Carrier VoIP

Core and Billing Manager 850 Security and Administration

NN10358-611

Document status: Standard
Document version: 04.04
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

Querying the status of non-secure network services

This section describes the procedures to query the status of common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime).

Application

To enable or disable non-secure network services, refer to the procedures Enabling non-secure network services and Disabling non-secure network services.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server

b. When prompted, enter your user ID and password.

c. Change to the root user by typing
```
$ su - root
```
and pressing the Enter key.

d. When prompted, enter the root password.

e. Proceed to step 4.

3 Log in to the SPFS-based server using SSH (secure) as follows:

a. Log in to the server by typing
```
> ssh -1 root <userid>
```
and pressing the Enter key.

where

server

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

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.

4 Navigate to the Security Services Configuration menu within the command line interface 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 Configuration
5 - COBRA Configuration
```

```
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup 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 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

5 Determine whether you choose to query the status of common services (for example, ftp and telnet), tools services (for example, time and daytime), or other services.

To query	Do
common services	step 6
tools services	step 9
other services	step 12

6 Enter the number next to the “Common Inet Services (ftp, tftp, telnet, snmp and nfs)" option in the menu.

Example response

```
Common Inet Services (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query)
2 - enable_common_inetd (Enable a service registered in
inetd.conf)
3 - disable_common_inetd (Disable a service registered
in inetd.conf)
x - exit
select -
```

7 Enter the number next to the “Query Common Inet (Services State Query)” option in the menu. The status of the common network services is displayed, as in the following example.

Example response

```
Common Inet Services States
0 - telnet      Enabled
1 - ftp         Enabled
2 - tftp        Enabled
3 - snmp        Disabled
4 - nfs_server  Enabled
5 - nfs_client  Enabled
=== | query_common_inetd | execution completed
```

8 Proceed to step 14.

9 Enter the number next to the “Tools Inet Services (time, daytime)” option in the menu.

Example response

```
Tools Inet Services (time, daytime)
1 - query_tool_inetd (Services State Query)
2 - enable_tool_inetd (Enable a service registered in
inetd.conf)
3 - disable_tool_inetd (Disable a service registered in
inetd.conf)
x - exit
select -
```

10 Enter the number next to the “Query tool inetd (Services State Query)” option in the menu. The status of the tools network services is displayed, as in the following example.

Example response

```
Toolnet Services States
0 - time      Enabled
1 - daytime   Enabled
=== | query_tool_inetd | execution completed
```

11 Proceed to step 14.

12 Enter the number next to the “Other Inet Services” option in the menu.

Example response

```
Other Inet Services
1 - query_tool_inetd (Services State Query)
2 - enable_tool_inetd (Enable a service registered in
inetd.conf)
3 - disable_tool_inetd (Disable a service registered in
inetd.conf)
x - exit
select -
```

13 Enter the number next to the “Quert tool inetd (Services State Query)” option in the menu. The status of other network services is displayed, as in the following example.

Only enabled services are displayed.

Example response

```
Other Inet Services States
0 - dtspc       stream  /usr/dt/bin/dtspcd
1 - 100134/1    tli     /usr/lib/krb5/ktkt_warnd
2 - 100229/1-2  tli     /usr/sbin/rpc.metad
3 - 100230/1    tli     /usr/sbin/rpc.metamhd
4 - 100242/1    tli     /usr/sbin/rpc.metamedd
5 - 100424/1    tli     /usr/lib/ST/stfsloader
x - exit
select -
```

14 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.

You have completed this procedure.

—End—

Enabling non-secure network services

Application

This section describes the procedures to query the status of common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime).

Use this procedure to enable common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime). To disable a non-secure network service, refer to the procedure Disabling non-secure network services. To view the status of non-secure network services, refer to the procedure Querying the status of non-secure network services.

Prerequisites

This procedure requires you to have root user privileges.

For CBM users, refer to the following prerequisites section.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

For CBM 850, root user ID and password are not required. You can use your own user ID in step 1 in this procedure.

For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Establish a connection to the active server through telnet or SSH, and log in using the root user ID and password.

2 Navigate to the Security Services Configuration menu within the command line interface 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 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup 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 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

The procedure to enable non-secure network services is the same regardless of whether you are disabling common, tools, or other services. The following procedure shows the steps required for the common services (Common Inet Services in the menu), although it also applies to the Tools Inet Services and Other Inet Services menu options.

3 Enter the number next to the “Common Inet Services (ftp, tftp, telnet, snmp and nfs” option in the menu.

Example response

```
Common Inet Services (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query)
2 - enable_common_inetd (Enable a service registered in
inetd.conf)
3 - disable_common_inetd (Disable a service registered
in inetd.conf)
x - exit
select -
```

4 Enter the number next to the “Enable Common Inetd (Enable a service registered in inetd.conf)” option in the menu.

Example response

```
=== Executing "enable_common_inetd"
Common Inet Services States
0 - telnet      Disabled
1 - ftp         Enabled
2 - tftp        Enabled
3 - snmp        Enabled
4 - nfs_server  Enabled
5 - nfs_client  Enabled
Select service number to enable [0-5]:
```

5 Enter the number next to the network service you wish to enable.

Example response

```
Operating system control files updated.
Operating system deamon re-initialized on mate.
=== "enable_common_inetd" execution completed
```

An audit log of services enabled using this procedure is maintained and stored in the file /var/log/auditlog.

6 If you choose to enable other network services, return to step 3. To confirm the service has been enabled, refer to the procedure "Querying the status of non-secure network services".

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.

You have completed this procedure.

—End—

Disabling non-secure network services

Application

Use this procedure to disable common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime). To enable a non-secure network service, refer to the procedure Enabling non-secure network services. To view the status of non-secure network services, refer to the procedure Querying the status of non-secure network services.

Prerequisites

This procedure requires you to have root user privileges.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

d. When prompted, enter the root password.

e. Proceed to step 4

3 Log in to the SPFS-based server 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 IP address or host name of the SPFS-based client server.

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.

4 Navigate to the Security Services Configuration menu within the command line interface 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 - OAMP Configuration
4 - COBRA Configuration
```

```
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -
```

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

Example response

```
=== Executing "enable_common_inetd"
Common Inet Services States
0 - telnet      Disabled
1 - ftp         Enabled
2 - tftp        Enabled
3 - snmp        Enabled
4 - nfs_server  Enabled
5 - nfs_client  Enabled
Select service number to enable [0-5]:
```

The procedure to disable non-secure network services is the same regardless of whether you are disabling common, tools, or other services. The following procedure shows the steps required for the common services (Common Inet Services in the menu), although it also applies to the Tools Inet Services and Other Inet Services menu options.

5 Enter the number next to the “Common Inet Services (ftp, tftp, telnet, snmp and nfs” option in the menu.

Example response

```
Common Inet Services (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query)
2 - enable_common_inetd (Enable a service registered in
inetd.conf)
3 - disable_common_inetd (Disable a service registered
in inetd.conf)
x - exit
```

```
select -
```

6 Enter the number next to the “Disable Common Inetd (Disable a service registered in inetd.conf)” option in the menu.

Example response

```
=== Executing "disable_common_inetd"
Common Inet Services States
0 - telnet      Enabled
1 - ftp         Enabled
2 - tftp        Enabled
3 - snmp        Enabled
4 - nfs_server  Enabled
5 - nfs_client  Enabled
Select service number to enable [0-5]:
```

7 Enter the number next to the network service you wish to disable.

Example response

```
Warning.  This operation may affect other application(s
) or package(s) installed on the system.
There were no application/package registered for this
service.
Applications may still use this service without
registration.
Are you sure you want to proceed [yes/no]:
```

Disabling a network service takes effect immediately. Current sessions depending on the service are not affected, but all new sessions depending on the service will be rejected.

8 If you choose to abort disabling the network service, enter no at the prompt and return to step 5. If you choose to disable the selected service, enter yes at the prompt.

Example response

```
Operation confirmed by operator.  Log will be
generated.
Operating system control files updated.
Operating system daemon re-initialized on mate.
=== "disable_common_inetd" execution completed
```

An audit log of services disabled using this procedure is maintained and stored in the file /var/log/auditlog.

9 If you choose to disable other network services, return to step 5. To confirm the service has been disabled, refer to the procedure "Querying the status of non-secure network services".

10 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.

You have completed this procedure.

—End—

Querying users defined in proftpd

Application

Use this procedure to query the proftpd userlist and view their login group, default path, and password requirement.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Step **Action**

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

d. When prompted, enter the root password.

e. Proceed to step 4

3 Log in to the SPFS-based server 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 IP address or host name of the SPFS-based client server.

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.

4 Navigate to the Security Services Configuration menu within the command line interface as follows:

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 -
```

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

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
```

```
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -
```

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

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

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

Example response

```
proftpd User Configuration
1 - query_proftpd_users (Query users defined
in       proftpd
2 - add_proftpd_user  (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user )
4 - del_proftpd_user (Delete a given user
from       proftpd)
5 - query_user_registry  (Query the packages
registered for ftp users)
x - exit
```

```
select -
```

8 Enter the number next to the “query_protftpd_users (Query users defined in proftpd)” option in the menu.

Example response

```
== Executing "query_proftpd_users"
List of already defined users.
```

Userid	Groupid	Default_path	Passwd_Reqr
patcher	other	/data/npm/Au	on
certuser	maint	/export/home/certuser	off
anonymous	maint2	/data/swd	off
image	other	/var/opt/nortel/gwc	on

```
=== "query_proftpd_users" execution completed
```

Other procedures exist to manage the list of proftpd users, including:

- Adding a user to proftpd
- Adding the default GWC anonymous user to proftpd
- Deleting a user from proftpd
- Querying the packages registered for ftp users

9 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.

You have completed this procedure.

—End—

Adding a User to Proftpd

Application

Use this procedure to add and configure a user to proftpd.

Prerequisites

This procedure requires you to have root user privileges.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

d. When prompted, enter the root password.

e. Proceed to step 4

3 Log in to the SPFS-based server 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 IP address or host name of the SPFS-based client server.

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.

4 Navigate to the Security Services Configuration menu within the command line interface as follows:

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 -
```

5 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 Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
```

```
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -
```

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

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

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

Example response

```
proftpd User Configuration
1 - query_proftpd_users (Query users defined
in       proftpd
2 - add_proftpd_user  (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user )
4 - del_proftpd_user (Delete a given user
from       proftpd)
5 - query_user_registry  (Query the packages
registered for ftp users)
x - exit
select -
```

8 Enter the number next to the “add_proftpd_user (Add a user to proftpd)” option in the menu

Example response

```
== Executing "add_proftpd_users"
List of already defined users.
```

Userid	Groupid	Default_path	Passwd_Reqr
patcher	other	/data/npm/Au	on
certuser	maint	/export/home/certuser	off
anonymous	other	/var/opt/nortel/gwc	on
image	maint2	/data/swd	off

```
Please enter default user path (path must exists):
```

9 Enter the default path, such as **/tmp** at the prompt and press the Enter key.

Example response

```
Please enter user_id:
```

10 Enter the user ID, for example, **bloggsj** at the prompt and press the Enter key.

Example response

```
Please enter user_id:
```

11 Enter the user’s group ID, for example, **maint2** at the prompt and press the Enter key.

Example response

```
Are there aliased for user bloggsj
<aliases separated by space/enter for none>:
```

12 Enter any aliases for the user ID entered in step 10, separated by spaces. Press the enter key when you have finished entering aliases, or if none exist.

Example response

```
Is password required for bloggsj in group maint2 (y/n):
```

CAUTION

It is strongly recommended that a password be applied to all ftp accounts in order to comply with your relevant security policies and guidelines. Creating an ftp account without a password is the equivalent to creating an anonymous ftp account and should be avoided at all times.

13 Determine whether a password is required for this new user, and enter y or n appropriately followed by the Enter key.

Example response

```
User is defined locally or centrally
```

Example response

```
When a user does not exist on the system You need to
do:  useradd -g maint2 bloggsj
```

14 If example response 1 is shown (that is, the user is already defined locally or centrally), skip to step 16.

15 Enter **y** at the prompt to add the new user to the system (necessary prior to adding the proftpd account)

If you enter **n** at this prompt, the user may not have access until the account is defined.

16 Depending on whether you requested a password for this account in step 12, proceed as follows:

If	Do
you requested a password	step 17
you did not request a password	step 18

17 The system prompts you to enter the user's new password twice.

Example response

```
Enter user password:
Re-enter user password:
```

Enter the password twice, once at each prompt.

18 *Example response*

```
Is default path read only (y/n):
```

19 Determine whether to choose the default path to be read only, and enter **y** or **n** appropriately, followed by the Enter key.

Example response

```
Is default path write only (y/n):
```

20 Determine whether to choose the default path to be write only, and enter **y** or **n** appropriately, followed by the Enter key.

Example response

```
Is user allowed to change directory (y/n):
```

21 Determine whether to choose the user to be able to change directory to that other than the default directory and enter **y** or **n** appropriately, followed by the Enter key.

Example response

```
Is user allowed to create/delete dir (y/n):
```

22 Determine whether to choose the user to be able to create and delete directories and enter **y** or **n** appropriately, followed by the Enter key.

Example response

```
Is user allowed to delete files (y/n):
```

23 Determine whether to choose the user to be able to delete files and enter **y** or **n** appropriately, followed by the Enter key.

Example response

```
Is user allowed to rename files (y/n):
```

24 Determine whether to choose the user to be able to rename files and enter y or n appropriately, followed by the Enter key.

Example response

```
User attributes entered were:
UID:bloggsj  GID:maint2  Path:/tmp
Alias(es) for bloggsj:
File system attributes:
READonly:NO     WRITEonly:NO
CHANGEdir:NO   ADD/DEL_dir:NO
DEL_file:YES   RENAME_file:YES
Proceed with current user attributes (y/n):y
```

25 Confirm the summary of your request is correct, and proceed as follows:

If	Do
the information is not correct	step 26
the information is correct	step 29

26 Enter **n** at the prompt, and press the Enter key.

Example response

```
Do you want to re-enter the values (y/n):
```

27 If you choose to re-enter the values, enter y and press the Enter key. Return to step 9.

28 If you do not choose to re-enter the values, and instead choose to cancel the creation of this proftpd user account, enter n and press

the Enter key. Either return to step 8 to start again and add a different proftpd user account, or skip to step 31to end this procedure.

29 Enter y at the prompt, and press the Enter key. The system creates the proftpd user account.

Example response

```
=== "add_proftpd_user " execution completed
```

30 If you choose to add other proftpd user accounts, return to step 8.

31 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.

You have completed this procedure.

—End—

Adding the default GWC anonymous user to proftpd

Application

Use this procedure to add the default GWC anonymous user account to proftpd. The anonymous user account has the following configuration:

- username: anonymous
- Usergroup: maint2
- Default directory: /data/swd
- Require password: no
- File access: read only

Prerequisites

This procedure requires you to have root user privileges.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing
```
$ su - root
```
and pressing the Enter key.

d. When prompted, enter the root password.

e. Proceed to step 4.

3 Log in to the SPFS-based server using SSH (secure) as follows:

a. Log in to the server by typing
```
> ssh -1 root <server>
```
and pressing the Enter key.

where

server

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

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.

4 Navigate to the Security Services Configuration menu within the command line interface 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 -
```

5 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 Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -
```

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

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

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

Example response

```
Security User Configuration
1 - query_proftpd_users (Query users defined
in      proftpd)
2 - add_proftpd_user  (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user )
```

