Core and Billing Manager 850 Security and Administration

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

What’s new in Core and Billing Manager 850 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.

Performing a backup of file systems on a Carrier VoIP SPFS-based server

Application

Use this procedure to perform a backup of the file systems on a Carrier Voice over IP (VoIP) Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240) running the (I)SN06.2 or greater release of the Carrier VoIP SPFS.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- you must be running Carrier VoIP SPFS (I)SN06.2 or greater
- you must perform a data backup prior to performing this procedure Refer to procedure Performing a backup of file systems on a Carrier VoIP SPFS-based server on page 2 to complete this task.

  Note: The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) product family.

- for a Sun Netra t1400, use a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for Sun Netra 240, use one or more blank CD-R, CD-RW, DVD-R or DVD-RW disks to store the data

  Note 1: The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

  Note 2: If you are using a new CD-RW or DVD-RW, or want to reuse a used CD-RW or DVD-RW and need to erase the contents, complete procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

ATTENTION
In a two-sever configuration, execute this procedure on the Active server.

At the server

1 Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the Active server.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Carrier VoIP SPFS-based server on which you are performing the backup

Enter the physical IP address of the Active server in a two-server configuration.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape for backup	step 6
a CD or DVD for backup	step 7

6 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

7 Back up the file systems by typing

```
# /opt/nortel/sspfs/bks/bkfullsys
```

and pressing the Enter key.

Example response:

```
Backup Completed Successfully
```

> ***Note:*** If you are using CD or DVD, the system will prompt you to insert another blank disk if more than one is needed.

If you are using	Do
a tape for backup	step 8
a CD or DVD for backup	step 11

8 Verify the backup to tape was successful. List the contents of the tape by typing

```
# gtar -tvMf /dev/rmt/0
```

and pressing the Enter key.

9 Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.

10 Skip to step step 16.

11 Verify the backup to CD or DVD was successful. Reinsert the backup CD or DVD into the drive.

12 List the content of the CD or DVD by typing

```
# gtar -tvMf /cdrom/*bkfullsys*/*.tar
```

and pressing the Enter key.

When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

13 Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

14 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

# /etc/init.d/volmgt stop

# /etc/init.d/volmgt start

Then, press the eject button located on the front of the DVD drive.

15 Remove the CD or DVD from the drive, label it, and store it in a safe place.

16 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Preparing a CD-RW or DVD-RW for use

Application

Use this procedure to verify the CD-RW or DVD-RW is ready for use when using it for the first time, or when you want to erase the contents of a used CD-RW or DVD-RW to use it again.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the server

1 Insert the CD or DVD into the drive.

Note: Only rewritable media can be erased. Verify that the CD or DVD you are attempting to erase is either a CD-RW or DVD-RW before inserting it into the drive.

At your workstation

2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Carrier VoIP SPFS-based server

3 When prompted, enter your user ID and password.

4 Use the following table to determine your next step.

If the CD or DVD is	Do
new	step 5
used	step 6

5 Verify the CD or DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 10
indicates “No CD writers found or no media in the drive”	step 6

6 Erase the contents of the CD or DVD by typing

```
$ cdrw -b all
```

and pressing the Enter key

> ***Note:*** Erasing a DVD-RW can take over two hours. You can also use the “fast” and “session” arguments. For more details, refer to the man pages by typing **`man cdrw`**.

7 Verify the CD or DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 10
indicates “No CD writers found or no media in the drive” or “Media in the device is not erasable”	step 8

8 Eject the CD from the drive as follows:

a Ensure you are at the root directory level by typing

```
$ cd /
```

and pressing the Enter key.

b Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

> ***Note:*** If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
>
> # **/etc/init.d/volmgt stop**
>
> # **/etc/init.d/volmgt start**
>
> Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

9 Obtain another CD or DVD and repeat the process starting with step 4.

10 Proceed to use the CD or DVD.

You have completed this procedure.

Adding a file system using the makelv command

Application

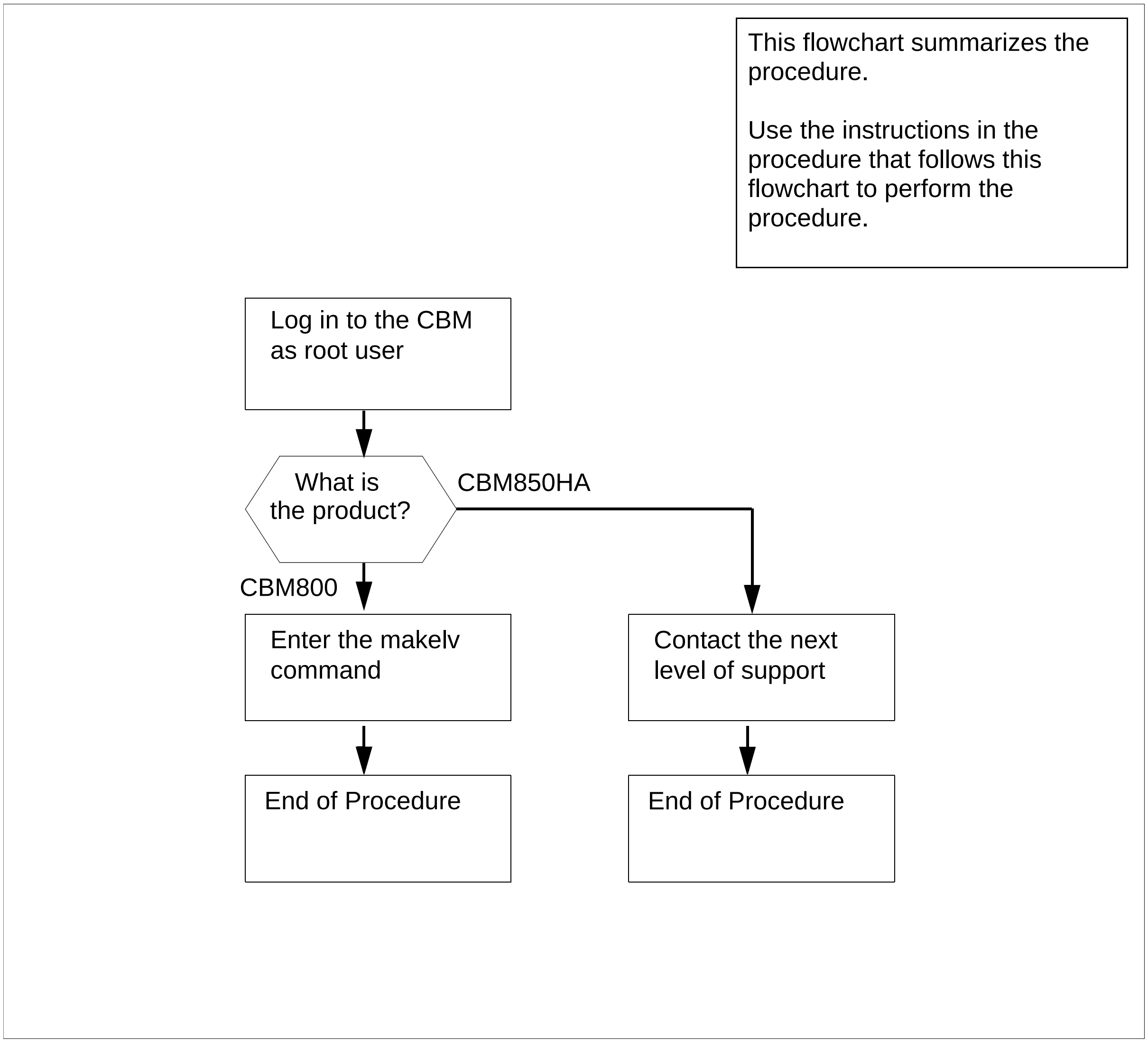
Use this procedure to create a new file system on the CBM product using the makelv command.

You must have root user privileges 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 adding a file system using the makelv command


This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the procedure.
Log in to the CBM as root user
What is the product?
CBM850HA
CBM800
Enter the makelv command
Contact the next level of support
End of Procedure
End of 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.

Adding a file system using the makelv command

At the local or remote VT100 terminal

1 Complete the steps for the CBM product.

If you have	Do
a CBM800	step 2
a CBM850HA	contact the next level of support

2 Log in to the CBM as the root user.

3 Add a file system by typing

```
makelv <file system name><file system size>
```

and pressing the Enter key.

where

file system name
is the mount point of the file system to be created

file system size
is the size of the file system in MegaBytes

4 You have completed this procedure.

Increasing the size of a file system on a Carrier VoIP SPFS-based server

Application

Use one of the following procedures to increase the size of a file system on a Carrier Voice over IP (VoIP) Server Platform Foundation Software (SPFS)-based server:

- Simplex configuration (one server) on page 12
- High-availability configuration (two servers) on page 17

It is recommended you perform this procedure during off-peak hours.

The Carrier VoIP SPFS creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The table below lists the file systems that cannot be increased, and lists examples of those that can be increased.

> ***Note:*** Not all the file systems that can be increased are listed.

SPFS file systems

Cannot be increased	Can be increased (examples)
/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
	/PROV_data
	/user_audio_files
	/data/qca
	/data/mg9kem/logs

While file systems are being increased, writes to the file system are blocked, and the system activity increases. The greater the size increase of a file system, the greater the impact on performance.

Prerequisites

It is recommended that you back up your file systems and oracle data (if applicable) prior to performing this procedure. Refer to procedure Performing a backup of file systems on a Carrier VoIP SPFS-based server on page 2 if required.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Determine the amount of disk utilization by the file systems as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View

  2 - Configuration

  3 - Other


 X - exit

select -
```

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

Example response

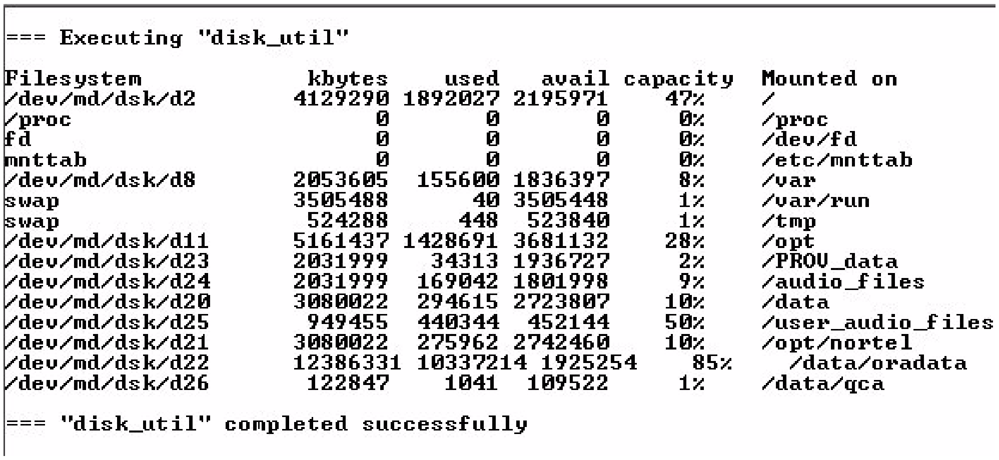
```
View
  1 - sspfs_soft (Display Software
      Installation Level Of SSPFS)
  2 - chk_sspfs (Check SSPFS Processes)
  3 - sw_conf (The software configuration of
      the znc0s0jx)
  4 - cpu_util (Overall CPU utilization)
  5 - cpu_util_proc (CPU utilization by
      process)
  6 - port_util (I/O port utilization)
  7 - disk_util (Filesystem utilization)

  X - exit

select -
```

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

Example response



```
=== Executing "disk_util"

Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2       4129290 1892027 2195971    47%    /
/proc                      0       0       0     0%    /proc
fd                         0       0       0     0%    /dev/fd
mnttab                     0       0       0     0%    /etc/mnttab
/dev/md/dsk/d8       2053605  155600 1836397     8%    /var
swap                 3505488      40 3505448     1%    /var/run
swap                  524288     448  523840     1%    /tmp
/dev/md/dsk/d11      5161437 1428691 3681132    28%    /opt
/dev/md/dsk/d23      2031999   34313 1936727     2%    /PROV_data
/dev/md/dsk/d24      2031999  169042 1801998     9%    /audio_files
/dev/md/dsk/d20      3080022  294615 2723807    10%    /data
/dev/md/dsk/d25       949455  440344  452144    50%    /user_audio_files
/dev/md/dsk/d21      3080022  275962 2742460    10%    /opt/nortel
/dev/md/dsk/d22      12386331 10337214 1925254    85%    /data/oradata
/dev/md/dsk/d26       122847    1041  109522     1%    /data/qca

=== "disk_util" completed successfully
```

The “capacity” column indicates the percentage of disk utilization by the file system, which is specified in the “Mounted on” column.

6 Note the file system you want to increase, as well as its current size (under column “Kbytes”).

7 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

8

ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 6).

For example, to determine the size by which to increase the “qca” file system, subtract its current size, 122847k from the desired size, for example, 256000k. You would increase the size of the “qca” file system by 133153k, or 133MB.

9 Determine the amount of free disk space that can be allocated to file systems as follows:

a Determine the amount of free disk space on your system by typing

```
# echo `/opt/nortel/sspfs/fs/meta.pl fs` 2048
/ 5000 - p | dc
```

and pressing the Enter key.

> ***Note:*** Use the back quote on the same key as the Tilda (~) for */opt/nortel/sspfs/fs/meta.pl fs.*

The resulting number is the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

If the value is	Do
less than zero (0)	contact Nortel Networks for assistance
more than zero (0)	step b

b Use the following table to determine your next step.

If	Do
the value you determined in step 8 (size by which to increase the file system) is greater than the value you obtained in step 9a (amount of free disk space you can allocate to file systems)	contact Nortel Networks for assistance
the value you determined in step 8 (size by which to increase the file system) is less than the value you obtained in step 9a (amount of free disk space you can allocate to file systems)	step 10

10

ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

Increase the size of the file system by typing

```
#  filesys grow -m <mount_point> -s <size>m
```

Where

mount_point
is the name of the file system you want to increase (noted in step 6)

size
is the size in megabytes (m) by which you want to increase the file system (determined in step 8)

Example

```
# filesys grow -m /data -s 512m
```

Note: The example above increases the “/data” file system by 512 megabytes (MB).

You have completed this procedure.

High-availability configuration (two servers)

ATTENTION
During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

At your workstation

1 For all users except those using Core and Billing Manager (CBM), start a login session using telnet. For CBM, start a login session connecting to the inactive node using ssh.

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 6

2 Log in to the Inactive node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the Inactive node in the cluster

Note: If you use the cluster IP address, you will log in to the Active node. Therefore, ensure you use the physical IP address of the Inactive node to log in.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

Note: Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

6 Log in using ssh (secure) as follows:

a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the inactive server

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter `yes` at the prompt.

b When prompted, enter the root password.

At the Inactive node

7 Verify the cluster indicator to ensure you are logged in to the Inactive node, by typing

```
# ubmstat
```

and pressing the Enter key.

If the system response is	Do
ClusterIndicatorSTBY	step 8
ClusterIndicatorACT	step 2

8 Verify the status of file systems on this server by typing

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step 9
not STANDBY normal UP clean	contact your next level of support

9 Determine the amount of disk utilization by the file systems as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View

  2 - Configuration

  3 - Other


 X - exit

select -
```

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

Example response

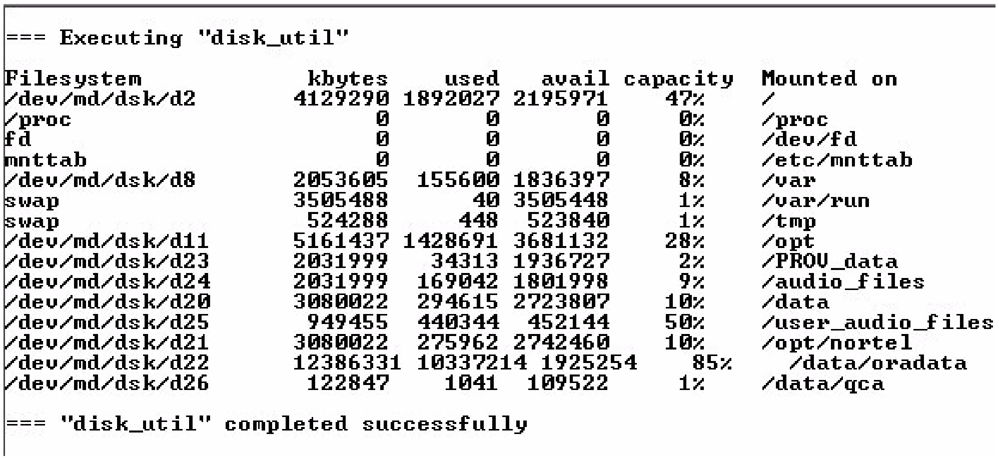
```
View
  1 - sspfs_soft (Display Software
      Installation Level Of SSPFS)
  2 - chk_sspfs (Check SSPFS Processes)
  3 - sw_conf (The software configuration of
      the znc0s0jx)
  4 - cpu_util (Overall CPU utilization)
  5 - cpu_util_proc (CPU utilization by
      process)
  6 - port_util (I/O port utilization)
  7 - disk_util (Filesystem utilization)

  X - exit

select -
```

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

Example response



```
=== Executing "disk_util"

Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2       4129290 1892027 2195971    47%    /
/proc                      0       0       0     0%    /proc
fd                         0       0       0     0%    /dev/fd
mnttab                     0       0       0     0%    /etc/mnttab
/dev/md/dsk/d8       2053605  155600 1836397     8%    /var
swap                 3505488      40 3505448     1%    /var/run
swap                  524288     448  523840     1%    /tmp
/dev/md/dsk/d11      5161437 1428691 3681132    28%    /opt
/dev/md/dsk/d23      2031999   34313 1936727     2%    /PROV_data
/dev/md/dsk/d24      2031999  169042 1801998     9%    /audio_files
/dev/md/dsk/d20      3080022  294615 2723807    10%    /data
/dev/md/dsk/d25       949455  440344  452144    50%    /user_audio_files
/dev/md/dsk/d21      3080022  275962 2742460    10%    /opt/nortel
/dev/md/dsk/d22      12386331 10337214 1925254    85%      /data/oradata
/dev/md/dsk/d26       122847    1041  109522     1%    /data/qca

=== "disk_util" completed successfully
```

The *capacity* column indicates the percentage of disk utilization by the file system, which is specified in the *Mounted on* column.

