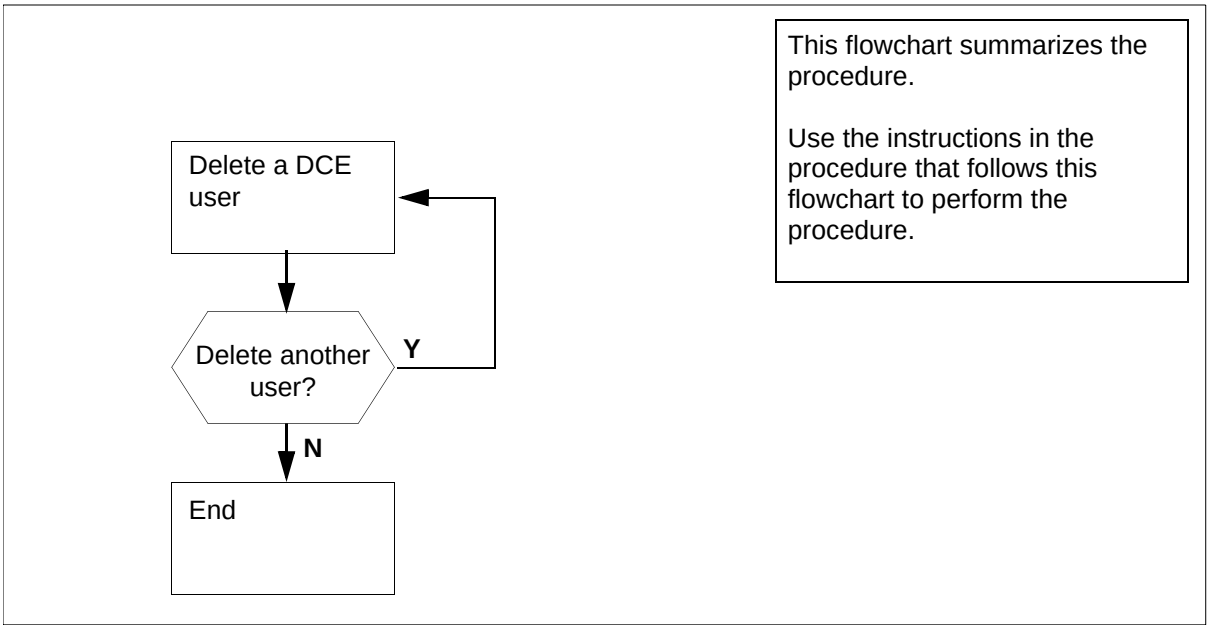
ATTENTION
Use a DCE master administration account (cell_admin) or a DCE sub administrator account (sdm_admin) to perform this procedure. You cannot use the sdm_admin account to delete a DCE user created by a cell_admin account.

The cell_admin account can delete any DCE users created by either the cell_admin or sdm_admin account.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of Deleting a DCE user



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Deleting a DCE user

At the core manager remote client workstation

1 Delete a DCE user:

/sdm/bin/delete_dce_user

Example response:

```
DCE administrator user ID [sdm_admin]:
```

2 Enter the DCE user ID.

Note: If you do not enter a user ID, the system enters the default value (sdm_admin).

Example response:

```
sdm_admin password:
```

3 Type your DCE administrator password.

Response:

```
DCE user ID to be deleted:
```

4 Enter the DCE user ID you want to delete.

Example response:

```
The DCE user ID “ops_1” has been deleted.
```

If	Do
wish to delete another user	step 2
finished	step 5

5 You have completed this procedure.

Establishing a modem connection

Purpose

Use the following procedure to establish a dial-up modem connection to the core manager from a remote location.