```
4 - del_proftpd_user (Delete a given user
from       proftpd)
5 - query_user_registry  (Query the packages
registered for ftp users)
x - exit
select -
```

8 Enter the number next to the “add_dflt_GWC_anonymous_user (Restore the GWC anonymous user)” option in the menu.

Example response

```
=== Executing "add_dflt_GWC_anonymous_user"
List of already defined users
```

Userid	Groupid	Default_path	Passwd_Reqr
patcher	other	/data/npm/Au	on
certuser	maint	/export/home/certuser	off
image	other	/var/opt/nortel/gwc	on

```
=== "add_dflt_GWC_anonymous_user" execution completed
```

9 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.

You have completed this procedure.

—End—

Deleting a user from proftpd

Application

Use this procedure to delete an existing user from proftpd.

Prerequisites

This procedure requires you to have root user privileges.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing
```
$ su - root
```
and pressing the Enter key.

d. When prompted, enter the root password.

e. Proceed to step 4.

3 Log in to the SPFS-based server using SSH (secure) as follows:

a. Log in to the server by typing
```
> ssh -1 root <server>
```
and pressing the Enter key.

where

server

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

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.

4 Navigate to the Security Services Configuration menu within the command line interface 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 -
```

5 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 Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
```

```
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -
```

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

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

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

Example response

```
Security User Configuration
1 - query_proftpd_users (Query users defined
in      proftpd)
2 - add_proftpd_user  (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user )
4 - del_proftpd_user (Delete a given user
from       proftpd)
5 - query_user_registry  (Query the packages
registered for ftp users)
x - exit
select -
```

8 Enter the number next to the “del_proftpd_user (Delete a given user from proftpd)” option in the menu.

Example response

```
=== Executing "del_proftpd_user"
List of already defined users
```

Userid	Groupid	Default_path	Passwd_Reqr
patcher	other	/data/npm/Au	on
certuser	maint	/export/home/certuser	off
anonymous	maint2	/data/swd	off
image	other	/var/opt/nortel/gwc	on

```
=== "add_dflt_GWC_anonymous_user" execution completed
```

9 Enter the userID of the user to be deleted from proftpd at the prompt, and press the Enter key.

Example response

```
Please enter group_id:
```

10 Enter the GroupID associated with the UserID you are deleting, and press the Enter key

Example response

```
Deleting ftp users may affect application(s) internal
or external to this server.
Are you sure you want to delete anonymous maint2 (y/n):
```

11 Confirm you wish to delete the selected user.

If	Do
you do not wish to delete the user	step 12
you wish to delete the user	step 13

12 At the prompt, enter **n**, and press the Enter key.

Example response

```
User delete aborted.
=== "del_proftpd_user" execution completed
```

Skip to step 14.

13 At the prompt, enter y to confirm you wish to delete the user, and press the Enter key.

Example response

```
Target user:  anonymous
Target group:  maint2
Preserved configuration file.
Updated configuration file.
```

```
Configuration successful.
Successfully deleted anonymous maint2.
```

14 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.

You have completed this procedure.

—End—

Querying the packages registered for ftp users

Application

Use this procedure to query the packages/applications registered for proftpd users.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the SPFS-based server using telnet (unsecure) as follows:

a. 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 SPFS-based server.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su - root
```
and pressing the Enter key.

d. When prompted, enter the root password.

e. Proceed to step 4.

3 Log in to the SPFS-based server using SSH (secure) as follows:

a. Log in to the server by typing
```
> ssh -1 root <server>
```
and pressing the Enter key.

where

server

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

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.

4 Navigate to the Security Services Configuration menu within the command line interface 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 -
```

5 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 Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
```

```
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -
```

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

Example response

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

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

Example response

```
Security User Configuration
1 - query_proftpd_users (Query users defined
in      proftpd)
2 - add_proftpd_user  (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user )
4 - del_proftpd_user (Delete a given user
from       proftpd)
5 - query_user_registry  (Query the packages
registered for ftp users)
x - exit
select -
```

8 Enter the number next to the “query_user_regsitry (Query the packages registered for ftp users)” option in the menu.

Example response

```
=== Executing "query_user_registry"
Package(s) registered for ftp user(s)
Table may be empty if no package has registered.

  Userid          Groupid         Package
  anonymous       maint2          BootP GWC loader


=== "add_dflt_GWC_anonymous_user" execution completed
```

9 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.

You have completed this procedure.

—End—

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.

Prerequisites

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

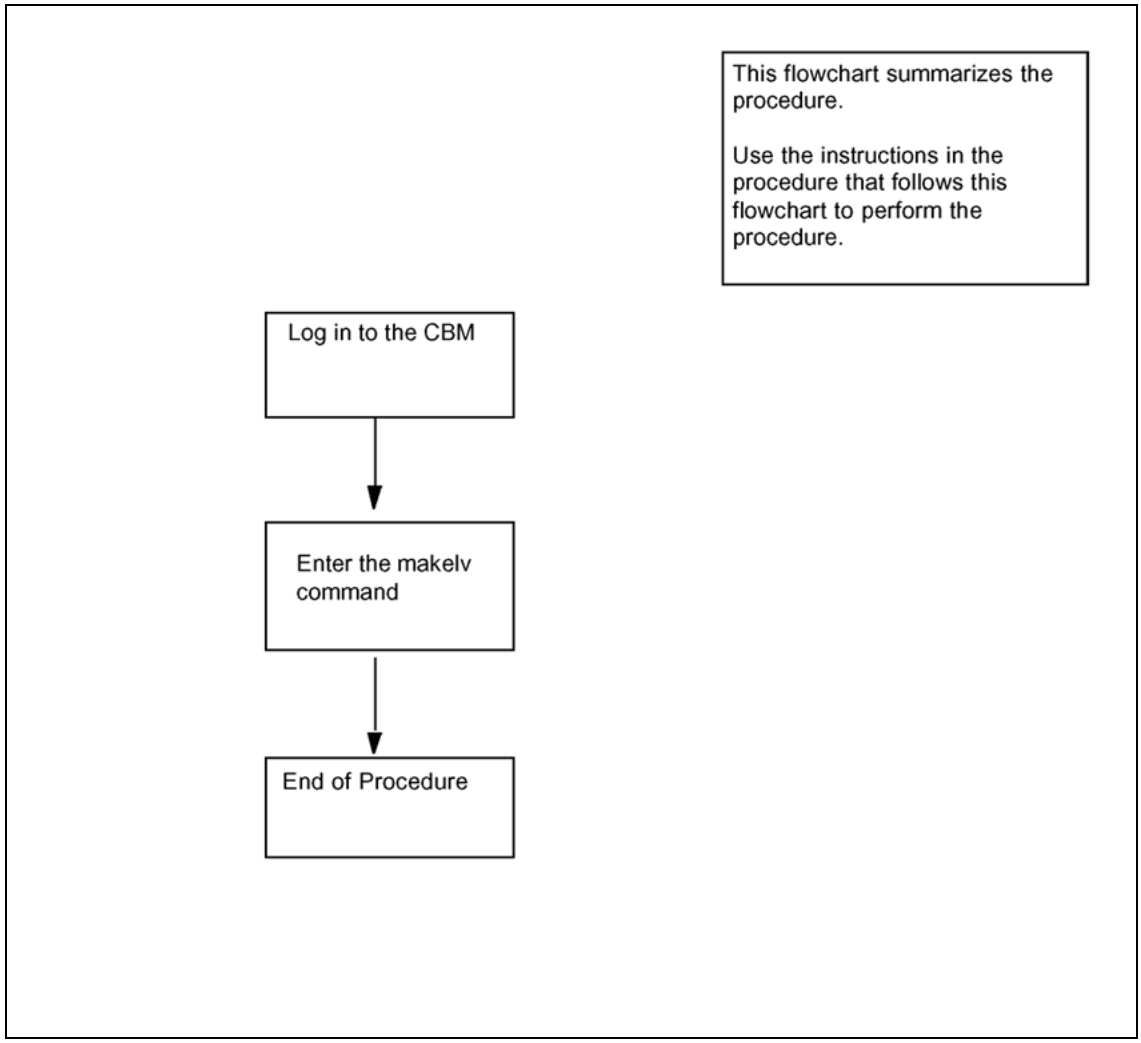
For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure
Logging in to the CBM
Requesting non-restricted shell access
Displaying actions a role group is authorized to perform

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



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

Step	Action

At the local or remote VT100 terminal

1

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

2 Log in to the core manager as a user authorized to perform config-admin actions.

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.

—End—

Preparing a DVD-RW for use

Application

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

Prerequisites for Core and Billing Manager 850

All users with non-restricted shell access are authorized to perform this procedure.

You require root-user access, or must be a user in a role group authorized to perform config-admin actions, if an error occurs when ejecting a DVD.

For more information about how to log in to the CBM as an authorized user, how to request non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration for GSM/UMTS, NN20000-321*
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration for GSM/UMTS, NN20000-321*
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration for GSM/UMTS, NN20000-321*

Action

Perform the following steps to complete this procedure.

Step	Action

At the server

1 Insert the DVD into the drive.

Only rewriteable media can be erased. Verify that the DVD you are attempting to erase is a 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 SPFS-based server

3 When prompted, enter your user ID and password.

4 Use the following table to determine your next step.

If the DVD is	Do
new	step 5
used	step 6

5 Verify the DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates "No CD writers found or no media in the drive"	step 6

6 Erase the contents of the DVD by typing

```
$ cdrw -b all
```

and pressing the Enter key

ATTENTION

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 Reinsert the DVD into the drive.

8 Verify the DVD is ready for use by typing

```
$ cdrw -l
```

and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates "No CD writers found or no media in the drive" or "Media in the device is not erasable"	step 9

9 Eject the DVD 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 DVD 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, re-try the "eject cdrom" command.

c. Remove the DVD from the drive.

10 Obtain another DVD and repeat the process starting with step 4.

11 Proceed to use the DVD.

You have completed this procedure.

—End—

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

Application

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

- "Simplex configuration (one server)" (page 56)
- "High-availability configuration (two servers)" (page 59)

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

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

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 procedures Performing a backup of oracle data on an SPFS-based server and Performing a backup of file systems on an SPFS-based server if required.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

Step	Action

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. You may log on as root or emsadm.

3 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 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS 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_uti’" option in the menu.

Example response

```
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d2         3.9G   1.6G   2.3G    42%    /
/proc                    0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
fd                       0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8         2.0G    86M   1.8G     5%    /var
swap                   2.5G   160K   2.5G     1%    /var/run
swap                   512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11        4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21        2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22        5.9G   145M   5.7G     3%    /var/mysql/data
/backup                3.9G   4.0M   3.9G     1%    /backup
/data                  2.9G   5.9M   2.9G     1%    /data
/data/oradata          9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch     963M    12M   893M     2%    /data/oradata/arch
/data/qca              9.8G    10M   9.7G     1%    /data/qca
```

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

4 Note the file system you want to increase, as well as its current size (under column ’size’).

5 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.

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.

6 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 “data/oradata” file system, subtract its current size, 10337 MB from the desired size, for example, 15000 MB. You would increase the size of the “data/oradata” file system by 4662786 KB, or 4663 MB.

7 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

```
# /opt/nortel/sspfs/fs/meta.pl free_space
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine 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 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 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 9 a (amount of free disk space you can allocate to file systems)	step 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.

8 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
```

The preceding example increases the '/data' file system by 512 megabytes (MB).

You have completed this procedure.

—End—

ATTENTION

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

High-availability configuration (two servers)

Step Action

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

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.

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

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 - SPFS_soft (Display Software
      Installation Level Of SPFS)
  2 - chk_SPFS (Check SPFS 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

```
Filesystem            size   used  avail capacity  Mounted on
/dev/md/dsk/d2        3.9G   1.6G   2.3G    42%    /
/proc                   0K     0K     0K     0%    /proc
mnttab                  0K     0K     0K     0%    /etc/mnttab
fd                      0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d8        2.0G    86M   1.8G     5%    /var
swap                  2.5G   160K   2.5G     1%    /var/run
swap                  512M   3.8M   508M     1%    /tmp
/dev/md/dsk/d11       4.9G   1.5G   3.4G    32%    /opt
/dev/md/dsk/d21       2.9G   111M   2.8G     4%    /opt/nortel
/dev/md/dsk/d22       5.9G   145M   5.7G     3%    /var/mysql/data
/backup               3.9G   4.0M   3.9G     1%    /backup
/data                 2.9G   5.9M   2.9G     1%    /data
/data/oradata         9.8G   2.5G   7.3G    26%    /data/oradata
/data/oradata/arch    963M    12M   893M     2%    /data/oradata/arch
/data/qca             9.8G    10M   9.7G     1%    /data/qca
```

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 'size').

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.

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.

12 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, 123 MB from the desired size, for example, 256 MB. You would increase the size of the 'qca' file system by 133153 KB, or 133 MB.

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

```
# /opt/nortel/sspfs/fs/meta.pl fs

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

and pressing the Enter key.

Divide the resulting number by 2048 to determine 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 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 13 a (amount of free disk space you can allocate to file systems)	contact Nortel 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 13 a (amount of free disk space you can allocate to file systems)	step 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.

14 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
```

The preceding example increases the '/data/qca' file system by 10 megabytes (MB).

15 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 16
otherwise	repeat step 15 until the file systems are "STANDBY normal UP clean".

16 Reboot the Inactive node by typing

```
# init 6
```

and pressing the Enter key.

Wait for the unit to recover before proceeding.

17 Perform a swact on the active unit by typing

```
# swact
```

and pressing the Enter key.

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

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.

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 *ClusterIndicator*ACT, which indicates you are on the Active server.

22 Verify all applications are running on the active node by typing

```
# servquery -status all
```

and pressing the Enter key.

Verify all applications are running.

23 Verify all replicated file systems are "active up normal" by typing

```
# udstat
```

and press the Enter key.

Ensure all file systems are in the "active up normal" state.

24 Clone the other node using procedure "Cloning the image of one server in a cluster to the other server", ensuring you log into the active node.

You have completed this procedure.

—End—

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)

  Under any of the previous 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.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

  Note: The root user ID and password are not required in steps 2c, 2d, 3 and 18. The user can use their own ID and execute the procedure.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Perform the following steps to complete this procedure.

ATTENTION
Perform the steps that follow on the active server.

Step Action

At your workstation

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

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the physical IP address of the active server

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d. When prompted, enter the root password.

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.

Proceed to step 4.

3 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 active server

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.

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.

On the active server

4 Access the command line interface to determine the server profile by typing

```
# cli
```

and pressing the Enter key.

Example response

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

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

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SPFS)
 2 - chk_sspfs (Check SPFS 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 -
```

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

Example response

```
=== Executing "sspfs_soft"
SPFS version:  09.0 Build:  200508421 Server
Profile:  cbm850
==="sspfs_soft" completed successfully
```

7 Note the server profile.

8 Exit the CLI by typing **x** until you return to the command prompt.

9 Use the following table to determine your next step.

If	Do
the Server Profile is cbm850	step 16
otherwise	step 10

10 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
```

11 Use the following table to determine your next step.

If	Do
all applications are running	step 14
otherwise	step 12

12 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

13 Use the following table to determine your next step.

If	Do
all applications started	step 14
otherwise	contact your next level of support

14 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 16
otherwise	step 15

15 Start the PSE server application by typing

pse start

and pressing the Enter key.