10 Note the file system you want to increase, as well as its current size (under column *Kbytes*).

11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

12

ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 10).

For example, to determine the size by which to increase the “qca” file system, subtract its current size, 122847k from the desired size, for example, 256000k. You would increase the size of the “qca” file system by 133153k, or 133MB.

13 Determine the amount of free disk space that can be allocated to file systems as follows:

a Determine the amount of free disk space on your system by typing

```
# echo `/opt/nortel/sspfs/fs/meta.pl fs` 2048
/ 5000 - p | dc
```

and pressing the Enter key.

Note: Use the back quote on the same key as the Tilda (~) for */opt/nortel/sspfs/fs/meta.pl fs.*

The resulting number is the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

If the value is	Do
less than zero (0)	contact Nortel Networks for assistance
more than zero (0)	step b

b Use the following table to determine your next step.

If	Do
the value you determined in step 12 (size by which to increase the file system) is greater than the value you obtained in step 13a (amount of free disk space you can allocate to file systems)	contact Nortel Networks for assistance
the value you determined in step 12 (size by which to increase the file system) is less than the value you obtained in step 13a (amount of free disk space you can allocate to file systems)	step 14

14

ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

Increase the size of the desired file system by typing

```
#  GrowClusteredFileSystem.ksh <mount_point>
<size>m
```

Where

mount_point
is the name of the file system you want to increase (noted in step 10)

size
is the size in megabytes (m) by which you want to increase the file system (determined in step 12)

Example

```
# GrowClusteredFileSystem.ksh /data/qca 10m
```

Note: The example above increases the “/data/qca” file system by 10 megabytes (MB).

15 Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

16 Wait for the Inactive node to reboot, then log in again using its physical IP address.

17 Verify the status of file systems on the Inactive node by typing

```
# udstat
```

and pressing the Enter key.

If the file systems are	Do
STANBY normal UP clean	step 18
not STANBY normal UP clean	contact your next level of support

18 Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the active node in the cluster

19 When prompted, enter your user ID and password.

20 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

21 When prompted, enter the root password.

Note: Ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display

ClusterIndicatorACT, which indicates you are on the Active server.

At the Active node

22 Stop the cluster by typing

```
# StopCluster
```

and press the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

At the newly Active node

23 Clone the other node using procedure Cloning the image of one server in a cluster to the other server on page 24 if required.

You have completed this procedure.

Cloning the image of one server in a cluster to the other server

Application

Use this procedure to clone the image of the active server in a cluster to the inactive server.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the inactive server under the following circumstances
  - — this is the first time you clone
  - — you replaced the inactive server
  - — you executed a reverse restore (that is, you switched unit 0 and 1)

  Note: Under any of the above circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.

ATTENTION
Ensure that no provisioning activities are in progress, or are scheduled to take place during this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Establish a login session to the active server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 7

2 Log in to the active server using telnet (unsecure) by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the cluster IP address, which automatically defaults to the active server in the cluster

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Proceed to step 9.

7 Log in to the active server using ssh (secure) by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server
is the cluster IP address, which automatically defaults to the active server in the cluster

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

8 When prompted, enter the root password.

On the active server

9 Verify the status of replicated disk volumes on the active server by typing

```
# udstat
```

and pressing the Enter key.

If	Do
all the file systems are ACTIVE normal UP clean	step 10
otherwise	contact your next level of support

10 Determine the server profile. Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

 X - exit

select -
```

11 Enter the number next to the View option in the menu.

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SSPFS)
 2 - chk_sspfs (Check SSPFS Processes)
 3 - sw_conf (The software configuration of
     the wrtypyxp)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by
     process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)

 X - exit

select -
```

12 Enter the number next to the sspfs_soft option in the menu.

Example response

```
=== Executing "sspfs_soft"

SSPFS version: 09.0 Build: 200508421 Server
Profile: cbm850

==="sspfs_soft" completed successfully
```

13 Note the server profile.

14 Exit the CLI by typing `x` until you return to the command prompt.

15 Use the following table to determine your next step.

If	Do
the Server Profile is cbm850	step 26
otherwise	step 16

16 Verify that all applications on the server are running by typing

```
# servquery -status all
```

and pressing the Enter key.

Example response:

```
APP NAME                        STATUS
========                        ======
SNMP_POLLER                     RUNNING
DELEGATE                        RUNNING
PROP_SRV                        RUNNING
WEBSERVER                       RUNNING
DATABASE                        RUNNING
SAM21EM                         RUNNING
SESMService                     RUNNING
CORBA                           RUNNING
ORA_ARCHIVE_ROTATOR             RUNNING
OMPUSH                          RUNNING
BOOTP                           RUNNING
WEBSERVICES                     RUNNING
ORA_AUTO_BACKUP                 RUNNING
IEMS                            RUNNING
APS                             RUNNING
NPM                             RUNNING
```

17 Use the following table to determine your next step.

If	Do
all applications are running	step 20
otherwise	step 18

18 Start each application that is not running by typing

```
# servstart <app_name>
```

and pressing the Enter key.

where

app_name
is the name of the application that is not in a RUNNING state, for example, SAM21EM

19 Use the following table to determine your next step.

If	Do
all applications started	step 20
otherwise	contact your next level of support

20 Verify the Patching Server Element (PSE) server application is running by typing

```
# pse status
```

and pressing the Enter key.

If	Do
PSE is running	step 22
otherwise	step 21

21 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

If	Do
PSE starts	step 22
otherwise	contact your next level of support

22 Use the following table to determine your next step.

If	Do
this server is running the CS 2000 Management Tools software	step 23
otherwise	step 26

23 Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS
-------------------------
COMPONENT                  STATUS
---------                  ------
Proxy Agent                RUNNING
RMI Registry               RUNNING
Snmpfactory                RUNNING
MI2 Server                 RUNNING

  Current number of SESM processes running: 4 (of 4)

  SESM APPLICATION STATUS: All Applications ready
```

24 Use the following table to determine your next step.

If	Do
the SESMService is fully functional	step 26
otherwise	contact your next level of support

25 Use the following table to determine your next step.

If	Do
the SESMService is fully functional	step 26
otherwise	contact your next level of support

26 Use the following table to determine your next step.

If	Do
this is the first time you are cloning the server, or you replaced the server or executed a reverse restore (i.e. switched unit 0 and unit 1) ***Note:*** Under any of the above circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.	step 27
otherwise	step 31

27 Use the following table to determine your next step.

If	Do
you do not know the Ethernet address of the inactive server	step 28
otherwise	step 29

At the console connected to the inactive server

28 Determine the Ethernet address of the inactive server as follows:

a Log in to the inactive server through the console (port A) using the root user ID and password.

Ensure you are on the inactive server by typing ubmstat. If ClusterIndicatorACT is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other server. The response must display ClusterIndicatorSTBY, which indicates you are on the inactive server.

b Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

c At the OK prompt, display the Ethernet address of the inactive server by typing

```
OK banner
```

and pressing the Enter key.

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved. OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

d Record the Ethernet address that is displayed.

On the active server

29 Start the cloning process on the active server by typing

```
# startb <Ethernet address>
```

and press the Enter key.

where

Ethernet address
is the Ethernet address of the inactive server

30 Proceed to step 32

On the active server

31 Start the cloning process on the active server by typing

```
# startb
```

and press the Enter key.

32 Use the following table to determine your next step.

If	Do
the system prompts you to enter the command “boot net - image”	step 33
otherwise	step 37

33 Connect to the console port of the inactive server.

If the console displays the	Do
login prompt	step 34
OK prompt	step 36

At the console connected to the inactive server

34 Log in to the inactive server using the root user ID and password.

35 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

36 At the OK prompt, boot the inactive server from the image of the active server by typing

OK **boot net - image**

and press the Enter key.

> ***Note:*** There must be a space between the “-” and “image”.

Example response

```
SC Alert: Host System has Reset
Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc.  All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

On active server

37 Monitor the progress of the cloning from the active server. Cloning the inactive server takes approximately 40 minutes to complete, but the time can vary depending on system configuration.

Example response:

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Jun 27 16:01:38 ucary0883c unix: /data: active up
repair - standby reflected (normal)
Deleted snapshot 2.
Deleted snapshot 1.
Deleted snapshot 0.
ucary0883c-unit0(active):/>
```

38 Once cloning is complete, wait approximately 5 minutes before you proceed to the next step.

On the active server

39 Verify the status of replicated disk volumes on the active server by typing

```
# udstat
```

and pressing the Enter key.

If	Do
all file systems are ACTIVE normal UP clean	step 40
otherwise	contact your next level of support

At your workstation

40 Establish a login session to the inactive server using one of the following methods:

If using	Do
telnet (unsecure)	step 41
ssh (secure)	step 46

41 Log in to the inactive server using telnet (unsecure) by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the inactive server in the cluster

42 When prompted, enter your user ID and password.

43 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

44 When prompted, enter the root password.

45 Proceed to step 48.

46 Log in to the inactive server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the inactive server in the cluster

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

47 When prompted, enter the root password.

On the inactive server

48 Verify the status of replicated disk volumes on the inactive server by typing

```
# udstat
```

and pressing the Enter key.

If	Do
all file systems are STANDBY normal UP clean	step 49
otherwise	contact your next level of support

On the active server

49 Complete the cloning process on the active server by typing

```
# finishb
```

and pressing the Enter key.

50 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

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

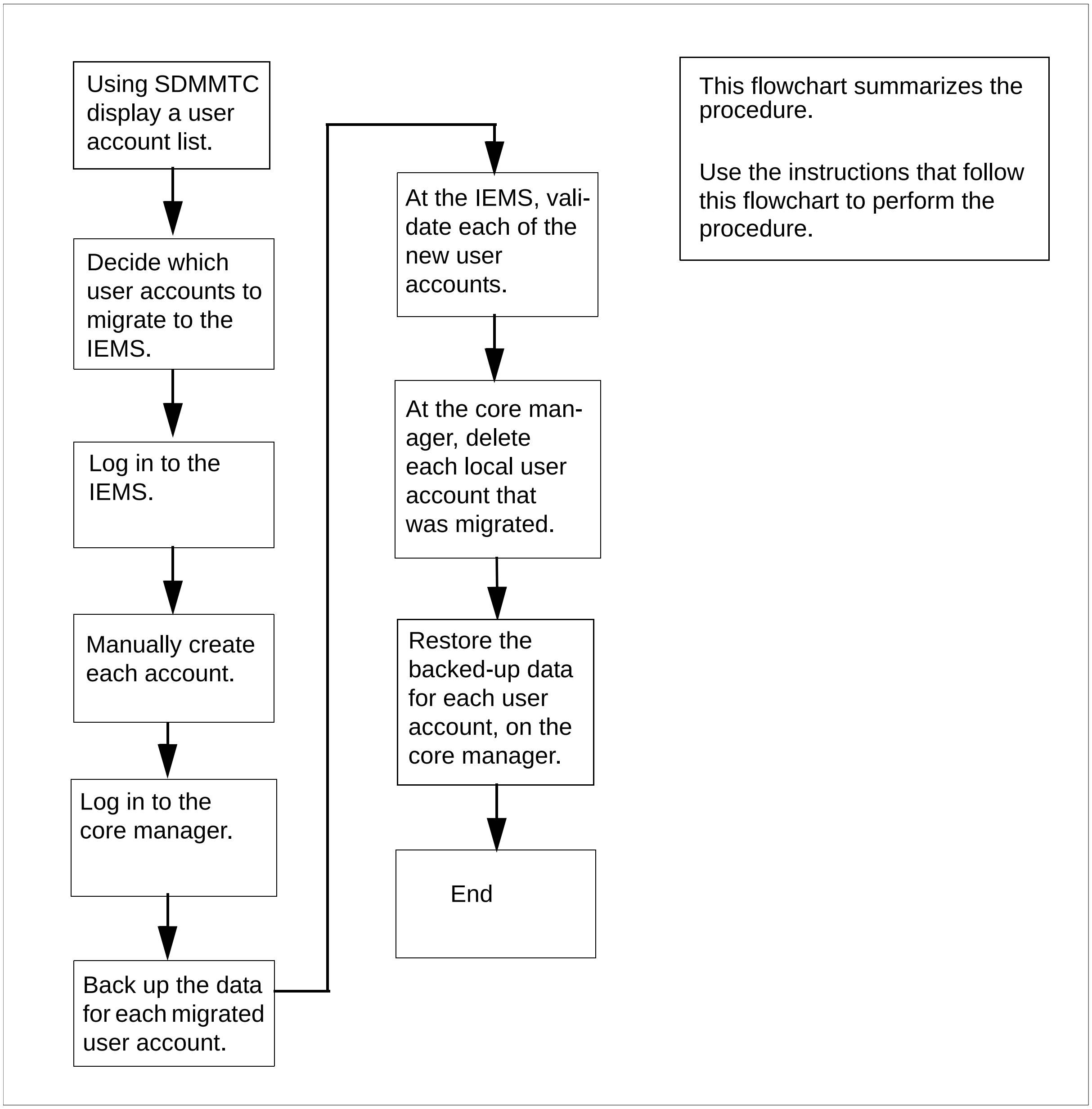
Local core manager user accounts can be migrated to the IEMS secure server either manually or through the exportLocalUser program. The manual migration method requires that you migrate each user account one-at-a-time on the IEMS. The exportLocalUser program, in contrast, enables you to migrate multiple 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 40 Migrating user accounts to the IEMS using exportLocalUser on page 42

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


Using SDMMTC display a user account list.
Decide which user accounts to migrate to the IEMS.
Log in to the IEMS.
Manually create each account.
Log in to the core manager.
Back up the data for each migrated user account.
At the IEMS, validate each of the new user accounts.
At the core manager, delete each local user account that was migrated.
Restore the backed-up data for each user account, on the core manager.
End
This flowchart summarizes the procedure.
Use the instructions that follow this flowchart to perform the procedure.

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 46

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 47

4 Remove the local user accounts on the core manager, using procedure Removing user accounts from the core manager on page 49

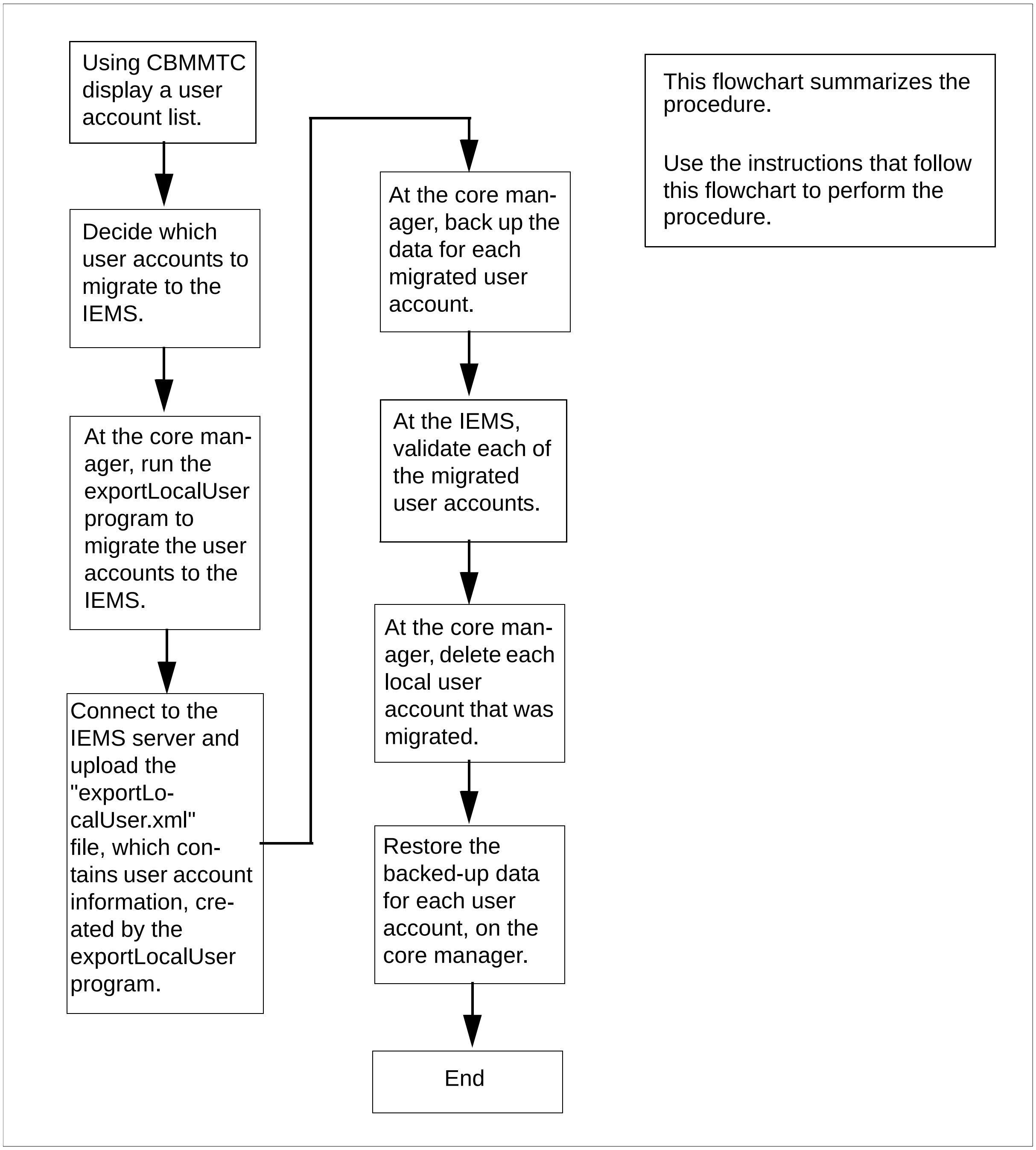
5 Restore the data you backed up in step 3 for each of the user accounts you migrated to the IEMS, using the procedure Restoring user accounts to the core manager on page 50

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


Using CBMMTC display a user account list.
Decide which user accounts to migrate to the IEMS.
At the core manager, run the exportLocalUser program to migrate the user accounts to the IEMS.
Connect to the IEMS server and upload the "exportLocalUser.xml" file, which contains user account information, created by the exportLocalUser program.
At the core manager, back up the data for each migrated user account.
At the IEMS, validate each of the migrated user accounts.
At the core manager, delete each local user account that was migrated.
Restore the backed-up data for each user account, on the core manager.
End
This flowchart summarizes the procedure.
Use the instructions that follow this flowchart to perform the procedure.

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 46

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 40

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 47

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 49

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 50

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 38.

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 38.

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

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 38.

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 38.

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.

Adding or removing a program from the maintenance class users' access

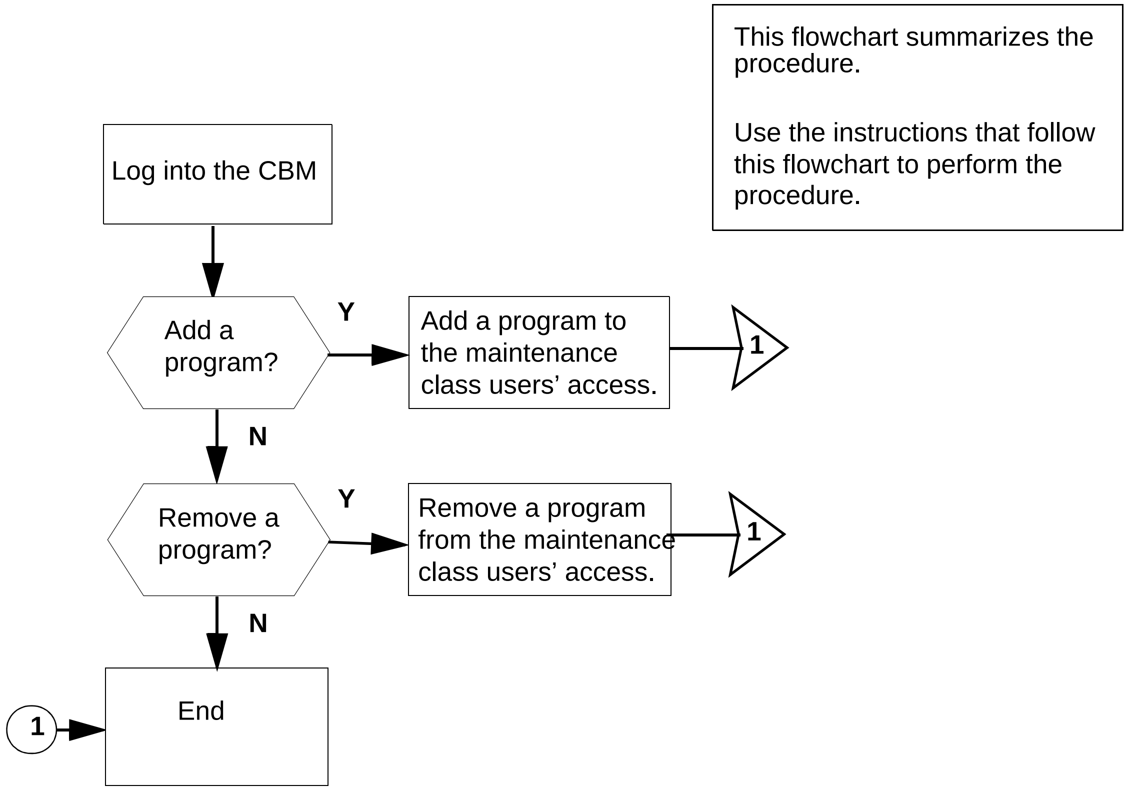
Application

Use this procedure to add or remove a program from the maintenance class users' access. This procedure must be performed by the root user.

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 task.

Summary of adding or removing a program from the maintenance class users' access


This flowchart summarizes the procedure.
Use the instructions that follow this flowchart to perform the procedure.
Log into the CBM
Add a program?
Y
Add a program to the maintenance class users' access.
1
N
Remove a program?
Y
Remove a program from the maintenance class users' access.
1
N
1
End

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 program to/from the maintenance class users' access

At the local or remote VT100 console

1 Log into the CBM as the root user

a using telnet, by typing:

```
telnet <IP address>
```

b using secure shell protocol (SSH), by typing:

```
ssh -1 root <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the CBM

2 When prompted, enter the root password.

3 Use the following table to determine your next step.

If you want to	Do
add a third party program to the maintenance class users' access	step 4
remove a third party program from the maintenance class users' access	step 5

4 Add a third party program to the maintenance class users' access by typing

```
custprog -a <program name>
```

and pressing the Enter key.

where

program name
is the location where the program is stored on the CBM

Note: The full path is required for the program name.

5 Remove a third party program from the maintenance class users' access by typing

```
custprog -d <program name>
```

and pressing the Enter key.

where

program name
is the name used in the maintenance class user's restrict shell

6 You have completed this procedure.

Connecting to the CM passthru

Application

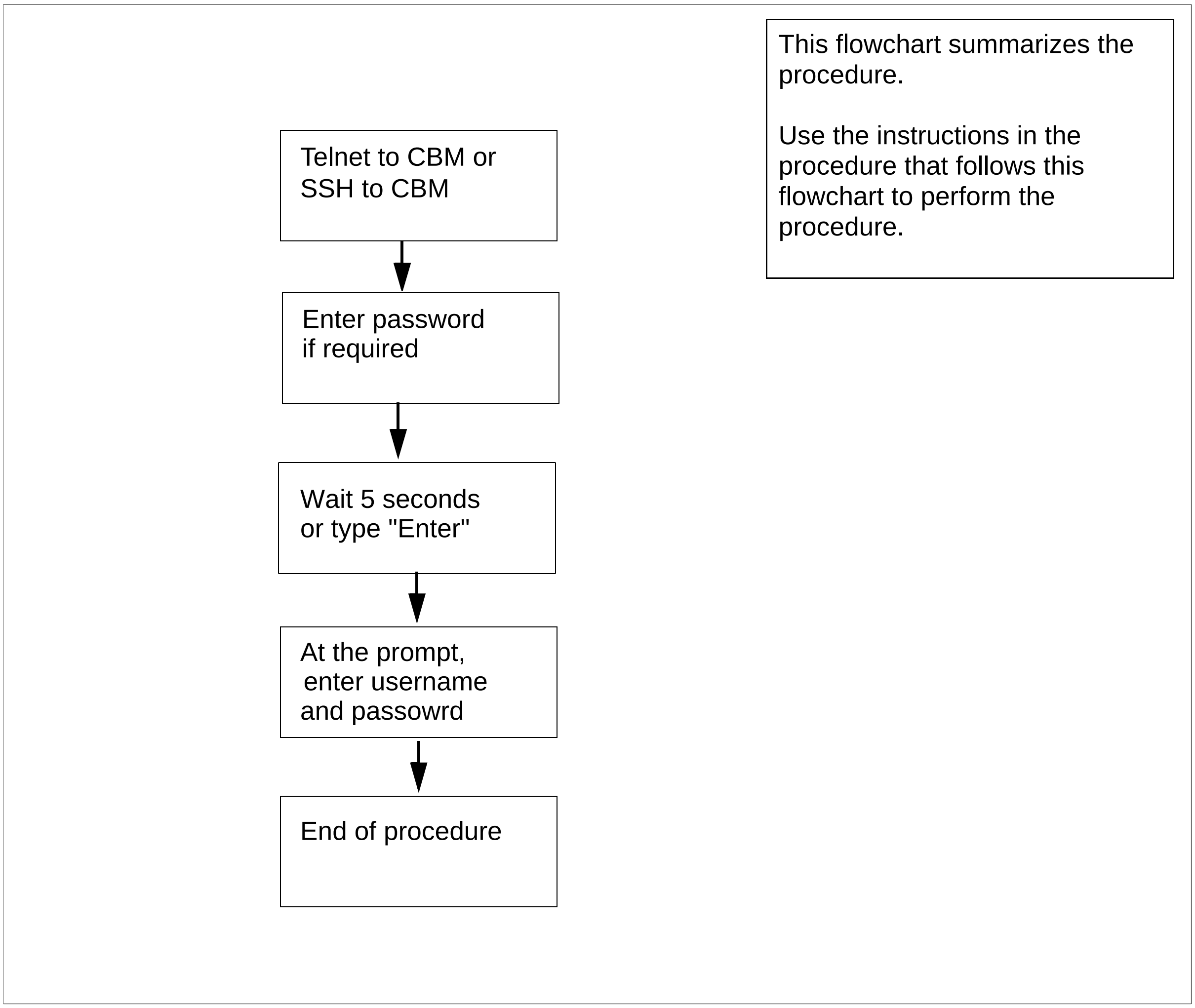
Use this procedure to access the CM through the CBM as a passthru user.

To configure a passthru user, use procedure Adding or removing a passthru user on page 63 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 connecting to the core passthru


Telnet to CBM or SSH to CBM
Enter password if required
Wait 5 seconds or type "Enter"
At the prompt, enter username and passowrd
End of procedure
This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the 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.

Connecting to the CM passthru

At the workstation

1 Log in to the CBM as a passthru user.

If you	Do
use telnet	step a
use SSH	step b

a Telnet to the CBM by typing

```
telnet <IP address>
```

and pressing the Enter key.

where

<IP address>
is the IP address of the CBM.

Continue with step 2.

b Open an SSH session by typing

```
ssh-l<passthru userID><IP address>
```

and pressing the Enter key.

where

<IP passthru userID>
is the IP address of the CBM.

2 If you are prompted for a password, enter your password.

Note: The following response is only displayed when the pasthru user is configured as "password required". Otherwise, the connection will be directly forwarded to the Core login prompt.

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.
```

3 Wait 5 seconds to continue or continue immediately by typing

`Enter`

and pressing the Enter key.

Example response:

```
Trying to complete connection. Please wait...
**********************************************

   WARNING...WARNING...WARNING...WARNING.

 ......In LINEMODE, To Enter into BREAK.....
  Press ^B, Type the Command and Press <Enter>
   Example:  ^Bhx <Enter>

**********************************************
Telnet LINEMODE.
Enter username and password
MIB variable CharOptionAllowed must be set first
to allow CHAR MODE.
>
```

4 At the prompt, enter the username and password for core login.

5 You have completed this procedure.

Adding or removing a maintenance user

Purpose

Use this procedure to add or remove a maintenance class user.

Application

Only the root user can add or remove a maintenance class user.

> **ATTENTION**
> For the *current release*, there is *no limit* to the number of telnet sessions allowed for maintenance and passthru users.

Prerequisites

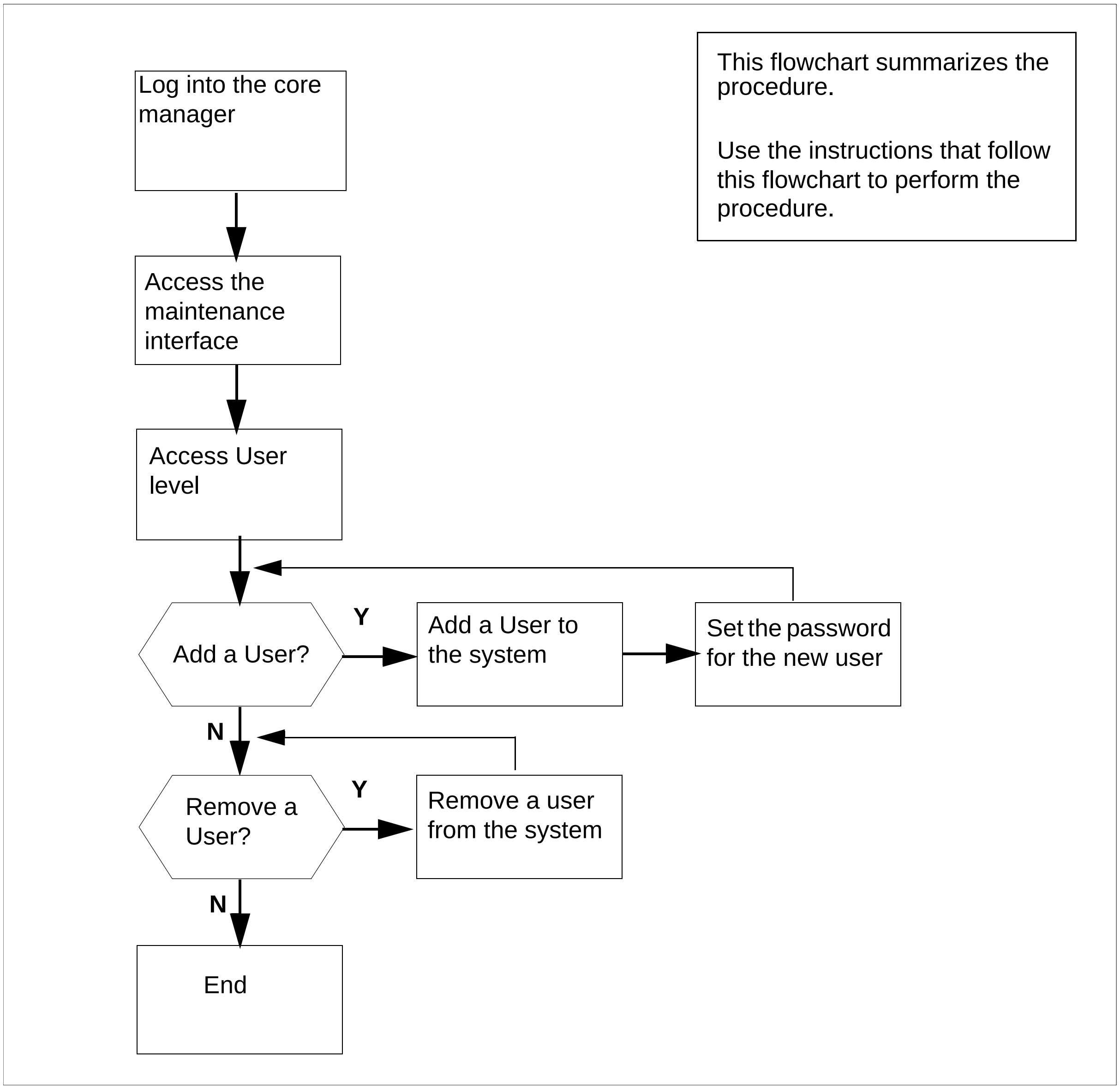
You must have the root user ID and password to log into the server.

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 step-action procedure that follows the flowchart to perform the task.

Summary of Adding or removing a maintenance user


Log into the core manager
Access the maintenance interface
Access User level
Add a User?
Y
Add a User to the system
Set the password for the new user
N
Remove a User?
Y
Remove a user from the system
N
End
This flowchart summarizes the procedure.
Use the instructions that follow this flowchart to perform the procedure.

Adding or removing a maintenance user

At the local or remote VT100 console

1 Log into the core manager.

2 Access the maintenance interface:

```
cbmmtc
```

3 Access the User level:

```
user
```

Example response:

```
 CBM  MATE  NET  APPL  SYS  HW  CLLI: CTAT1
  .    -     .     .   Host: TAK2_svr
                          Active
User
 0 Quit
 2           Maintenance users
 3 PassThru  anonymous
 4           certuser
 5           image
 6           maint
 7           mgems
 8           npm
 9           npmftp
10            patcher
11            pfrs
12 Up           poller
13 Down           ptm
14           sam21cm
15               Maintenance Users 1 to 12 of 13
16
17 Help
18 Refresh
  root
Time  12:54  >
```

If you want to	Do
add a user	step 4
remove a user	step 9

4 Add a maintenance class user:

add <*userID*>

where

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

Note: To activate a user, you need to set the password. Use the change command to set the password.

5 Set password for the user:

change <*userID*>

where

<userID> **is the userID of the user for whom you are setting the password**

Note: If no userID is specified, the system changes the password of the root user.

6 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.

7 Enter the password again.

8 Press Enter again to continue.

If you	Do
want to add another user	step 4
do not want to add another user	step 11

9 Remove a user:

```
delete <userID>
```

where

<userID>
is the userID of the new user

Are you sure you want to delete this user?

Do you wish to proceed?

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

10 Confirm that you want to delete the user:

y

If you	Do
want to delete another user	step 9
do not want to delete another user	step 11

11 Exit the maintenance interface:

```
quit all
```

12 You have completed this procedure.

Adding or removing a passthru user

Application

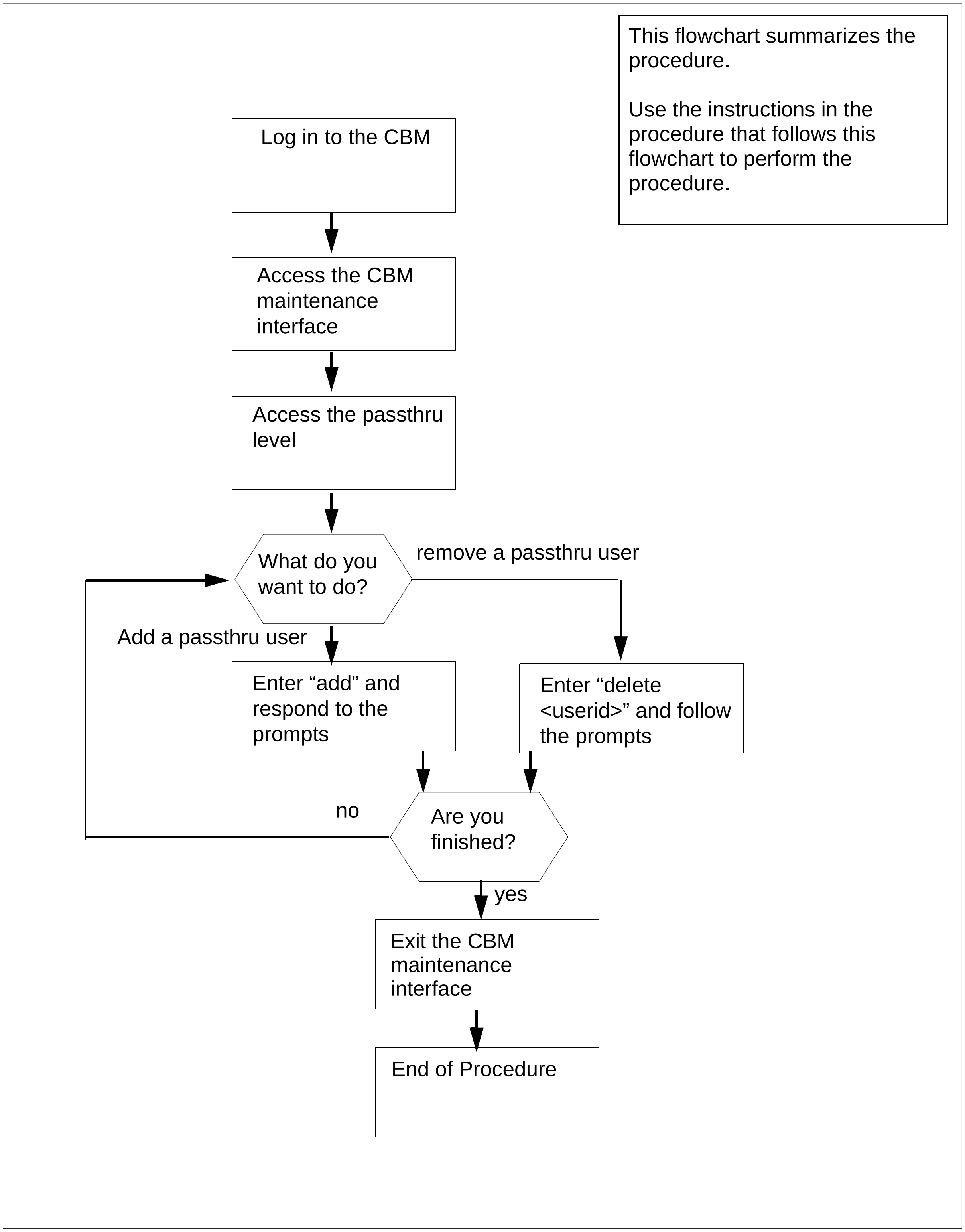
Use this procedure to add or remove a passthru user.

You must have root user privileges 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 adding or removing a passthru user


This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the procedure.
Log in to the CBM
Access the CBM maintenance interface
Access the passthru level
What do you want to do?
remove a passthru user
Add a passthru user
Enter “add” and respond to the prompts
Enter “delete <userid>” and follow the prompts
no
Are you finished?
yes
Exit the CBM maintenance interface
End of 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.

Adding or removing a passthru user

At the CBM

1 Log in to the CBM as root user.

2 Access the CBM maintenance interface by typing

`cbmmtc`

and pressing the Enter key.

3 Access the passthru level by typing

`passthru`

and pressing the Enter key.

Example response:

```
 CBM  MATE  NET  APPL  SYS  HW  CLLI: CTAT1
  .    -     .     .Host: TAK2_svr
                       Active
PassThru
 0 Quit
 2    UserName RealName  Passthru Action FTP CM
 3    tester1 TEST     telnet cm       Yes
 4                   PassThru Users: 1 to 1 of 1
 5
 6
 7
 8
 9
10
11
12 Up
13 Down
14
15
16
17 Help
18 Refresh  Add - Command complete
  root
Time  12:58  >
```

4 Use the following table to determine your next step.

If you want to	Do
add a passthru user	step 5
delete a passthru user	step 16

5 Add a passthru user by typing

`add`

and pressing the Enter key.

6 When prompted, type the user name for the new user and press the Enter key.

> ***Note:*** The user name must not be more than 8 characters. The user name can include lowercase letters, numbers, or the ‘.’ , ‘_’, or ‘-’ characters.

7 When prompted, type the real name for the passthru user and press the Enter key.

8 When prompted, type the Telnet command arguments for the passthru user, and press the Enter key.

> ***Note:*** Type “cm” for the Core passthru.

9 When prompted, indicate whether a password is required, and press the Enter key.

Response:

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

10 Confirm the data you entered by typing Y or N and pressing the Enter key.

If you indicated a password	Do
is required	step 11
is not required	step 15

11 When prompted to set the initial password, press the Enter key.

12 When prompted, type the new password for the user and press the Enter key.

13 When prompted, re-type the password and press the Enter key.

14 When prompted, press the Enter key to continue.

The system returns you to the passthru level.

15 Use the following table to determine your next step.

If you	Do
want to add another user	step 5
do not want to add another user	you have completed this procedure

16 Delete a passthru user by typing

`delete <userid>`

and pressing the Enter key.

where

<userid>
is the userID of the user you are deleting

Example response:

```
9
10             Delete PassThru User
11             PassThru user to be deleted:
12 Up
13 Down           Username: coreusr1
14                Name: core user1
15                Action: telnet core
16
17 Help        Do you wish to proceed?
18 Refresh    Please confirm ("YES","Y",or"N",)
root
Time  00:40  >
```

17 When prompted, confirm you want to delete the user by typing

`Y`

and pressing the Enter key.

18 Use the following table to determine your next step.

If you	Do
want to delete another user	step 16
do not want to delete another user	step 19

19 Exit the CBM maintenance interface by typing

`quit all`

and pressing the Enter key.

20 You have completed this procedure.

Setting up local user accounts on a Carrier VoIP SPFS-based server

Application

Use this procedure to add local user accounts on a Carrier Voice over IP (VoIP) Server Platform Foundation Software (SPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see Additional information on page 71.

If you choose to centrally manage your user accounts, refer to procedure “Adding new users” in the Integrated EMS Security and Administration document, NN10336-611.

> ***Note:*** All user account management activities, such as setting up users, removing users, and changing passwords, are performed on the Active server and then propagated from the Active to the Inactive server.

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSFPS-based server

Note: In a two-server configuration, log in to the Active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group *succssn* by typing

```
# useradd -g succssn <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd -r files <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table Secondary user groups on page 71) and any other user groups you noted in step 12 to which the user already belonged

Include a comma between groups, but no space.

userid
is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

Note: The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

You have completed this procedure.

Additional information

Users of the Nortel Networks OAM&P client applications must belong to the primary user group *succssn* for login access. Users must also belong to one or more secondary user groups listed in the table below, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm
trkrw	lnrw	mgcrw	mgrw	emsrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
trkro	lnro	mgcro	mgro	emsro

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the following table:

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operation

A user group operation dictates the operations a user can perform using the Nortel Networks OAM&P client applications. The user group operations are listed in the following table:

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.

Operation	User role mapping
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

- Node provisioning operations on page 74
- Audit operations on page 75
- Carrier provisioning operations on page 76
- Alarm operations on page 76
- Internet transparency operations on page 76
- Trunk provisioning operations on page 77
- Trunk maintenance operations on page 77
- ADSL provisioning operations on page 78
- Line provisioning operations on page 78
- Line maintenance operations on page 78
- V5.2 provisioning operations on page 79
- Patching operations on page 80
- Automated upgrade operations on page 81

Node provisioning operations (Sheet 1 of 2)

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			

Node provisioning operations (Sheet 2 of 2)

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x

Trunk provisioning operations

	User group				
Command	**trkadm**	**trkrw**	**trkmtc**	**trksprov**	**trkro**
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

	User group				
Command	**trkadm**	**trkrw**	**trkmtc**	**trksprov**	**trkro**
Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Validate line using DN CLLI					x
Validate line using TID CLLI					x

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Get line post info					x
Busy line			x		
Return line to service			x		
Force release line			x		
Installation busy line			x		
Cancel deload			x		
Get CM CLLI					x
Get endpoint state					x
GetGwlp					x
run all TL1 line test commands			x		

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5Ring)					x					x

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, modify, delete ringing cadence mapping (V5Ring)		x					x			
View signalling characteristic profile, update list (V5Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

	User group									
Command	emsadm	emsrw	emsmtc	emssprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Access and run the GWC uprade CLUI			x					x		
Access and run the SC uprade CLUI			x					x		

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 core user using FTPProxy on page 102 in this document.

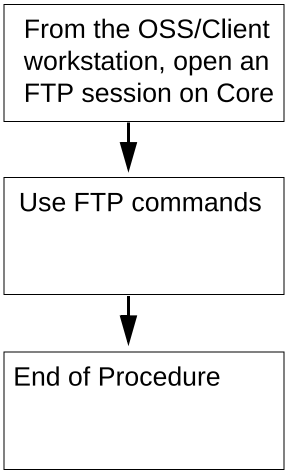
Action

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

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.


From the OSS/Client workstation, open an FTP session on Core
Use FTP commands
End of 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.

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.

Configuring a Carrier VoIP SPFS-based central security client

Application

Use this procedure to configure a Carrier Voice over IP (VoIP) SPFS-based central security client to use the Integrated Element Management System (IEMS) central security server.

> **ATTENTION**
> You can revert to the previous configuration of the client server using procedure Reverting the client server to its previous configuration on page 94.

In the event you want to reconfigure the central security client to use a new IEMS server IP, perform steps 2 and 3 of this procedure.

Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the IEMS central security server is already configured and activated in the network (see *NN10402-600 ATM/IP Solution-level Security and Administration* if required)
- perform this procedure on each Carrier VoIP SPFS-based server that is not the IEMS central security server to activate centralized security

Action

Perform the following steps to complete this procedure.

At your workstation

1 Migrate the user accounts you want to centrally manage, from the local security database on the Carrier VoIP SPFS-based client to the central administration system as follows:

> ***Note 1:*** It is recommended to migrate all user accounts that exist on Carrier VoIP SPFS-based servers to the central administration system with the following exceptions:
>
> root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, and oracle.
>
> ***Note 2:*** If the central security administration application is a third-party application and not the IEMS, follow the procedures in the third party documentation.

a If the central administration system is the IEMS, launch the Security Administration tool of the IEMS, and add the user accounts plus any additional required user groups you want to centrally manage. If required, refer to “Adding new users”, “Adding new groups”, and “Assigning a user to a group” in *Integrated EMS Security and Administration*, NN10336-611.

> ***Note:*** All users added through the IEMS Security Administration tool, are by default assigned to the *succssn* user group for login access.

b Delete the user accounts you just added to the IEMS central security server.

Log in to the client server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Carrier VoIP SPFS-based client server

c When prompted, enter the user ID and password for an account that was migrated to the IEMS central security server.

d Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

e When prompted, enter the root password.

f Delete the user account by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

Repeat this step for each user account you migrated to the IEMS central security server.

2 Configure the IEMS security server address as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

select -
```

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

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

c Enter the number next to the “Security Services Configuration” option in the menu.

Example response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

d Enter the number next to the “IEMS Server Location Configuration” option in the menu.

Example response

```
IEMS Server Location Configuration
 1 - iems_ip (Configure IEMS Server IP)

 x - exit

select -
```

e Enter the number next to the “iems_ip” option in the menu.

Example response

```
===Executing “iems_ip”

Enter the IEMS Server IP Address (default
45.12.23.56):
```

f When prompted, enter the virtual IP address of the IEMS server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter IEMS Fully Qualified Domain Name
(default :test3iems.us.nortel.com):
```

g When prompted, enter the Fully Qualified Domain Name (FQDN) of the IEMS server, or press the Enter key to accept the default value if one is specified.

Example response

```
IEMS IP: 45.12.23.56
IEMS Fully Qualified Domain
Name:test3iems.us.nortel.com

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

h Accept the IP address and FQDN you just entered by typing

`ok`

and pressing the Enter key.

Example response

```
=== “iems_ip” completed successfully
```

i Return to the Security Services Configuration menu, by typing

`select -` **`x`**

and pressing the Enter key.

Response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

3 Configure PAM and NNSwitch SPI configuration as follows:

a Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

 x - exit

select -
```

b Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)
 3 - saml_passwd_conf (Configure saml
     password)

 x - exit

select -
```

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

Example response

```
===Executing “pam_radius”

Activating pam radius components

IEMS Security Server IP: 45.12.23.56
IEMS Fully Qualified Domain Name:
test3iems.us.nortel.com
Enter the Shared Secret (default:
nortelnetworks):
```

d When prompted, enter the shared secret, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter Radius Client Timeout (default: 12):
```

e When prompted, enter the Radius Client timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Server Protocol (default: https):
```

f When prompted, enter the SAML server protocol (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Server Port (default: 58081):
```

g When prompted, enter the SAML server port (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Connection Timeout (default: 20):
```

h When prompted, enter the SAML connection timeout (used to establish SAML connections with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response

```
Enter SAML Request Timeout (default: 10):
```

i When prompted, enter the SAML request timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

Example response with default values

```
** Confirm Settings **

IEMS Security Server IP: 45.12.23.56
IEMS Server Domain Name:
test3iems.us.nortel.com
Shared Secret: nortelnetworks
Radius Client Timeout: 12
SAML server Protocol: https
SAML server Port: 58081
SAML Connection Timeout: 20
SAML Request Timeout: 10
Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

j Accept the PAM configuration update by typing

`ok`

and pressing the Enter key.

Example response

```
Configuring pam_radius

configuring nsssaml

Updating PAM Configuration to use IEMS
Security Server

Restarting name service daemon

===”pam_radius” completed successfully
```

k Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

l If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

4 To configure a saml password, from the menu prompt in step 3b above:

a enter the number next to the “saml_passwd_conf (Configure saml password)” option

b when prompted, enter the default SAML password (slisamadmin) or a new password you have chosen:

Example response

```
** Confirm Settings **

SAML Password: slisamadmin
Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
ok
Configure Password Successful
=== “saml_passwd_conf” completed
successfully
```

5 Set up platform User Environment. Before enabling access to a Carrier VoIP SPFS platform, and administrator must set up the user’s environment on the platform. Refer to information on setting up platform access for central account users, *NN10402-600 ATM/IP Solution-level Security and Adminstration* for details on setting up user environment.

6 Set up platform access for central account users. A user's home directory and shell profiles must be set up before a central account user can gain platform access. Refer to information on setting up platform access for central account users, *NN10402-600 ATM/IP Solution-level Security and Adminstration.*

You have completed this procedure.

Reverting the client server to its previous configuration

Application

Use this procedure if you configured a Carrier VoIP SPFS-based central security client to use the Integrated Element Management System (EMS) central security server, but want to revert to its previous configuration, which is not to use the Integrated EMS central security server.

Prerequisites

To perform this procedure, you need to have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Carrier VoIP SPFS-based server on which you want to revert the configuration

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Configure PAM as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

select -
```

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

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

c Enter the number next to the “Security Services Configuration” option in the menu.

Example response

```
Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 x - exit

select -
```

d Enter the number next to the “PAM Configuration” option in the menu.

Example response

```
PAM Configuration
 1 - Central Security Client Configuration

 x - exit

select -
```

e Enter the number next to the “Central Security Client Configuration” option in the menu.

Example response

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

 x - exit

select -
```

f Enter the number next to the “pam_orig” option in the menu.

Example response

```
===Executing “pam_orig”

Switching to original PAM configuration

Enter “ok” to continue
Enter anything else to exit
```

g Accept to switch to the original PAM configuration by typing

```
ok
```

and pressing the Enter key.

Example response

```
Stopping pam_radius

Deconfiguring pam_radius

===”pam_orig” completed successfully
```

h Exit each menu level of the command line interface to eventually exit the command line interface , by typing

```
select - x
```

and pressing the Enter key.

6 Re-provision the user accounts in Unix. In a two-server configuration, reprovision the user accounts on the active server. If required, refer to procedure Setting up local user accounts on a Carrier VoIP SPFS-based server on page 69.

You have completed this procedure.

Configuring IPSec and IKE on the CBM 850

Application

Use this procedure to configure IP Security (IPSec) and Internet Key Exchange (IKE) on a CBM 850 for secure communication with an OSS. Included are steps both to add IPSec/IKE to the CBM 850 and to remove IPSec/IKE from the CBM 850.

> ***Note:*** For a procedure used to configure IPSec and IKE on the OSS (Solaris 5.9 machine), see Configuring IPSec and IKE on the OSS on page 186

Prerequisites

IPSec and IKE configuration parameters that are provisioned on the CBM 850 must match the corresponding parameters configured on the OSS.

For each of the procedures below, you should NOT log in to the CBM 850 from the OSS. All telnet sessions between the CBM 850 and OSS should be closed down before the procedures below are performed.

> ***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.

Procedures

Use the following table to determine the procedure to perform.

Procedure to perform
Configuring IPSec on the CBM 850 on page 100
Removing IPSec from the CBM 850 on page 101

Configuring IPSec on the CBM 850

At the CBM 850

1 Deactivate (turn OFF) any outbound file transfer schedules (such as those for OMDD, SBA, or Logdelivery) which are already active between the CBM 850 and the OSS. For procedures to use, refer to the appropriate document in the CBM 850 OUFCAPS suite.

2 Configure an IPSec rule with the appropriate values, using the procedure Configuring IPSec and IKE on a Carrier VoIP SPFS-based server on page 170

> ***Note:*** If the IPSec rule being configured applies to the entire system, port entries for the rule should be specified as “all”. If the IPSec rule is being configured for connection on a specific port, that port number must be specified.

3 Configure the IKE rule corresponding to the IPSec rule you created in step 2, using the procedure Configuring IPSec and IKE on a Carrier VoIP SPFS-based server on page 170

4 Configure the OSS for the IPSec and IKE rules you have just created, using the procedure Configuring IPSec and IKE on the OSS on page 186

5 Reactivate the outbound file transfer schedules that you deactivated in step 1.

6 You have completed this procedure.

Removing IPSec from the CBM 850

At the CBM 850

1. Deactivate (turn OFF) any outbound file transfer schedules (such as those for OMDD, SBA, or Logdelivery) which are already active between the CBM 850 and the OSS. For procedures to use, refer to the appropriate document in the CBM 850 OUFCAPS suite.
2. Delete the appropriate IPSec rule, using the procedure Configuring IPSec and IKE on a Carrier VoIP SPFS-based server on page 170
3. Delete the IKE rule corresponding to the IPSec rule that you deleted in step 2, using the procedure Configuring IPSec and IKE on a Carrier VoIP SPFS-based server on page 170
4. Remove the IPSec and IKE rules that you have just deleted, from the OSS by performing Configuring IPSec and IKE on the OSS on page 186
5. Reactivate the outbound file transfer schedules that you deactivated in step 1.
6. You have completed this procedure.