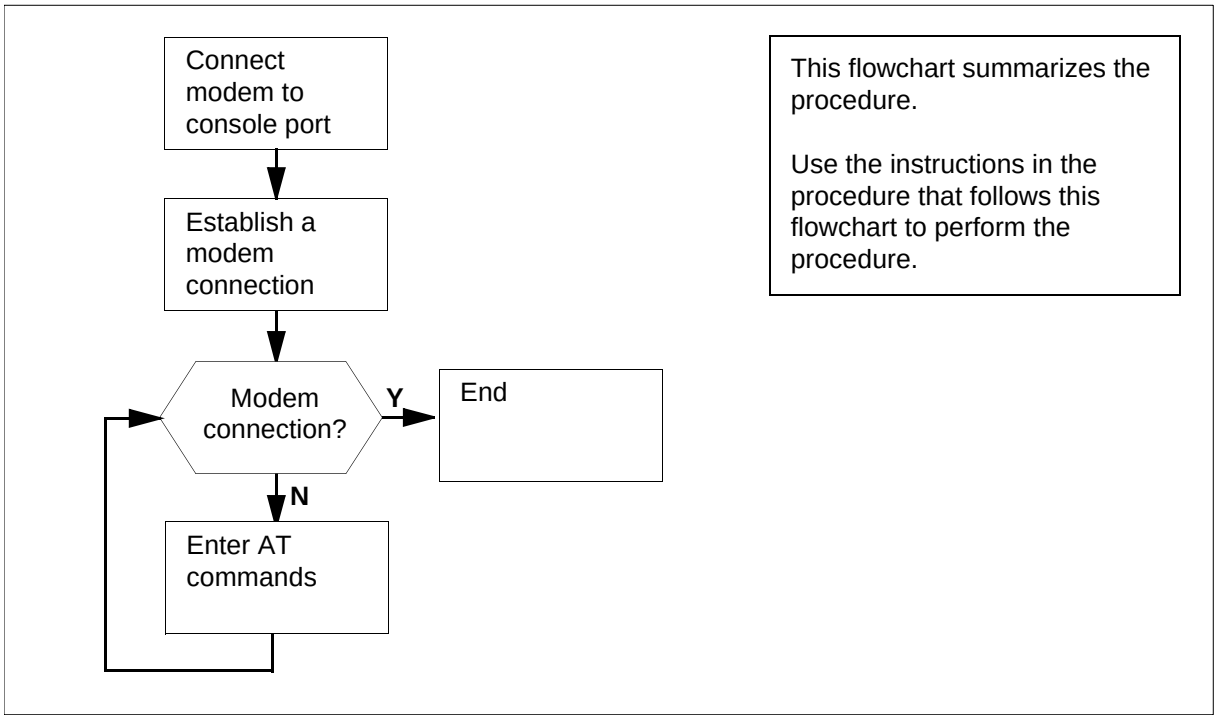
Application

Use the General DataComm (GDC) maintenance modem provided with the core manager equipment whenever a console dial-up modem connection to the core manager from a remote location is required. The GDC maintenance modem is installed and configured as part of the installation of the core manager.

Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of establishing a modem connection



Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

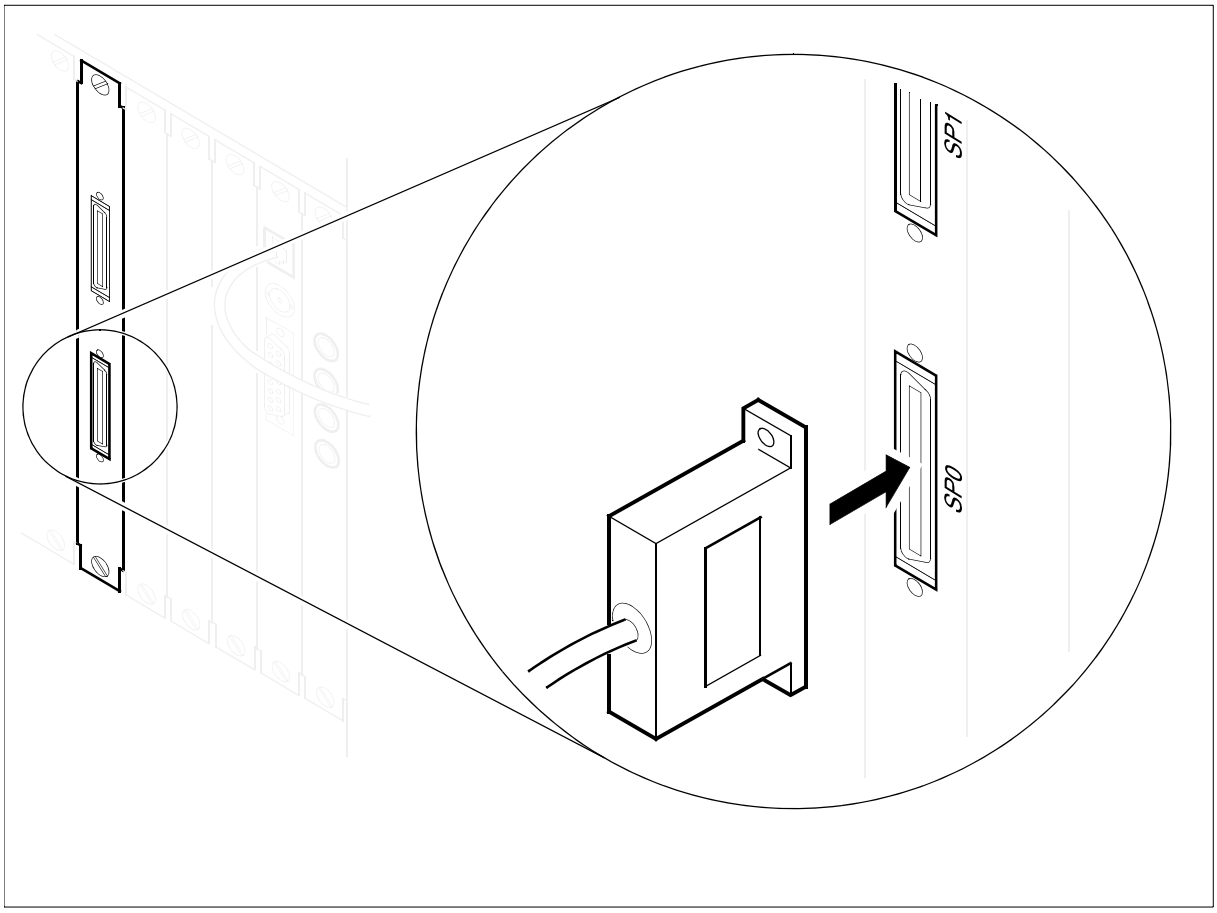
Establishing a modem connection

At the core manager

1 Ensure that no other terminal device cables are connected to console port SP0 on the CPU personality module.

2 If necessary, connect the NTRX5093 cable connected to the GDC maintenance modem to port SP0, and ensure a phone line is connected to the GDC maintenance modem. See the diagram below.

Note: The modem is located in the appropriate MIS frame.



At a remote VT100 console

3 Use a terminal connected to a V.34 Hayes-compatible modem (or to other compatible communications equipment connected to a V.34 modem) to establish remote connection to the core manager console port.

4 Establish a modem connection to the core manager by entering

atdt <*dial_in_number*>

where

<dial_in_number>
is the telephone number for the modem attached to serial port 1

Note: For information on establishing a modem-to-modem connection, refer to the dial-up connection instructions provided with the communications equipment you are using.

5 Determine if the connection has been established.

If you	Do
receive a login prompt	log in using your user ID and password you have completed this procedure
do not receive a login prompt	step 6

6 Execute the following steps to reconfigure your modem, starting at step 8. If you have connection problems, contact your next level of support.

7 Configure the GDC maintenance modem by connecting a VT100 console set to communicate at 9600 baud directly to the DTE connector on the GDC maintenance modem.

8 Enter the AT commands by first entering:

AT&F0

Note 1: Echo of the command entry depends on the previous configuration.

Note 2: If you make a mistake when entering the AT commands, restart the procedure at step 1

9 When the modem responds “OK”, enter

AT\T7

10 When the modem responds “OK”, enter

AT&R2

11 When the modem responds “OK”, enter

AT&C1

12 When the modem responds “OK”, enter

ATE0

13 When the modem responds “OK”, enter

AT%K1

Note: This command is not echoed on the screen.