If	Do
PSE starts	step 16
otherwise	contact your next level of support

16 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 you executed a reverse restore (that is, switched unit 0 and unit 1) Under any of the previous 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 17
otherwise	step 21

17 Use the following table to determine your next step.

If	Do
you do not know the Ethernet address of the inactive server	step 18
otherwise	step 19

At the console connected to the inactive server

18 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

19 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

20 Proceed to step 22

On the active server

21 Start the cloning process on the active server by typing

startb

and press the Enter key.

22 Use the following table to determine your next step.

If	Do
the system prompts you to enter the command "boot net - image"	step step 86
otherwise	step 27

23 Connect to the console port of the inactive server.

If the console displays the	Do
login prompt	step 24
OK prompt	step 26

At the console connected to the inactive server

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

25 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

26 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.

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 the active server

27 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):/>
```

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

On the active server

29 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 30
otherwise	contact your next level of support

At your workstation

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

If using	Do
telnet (unsecure)	step 31
ssh (secure)	step 36

31 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

32 When prompted, enter your user ID and password.

33 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

34 When prompted, enter the root password.

35 Proceed to step 41.

36 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

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.

37 When prompted, enter the root password.

On the inactive server

38 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 39
otherwise	contact your next level of support

39 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Adding or removing a program to or from access to all CBM users

Application

Use this procedure to add or remove a program from all CBM users' access.

Prerequisites

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

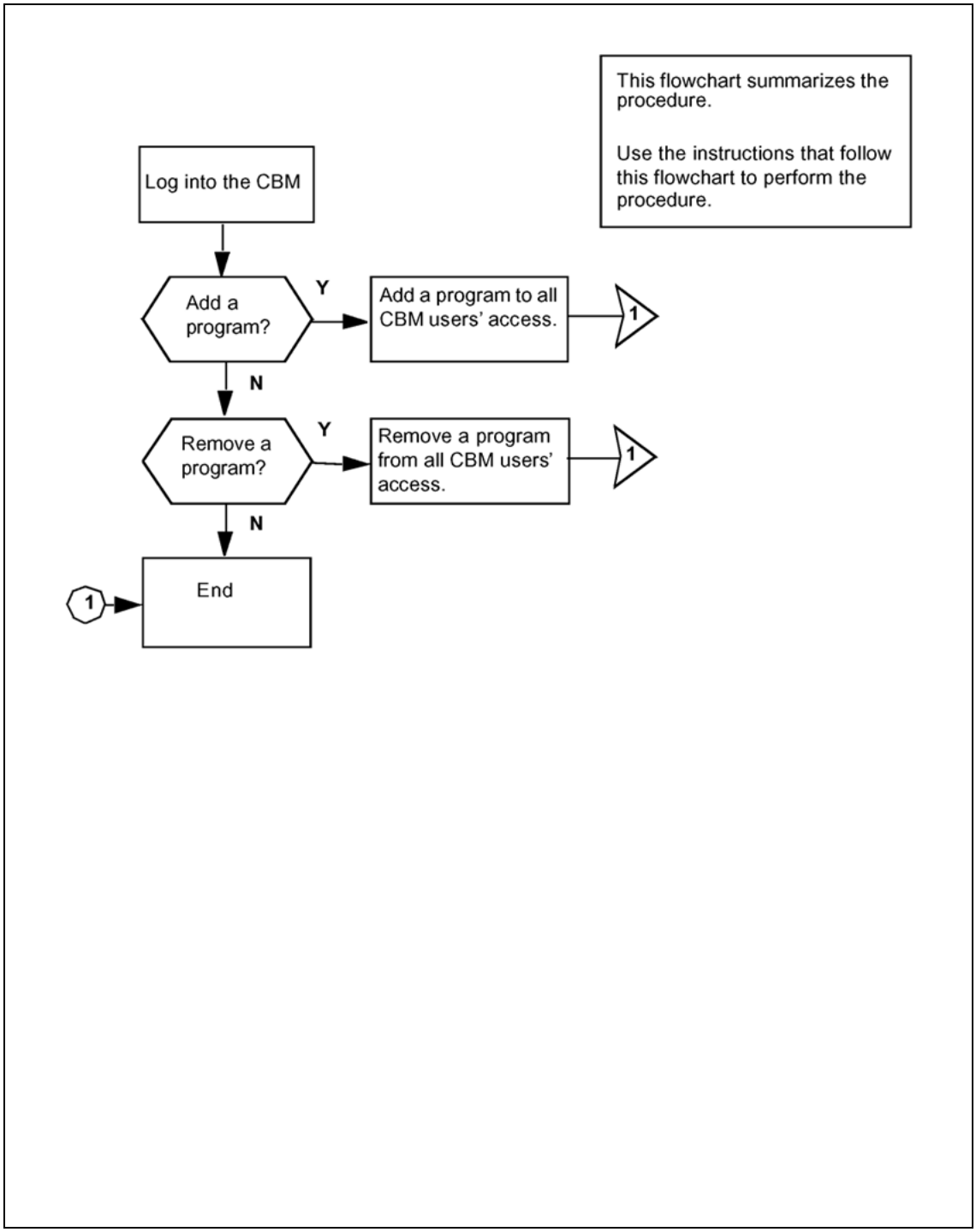
For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Procedure
Logging in to the CBM
Requesting non-restricted shell access
Displaying actions a role group is authorized to perform

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 all CBM users access



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 all CBM users access

Step	Action

At the local or remote VT100 console

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

a. using telnet, by typing:

```
telnet <IP address>
```

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

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

and pressing the Enter key.

where

`<userID>` is the user ID of the user
`IP address` is the IP address of the CBM

2 When prompted, enter the user's password.

3 Use the following table to determine your next step.

If you want to	Do
add a third party program to all CBM users' access	step 4
remove a third party program from all CBM users' access	step 5

4 Add a third party program to all CBM 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

The full path is required for the program name.

5 Remove a third party program from all CBM users' access by typing

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

and pressing the Enter key.

where

`program name` is the name used in the CBM user's restrict shell

6 You have completed this procedure.

—End—

Connecting to the CM passthru

Application

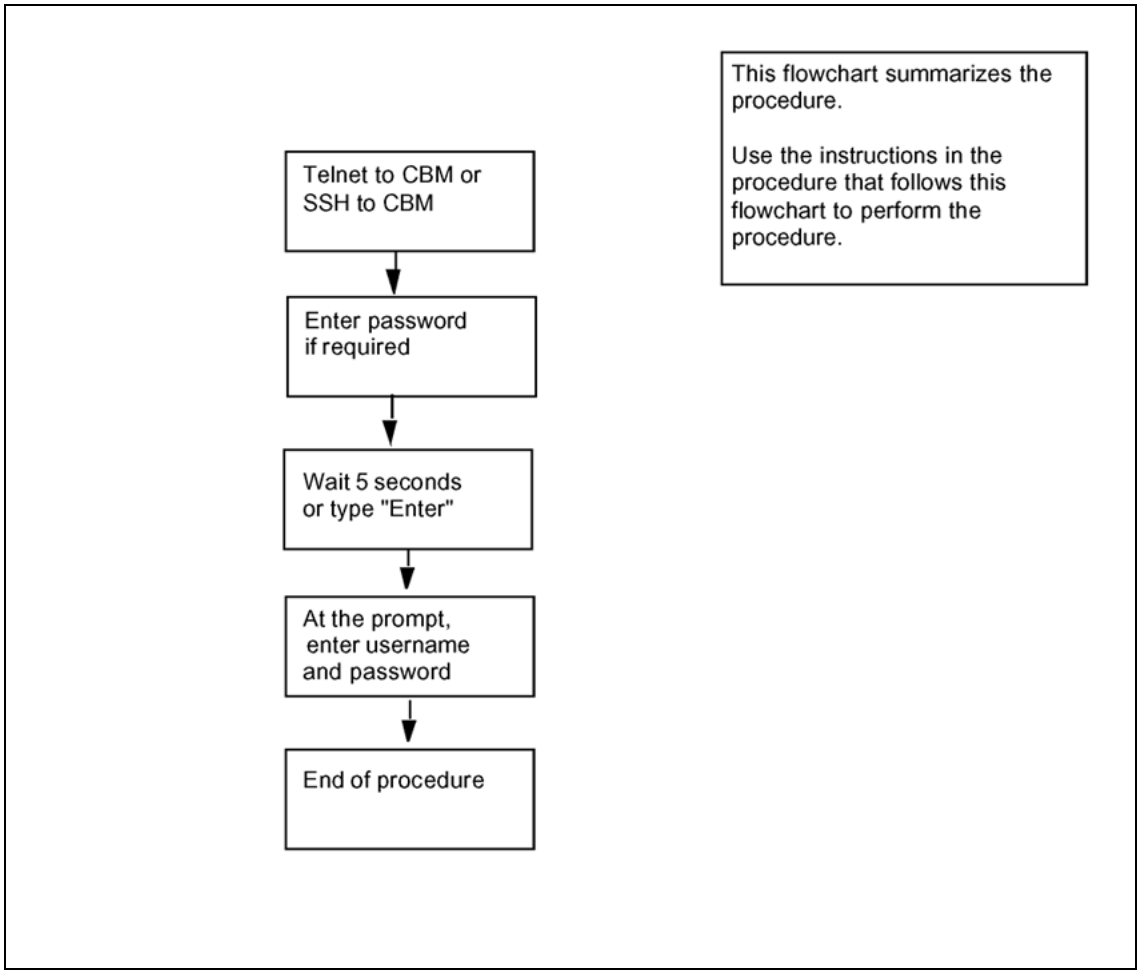
Use this procedure to access the CM through the CBM as a passthru user.

To configure a passthru user, use procedure Adding or removing a passthru user 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



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

Step	Action

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 address>` is the IP address of the CBM.

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

The following response is only displayed when the passthru 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.

—End—

Adding or removing a passthru user

Application

Use this procedure to add or remove a passthru user.

Prerequisites

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

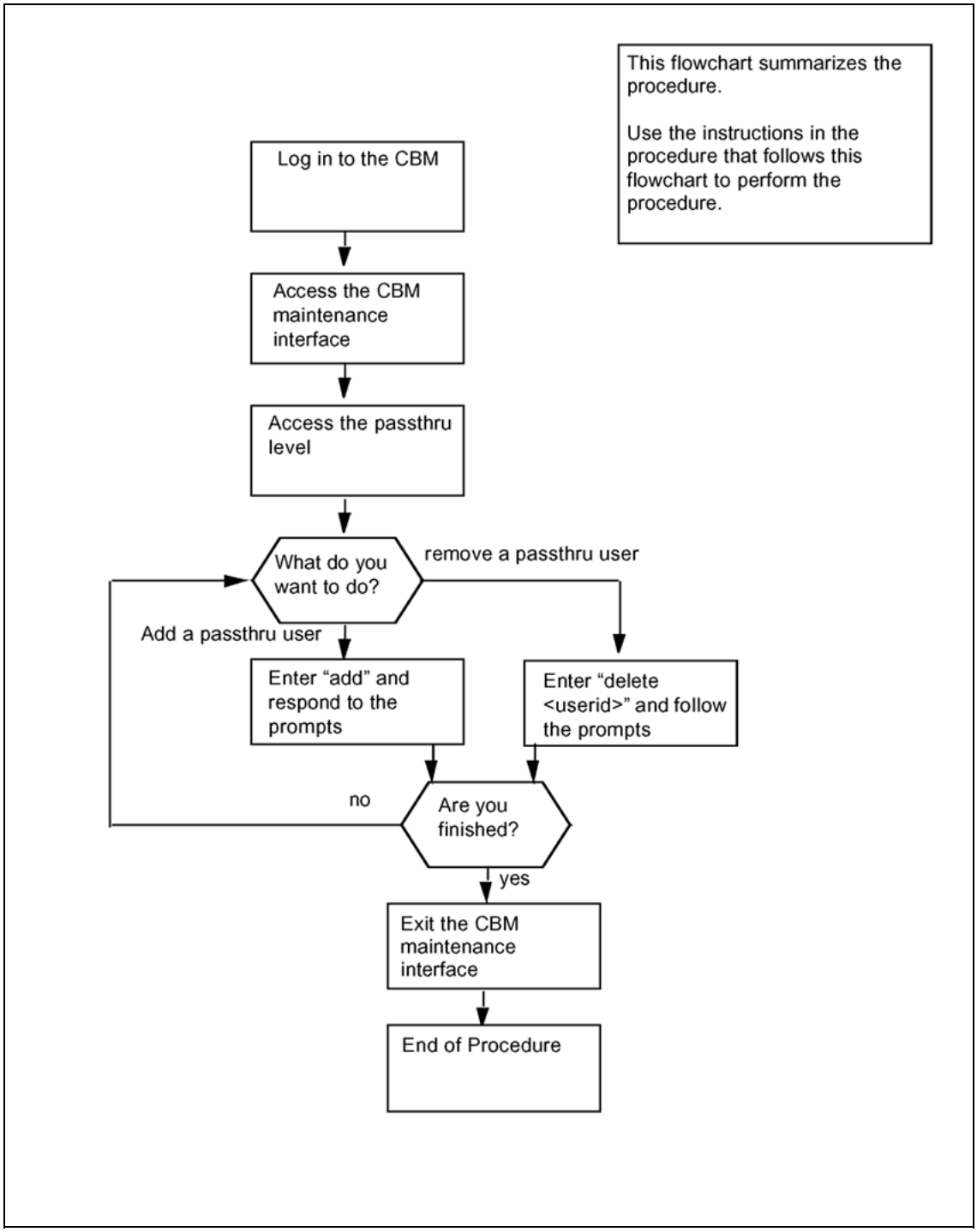
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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.

ATTENTION

Use the SSH client, not telnet, to initiate a passthru session if the user account is configured as "no password" to maintain its "no password" status. Otherwise, the system will prompt the user to enter a new password and the user must supply the password in the subsequent login. This is required from the default system level configuration.

Adding or removing a passthru user

Step	Action

At the CBM

1 Log in to the core manager as a user authorized to perform security-admin actions.

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.

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.

Type "cm" for the Core passthru.

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

If you choose the "no password required" option and login using telnet, the system will force you to add one by prompting you for a new password during the first login. By default the system level configuration will not permit a telnet login without a password and this requirement is not specific to passthru users. To maintain "no password" status, you must use the SSH client to login to the CBM as passthru user.

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

Response:

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

If	Do
Y	go to step 11 if "passwd required" for the user. go to step 15 if "no password required" for the user.
N	go to step 15
E	go to step 6

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.

—End—

Setting up local user accounts on an SPFS-Based Server

Application

Use this procedure to add local user accounts on a 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" (page 92).

If you choose to centrally manage your user accounts, refer to procedure "Adding new users" in *IEMS Security and Administration* (NN10336-611).

If you want to launch the ping and traceroute operations that are performed remotely on SPFS-based platforms from a centralized GUI on Integrated Element Management System (IEMS), refer to procedures "Running a ping test on the GWC network element or SPFS platform" and "Running a traceroute test on the GWC network element or SPFS platform" in *IEMS Basics* (NN10329-111).

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other 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.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action
	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 SSFPS-based server

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 -
```