Transferring files as a core user using FTPProxy

Application

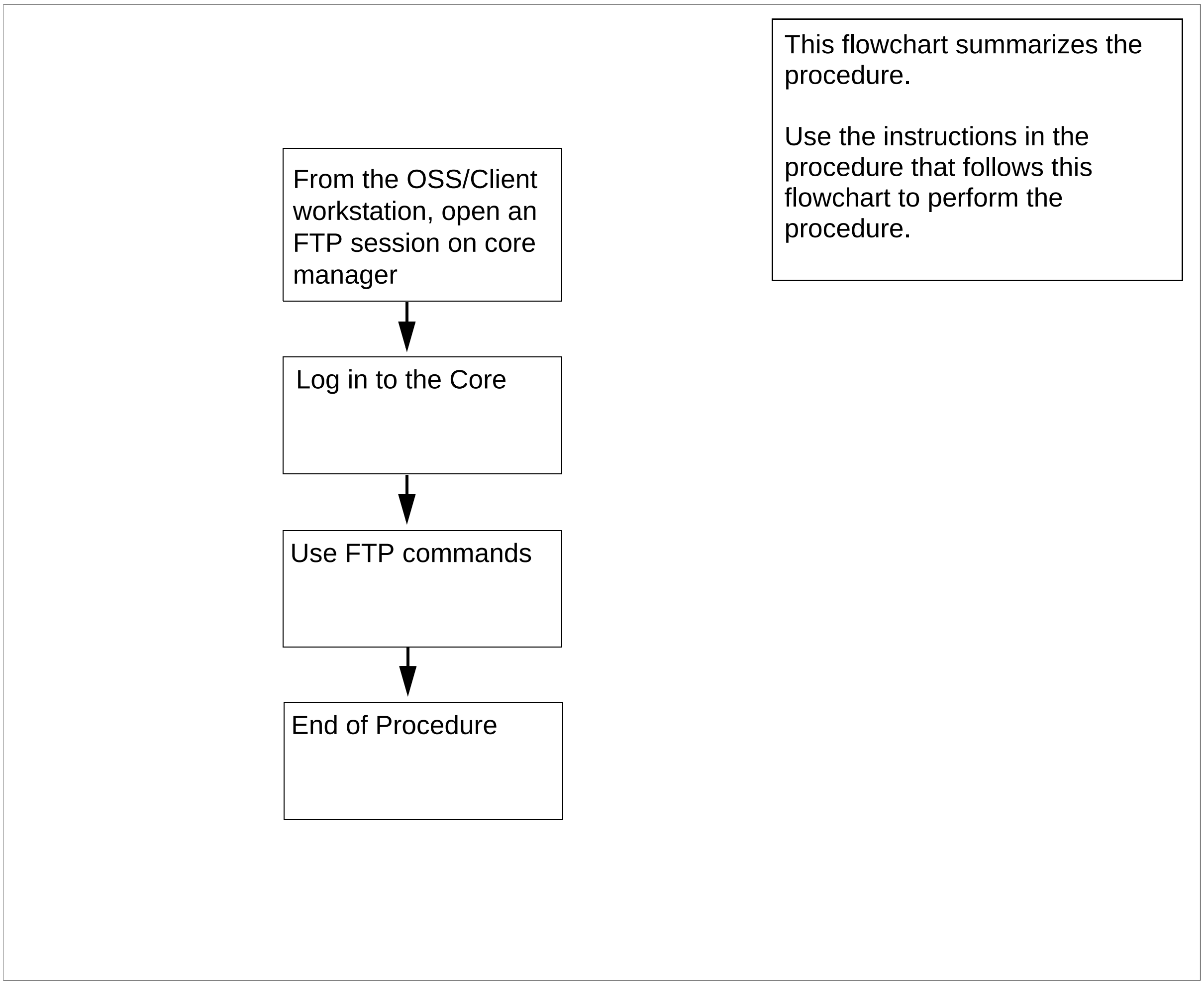
Use this procedure to transfer files between the OSS machine and the Core using the FTPProxy application. Use this procedure if you have core user privileges. Core user privileges include mgcadm, mgcrw, mgcsprov, mgcmtce,and mgcro.

If you have passthru user privileges, refer to Transferring files as a passthru user using FTPProxy on page 82 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


This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

From the OSS/Client workstation, open an FTP session on core manager
Log in to the Core
Use FTP commands
End of 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.

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 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.

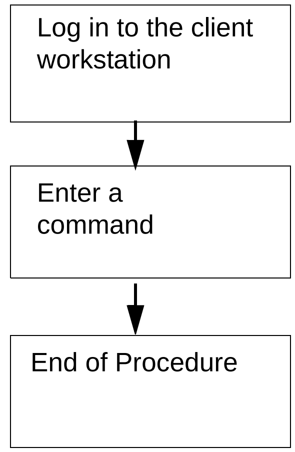
Nortel recommends that all component level security management connections to the core be made using SCFT.

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



This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

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 118
- Listing volumes on Core using SCFT on page 123
- Removing a file from Core using SCFT on page 115
- Transferring files from Core using SCFT on page 107
- Transferring files to Core using SCFT on page 111

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.

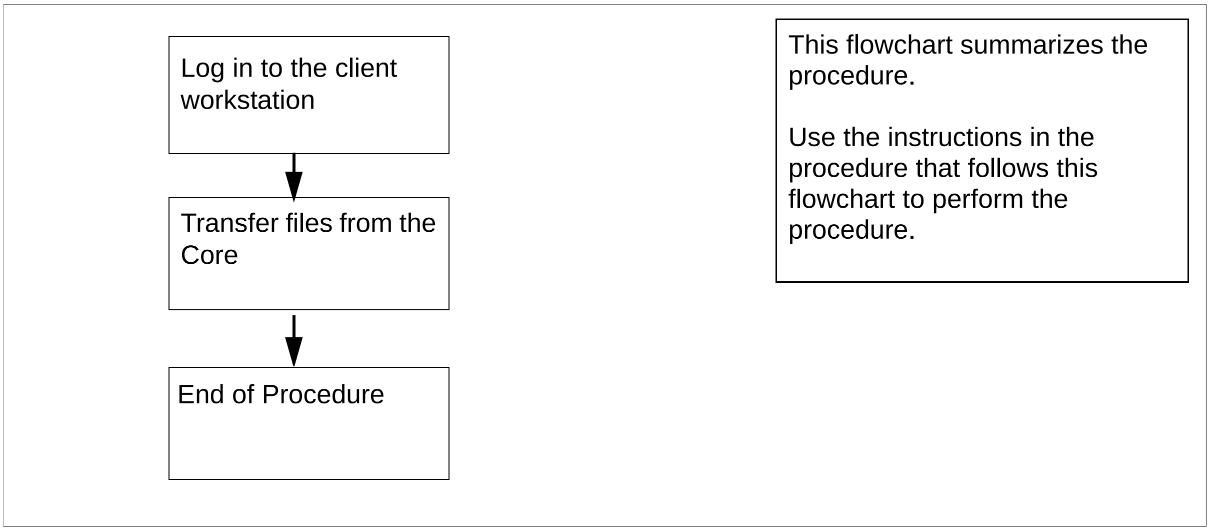
You must have root user privileges on the core module to perform this procedure.

> ***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


Log in to the client workstation
Transfer files from the Core
End of Procedure
This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the procedure.

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.

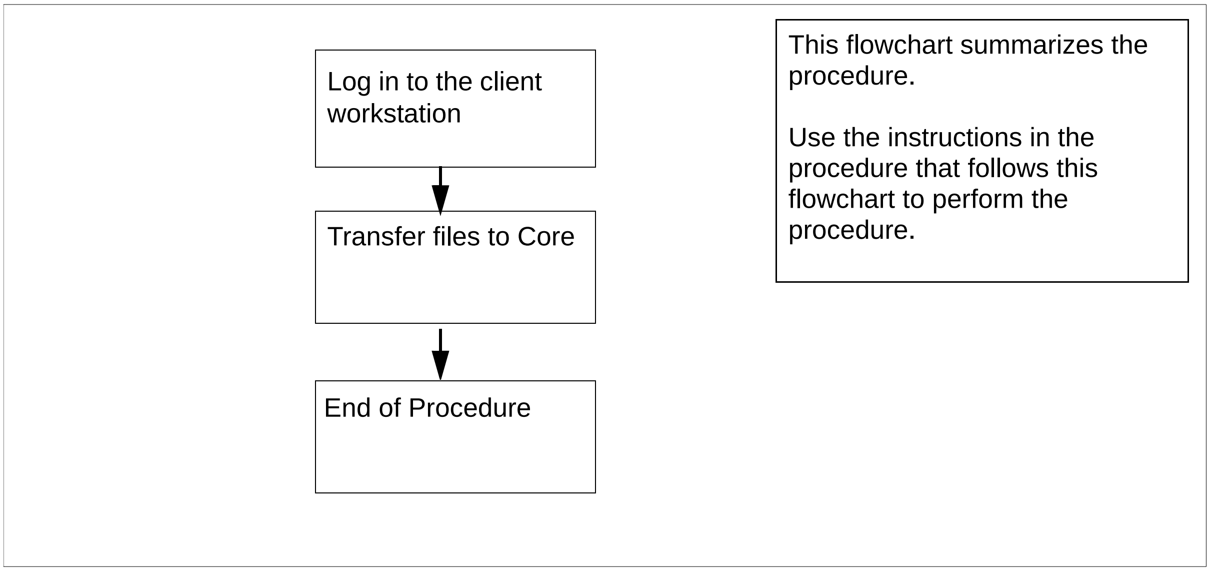
Logging on to the Core and Billing Manager

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



This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the 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.

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.

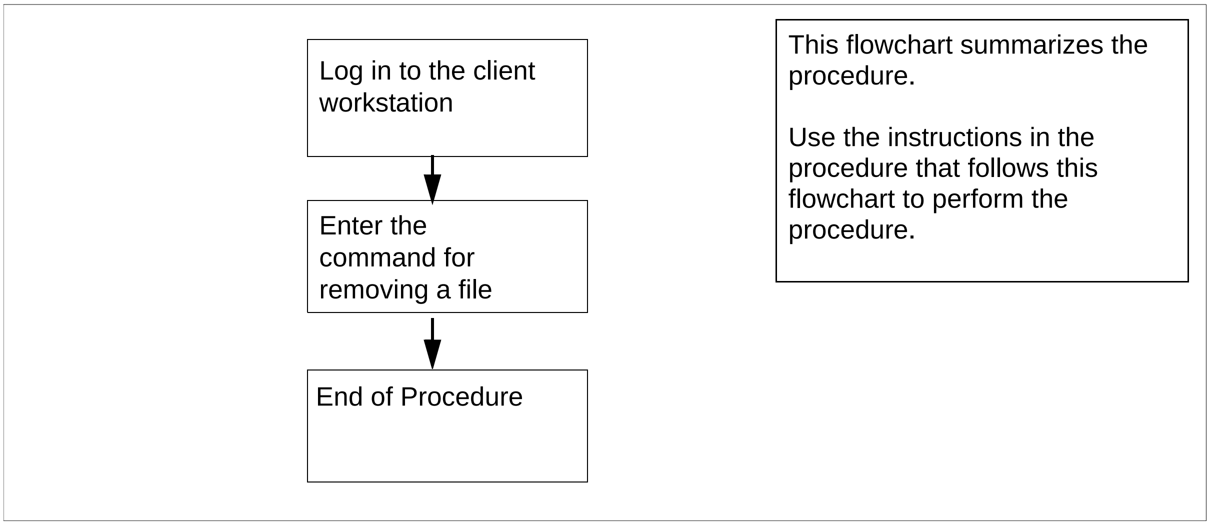
Logging on to the Core and Billing Manager

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


Log in to the client workstation
Enter the command for removing a file
End of Procedure

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the 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.

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.

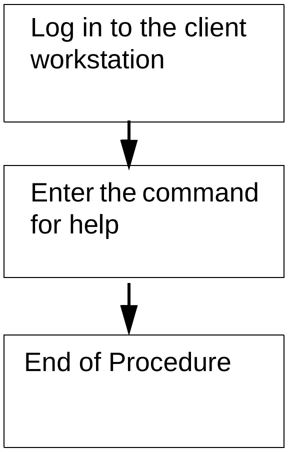
Logging on to the Core and Billing Manager

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



This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the 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.

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.

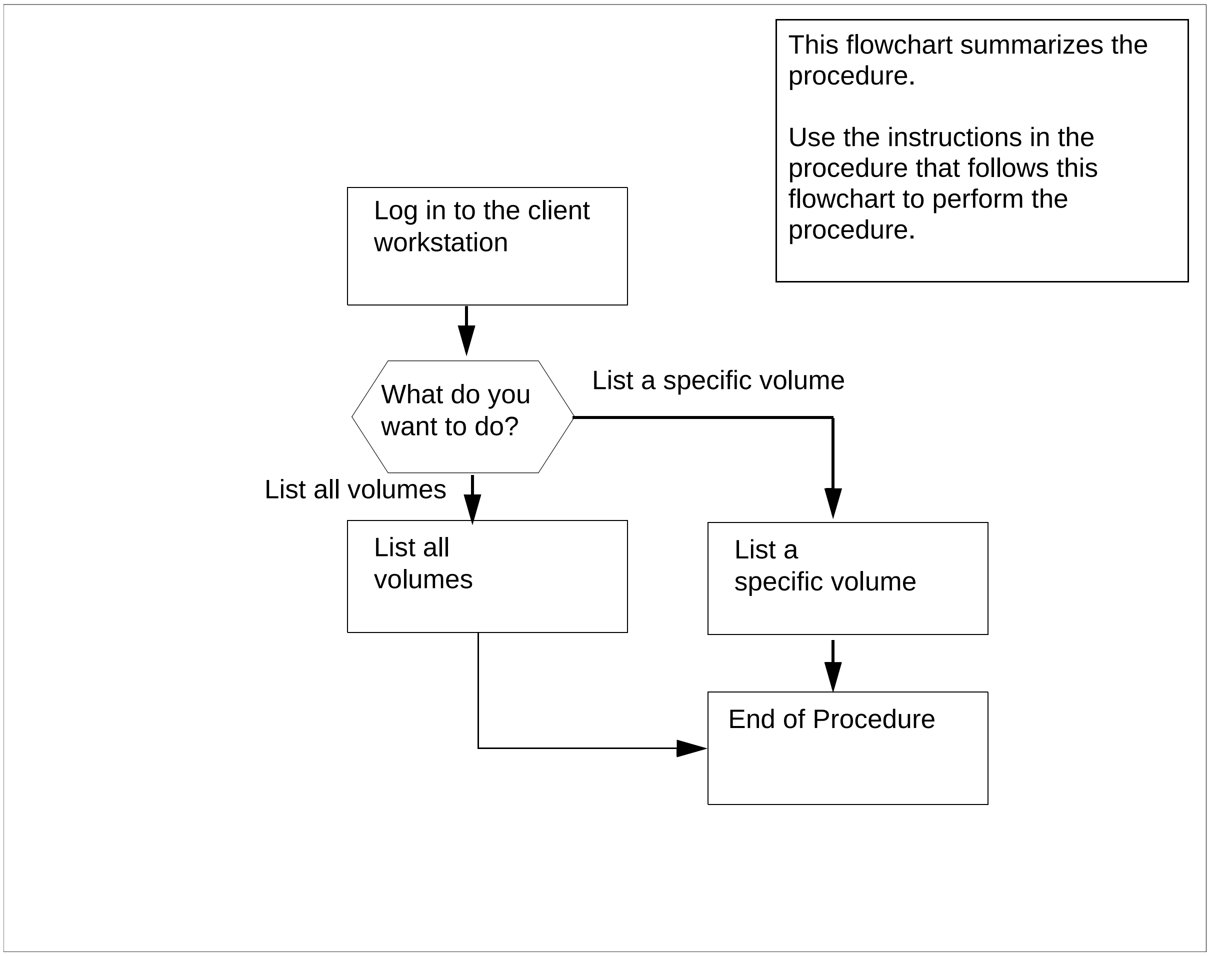
Logging on to the Core and Billing Manager

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


This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.
Log in to the client workstation
What do you want to do?
List a specific volume
List all volumes
List all volumes
List a specific volume
End of 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.

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 -1 <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 -1 <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.

Configuring the time zone on a Carrier VoIP SPFS-based server

Application

Use this procedure to configure the time zone on a Carrier Voice over IP (VoIP) Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Carrier VoIP SPFS-based server on which you want to configure the time zone

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View

 2 - Configuration

 3 - Other
 X - exit

select -
```

6 Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit


Select -
```

7 Enter the number next to the “Location Configuration” option in the menu.

Example response

```
Location Configuration
 1 - Chg_tz (Change Timezone
 2 - sys_loc (System Location)

 X - exit

select -
```

8 Enter the number next to the “chg_tz” option in the menu.

Example response

```
=== Executing “chg_tz”

WARNING: Changing the timezone will require a
reboot

Current setting:
Timezone:       US/Eastern

Enter the timezone for this host <default:
US/Eastern>:
```

9 When prompted, enter the correct time zone and press the Enter key.

Example response

```
New setting:
Timezone:       US/Eastern

Enter “ok” to commit changes
Enter “quit” to exit
Enter anything else to re-enter settings
```

10 When prompted, confirm the change by typing

```
ok
```

and pressing the Enter key.

11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

12 You have completed this procedure.

Changing a user password on a Carrier VoIP SPFS-based server

Application

Use this procedure to change a user password on a Carrier Voice over IP Server Platform Foundation Software (SPFS)-based server.