14 When the modem responds “OK”, enter

ATQ1

Note: The command is not echoed on the screen.

15 Enter:

AT&W0

Note: The command is not echoed on the screen.

16 Enter:

AT&Y0

Note: The command is not echoed on the screen.

17 Return to step 4 and try to establish a modem connection again.

18 You have completed this procedure.

Getting ERA values for CM userIDs

Purpose

Use the following procedure to display the ERA values for CM userIDs.

Application

The show_cm_userid command displays an ERA value for CM userIDs. The information assists the administrator to reset the ERA values for CM userIDs.

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Getting ERA values for CM userIDs

At the client workstation

1 Log into the client workstation.

2 Log into DCE using the administrator userID:

`dce_login <DCE_admin_user>`

where

<DCE_admin_user>
is the administrator userID

3 Enter your DCE password.

4 Access the bin directory:

`cd /sdm/bin`

5 Get the ERA value for the CM userID:

`./show_cm_userid <principal_name>`

where

<principal_name>
is the CM userID for the CM ERA values to obtain

6 You have completed this procedure.

Getting the ERA value for core manager userID

Purpose

Use this procedure to reset the ERA value for the userID.

Note: Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

Getting the ERA value for the userID

At the client workstation

1 Log into the client workstation.

2 Log into DCE using the administrator userID:

dce_login <DCE_admin_user>

where

<DCE_admin_user>
is the administrator userID

3 Enter your DCE password.

4 Change to the bin directory:

cd /sdm/bin

5 Get the ERA value for the userID and password.

/show_sdm_userid <principal_name>

where

<principal_name>
is the userID for the ERA value you wish to obtain.

6 You have completed this procedure.

Increasing the size of a logical volume

Purpose

Use this procedure to allocate more disk space to a logical volume.

Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display other information about a user or role group, review the procedures in the following table.

Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	2
Displaying information about a user or role group	20

Application

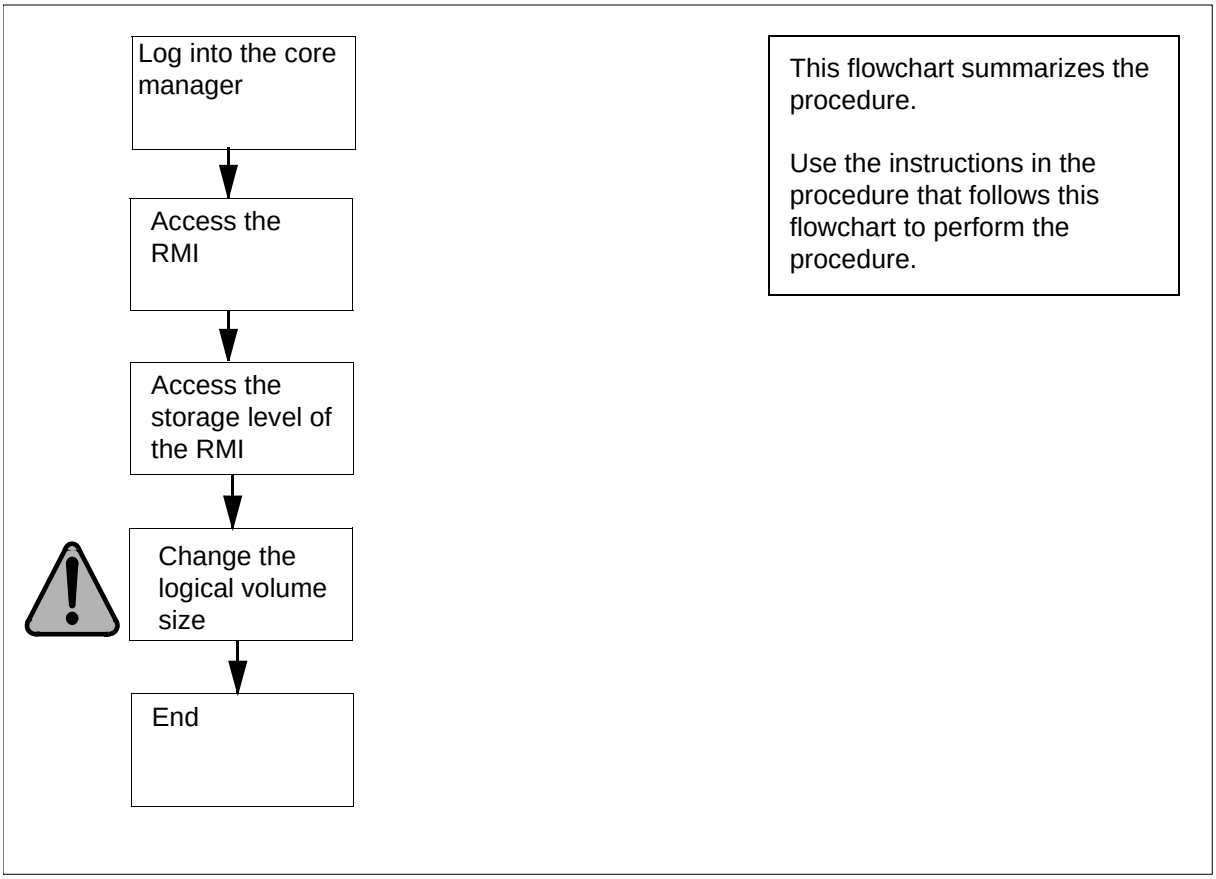
DANGER
Increasing the size of a logical volume can limit future software upgrade capability
core manager logical volumes are pre-engineered to sizes that are adequate for Nortel customers. Do not increase the size of a logical volume unless absolutely necessary.