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 -d /export/home/<userid> -g succssn -G
<any additional groups> -m <userid>
```

and press 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 press 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.

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" (page 92)) 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

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.

—End—

Additional information

Users of the Nortel 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 following table, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm	secadm
trkrw	lnrw	mgcrw	mgrw	emsrw	secrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov	secmtc
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc	secro
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 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.
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:

The mappings of commands to secondary user groups in the tables in this section do not apply to Multiservice Data Manager (MDM) when installed on a SPFS-based server.

Node provisioning operations

Command	User group				
	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

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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			

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
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

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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
addMPGroup	x	x			
changeMPGroup	x	x			
queryMPGroup	x	x	x	x	x
deleteMPGroup	x	x			
addVPN	x	x			
deleteVPN	x	x			
queryVPN	x	x	x	x	x

Trunk provisioning operations

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

Trunk maintenance operations

Command	User group				
	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	

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
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
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			

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

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View signalling characteristic profile, update list (V5 Sig)					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	x				

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
smartimage from the NPM GUI or CLUI					
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

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

Ping and traceroute operations

Command	User group		
	emsadm	emsrw	emsmtc

Launch remote ping	x	x	x
Launch remote traceroute	x	x	x
These operations are for remote operations performed on SPFS platforms but launched from a centralized GUI on IEMS.			

Node provisioning operations

Command	User group				
	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

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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			

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact (refer to the notes that follow this table)			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

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
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

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

Trunk maintenance operations

Command	User group				
	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

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set Auto Refresh					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 15000 Manager GUI		x			

Automated upgrade operations

Command	User group									
	emsadm	emsrw	emsmtc	emssprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

Transferring files as a passthru user using FTPProxy

Purpose

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.

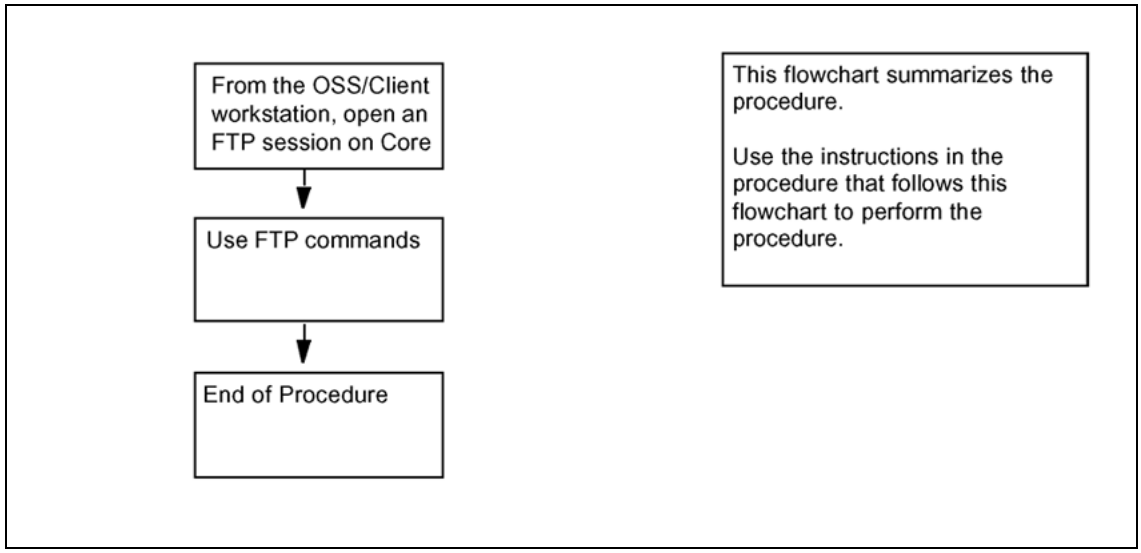
Application

If you have core user privileges (mgcadm, mgcrw, mgcsprov, mgcmtce, and mgcro), refer to "Transferring files as a core user using FTPProxy" (page 125) in this document.

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 as a passthru user using FTPProxy



Transferring files as a passthru user using FTPProxy

Step	Action
	At the OSS/Client workstation
1	Open an FTP session to the CBM: `> ftp <IP_address>` where `<IP_address>` is the IP address of the CBM.

2 At the prompt, enter your passthru userID.

3 At the prompt, enter your passthru password.

The FTPProxy application authenticates your userID and password and logs you in to the Core.

4 Use the commands in the table to transfer files.

If you want to	At the ftp> prompt, enter the following command
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	ls
	dir
view the current directory on the core	pwd
log out of the ftp session	bye

5 You have completed this procedure.

—End—

Configuring an SPFS-based central security client

Application

Use this procedure to configure an SPFS-based central security client to use the Nortel 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 184.

In the event you want to reconfigure the central security client to use a new Nortel central security server IP, perform steps 1, 3 and step 5 of this procedure.

Prerequisites

This procedure has the following prerequisites:

- the central security server is already configured and activated in the network (see Section "CNM centralized authentication and single sign on" in NN10300-031 Nortel Network Management Systems Security if required).
- The SSL should be turned on on the central security server (see the Section "Enabling SSL on the primary main server" in NN10300-031 Nortel Network Management Systems Security if required).
- perform this procedure on each SPFS-based server that is not the central security server to activate centralized security
- You must be a user in a role group authorized to perform config-admin actions
- You must obtain non-restricted shell access
- You must have the root userID and password to complete step 5 and Step 5d of this procedure.

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

Procedure	Document
Logging in to the CBM	Logging in to the CBM
Displaying actions a role group is authorized to perform	Displaying actions a role group is authorized to perform

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Configure the Nortel central 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 - OAMP Application Configuration
 4 - CORBA Configuration
  5 - IP Configuration
 6 - DNS Configuration
  7 - Syslog Configuration
 8 - Remote Backup Configuration
 9 - Database Configuration
10 - NFS Configuration
 11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
 16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup 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 - Security Server Location Configuration
 3 - PAM Configuration
x - exit
select -
```

d. Enter the number next to the "Security Server Location Configuration" option in the menu.

Example response

```
Security Server Location Configuration
1 - security-server_ip (Configure Server IP)
x - exit
select -
```

e. Enter the number next to the "security-server_ip" option in the menu.

Example response

```
===Executing "security-server_ip"
Enter the Server IP Address (default 45.12.23.56):
```

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

Example response

```
Enter the Server Fully Qualified Domain Name
(default
:test3security-serve.us.nortel.com):
```

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

Example response

```
IP: 45.12.23.56
Fully Qualified Domain
Name:test3security-server.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

```
=== "security-server_ip" completed successfully
```

i. Return to the Security Services Configuration menu, by typing

select - x

and pressing the Enter key.

Response

2

```
Security Services Configuration
  1 - Socks Configuration
 2 - Security 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
IP: 45.12.23.56
Fully Qualified Domain Name:
test3security-server.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 timeout (time to wait for a RADIUS response from 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):
```

f. 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):
```

g. 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 **
Security Server IP: 45.12.23.56
Server Domain Name:  test3security-server.us.norte
l.com
Shared Secret:  nortelnetworks
Radius Client Timeout:  12
SAML Connection Timeout:  20
SAML Request Timeout:  10
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

h. 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 Security Server
Restarting name service daemon
==="pam_radius" completed successfully
```

i. 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.

j. 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 preceding step 3b:

a. enter the number next to the "saml_passwd_conf (Configure saml password)" option

b. when prompted, enter the default SAML password (s1isamadmin) or a new password you have chosen:

Example response

```
** Confirm Settings **
SAML Password:  s1isamadmin
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 To add a security server to the host, complete the following:

a. Change to the root user by typing:

```
$ su - root
```

and pressing the Enter key.

b. When prompted, enter the root password.

c. enter the command:

```
# /sdm/saml/nss/addSecurityServerToHost
```

d. when prompted, press enter to accept default values or enter required values. Type ok to confirm.

```
Enter Server IP Address (default:  192.151.33.186):
Enter Fully Qualified Domain Name(default:
server1.thecompany.com):
Central Security Server IP:
192.151.33.186
Central Security Server Fully Qualified Domain
Name:     server1.thecompany.com
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok
```

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

It is recommended to migrate all user accounts that exist on 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.

If the central security administration application is a third-party application and not the Nortel central security server, follow the procedures in the third party documentation.

To migrate Core Manager user accounts to the Nortel central security server, refer to Migrating core manager user accounts to the Nortel central security server.

a. If the central administration system is the Nortel central security server, launch the Security Administration tool of the Nortel central security server, and add the user accounts plus any additional required user groups you want to centrally manage.

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

   Log in to the central security client (for example, CBM) by typing

   `> telnet <server>`

   and pressing the Enter key.

   where

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

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

—End—

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.

For a procedure used to configure IPSec and IKE on the OSS (Solaris 5.9 machine), see Configuring IPSec and IKE on the OSS.

Prerequisites

You must be a root user to execute this procedure.

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 following procedures, 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 following procedures are performed.

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" (page 122)
"Removing IPSec from the CBM 850" (page 123)

Configuring IPSec on the CBM 850

Step	Action
	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 an SPFS-based server on page 281

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 an SPFS-based server on page 281

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 278

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

6 You have completed this procedure.

—End—

Removing IPSec from the CBM 850

Step	Action
	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 an SPFS-based server on page 281
3	Delete the IKE rule corresponding to the IPSec rule that you deleted in step 2, using the procedure Configuring IPSec and IKE on an SPFS-based server on page 281
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 278
5	Reactivate the outbound file transfer schedules that you deactivated in step 1.
6	You have completed this procedure.

—End—

Transferring files as a core user using FTPProxy

Application

This procedure can be performed by all users.

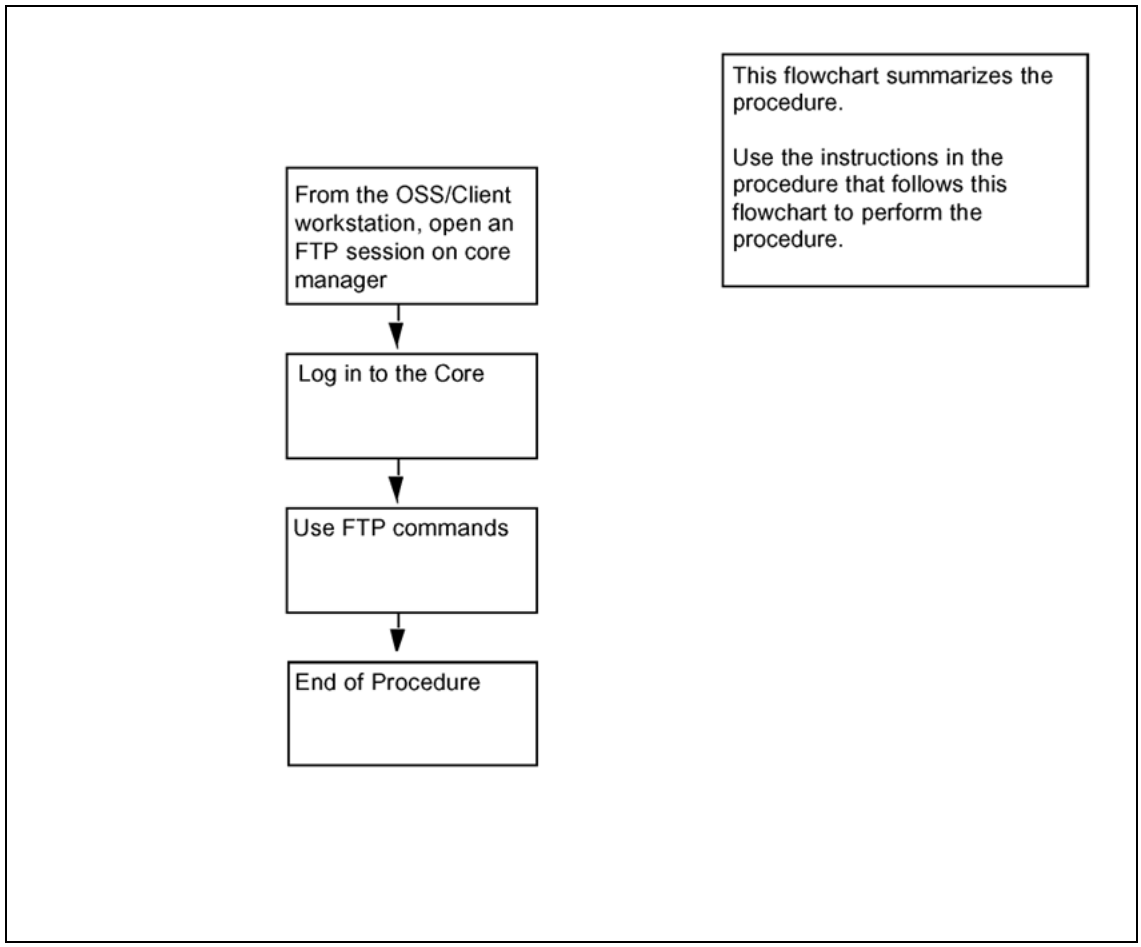
Use this procedure to transfer files between the OSS machine and the Core using the FTPProxy application. Use this procedure if you have core user privileges. Core user privileges include mgcadm, mgcrw, mgcsprov, mgcmtce, and mgcro.

If you have passthru user privileges, refer to "Transferring files as a passthru user using FTPProxy" (page 112) 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



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

Step	Action

At the OSS/Client workstation

1 Open an FTP session 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
view the current directory on the core	pwd
log out of the ftp session	bye

4 You have completed this procedure.

—End—

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.

CBM 850 Core Manager Configuration Management, NN10353-511

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

Prerequisites

All users are authorized to perform this procedure.

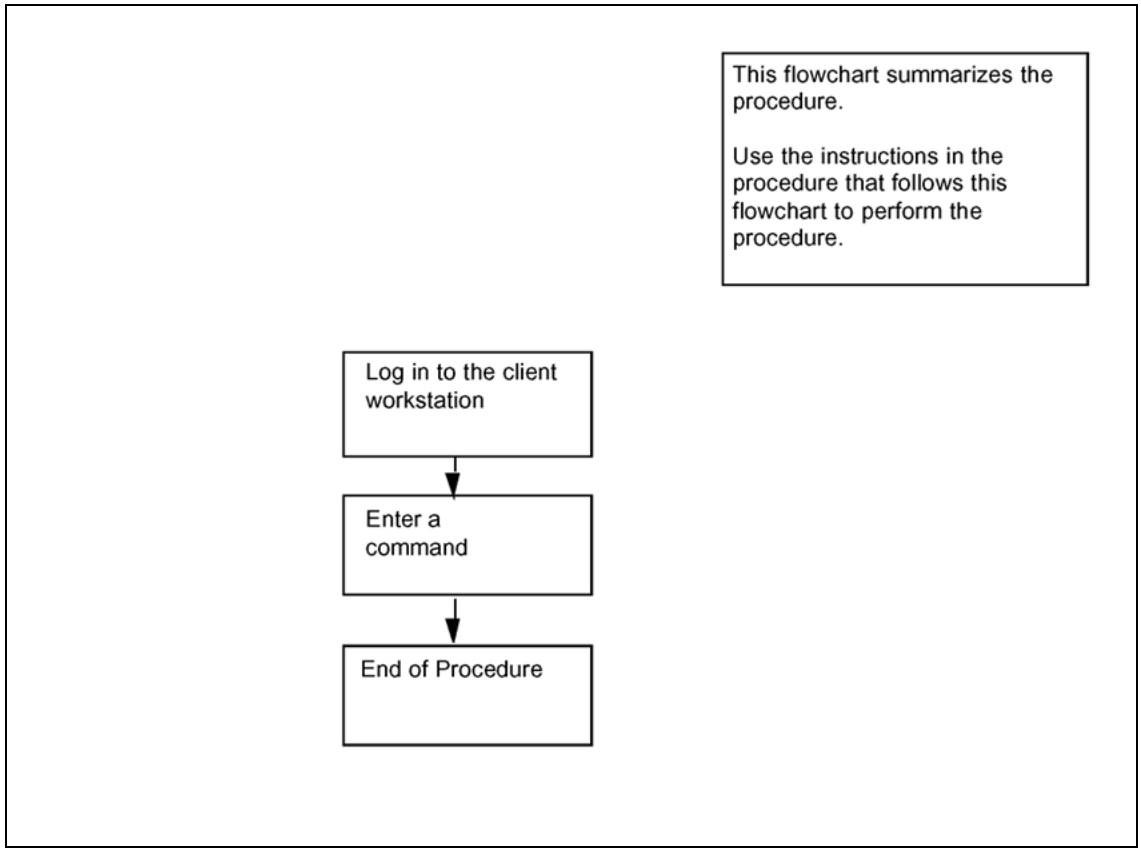
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

Action

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

Summary of starting an SCFT client session



Starting an SCFT client session

Step	Action

At the client workstation

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

- "Displaying help for SCFT" (page 146)
- Listing volumes on Core using SCFT
- Removing a file from Core using SCFT
- Transferring files from Core using SCFT
- Transferring files to Core using SCFT

2 You have completed this procedure.

—End—

Transferring files from Core using SCFT

Purpose

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

Prerequisites

All users are authorized to perform this procedure.