> ***Note:*** All user account management activities, such as setting up users, removing users, and changing passwords, are performed on the Active server and then propagated from the Active to the Inactive server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Carrier VoIP SPFS-based server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change the password for a specific user by typing

```
# passwd -r files <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user’s login identification

6 When prompted, enter a password of at least three characters.

> ***Note:*** It is not recommended to set a password with an empty value. Use a minimum of three characters.

7 When prompted, enter the password again for verification.

You have completed this procedure.

Changing a passthru user password

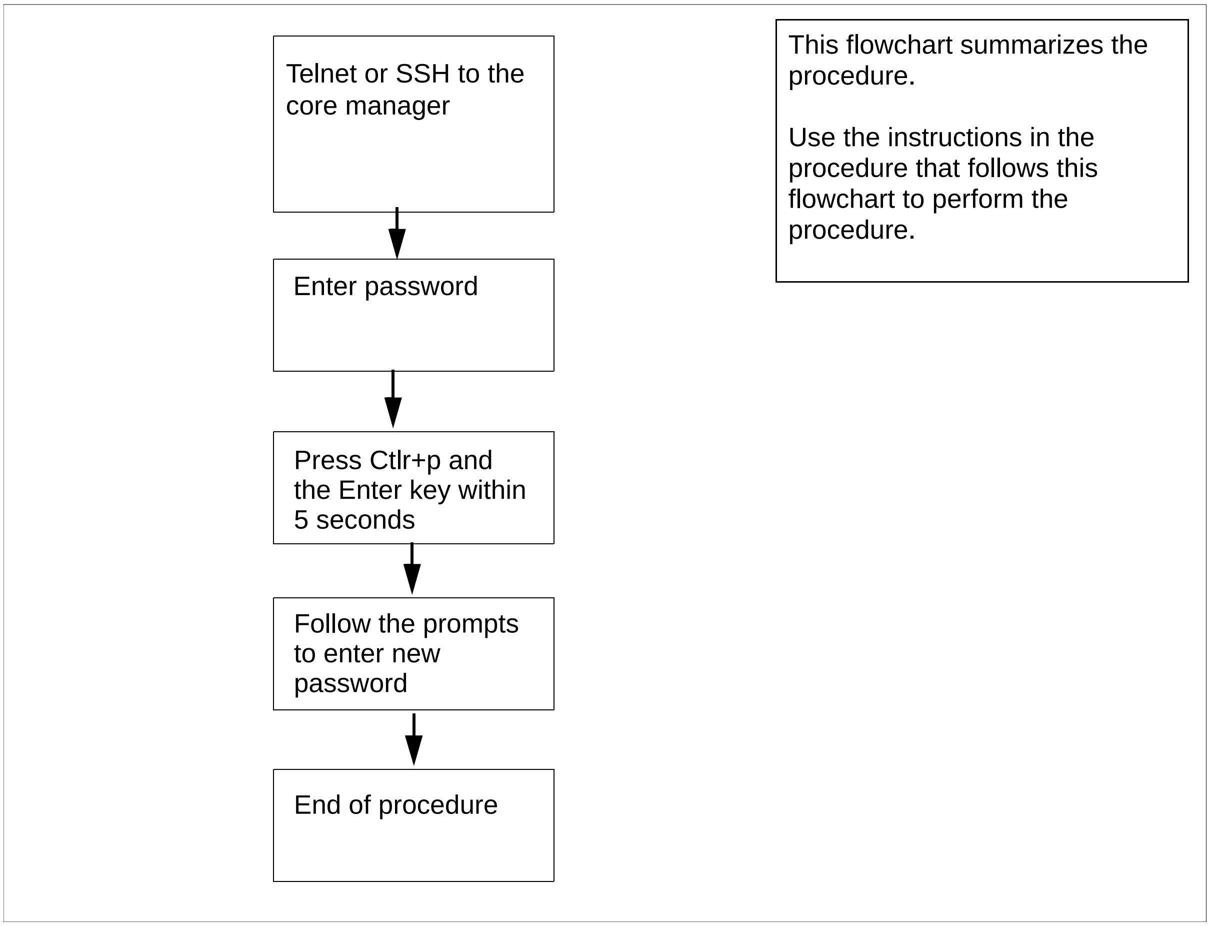
Purpose

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


Telnet or SSH to the core manager
Enter password
Press Ctlr+p and the Enter key within 5 seconds
Follow the prompts to enter new password
End of procedure
This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the 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.

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.

Setting the threshold for file systems on a Carrier VoIP SPFS-based server

Application

Use this procedure to change the default threshold for a file system on a Carrier Voice over IP (VoIP) Server Platform Foundation Software (SPFS)-based server. The default threshold is 90%. An alarm is raised when the file system exceeds the specified threshold, and log SPFS350 is generated.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Carrier VoIP SPFS-based server on which you are setting the file system threshold

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Set the threshold by typing

```
# filesys update -m <mount_point> -a <threshold>
```

and pressing the Enter key.

Where

mount_point
is the directory of the file system you are setting the threshold for

threshold
is 0 to 99% (default is 90%)

Example

```
filesys update -m /data -a 80
```

The example above sets the threshold for the /data file system to 80%.

6 You have completed this procedure.

Starting an application

Application

Use this procedure to start (return to service) a CBM software application.

> ***Note:*** For CBM850, you must perform this procedure on the active server.

Only perform this procedure when the application group is in service (InSv, ISTb, SysB).

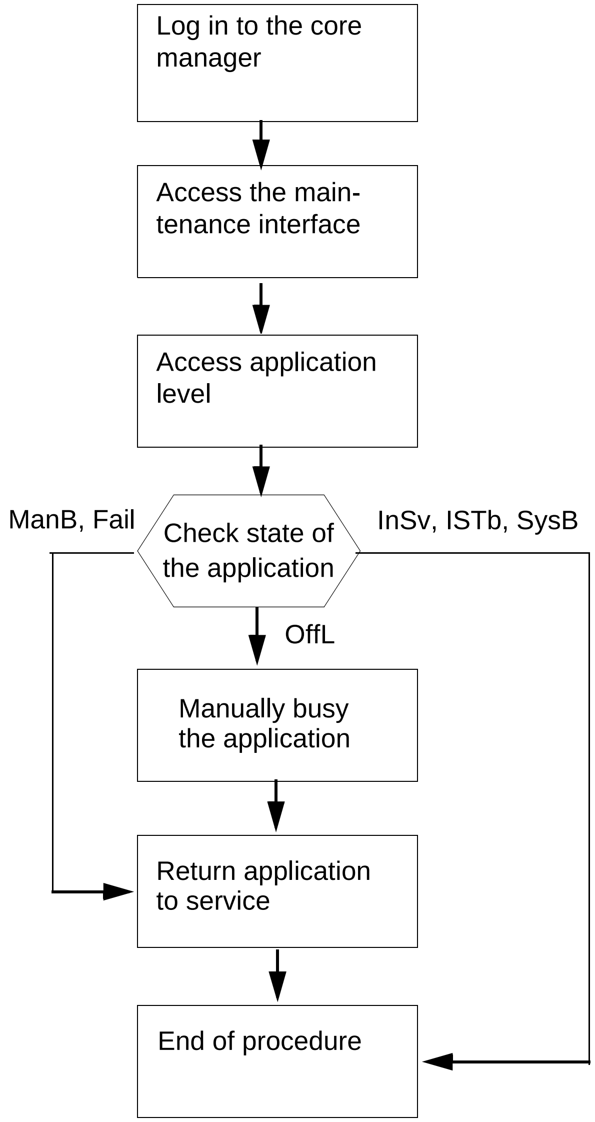
Action

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 application

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.


Log in to the core manager
Access the maintenance interface
Access application level
ManB, Fail
Check state of the application
InSv, ISTb, SysB
OffL
Manually busy the application
Return application to service
End of 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.

Starting an application

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

```
cbmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
appl
```

and pressing the Enter key.

4 Check the state of the application group, as displayed directly above the individual applications.

If	Do
the group is OffL	step 5
the group is ManB, Fail	step 6
the group is InSv, ISTb, SysB	step 7

5 Busy the software application group by typing.

```
bsy <n>
```

where

n
is the number next to the application you want to busy

and pressing the Enter key.

Example response:

```
Bsy application - Command complete.
```

6 Return the application group to service by typing.

```
rts <n>
```

where

n

is the number next to the application you want to return to service

and pressing the Enter key.

Response:

```
Application RTS - Command initiated.

Please wait...
```

Response:

```
Application RTS - Command complete.
```

7 You have completed this procedure.

Starting the application group

Application

Use this procedure to start (return to service) CBM software applications.

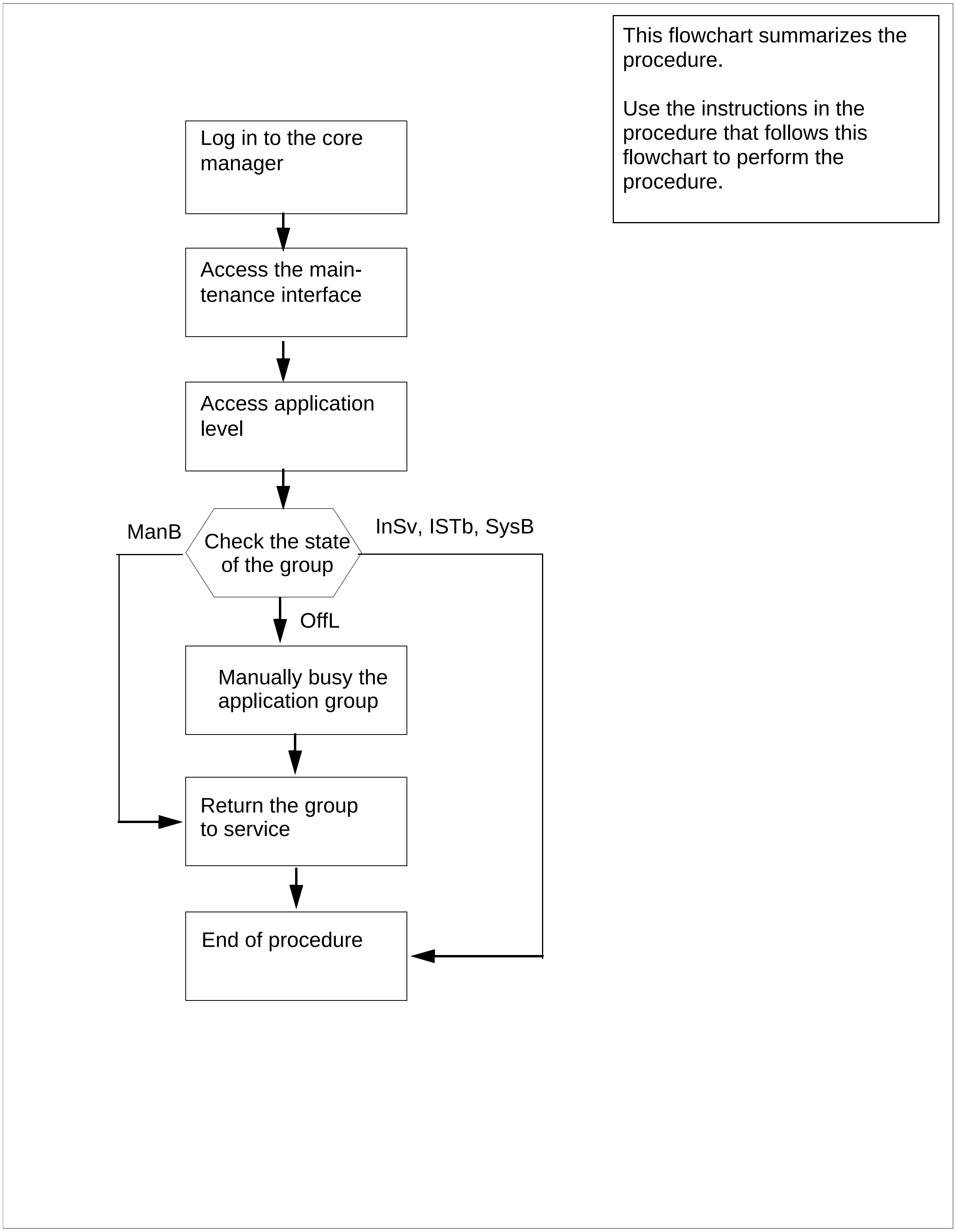
> ***Note:*** For CBM850, you must perform this procedure on the active server.

Action

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

> ***Note:*** This procedure does not affect offline applications. Offline applications can be started after the application group is returned to service.

Summary of starting the application group


This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the procedure.
Log in to the core manager
Access the maintenance interface
Access application level
Check the state of the group
ManB
InSv, ISTb, SysB
OffL
Manually busy the application group
Return the group to service
End of 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.

Starting the application group

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

```
cbmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
appl
```

and pressing the Enter key.

4 Check the state of the application group, as displayed directly above the individual applications.

If	Do
the group is OffL	step 5
the group is ManB	step 6
the group is InSv, ISTb, SysB	step 7

5 Busy the software application group by typing.

```
bsy group
```

and pressing the Enter key.

Response:

```
Bsy Group - Command complete.
```

6 Return the application group to service by typing.

```
rts group
```

and pressing the Enter key.

Response:

```
RTS GROUP - Command initiated.
Please wait...
```

Response:

```
RTS GROUP - Command complete.
```

7 You have completed this procedure.

Stopping an application

Application

Use this procedure to stop (manually busy) a CBM software application.

> ***Note:*** For CBM850, you must perform this procedure on the active server.

You cannot stop an application when the application group is offline.

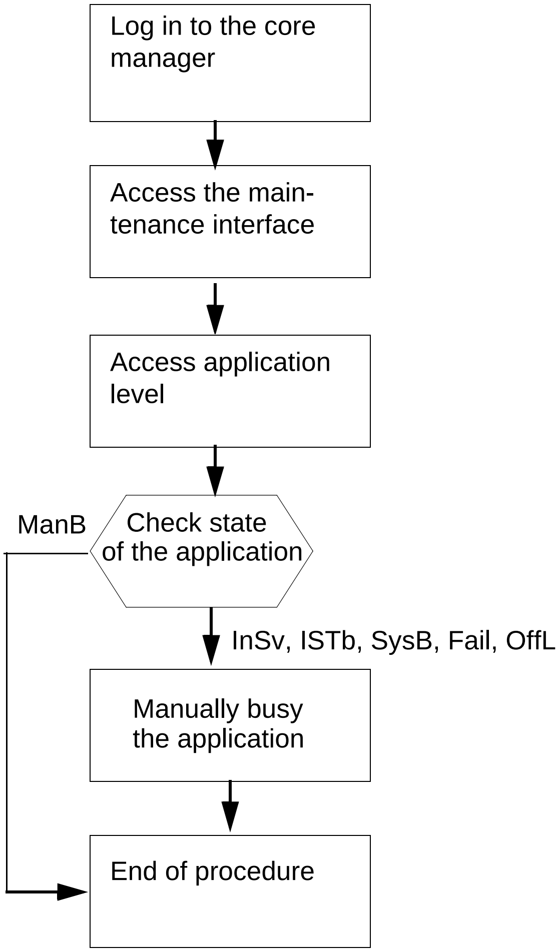
An application in the manually busy (ManB) state raises a minor alarm. If the group state was in service (InSv), the group state changes to in service trouble (ISTb).

Manually busy is a transitional state. Operations to the application group state or to the server impact an application that is in the ManB state.

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 stopping an application


Log in to the core manager
Access the maintenance interface
Access application level
Check state of the application
ManB
InSv, ISTb, SysB, Fail, OffL
Manually busy the application
End of procedure

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the 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.

Stopping an application

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

`cbmmtc`

and pressing the Enter key.

3 Access the application level by typing

`appl`

and pressing the Enter key.

4 Check the state of the application group, as displayed directly above the individual applications.

If	Do
the application is OffL, InSv, ISTb, SysB, Fail	step 5
the application is ManB	step 7

5 Busy the software application group by typing.

`bsy <n>`

where

n
is the number next to the application you want to busy

and pressing the Enter key.

Example response:

```
Bsy application: 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 16 seconds.*

If	Do
prompted to confirm the busy	step 6
no prompt	step 7

6 Confirm the Busy command by typing.

```
y
```

and pressing the Enter key.

After you confirm the Bsy command, the following is displayed:

Response:

```
Bsy application - Command initiated. Please
wait...
```

Response:

```
Bsy application - Command complete.
```

7 You have completed this procedure.

Stopping the application group

Application

Use this procedure to stop (manually busy) CBM software applications.

> ***Note:*** For CBM850, you must perform this procedure on the active server.

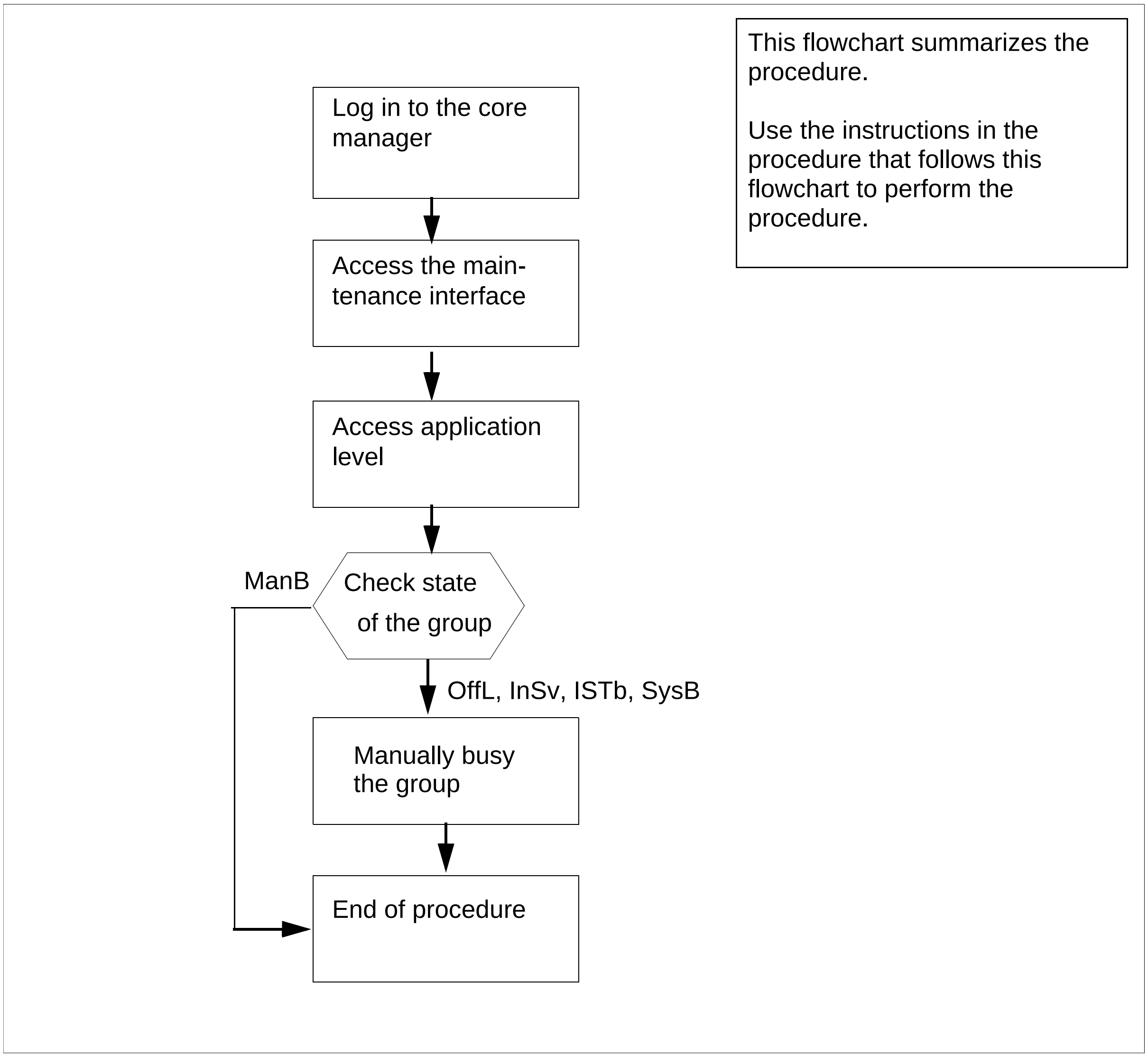
This procedure prevents an individual application from providing service.