If you need to change the size of a logical volume, do so only with the assistance of Nortel Technical Assistance and Support. Failure to follow this warning may jeopardize future software upgrade capability.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of increasing the size of a logical volume



Increasing the size of a logical volume

At the local VT100 console

1 Log into the core manager as a user authorized to perform config-admin actions.

2 Access the top menu level of the remote maintenance interface (RMI):

 # sdmmtc

3 Access the system (Sys) menu level of the RMI:

> sys

4 Access the storage menu level of the RMI:

> storage

Example response:

```
Volume Group      Status      Free (MB)
rootvg            mirrored    1932
datavg            mirrored    7760

Logical Volume    Location     Size (MB) %
full/threshold 1 /         rootvg       88
11/ 80
2 /usr           rootvg      600          28/ 90
3 /var           rootvg      200           7/ 70
4 /tmp           rootvg      24            5/ 90
5 /home          rootvg      304          11/ 90
6 /sdm           rootvg      504          23/ 90
7 /data            datavg       208
   6/ 80
                Logical volumes showing: 1 to 7 of 7
```

Note: The example response only shows part of the information displayed at the storage menu level of the RMI.

5 Determine if there is un-allocated disk space that can be used to increase a logical volume.

If there is	Do
enough disk space	step 6
not enough disk space	step 10

6 Identify the logical volume to increase in size. Record the volume name of the logical volume on the left of the System menu of the RMI.

7

ATTENTION
A logical volume on the core manager must never reach 100% full. System behavior cannot be predicted when a logical volume reaches 100% full.

Change the size of the logical volume:

> change lv /<logical_vol> <Mbyte>

where

<logical_vol>
is the name of the logical volume

<Mbyte>
is the size in Mbytes to be added to the logical volume. The size must be less than the amount of un-allocated disk space.

Example input:

> change lv /home 48

Example response:

```
Expanding Volume /home
Expanding Volume /home - Command complete
```

Note: The core manager can round the new size to the nearest 8-, or 16-Mbyte increment.

8 For a 4 Gbyte disk, add 8- or 16-Mbyte multiples. When the logical volume is created, the operating system determines the multiple that has to be used.