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

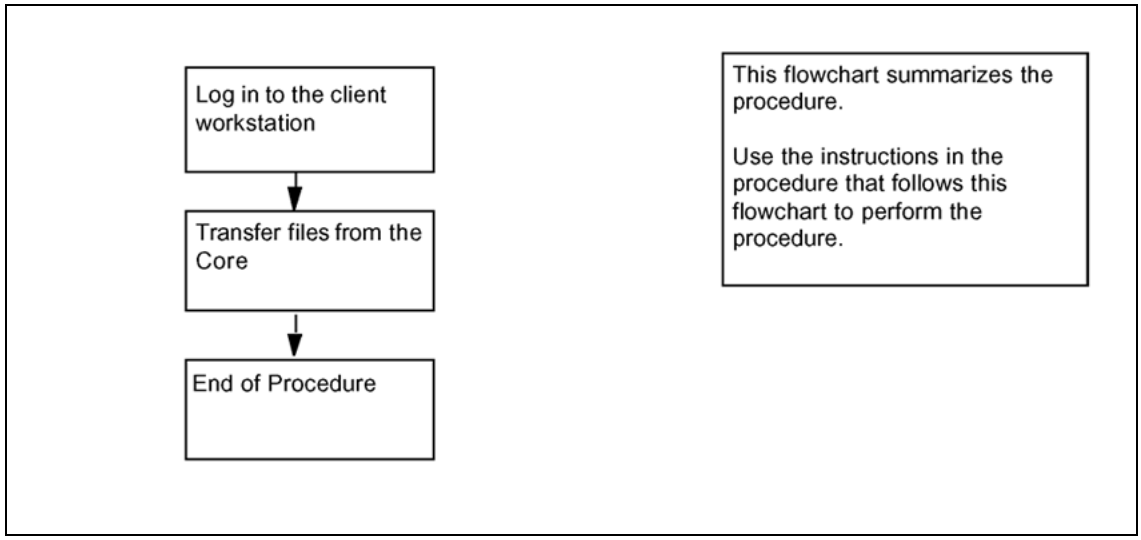
Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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

Procedure

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

Summary of transferring files from core using SCFT



Transferring files from core using SCFT

Step	Action

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

where

<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

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

where

<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 -a -s 1024 alex@host1:/sfdev/file1 /localdir/loc
alfile
```

Example response:

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

5 You have completed this procedure.

—End—

Transferring files to Core using SCFT

Purpose

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

Prerequisites

All users are authorized to perform this procedure.

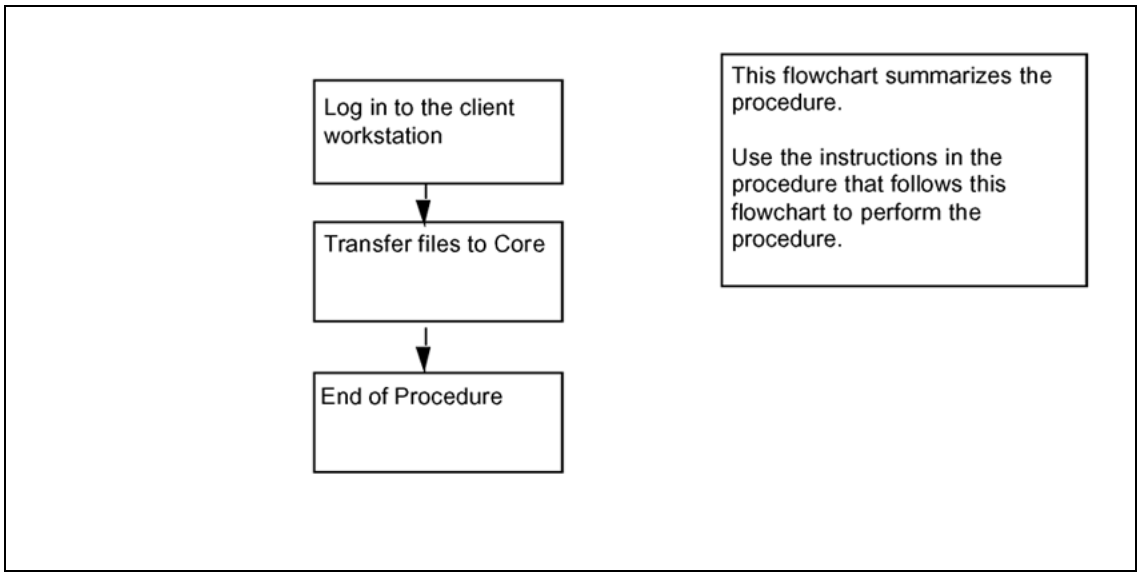
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action

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

where

<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

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> < -sreclen><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

where

<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.

—End—

Configuring an SPFS-based central security client

Application

Use this procedure to configure an SPFS-based central security client to use the Nortel central security server.

In the event you want to reconfigure the central security client to use a new Nortel central security server IP, perform steps 1, 3 and 5 of this procedure.

Prerequisites

This procedure has the following prerequisites:

- the central security server is already configured and activated in the network (see Section "CNM centralized authentication and single sign on" in NN10300-031 Nortel Network Management Systems Security if required).
- The SSL should be turned on on the central security server (see the Section "Enabling SSL on the primary main server" in NN10300-031 Nortel Network Management Systems Security if required).
- perform this procedure on each SPFS-based server that is not the central security server to activate centralized security
- You must be a user in a role group authorized to perform config-admin actions
- You must obtain non-restricted shell access
- You must have the root userID and password to complete 5 and Step 5 d of this procedure.

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

Procedure	Document
Logging in to the CBM	Logging in to the CBM
Displaying actions a role group is authorized to perform	Displaying actions a role group is authorized to perform

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation

1 Configure the Nortel central 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 - OAMP Application Configuration
 4 - CORBA Configuration
  5 - IP Configuration
 6 - DNS Configuration
  7 - Syslog Configuration
 8 - Remote Backup Configuration
 9 - Database Configuration
10 - NFS Configuration
 11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
 16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup 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 - Security Server Location Configuration
 3 - PAM Configuration
x - exit
select -
```

d. Enter the number next to the "Security Server Location Configuration" option in the menu.

Example response

```
Security Server Location Configuration
1 - security-server_ip (Configure Server IP)
x - exit
select -
```

e. Enter the number next to the "security-server_ip" option in the menu.

Example response

```
===Executing "security-server_ip"
Enter the Server IP Address (default 45.12.23.56):
```

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

Example response

```
Enter the Server Fully Qualified Domain Name
(default
:test3security-serve.us.nortel.com):
```

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

Example response

```
IP: 45.12.23.56
Fully Qualified Domain
Name:test3security-server.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

```
=== "security-server_ip" completed successfully
```

i. Return to the Security Services Configuration menu, by typing

`select - x`

and pressing the Enter key.

Response

2

```
Security Services Configuration
  1 - Socks Configuration
 2 - Security 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
IP: 45.12.23.56
Fully Qualified Domain Name:
test3security-server.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 timeout (time to wait for a RADIUS response from 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):
```

f. 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):
```

g. 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 **
Security Server IP: 45.12.23.56
Server Domain Name:  test3security-server.us.norte
l.com
Shared Secret:  nortelnetworks
Radius Client Timeout:  12
SAML Connection Timeout:  20
SAML Request Timeout:  10
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

h. 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 Security Server
Restarting name service daemon
==="pam_radius" completed successfully
```

i. 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.

j. 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 preceding step 3b:

a. enter the number next to the "saml_passwd_conf (Configure saml password)" option

b. when prompted, enter the default SAML password (s1isamadmin) or a new password you have chosen:

Example response

```
** Confirm Settings **
SAML Password:  s1isamadmin
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 To add a security server to the host, complete the following:

a. Change to the root user by typing:

```
$ su - root
```

and pressing the Enter key.

b. When prompted, enter the root password.

c. enter the command:

```
# /sdm/saml/nss/addSecurityServerToHost
```

d. when prompted, press enter to accept default values or enter required values. Type ok to confirm.

```
Enter Server IP Address (default:  192.151.33.186):
Enter Fully Qualified Domain Name(default:
server1.thecompany.com):
Central Security Server IP:
192.151.33.186
Central Security Server Fully Qualified Domain
Name:     server1.thecompany.com
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok
```

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

It is recommended to migrate all user accounts that exist on 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.

If the central security administration application is a third-party application and not the Nortel central security server, follow the procedures in the third party documentation.

To migrate Core Manager user accounts to the Nortel central security server, refer to Migrating core manager user accounts to the Nortel central security server.

a. If the central administration system is the Nortel central security server, launch the Security Administration tool of the Nortel central security server, and add the user accounts plus any additional required user groups you want to centrally manage.

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

   Log in to the central security client (for example, CBM) by typing

   `> telnet <server>`

   and pressing the Enter key.

   where

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

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

—End—

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

All users are authorized to perform this procedure.

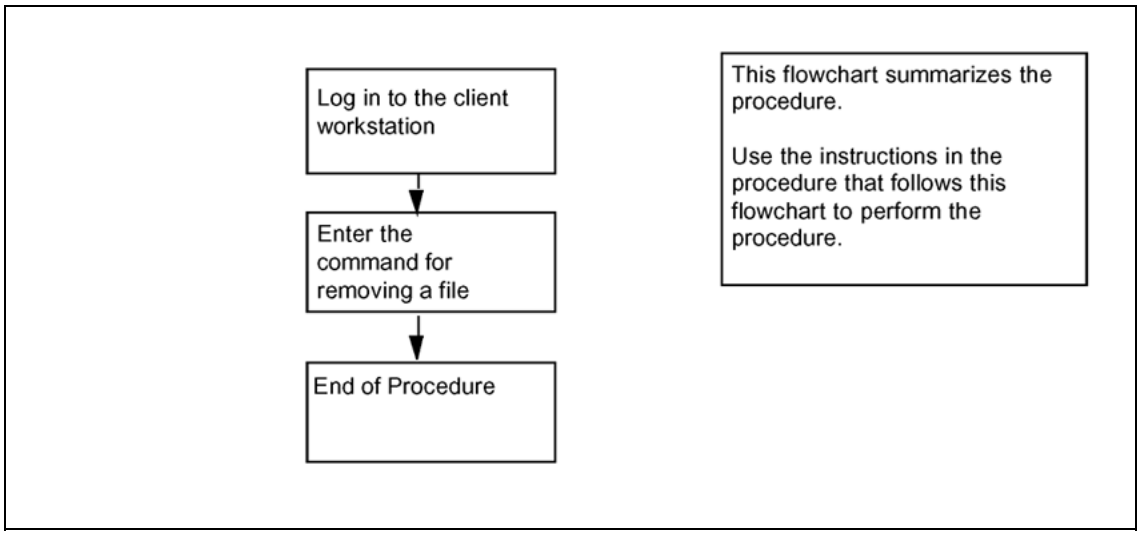
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action

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

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.

—End—

Displaying help for SCFT

Purpose

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

Prerequisites

All users are authorized to perform this procedure.

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

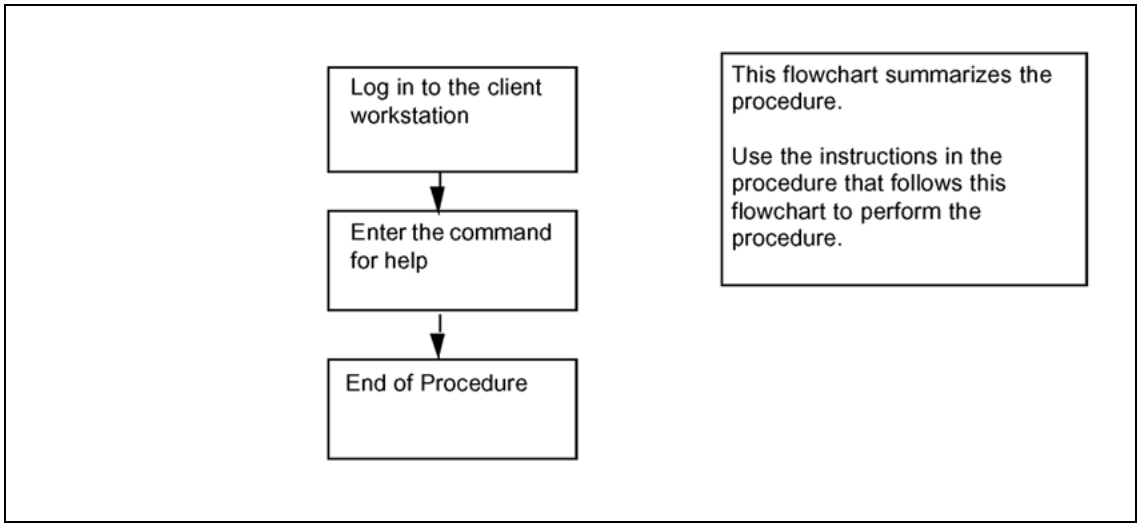
Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN20000-320
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN20000-320

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



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

Step	Action

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

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.

—End—

Listing volumes on Core using SCFT

Purpose

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

Prerequisites

All users are authorized to perform this procedure.