Action

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

> ***Note:*** This procedure does not affect offline applications. You can change offline applications to manually busy after this procedure is complete.

Summary of stopping the application group



This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the 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.

Stopping the application group

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

```
cbmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
appl
```

and pressing the Enter key.

4 Check the state of the application group, as displayed directly above the individual applications.

If	Do
the group is ManB	step 7
the group is any other state	step 5

5 Busy the software application group by typing.

```
bsy group
```

and pressing the Enter key.

Response:

```
Bsy Group: The group 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 group as shown performs an orderly shutdown and can take up to 16 seconds.*

If	Do
prompted to confirm the busy	step 6
no prompt	step 7

6 Confirm the Busy command by typing.

```
y
```

and pressing the Enter key.

After you confirm the Bsy command, the following is displayed:

Response:

```
Bsy Group - Command initiated. Please wait...
```

Response:

```
Bsy Group - Command complete.
```

7 You have completed this procedure.

Stopping and restarting an application

Application

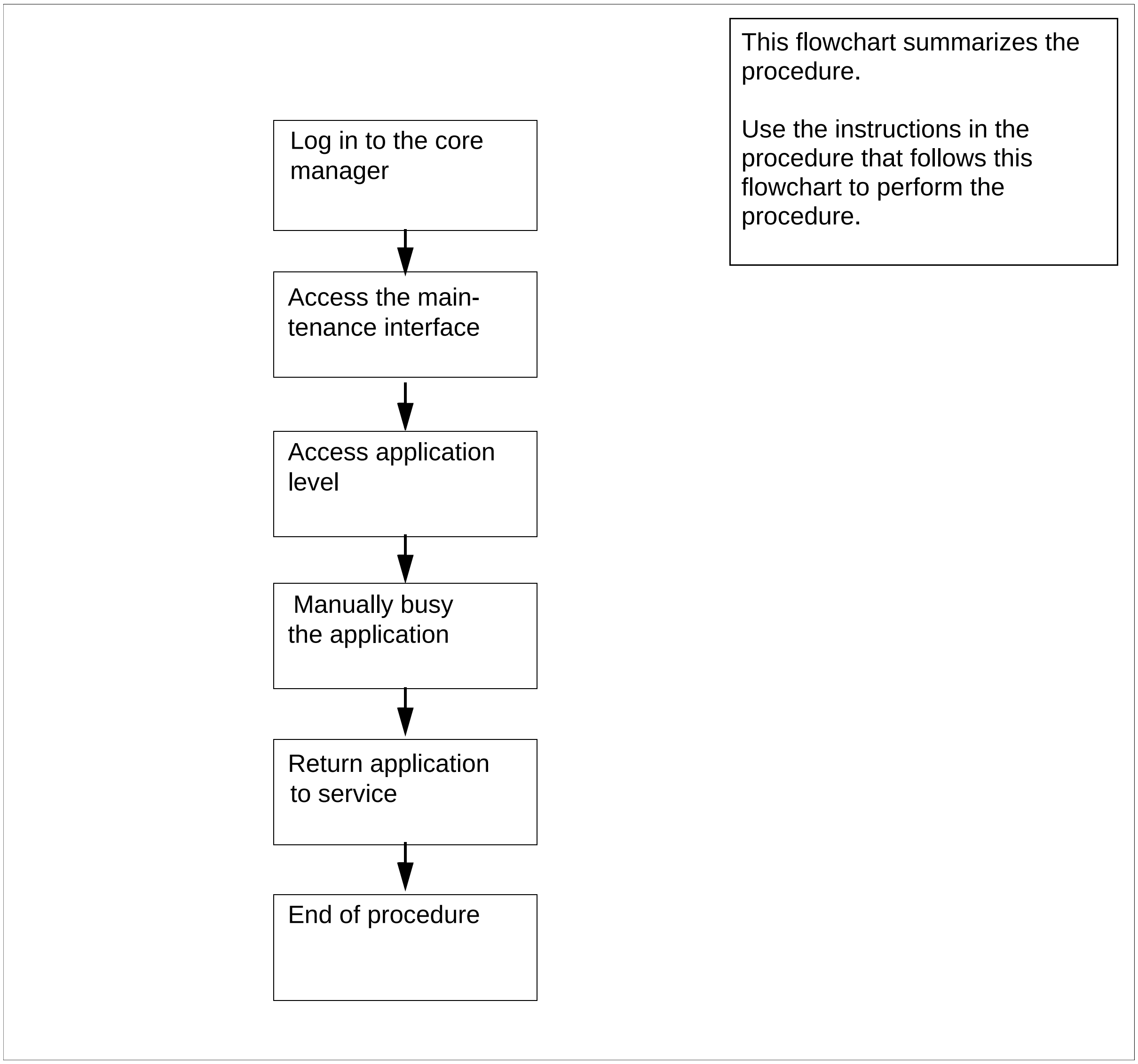
Use this procedure to stop (manually busy) and restart (return to service) CBM software applications.

Note: For CBM850, you must perform this procedure on the active 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 stopping and restarting an application


This flowchart summarizes the procedure.
Use the instructions in the procedure that follows this flowchart to perform the procedure.
Log in to the core manager
Access the maintenance interface
Access application level
Manually busy the application
Return application to service
End of 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.

Stopping and restarting an application

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

```
cbmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
appl
```

and pressing the Enter key.

4 Busy the software application group by typing.

```
bsy <n>
```

where

n
is the number next to the application you want to busy

and pressing the Enter key.

Example response:

```
Bsy application: 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 16 seconds.*

5 Confirm the Busy command by typing.

```
y
```

and pressing the Enter key.

After you confirm the Bsy command, the following is displayed:

Response:

```
Bsy application - Command initiated. Please
wait...
```

Response:

```
Bsy application - Command complete.
```

6 Return the application to service by typing

```
rts <n>
```

where

n
is the number next to the application you want to return to service

and pressing the Enter key.

Response:

```
RTS application - Command initiated.
```

Response:

```
RTS application - Command complete.
```

7 You have completed this procedure.

Offlining an application

Application

Use this procedure to offline a CBM software application.

> ***Note:*** For CBM850, you must perform this procedure on the active server.

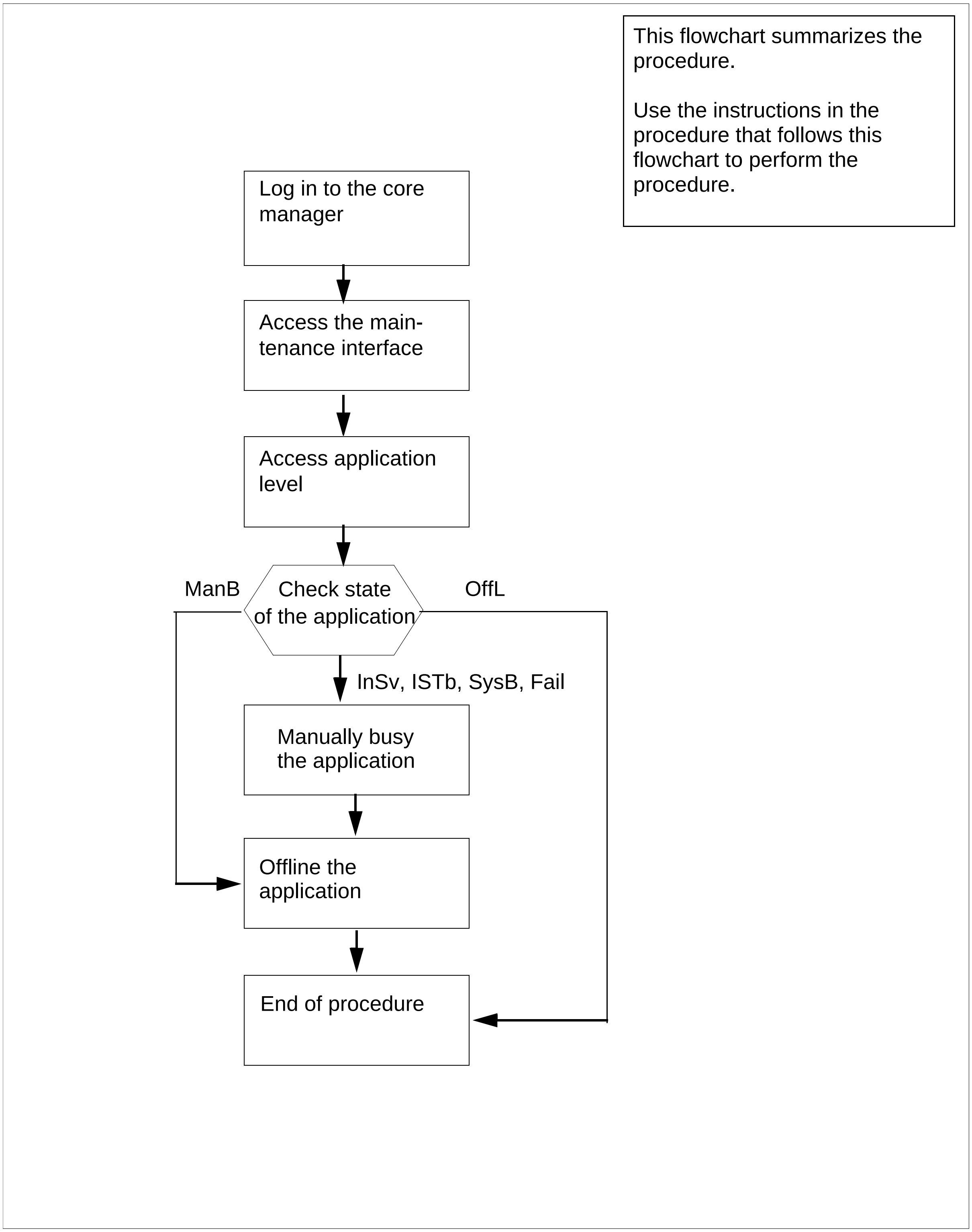
Once an application is offline, the application state does not change when a server reboots or the application group state changes.

An offline application clears any alarms for the application.

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 offlining an application


This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.
Log in to the core manager
Access the maintenance interface
Access application level
Check state of the application
ManB
OffL
InSv, ISTb, SysB, Fail
Manually busy the application
Offline the application
End of 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.

Offlining an application

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

```
cbmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
appl
```

and pressing the Enter key.

4 Check the state of the application group, as displayed directly above the individual applications.

If	Do
the group is InSv, ISTb, SysB, Fail	step 5
the groups is ManB	step 7
the group is OffL	step 8

5 Busy the software application group by typing.

```
bsy <n>
```

where

n
is the number next to the application you want to busy

and pressing the Enter key.

Example response:

```
Bsy application: 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 16 seconds.*

6 Confirm the Busy command by typing.

```
y
```

and pressing the Enter key.

After you confirm the Bsy command, the following is displayed:

Response:

```
Bsy application - Command initiated. Please
wait...
```

Response:

```
Bsy application - Command complete.
```

7 Offline the application by typing

```
offl <n>
```

where

n
is the number next to the application you want to offline

and pressing the Enter key.

Response:

```
OffL application - Command complete.
```

8 You have completed this procedure.

Offlining the application group

Application

Use this procedure to offline the application group.

> ***Note:*** For CBM850, you must perform this procedure on the active server.

This procedure prevents an individual application from providing service.

Action

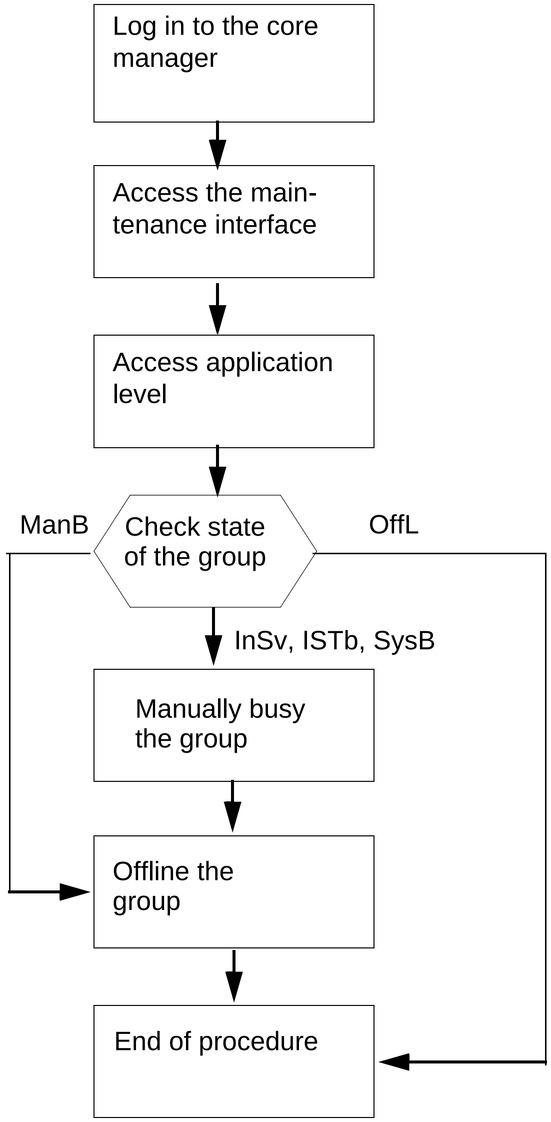
The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

> ***Note:*** After this procedure, the application group is in an offline state and the individual application states are ManB. Applications that were previously offline remain offline.

Summary of offlining the application group

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the 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.

Offlining the application group

At the local or remote VT100 terminal

1 Log in to the CBM as the root user or a maint class user.

2 Access the maintenance interface by typing

```
cbmmtc
```

and pressing the Enter key.

3 Access the application level by typing

```
appl
```

and pressing the Enter key.

4 Check the state of the application group, as displayed directly above the individual applications.

If	Do
the group is InSv, ISTb, SysB	step 5
the groups is ManB	step 7
the group is OffL	step 8

5 Busy the software application group by typing.

```
bsy group
```

and pressing the Enter key.

Example response:

```
Bsy Group: The group 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 group as shown performs an orderly shutdown and can take up to 16 seconds.*

6 Confirm the Busy command by typing.

```
y
```

and pressing the Enter key.

After you confirm the Bsy command, the following is displayed:

Response:

```
Bsy Group - Command initiated. Please wait...
```

Response:

```
Bsy Group - Command complete.
```

7 Offline the application group by typing

`offl group`

and pressing the Enter key.

Response:

```
OffL Group - Command complete.
```

8 You have completed this procedure.

Displaying the CLLI from the command line

Use the following procedure to display the Common Language Location Identifier (CLLI) of the Core from the command line.

Prerequisites

This procedure requires access to the Core and Billing Manager through a telnet 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

From any workstation or console

1 Access the core manager.

From the command line

2 Display the CLLI of the Core by typing

```
clli
```

and pressing the Enter key.

Response

The system displays the CLLI of the Core.

Example

```
EAST_CS01
```

3 You have completed this procedure.

Displaying the CLLI from BILLMTC

Use the following 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 and Billing Manager through a telnet 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

From any workstation or console

1 Access the core manager.

2 Access the billing maintenance by typing

```
billmtc
```

and pressing the Enter key.

Response

The billing maintenance interface opens.

From any level of BILLMTC

3 Display the CLLI of the Core by typing

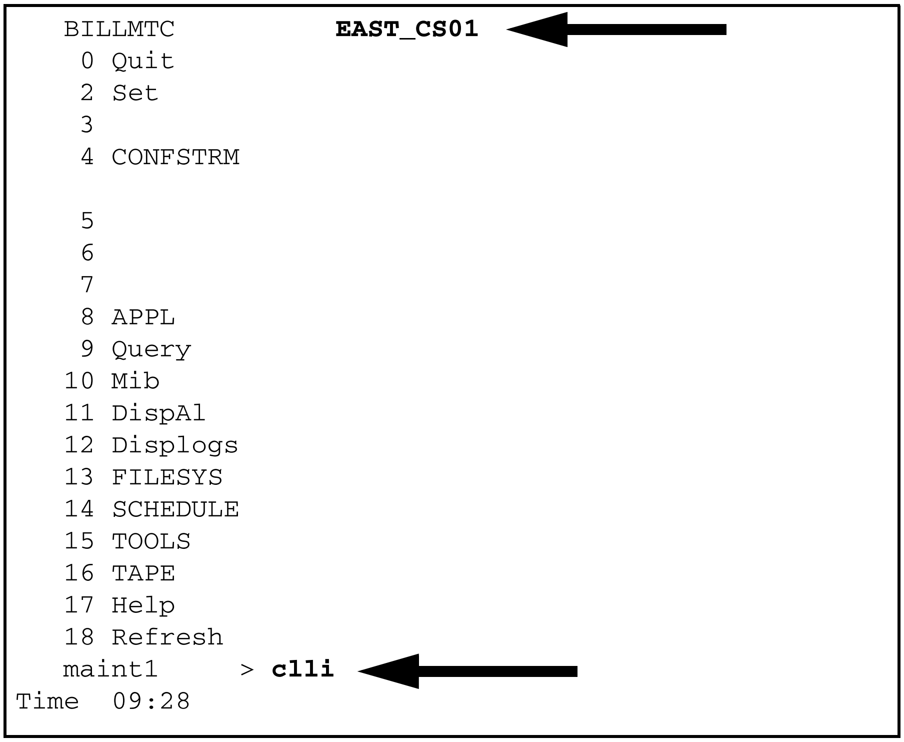
`clli`

and pressing the Enter key.