9 If the occupancy level of the specified logical volume has exceeded its alarm threshold, contact your system administrator to assess the current condition of the logical volume.

10 You have completed this procedure.

Managing ETA extended registry attributes

ATA and ETA client principal account information is stored on the DCE security server and managed by the DCE admin user. Users can change the CM password that belongs to their principal account.

You can access one MAP/CI session with each CM userID and password. To bypass this limitation, an ATA or ETA client user can access a pool of CM user accounts (userIDs and passwords) to establish multiple MAP/CI sessions.

Depending on the user profile, an ATA or ETA client user can have one core manager userID assigned to a principal account. The core manager userID is used to access one or more core manager sessions.

ATA and ETA clients can share core manager user accounts with each other because the core manager has a limited and restricted list of user accounts, typically root and maint.

The core manager userID, CM userID and CM password information are stored in the extended registry attributes (ERA) of the DCE principal. ERA is administered by the DCE administrator user.

Displaying the CLLI from the command line

Purpose

Use this procedure to display the Common Language Location Identifier (CLLI) of the Core from the command line.

Prerequisites

This procedure requires access to the core manager through telnet, Enhanced Terminal Access (ETA) or ASCII Terminal Access (ATA). This procedure does not support access to the core manager through SDMRLOGIN.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

From any workstation or console

1 Access the core manager.

From the command line

2 Display the CLLI of the Core:

```
clli
```

The system displays the CLLI of the core.

Example response:

```
EAST_CS01
```

3 You have completed this procedure.

Displaying the CLLI from BILLMTC

Purpose

Use this procedure to display the Common Language Location Identifier (CLLI) of the Core from the Billing Maintenance (billmtc) interface.

Prerequisites

This procedure requires access to the core manager through telnet, Enhanced Terminal Access (ETA) or ASCII Terminal Access (ATA). This procedure does not support access to the core manager through SDMRLOGIN.

Note: Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Procedure

From any workstation or console

1 Access the core manager.

2 Access the billing maintenance:

```
billmtc
```

The billing maintenance interface opens.

From any level of BILLMTC

3 Display the CLLI of the Core:

clli

BILLMTC interface displays the CLLI at the top of the screen.

Example response:

```
   BILLMTC          EAST_CS01
    0 Quit
    2 Set
    3
    4 CONFSTRM

    5
    6
    7
    8 APPL
    9 Query
   10 Mib
   11 DispAl
   12 Displogs
   13 FILESYS
   14 SCHEDULE
   15 TOOLS
   16 TAPE
   17 Help
   18 Refresh
   maint1       > clli
Time  09:28
```

4 You have completed this procedure.

Configuring secure outbound transfer of OMs

Purpose

Use this procedure to configure secure outbound transfer of Operational Measurements (OM).

Prerequisites

To use secure file transfer, you must install the OpenSSH fileset.