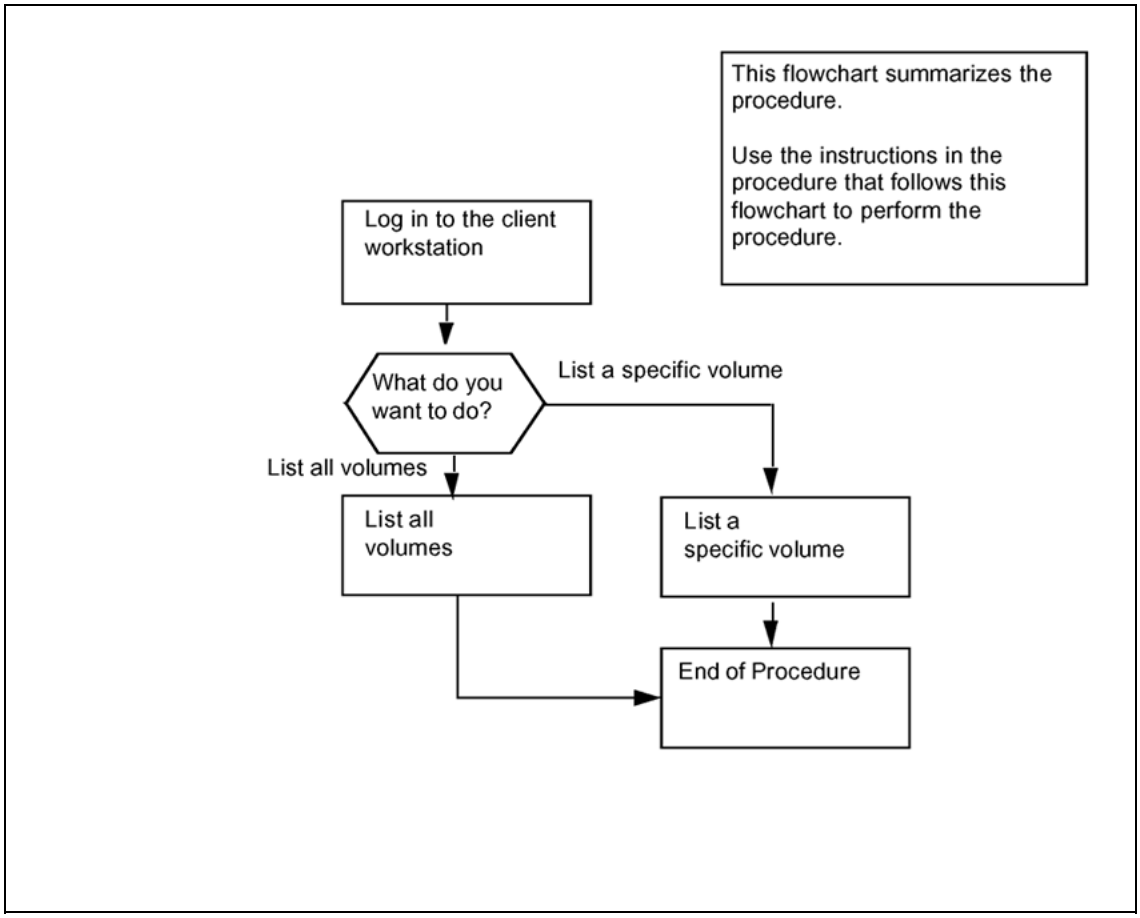
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action

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 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

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

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

Example response:

```
LOGIN STDFAULT
```

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

5 You have completed this procedure.

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

6 List all volumes on the Core:

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

where

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

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

Example response:

```
SFDEV
S01DIMAGE
S00DIMAGE1
S00DAMA
S01DPMLOADS
S01DPERM
S01DDLOG
S01DTEMP
Command complete
```

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

7 List a specific volume on the Core:

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

and pressing the Enter key.

where

<user> the user name you are using to log on to the core manager
<host> the name or IP address of the core manager
<volume> is the name of the volume on the core manager

Example response:

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

8 You have completed this procedure.

—End—

Configuring the Time Zone on an SPFS-Based Server

Application

Use this procedure to configure the time zone on a Server Platform Foundation Software (SPFS) based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

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 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 -
```

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 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup 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/Easter
n>:
```

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.

—End—

Changing a passthru user password

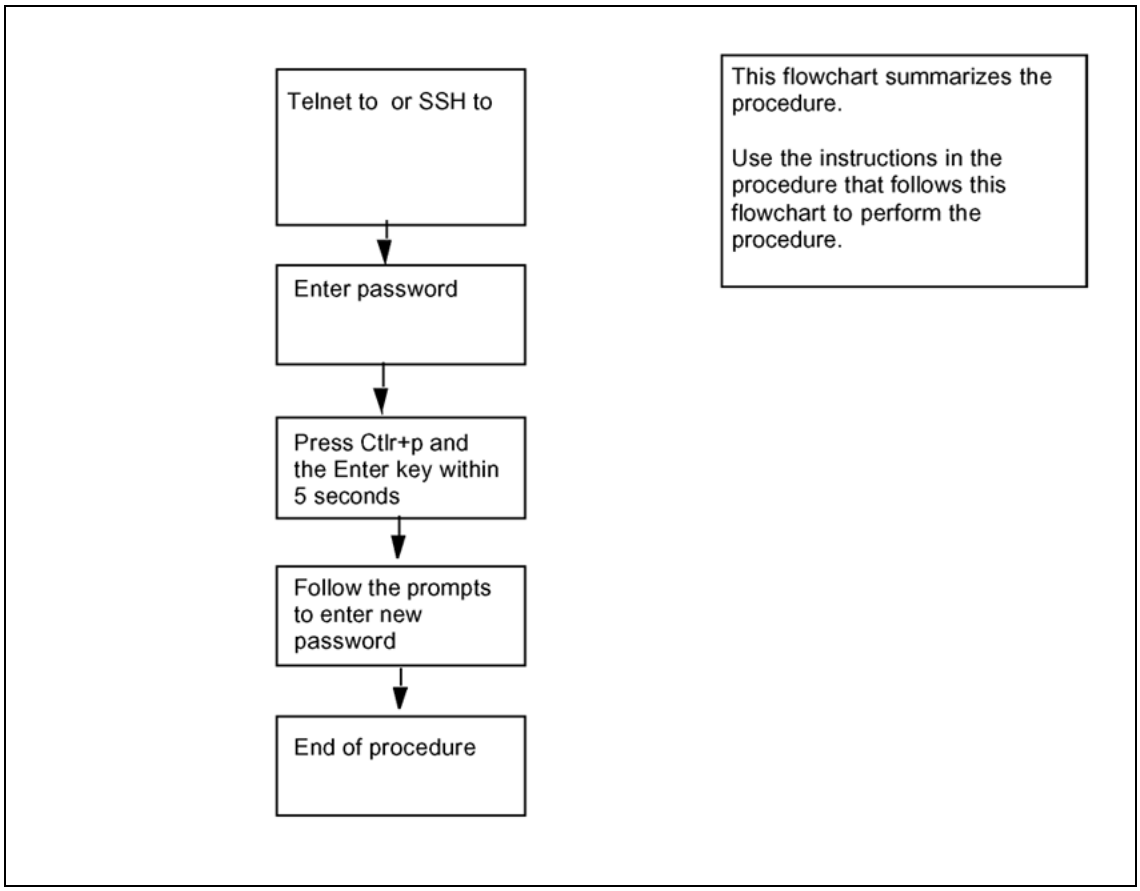
Purpose

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



Changing a passthru user password

Step	Action
	At the workstation

1 Log in to the CBM as a passthru user.

If you	Do
use telnet	step 2
use SSH	step 3

2 Telnet to the CBM:

```
> telnet <IP address>
```

where

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

Continue with step 4.

3 Open an SSH session:

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

where

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

4 At the prompt, enter your password.

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.

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.

—End—

Changing a user password on an SPFS-based server

Application

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

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action
	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 SPFS-based server 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
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.

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.

—End—

Setting the Threshold for File Systems on an SSPFS-Based Server

Application

Use this procedure to change the default threshold for a file system on a Succession Server Platform Foundation Software (SSPFS)-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.

Setup the threshold for file systems

Step	Action
	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 SSPFS-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 preceding example sets the threshold for the /data file system to 80%.

6 You have completed this procedure.

—End—

Starting an application

Application

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

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).

Prerequisites

All users are authorized to perform this procedure.

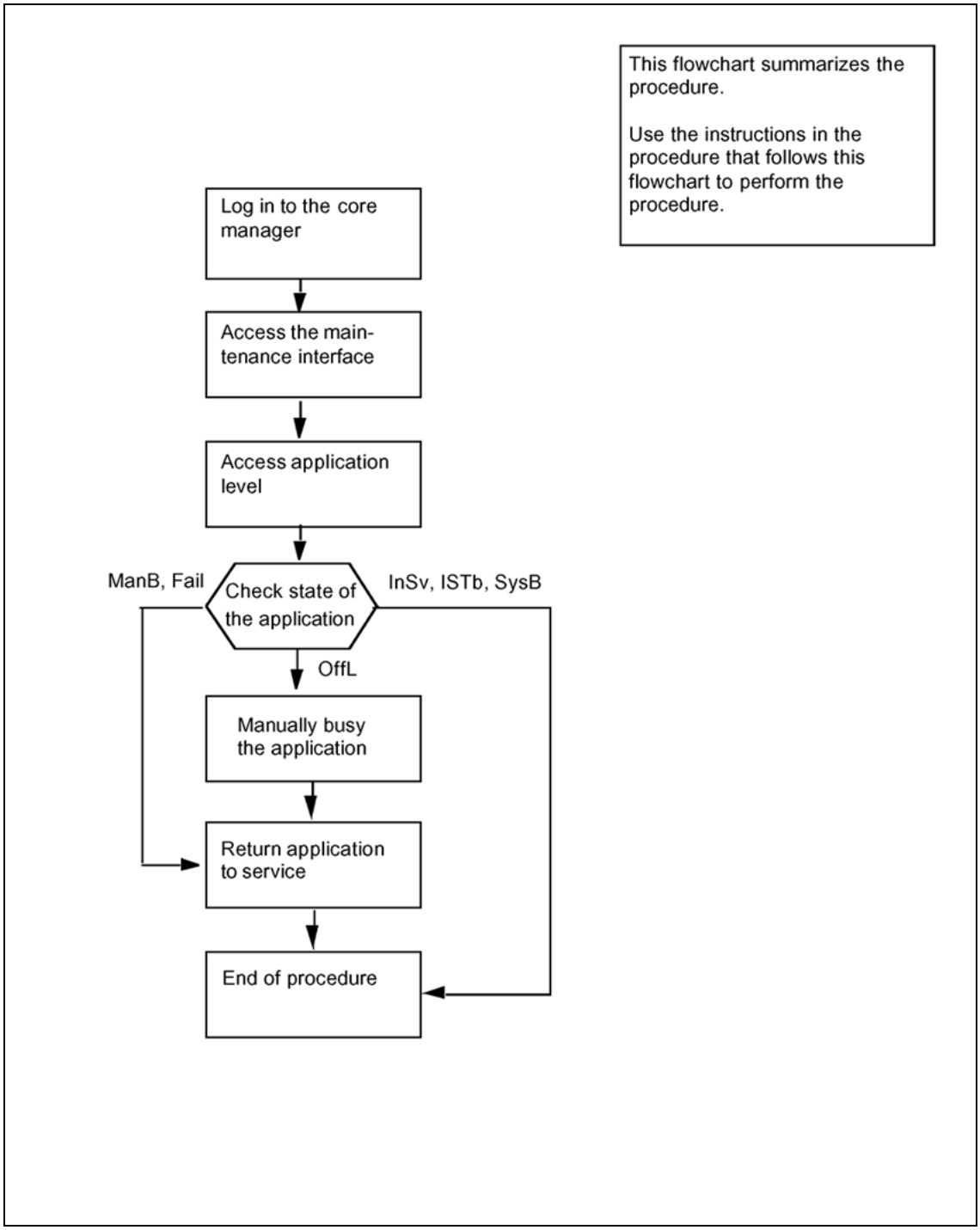
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action

At the local or remote VT100 terminal

1 Log in to the core manager.

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.

—End—

Starting the application group

Application

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

For CBM850, you must perform this procedure on the active server.

Prerequisites

All users are authorized to perform this procedure.

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

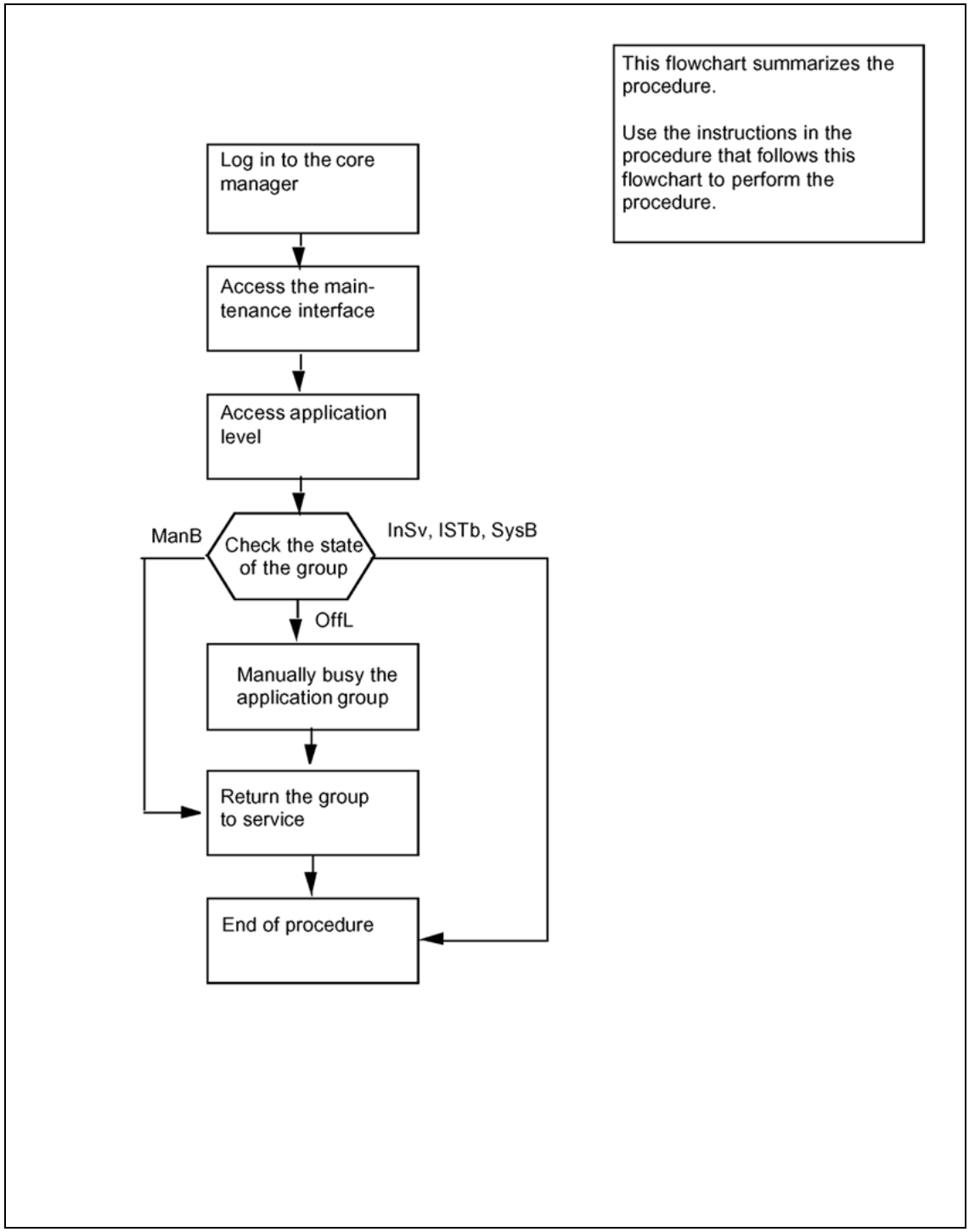
Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

Action

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

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



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

Step	Action

At the local or remote VT100 terminal

1 Log in to the core manager.

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.

—End—

Stopping an application

Application

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

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.

Prerequisites

All users are authorized to perform this procedure.