Response

BILLMTC displays the CLLI at the top of the screen.

Example



```
   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 IPSec and IKE on a Carrier VoIP SPFS-based server

Application

Use this procedure to configure IP Security (IPSec) and Internet Key Exchange (IKE) on a Carrier Voice over IP (VoIP) Server Platform Foundation Software (SPFS)-based server, for secure communication with downstream interfaces.

Prerequisites

IPSec and IKE configuration parameters that are provisioned on the OSS must match the corresponding parameters configured through this procedure.

> ***Note 1:*** 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.
>
> ***Note 2:*** When performing this procedure, each time you enter **x** when it is a valid response to a CLI tool prompt, you exit from the current menu level of the interface. Repeatedly entering x eventually enables you to exit from the CLI tool.

Procedures

Use the following table to determine the procedure to perform.

Procedure to perform
Procedure to access CLI in order to perform IPSec and IKE configuration on page 170
Procedure to add an IPSec rule on page 175
Procedure to delete an IPSec rule on page 178
Procedure to list an IPSec rule on page 179
Procedure to add an IKE rule on page 180
Procedure to delete an IKE rule on page 183
Procedure to list IKE entries on page 184
Procedure to change a preshared key for an IKE entry on page 185

Procedure to access CLI in order to perform IPSec and IKE

configuration

At your workstation

1 Telnet to the server:

```
telnet <server>
```

where

server
is the IP address or host name of the Carrier VoIP SPFS-based server on which you want to configure IPSec and IKE.

2 When prompted, enter your user ID and password.

3 Change to the root user:

```
su - root
```

4 When prompted, enter the root password.

5 Access the command line interface:

```
cli
```

Example response

```
Command Line Interface
 1 - View

 2 - Configuration

 3 - Other


 X - exit

select -
```

6 Enter the number next to the “Configuration” option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
19 - backup_config (Backup Configuration)

 X - exit


Select -
```

7 Enter the number next to the “IP Configuration” option in the menu.

Example response

```
IP Configuration
1 - config_router (Configure Default Router and
     Netmask)
2 - config_data (Configure System Data IP
     Addresses)
3 - ipsecike_config (Configure IPSec/IKE Rules)

X - exit

select -
```

8 Enter the number next to the “ipsecike_config” option in the menu.

Example response

```
IPSec/IKE Configuration Menu
1 - IPSec Configuration
2 - IKE Configuration

X - exit

Select -
```

If	Do
you wish to configure IPSec parameters	step 9
you wish to configure IKE parameters	step 10

9 Enter the number next to the “IPSec Configuration” option in the menu.

Example response

```
IPSec Configuration Menu
1 - Add IPSec entry
2 - Delete IPSec entry
3 - List All IPSec entries

X - exit

Select -
```

If	Procedure to perform
you wish to add an IPSec rule	Procedure to add an IPSec rule on page 175
you wish to delete an IPSec rule	Procedure to delete an IPSec rule on page 178
you wish to list all IPSec rules	Procedure to list an IPSec rule on page 179

10 Enter the number next to the “IKE Configuration” option in the menu.

Example response

```
IKE Configuration Menu
1 - Add IKE entry
2 - Delete IKE entry
3 - List IKE entries
4 - Change Preshared key for IKE entry

X - exit

Select -
```

If	Procedure to perform
you wish to add an IKE entry	Procedure to add an IKE rule on page 180
you wish to delete an IKE entry	Procedure to delete an IKE rule on page 183
you wish to list IKE entries	Procedure to list IKE entries on page 184
you wish to change a preshared key for an IKE entry	Procedure to change a preshared key for an IKE entry on page 185

11 When you have completed the configuration, and you wish to exit from the CLI tool, exit each menu level of the command line interface by entering **x** in response to the select prompt.

12 You have completed this procedure.

Procedure to add an IPSec rule

At the CLI tool IPSec Configuration Menu

1 Enter the number next to the “Add IPSec entry” option in the menu. The CLI tool displays a collection of prompts for IPSec rule parameters, as shown below.

Example response

```
Enter the Remote IP Address:
Enter the Remote Port No [1-65535,all]:
Enter the Local IP Address [<IP address>]:
Enter the Local Port No [1-65535,all]:
Enter the Upper Layer Protocol
         [any,udp,tcp,icmp]:
Enter the Direction [in,out,both]:
Enter the Action [ipsec,drop,bypass]:
Enter the ESP Header
 Authentication Algorithm [md5,sha 1,none,any]:
 Encryption Algorithm [none,Null,des,3des,
           aes,blowfish]:
Enter the AH Header
 Authentication Algorith [md5,sha1,none,any]:
```

Use the following table to determine the information to enter in response to each of the prompts.

Field	Entry	Explanation
Remote Address	a numeric internet IP address of the form: www.xxx.yyy.zzz	source address on incoming packets and destination address on outgoing packets
Remote Port	1-65535,all	IP port of the remote system communicating with the server
Local Address ***Note:*** This is the cluster IP address if the system is an HA cluster configuration. If the system is a simplex configuration, this is the address of this node.	a numeric internet IP address of the form: www.xxx.yyy.zzz	destination address on incoming packets and source address on outgoing packets
Local Port	1-65535,all	IP port of this server

Field	Entry	Explanation
Upper Layer Protocol	any,udp,tcp,icmp	determines which protocol traffic this entry is matched against
Direction	in,out,both	determines whether this entry is for inbound or outbound traffic
Action	bypass,drop,ipsec	determines the action to be taken when the traffic pattern is matched
ESP Encryption	none,any,NULL,DES, 3DES	encryption algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.
ESP Authentication	none,any,SHA1,MD5	authentication algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.
AH Authentication	none,any,SHA1,MD5	authentication algorithm that will be used to apply the IPSec AH protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.

You will be prompted to save the entries, edit the entries, or abort and lose all of the entry information you have entered in this session.

If	Do
you wish to save the IPSec rule entries	Enter **save** You have completed this procedure

If	Do
you wish to edit the IPSec rule entries	Enter **edit** and go to step 2
you wish to abort and lose all entry information that you have entered in this session	Enter **abort** You have completed this procedure.

2 If you have chosen to edit the IPSec rule entries, the CLI tool displays the IPSec rule entries you have made in this session. You may change any of the entries that you have made.

Example

```
Remote IP Address [47.135.210.64]:
Remote Port No [all]:
Local IP Address [47.135.210.119]:
Local Port No [all]:
Upper Layer Protocol [any]:
Direction [both]:
Action [ipsec]:
ESP Encryption Algorithm [3des]
ESP Authentication Algorithm [sha1]:
AH Authentication Algorithm [md5]:
```

After you have completed making any changes and press Enter, you are prompted to either save the new IPSec rule configuration, edit the configuration again, or abort the session and lose all of the changes you have made.

If	Do
you wish to save the IPSec rule entries	Enter **save** You have completed this procedure.
you wish to edit the IPSec rule entries again	Enter **edit** and repeat this step.
you wish to abort and lose all entry information that you have entered in this session	Enter **abort** You have completed this procedure.

Procedure to delete an IPSec rule

At the CLI tool IPSec Configuration Menu

1 Enter the number next to the “Delete IPSec entry” option in the menu. The CLI tool displays the IPSec rules that have been configured, as shown below.

Example response

```
------------------------------------------------------
indexID  raddr     laddr        lport rport dir status
------------------------------------------------------
1   47.130.222.110 47.130.222.90 all   all  both  up
2   47.130.222.88  47.130.222.7  all   all  both  down

Enter the indexID of rule to be deleted (x to exit) -
```

Enter the number next to the IPSec rule that you want to delete.

The CLI tool displays the entries for the IPSec rule that you want to delete.

Respond to the prompts to delete the rule.

2 You have completed this procedure.

Procedure to list an IPSec rule

At the CLI tool IPSec Configuration Menu

1 Enter the number next to the “List All IPSec entries” option in the menu. The CLI tool displays the IPSec rules that have configured, as shown below.

Example response

```
------------------------------------------------------
indexID  raddr     laddr        lport rport dir status
------------------------------------------------------
1   47.130.222.110 47.130.222.90 all   all  both  up
2   47.130.222.88  47.130.222.7  all   all  both  down

Enter the indexID of rule to be detailed (x to exit) -
```

Enter the number next to the IPSec rule whose details you want to display.

The CLI tool displays the entries for the IPSec rule that you selected.

You may choose either to enter another rule whose details you wish to display or you may exit to a previous menu level.

2 You have completed this procedure.

Procedure to add an IKE rule

At the CLI tool IKE Configuration Menu

1 Enter the number next to the “Add IKE entry” option in the menu. The CLI tool displays a collection of prompts for IKE rule parameters, as shown below.

Example response

```
Enter the Remote IP Address:
Enter the Local IP Address [<IP address>]:
Enter the Oakley Group [1,2,5]:
Enter the Authentication Method [preshared]:
Enter the Encryption Algorithm [des,3des];
Enter the Authentication Algorithm [md5,sha1]:
Enter the PFS Group ID [0,1,2,5]:
Enter the IKE Lifetime value:
Enter the IKE Lifetime unit [secs,min,hrs]:
Enter the IPSec Lifetime Value:
Enter the IPSec Lifetime unit [secs,min,hrs]:
Enter the IKE Preshared Key file location (full
  path):
```

Use the following table to determine the information to enter in response to each of the prompts.

> ***Note:*** The preshared key, in hex format, should be stored in a file on the system. You will need to provide this file when you are configuring the IKE rule.

Field	Entry	Explanation
Remote Address	a numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of the remote system communicating with this server
Local Address	a numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of this server
Oakley Group	1 (768 bit), 2 (1024 bit), 5 (1536 bit)	the Oakley Diffie-Hellman group used for IKE Security Association key derivation
Authentication Method	Preshared	authentication method used for IKE phase 1

Field	Entry	Explanation
Encryption	DES,3DES	specifies the encryption algorithm for a security association
Authentication	SHA1,MD5	specifies the authentication algorithm for a security association
PFS Group ID	0 (do not use Perfect Forward Secrecy for IPSec SAs), 1 (768 bit), 2 (1024 bit), 5 (1536 bit)	Oakley Diffie-Hellman group used for IPSec Security Association key derivation
Preshared Key File	String (file name with full path)	Specifies the file with complete path that contains the preshared key. This file contains the preshared key for this Security Association.
IKE Lifetime	Maximum allowed value is 2419200 seconds, 40320 minutes, 672 hours, or 28 days	Specifies the lifetime for an IKE phase 1 Security Association
IPSec Lifetime	Maximum allowed value is 2419200 seconds, 40320 minutes, 672 hours, or 28 days	Specifies the lifetime for an IPSec Security Association

You will be prompted to either save the entries, edit the entries, or abort and lose all of the entry information you have entered in this session.

If	Do
you wish to save the IKE rule entries	Enter **save** You have completed this procedure.

If	Do
you wish to edit the IKE rule entries	Enter **edit** and go to step 2
you wish to abort and lose all entry information that you have entered in this session	Enter **abort** You have completed this procedure.

2 If you have chosen to edit the IKE rule entries, the CLI tool displays the IKE rule entries you have made in this session. You may change any of the entries that you have made.

Example

```
Remote IP Address [47.135.214.53]:
Local IP Address [47.135.214.30]:
Oakley Group [2]:
Authentication Method [preshared]:
Encryption Algorithm [3des]:
Authentication Algorithm [sha1]:
PFS Group ID [0]
IKE Lifetime value [400]:
IKE Lifetime Unit [secs]:
IPSec Lifetime Value [400]:
IPSec Lifetime Unit [secs]:
IKE Preshared key File location [/tmp/site1]:
```

After you have completed making any changes and press Enter, you will be prompted to either save the new IKE rule configuration, edit the configuration again, or abort the session and lose all of the changes you have made.

If	Do
you wish to save the IKE rule entries	Enter **save** You have completed this procedure.
you wish to edit the IKE rule entries again	Enter **edit** and repeat this step.
you wish to abort and lose all entry information that you have entered in this session	Enter **abort** You have completed this procedure.

Procedure to delete an IKE rule

At the CLI tool IKE Configuration Menu

1 Enter the number next to the “Delete IKE entry” option in the menu. The CLI tool displays the IKE rules that have configured, as shown below.

Example response

```
------------------------------------------------------
indexID  raddr        laddr
------------------------------------------------------
1      47.135.142.53  47.135.142.30
2      47.130.221.88  47.130.221.7

Enter the indexID of rule to be deleted (x to exit) -
```

Enter the number next to the IKE rule that you want to delete.

The CLI tool displays the entries for the IKE rule that you want to delete.

Respond to the prompts to delete the rule.

2 You have completed this procedure.

Procedure to list IKE entries

At the CLI tool IKE Configuration Menu

1 Enter the number next to the “List IKE entries” option in the menu. The CLI tool displays the IKE rules that have been configured, as shown below.

Example response

```
------------------------------------------------------
indexID  raddr        laddr
------------------------------------------------------
1     47.135.142.53  47.135.142.30
2     47.130.221.88  47.130.221.7

Enter the indexID of rule to be detailed (x to exit) -
```

Enter the number next to the IKE rule whose details you want to display.

The CLI tool displays the entries for the IKE rule that you selected.

You may choose either to enter another rule whose details you wish to display or you may exit to a previous menu level.

2 You have completed this procedure.

Procedure to change a preshared key for an IKE entry

At the CLI tool IKE Configuration Menu

1 Enter the number next to the “Change Preshared key for IKE entry” option in the menu. The CLI tool displays the IKE rules that have been configured.

Example

```
------------------------------------------------------
indexID  raddr       laddr
------------------------------------------------------
1     47.135.142.53  47.135.142.30
2     47.130.221.88  47.130.221.7

Enter the indexID of rule whose key is to be changed (x
to exit) -
```

Enter the number next to the IKE rule whose key is to be changed. The CLI tool displays the entries for the IKE rule that you selected, as shown below:

Example

```
Remote IP Address [47.135.214.53]:
Local IP Address [47.135.214.30]:
Oakley Group [2]:
Authentication Method [preshared]:
Encryption Algorithm [3des]:
Authentication Algorithm [sha1]:
PFS Group ID [0]
IKE Lifetime [400]:
IPSec Lifetime [800]:
IKE Preshared key [********]:

Do you wish to change key for above IKE rule
Select [Yes, No, Exit (x)] -
```

In response to the prompts, enter Yes to change to key, enter the full path location of the preshared key file, and confirm the change.

2 You have completed this procedure.

Configuring IPSec and IKE on the OSS

Application

Use this procedure to configure IP Security (IPSec) and Internet Key Exchange (IKE) on the OSS. Included are steps both to add IPSec/IKE to the OSS and to remove IPSec/IKE from the OSS. In this procedure, the OSS is assumed to be a Solaris 5.9 machine.

Prerequisites

IPSec and IKE configuration parameters that are provisioned on the OSS must match the corresponding parameters provisioned on the server to which a secure connection is being configured.

> ***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.

Procedures

Use the following table to determine the procedure to perform.

Procedure to perform
Configuring IPSec on the OSS (Solaris 5.9 machine) on page 187
Removing IPSec from the OSS (Solaris 5.9 machine) on page 188

Configuring IPSec on the OSS (Solaris 5.9 machine)

At the OSS

1 Make required changes in the following files on the OSS. The changes correspond to the server to which the secure connection is being configured.

- /etc/inet/ipsecinit.conf
- /etc/inet/ike/config
- /etc/inet/secret/ike.preshared

Note: When IPSec and IKE are configured on a Carrier VoIP SPFS-based server through the CLI tool, sample downstream configuration files are generated. These files are "downstream.ipsec" and "downstream.ike", located in the /etc/inte/remotesystem/solaris directory on the Carrier VoIP SPFS-based server. The information in these two files can be used to update the files shown above.

2 Enable IPSec communication from the OSS by performing the following steps:

- restart the iked daemon:

```
pkill in.iked
```

```
/usr/bin/inet/in.iked
```

- activate IPSec policy:

```
ipsecconf -a /etc/inet/ipsecinit.conf
```

3 You have completed this procedure.

Note: If the Carrier VoIP SPFS software load for release SN09 is running on the OSS, the CLI tool can be used for configuring IPSec on the OSS. The procedure to use is "Configuring IPSec and IKE on a Carrier VoIP SPFS-based server" located in *ATM/IP Solution-level Security and Administration*, NN10402-600.

Removing IPSec from the OSS (Solaris 5.9 machine)

At the OSS

1 Remove the appropriate IPSec and IKE entries from the following files. These entries correspond to the server from which the secure connection is being removed.

- /etc/inet/ipsecinit.conf
- /etc/inet/ike/config
- /etc/inet/secret/ike.preshared

2 Remove the IPSec security from the link by performing the following steps:

- restart the iked daemon:

```
pkill in.iked
/usr/bin/inet/in.iked
```

- activate IPSec policy:

```
ipsecconf -a /etc/inet/ipsecinit.conf
```

3 You have completed this procedure.

Note: If the Carrier VoIP SPFS software load for release SN09 is running on the OSS, the CLI tool can be used for removing IPSec from the OSS. The procedure to use is “Configuring IPSec and IKE on a Carrier VoIP SPFS-based server” located in *ATM/IP Solution-level Security and Administration*, NN10402-600.