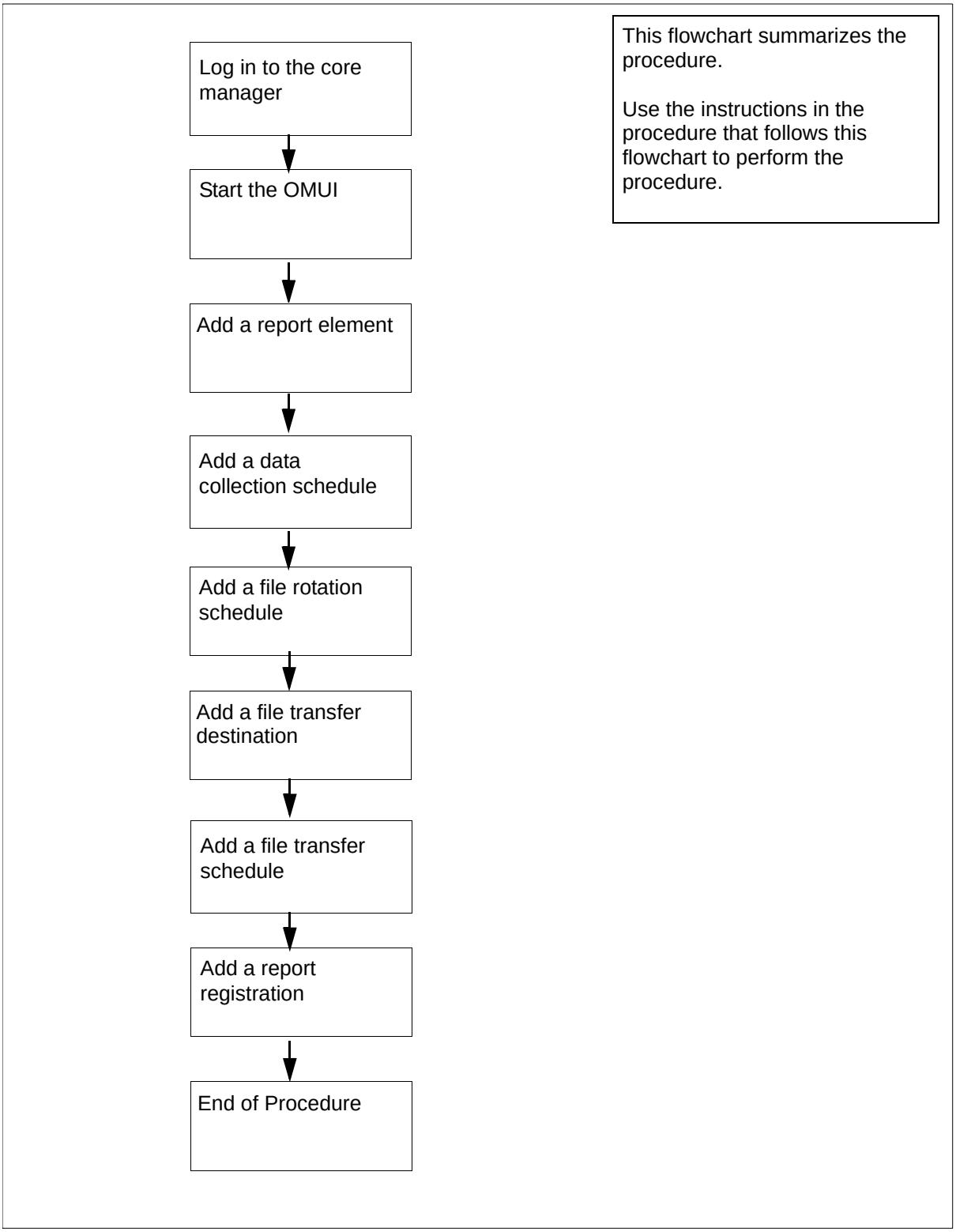
Application

This procedure provides the high level steps. For information on how to use the Operational Measurements User Interface (OMUI) and for details for each step, refer to the Performance Management document.

Performance

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of configuring secure outbound transfer of OMs



Configuring secure outbound transfer of OMs

At the workstation UNIX prompt or VT-100 terminal prompt:

1 Log in to the core manager.

2 Start the OMUI.

Refer to "Starting the OMUI" in the Performance Management document.

3 Add a report element.

Refer to "Adding a report element" in the Performance Management document.

4 Add a data collection schedule.

Refer to "Adding a data collection schedule" in the Performance Management document.

5 Add a file rotation schedule.

Refer to "Adding a file rotation schedule" in the Performance Management document.

6 Add a file transfer destination. When prompted, enter the file type:

`secure`

and pressing the Enter key.

Note: If you choose standard, the outbound OM CSV files will be transferred using standard unencrypted FTP.

Refer to "Adding a file transfer destination" in the Performance Management document.

7 Using the file transfer destination in step 6, add a file transfer schedule.

Refer to "Adding a file transfer schedule" in the Performance Management document.

8 Using the report registration from step 3, the data collection schedule from step 4, file rotation schedule from step 5, and the file transfer schedule from step 7, add a report registration.

Refer to "Adding a report registration" in the Performance Management document.

9 You have completed this procedure.