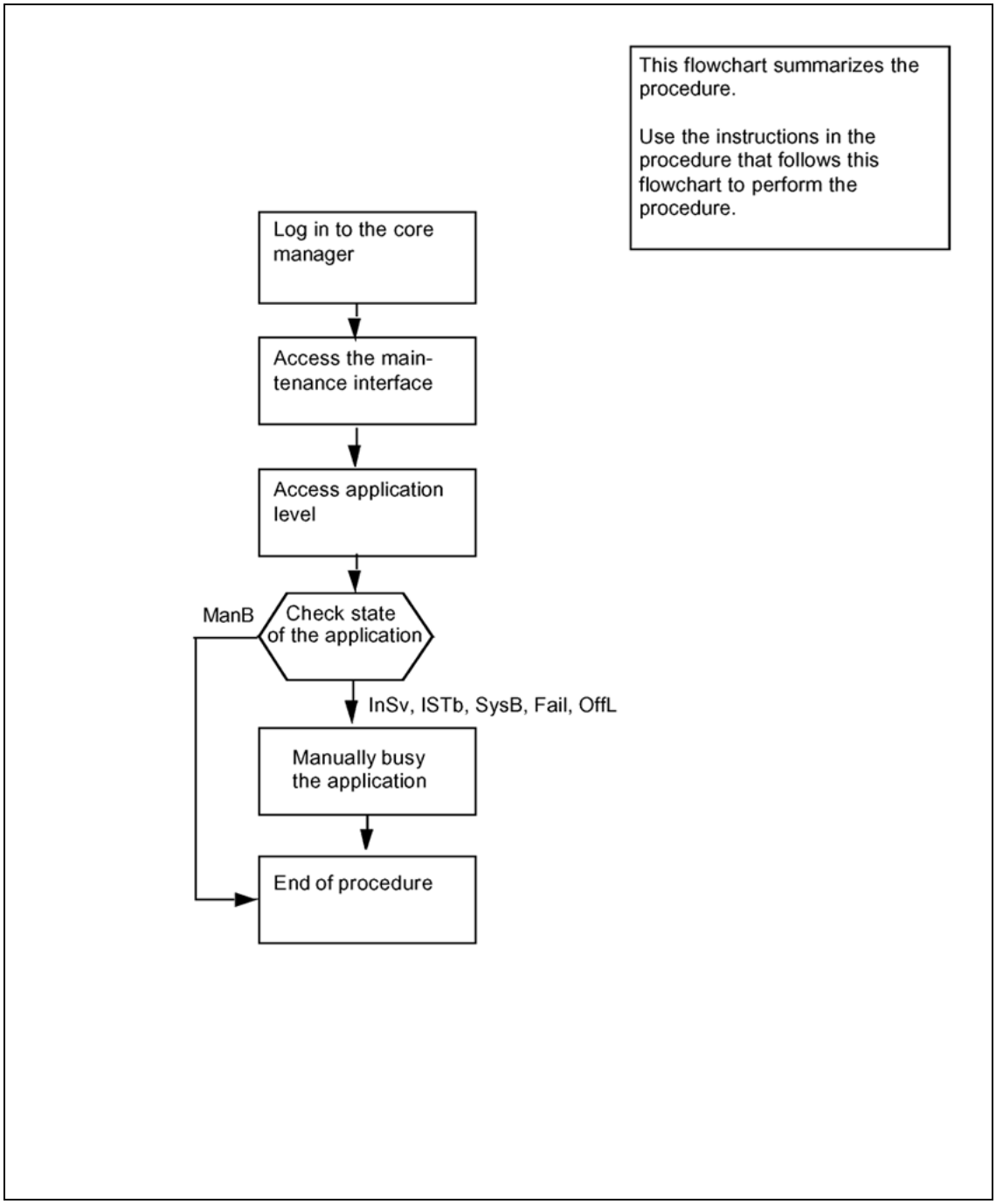
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action

At the local or remote VT100 terminal

1 Log in to the core manager.

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"):
```

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.

—End—

Stopping the application group

Application

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

For CBM850, you must perform this procedure on the active server.

This procedure prevents an individual application from providing service.

Prerequisites

All users are authorized to perform this procedure.

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

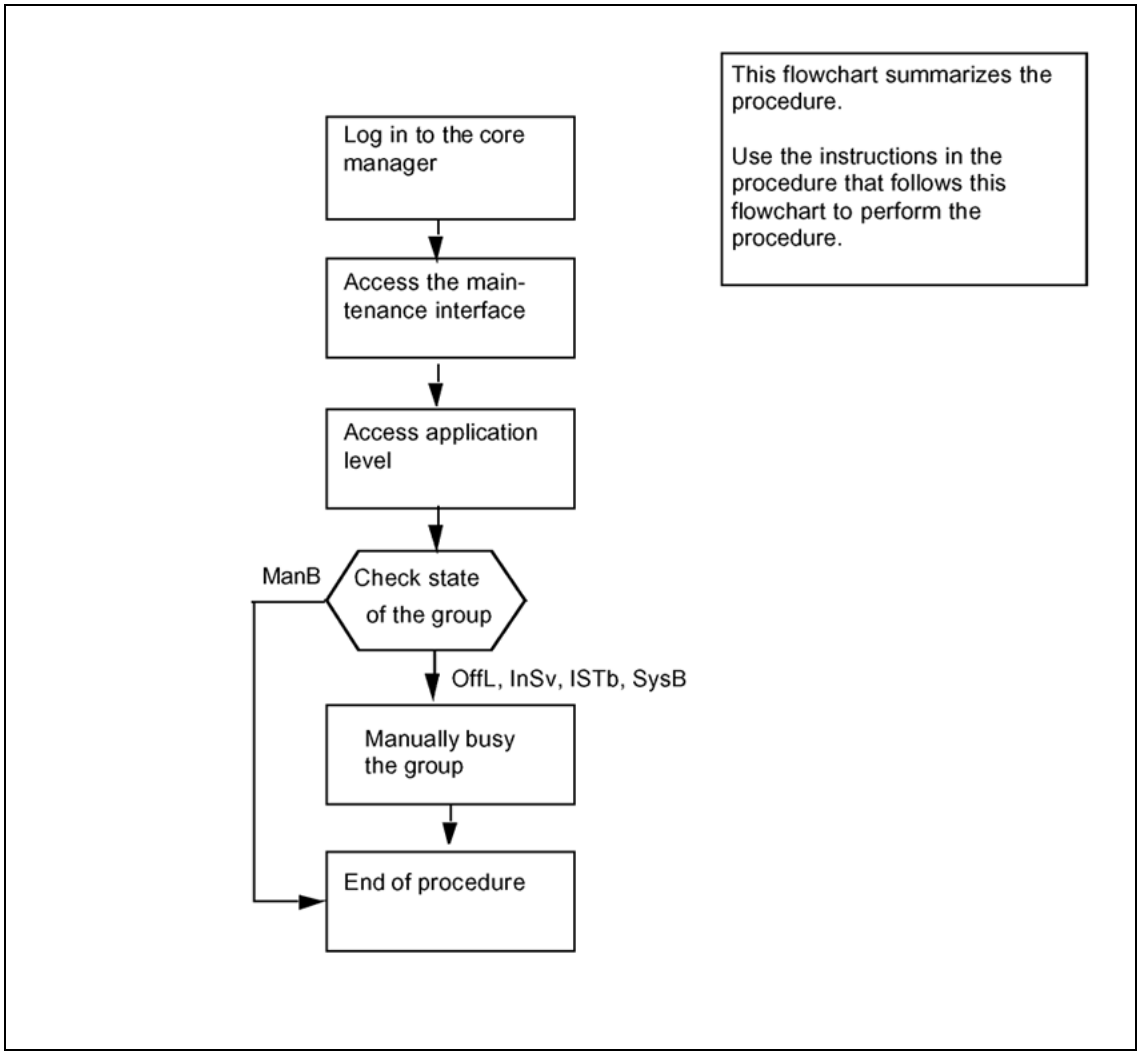
Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

Action

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

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



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

Step	Action
	At the local or remote VT100 terminal
1	Log in to the core manager.
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.

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"):
```

Busying the application group as shown performs an orderly shutdown and can take up to 16 seconds.

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.

—End—

Stopping and restarting an application

Application

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

For CBM850, you must perform this procedure on the active server.

Prerequisites

All users are authorized to perform this procedure.

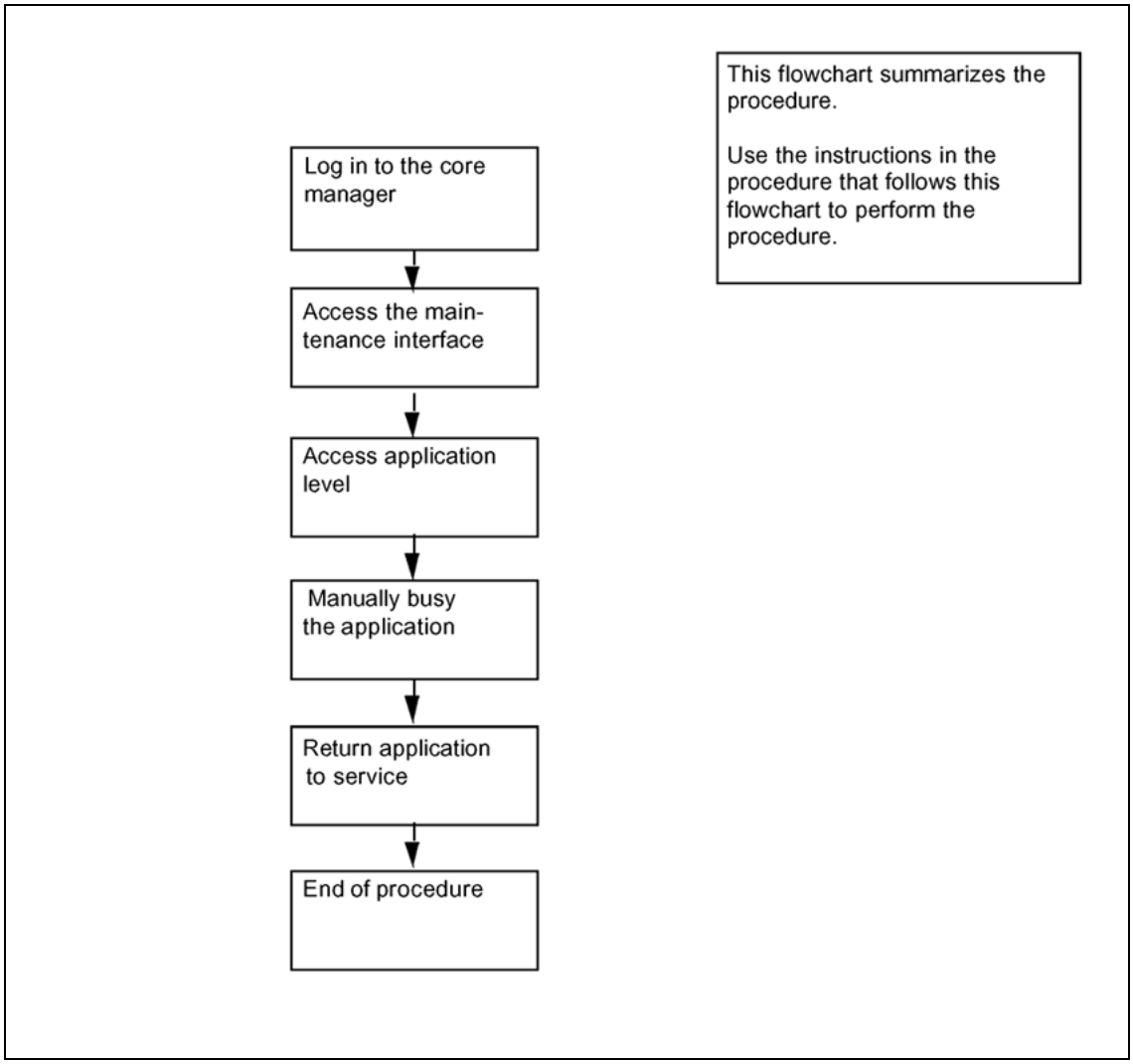
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action
	At the local or remote VT100 terminal
1	Log in to the core manager.
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"):
```

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.

—End—

Offlining an application

Application

Use this procedure to offline a CBM software application.

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.

Prerequisites

All users are authorized to perform this procedure.

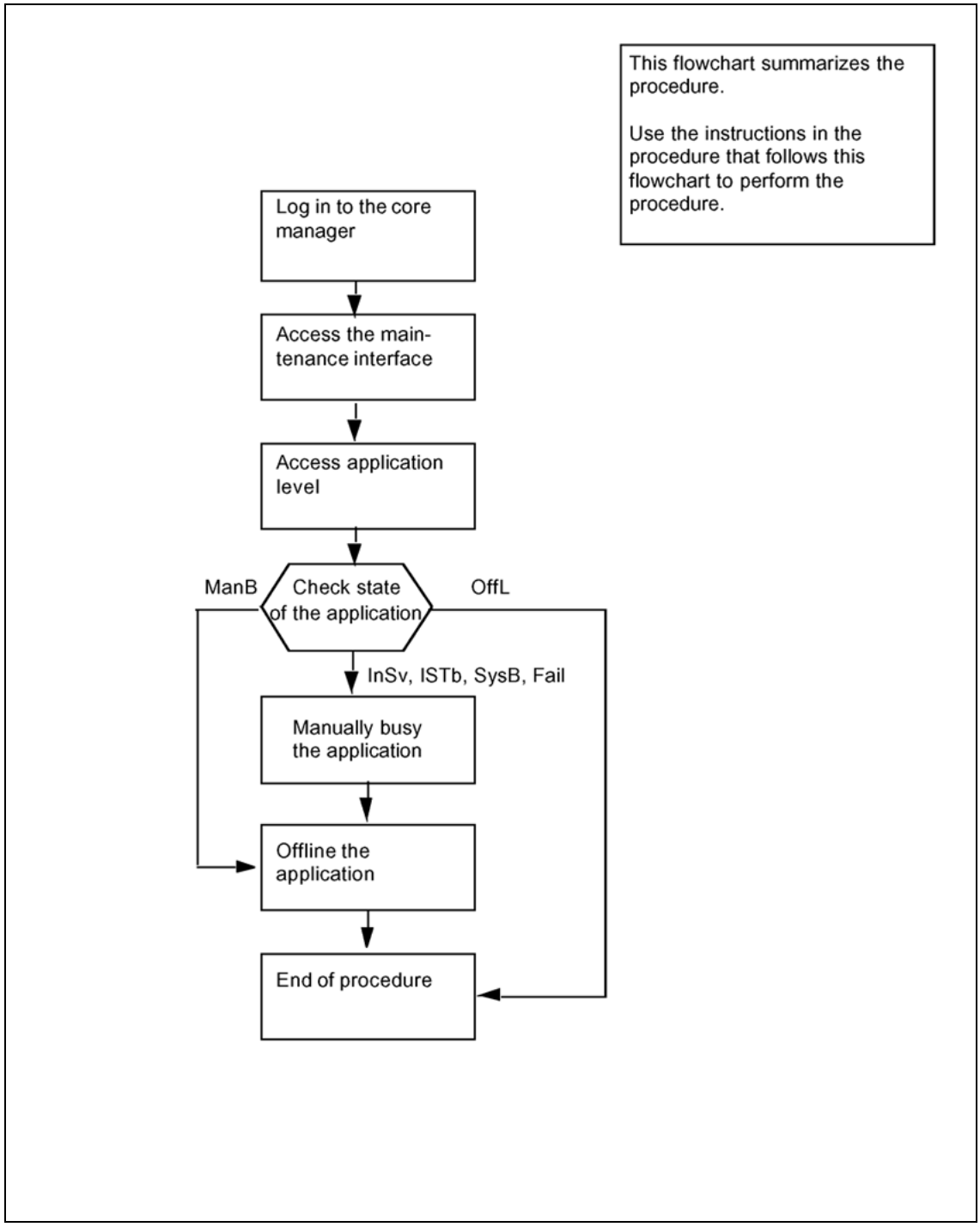
For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Logging in to the CBM
Displaying actions a role group is authorized to perform

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



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

Step	Action

At the local or remote VT100 terminal

1 Log in to the core manager.

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.

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"):
```

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.

—End—

Offlining the application group

Application

Use this procedure to offline the application group.

For CBM850, you must perform this procedure on the active server.

This procedure prevents an individual application from providing service.

Prerequisites

All users are authorized to perform this procedure.

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

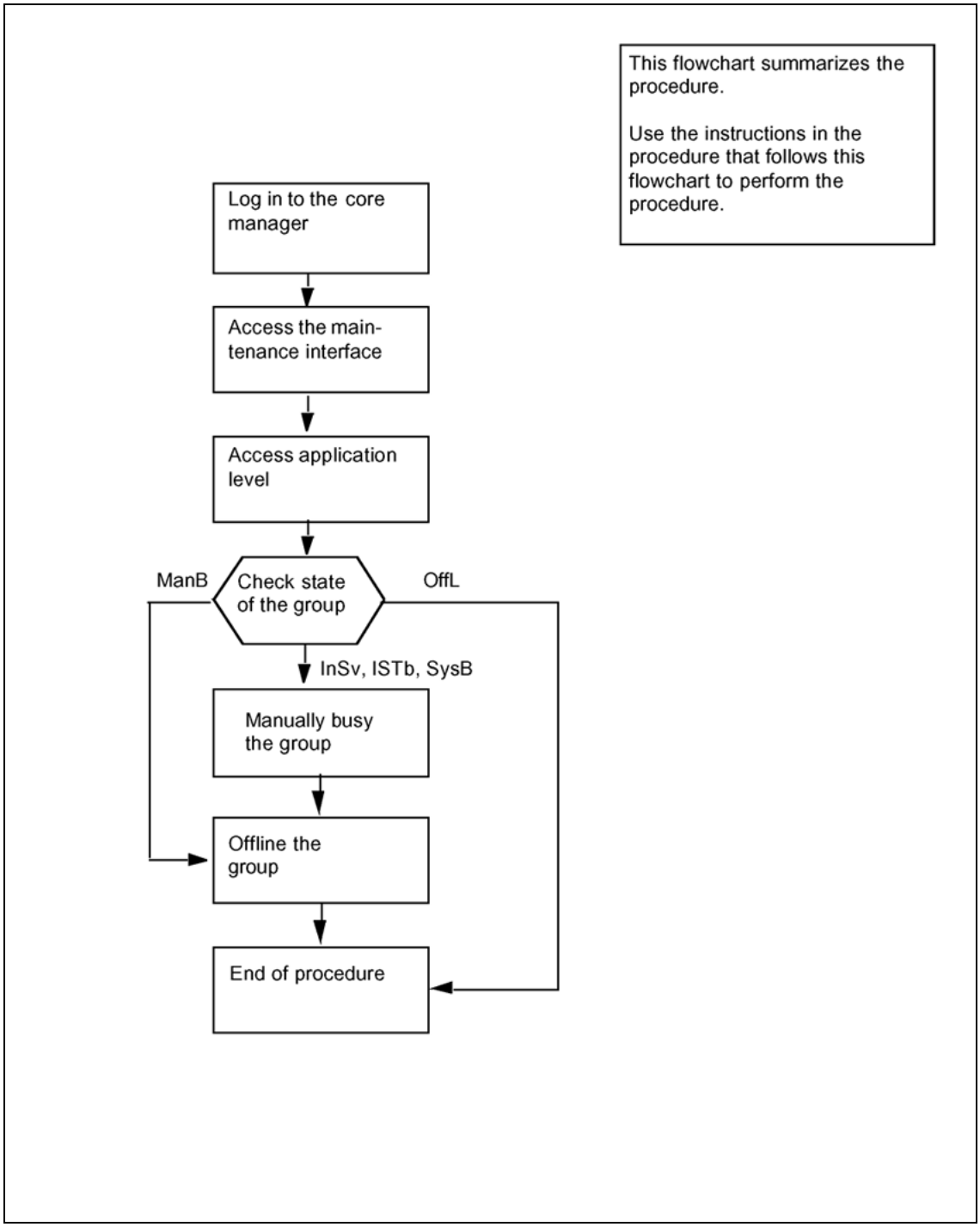
Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

Action

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

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



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

Step	Action

At the local or remote VT100 terminal

1 Log in to the core manager.

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 7

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"):
```

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.

—End—

Configuring the PAM to authenticate with a LDAP security server

Purpose

Do not use this procedure to configure the CBM for central user authentication with a Nortel central security server. These servers use RADIUS as the authentication protocol.

This procedure provides an example of configuring a CBM with central user authentication capabilities using pam_ldap (Pluggable Authentication Module - Lightweight Directory Access Protocol).

Application

The CBM platform provides the capability for central user authentication using the Pluggable Authentication Module (PAM). PAM consists of a set of libraries and an Application Programming Interface (API) that can be used to perform authentication tasks. Privilege granting programs, such as login and other access rights, use the API to perform standard authentication tasks.

Use this procedure to configure the PAM for communication with the LDAP server. This procedure must be performed on both the active and the inactive node. After the procedure is complete, ensure that the ldap_cachemgr daemon is running on CBM.

This procedure was tested using the Sun Solaris IPlanet directory server [idS5.2].

ATTENTION

LDAP password policies are not supported

The parameters for the password expiry and account lockout policies can be set in the LDAP server but are not supported by the Solaris 9 LDAP client. Therefore,

1) The passwords for CBM users that are defined in an LDAP server do not expire and can be used to log into the CBM even if the password has not been changed for a period that is longer than is defined in the security policy of the LDAP server.

2) The accounts for CBM users that are defined in an LDAP server do not get locked and can be used to log into the CBM even if the account login exceeds the maximum failure defined in the security policy of the LDAP server.

3) When logged in as a secadm user, and changing the password of another LDAP user, the password will change successfully, however an incorrect prompt will be displayed.

4) If the password of the local user expires and the same local user logs into the CBM; the OS will prompt for the new password, but the password will fail and the user will not be able to login.

ATTENTION

Possibility of hanging during reboot if step 13 is not performed

If step 13 is not performed in this procedure, whenever the LDAP server is down or not reachable, and if a reboot is given for any of the units [active or inactive] of the CBM, the corresponding unit will hang waiting for the response from the LDAP server for an infinite time.

Prerequisites

Assign /bin/rash as the profile shell to all users on the LDAP server that are to access the CBM.

You must be logged into the CBM as the root user to perform this procedure.

Prior to performing this procedure, the following information must be collected:

- the name of the supported credential level
- the name of the supported authentication method
- the name of the domain
- the search base distinguished name (DN)
- the name of the proxy agent (DN)
- the password of the proxy agent
- the IP address of the LDAP server

Procedure

Step	Action

At your workstation

1 Log into the CBM as the root user

a. using telnet, by entering:

```
telnet <IP address>
```

```
Login: <login>
Password: <password>
```

Change to the root user by typing

```
$ su - root
```

When prompted, enter the root password.

b. using secure shell protocol (SSH), by entering:

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

```
User@host's password: <password>
```

where

IP address is the IP address of the CBM

If ssh keys were configured, the password is not needed.

2 Display the contents of file /etc/pam.conf to confirm whether the CBM is configured to authenticate against a RADIUS server.

If file /etc/pam.conf does not contain any occurrences of "pam_radius_auth.so", the CBM is not configured to authenticate against a RADIUS server. Go to step 11.

If file /etc/pam.conf contains any occurrences of "pam_radius_auth.so", the CBM is configured to authenticate against a RADIUS server. Go to the next step to remove this configuration.

3 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

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

4 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 -
```

5 Enter the number next to the "Security Services Configuration" option in the menu.

Example response

```
Security Services Configuration
  1 - Socks Configuration
  2 - Security Server Location Configuration
  3 - PAM Configuration
  4 - Common Inet Services (ftp, tft, telnet,
      snmpand nfs)
  5 - Tools Inet Services (time, daytime)
  6 - Other Inet Services
  7 - proftpd User Configuration
  8 - PKManager Certificate Installation
  9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services
       Package Registration)
X - exit
select -
```

6 Enter the number next to the "PAM Configuration" option in the menu.

Example response

```
PAM Configuration
  1 - Central Security Client Configuration
X - exit
select -
```

7 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 -
```

8 Enter the number next to the "pam_orig" option in the menu. The default PAM configuration does local authentication only.

Example response

```
=== Executing "pam_orig"
Switching to original PAM and Nsswitch configuration
Enter "ok" to continue
Enter anything else to exit
```

9 Enter "ok".

Example response

```
Restarting name service daemon
=== "pam_orig" execution completed
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 -
```

10 Exit the command line interface by entering

```
select - x
```

and pressing the Enter key.

11 Replace file /etc/nsswitch.ldap with nsswitch.conf.

```
> # cp /etc/nsswitch.conf /etc/nsswitch.ldap
```

12 In file /etc/nsswitch.ldap, edit the entries for "passwd" and "group" to appear as follows:

```
passwd:  files rbacmap ldap
group:  files ldap
```

13 Edit file /etc/init.d/ldap.client so that it appears as follows:

```
case "$1" in
start)
[ -f /var/ldap/ldap_client_file ] && \
[ -f /usr/lib/ldap/ldap_cachemgr ] || exit 0
/usr/lib/ldap/ldap_cachemgr &
;;
```

This executes the ldap_cachemgr daemon as a background process.

14 Run the ldapclient command.

```
> /usr/sbin/ldapclient -v manual \
-a credentialLevel=<credential_level> \
-a authenticationMethod=<auth_method_name> \
-a domainName=<domain> \
-a defaultSearchBase=<search_base_DN> \
-a proxyDN=<proxyagent_DN> \
-a proxyPassword=<proxyagent_pswd> <IP_address>
```

where

auth_method_name is the authentication method used by all services unless overridden by attribute serviceAuthenticationMethod. Attribute authenticationMethod

is ignored when credentialLevel is set to anonymous. Specify multiple values by separating each value with a semi-colon (;). Valid values are:
none (default value)
simple
sasl/CRAM-MD5
sasl/DIGEST-MD5
tls:simple
tls:sas/CRAM-MD5
tls:sasl/DIGEST-MD5

credential_level is the credential level the client uses to contact the directory. Valid values are proxy and anonymous. If credentialLevel is set to proxy, you need to set attribute authenticationMethod. Also, if credentialLevel is set to proxy and at least one of the authentication methods requires a bind DN, you need to set attributes proxyDN and proxyPassword. During lab testing, credentialLevel was set to proxy.

domain is the DNS domain name and becomes the default domain for the machine. This attribute is only used in client initialization. The default value is the current domain name.

IP_address is the address or name for the LDAP server from which the profile will be loaded. The current naming service specified in file nsswitch.conf is used. Once the profile is loaded, the preferredServerList and defaultServerList specified in the profile are used.

proxyagent_DN is the Bind Distinguished Name for the proxy identity. This attribute has no default value. This attribute is required when credentialLevel is proxy and at least one of the authentication methods requires a bind DN.

proxyagent_pswd is the client proxy password. This attribute has no default value. This attribute is required when credentialLevel is proxy and at least one of the authentication methods requires a bind DN.

search_base_DN is the search base DN. This attribute has no default value. Use attribute serviceSearchDescriptor to override the defaultSearchBase for given services.

15 If module pam_mkhomedir is not present in directory /usr/lib/security, execute the following commands to activate and configure the module.

```
> # /opt/nortel/applications/management/
swmgmt_MIP4.0.0/swmgmt/bin/activate_swmgmt.sh
> # /opt/nortel/applications/security/ pamrad-
clt_1.1.0/swmgmt/bin/
activate_pamradclt.sh
```

```
> # /opt/nortel/applications/security/ pamrad-
clt_1.1.0/swmgmt/bin/
configure_pamradclt.sh - subcomponent libs
```

16 Open the /etc/pam.conf file and edit it as follows:

```
# Authentication management
#
# login service (explicit because of
# pam_dial_auth)
login   auth requisite
pam_authtok_get.so.1
login   auth required          pam_dhkeys.so.1
login   auth required          pam_dial_auth.so.1
login   auth binding           pam_unix_auth.so.1
server_policy
login   auth required          pam_ldap.so.1
use_first_pass
login   auth required          pam_mkhomedir.so.1
#
# rlogin service (explicit because of
# pam_rhost_auth)
rlogin auth sufficient pam_rhosts_auth.so.1
rlogin auth requisite  pam_authtok_get.so.1
rlogin auth required   pam_dhkeys.so.1
rlogin auth binding    pam_unix_auth.so.1
server_policy
rlogin auth required   pam_ldap.so.1
use_first_pass
rlogin auth required   pam_mkhomedir.so.1
#
# rsh service (explicit because of
# pam_rhost_auth and pam_unix_auth for
# meaningful pam_setcred)
rsh auth sufficient  pam_rhosts_auth.so.1
rsh auth binding     pam_unix_auth.s0.1
server_policy
rsh auth required    pam_ldap.so.1
use_first_pass
rsh auth required    pam_mkhomedir.so.1
#
# PPP service (explicit because of
# pam_dial_auth)
ppp     auth requisite
pam_authtok_get.so.1
ppp     auth required          pam_dhkeys.so.1
ppp     auth required          pam_dial_auth.so.1
ppp     auth binding           pam_unix_auth.so.1
server_policy
ppp     auth required          pam_ldap.so.1
use_first_pass
```

```
ppp     auth required           pam_mkhomedir.so.1
#
# Default definitions for authentication
# management
# Used when service name is not explicitly
# mentioned for authentication
other auth requisite  pam_authtok_get.so.1
other auth required   pam_dhkeys.so.1
other auth binding    pam_unix_auth.so.1
server_policy
other auth required   pam_ldap.so.1
use_first_pass
other auth required   pam_mkhomedir.so.1
#
# passwd command (explicit because of a
# different authentication module)
passwd auth binding   pam_passwd_auth.so.1
server policy
passwd auth required  pam_ldap.so.1
use_first_pass
#
# cron service (explicit because of non-usage of
# pam_roles.so.1
cron account required  pam_projects.so.1
cron account required  pam_unix_account.so.1
# Default definition for account management
# Used when service name is not explicitly
# mentioned for account management
other account requisite  pam_mkhomedir.so.1
other account requisite  pam_roles.so.1
other account required   pam_projects.so.1
other account binding    pam_unix_account.so.1
server policy
other account required   pam_ldap.so.1
use_first_pass
# Default definition for session management
# Used when service name is not explicitly
# mentioned for session management
other session required pam_mkhomedir.so.1
other session required pam_unix_session.so.1
#
# Default definition for password management
# Used when service name is not explicitly
# mentioned for password management
other password required
/usr/lib/security/$ISA/pam_authtok_rep.so.1
# Ensure that the system has the current patches for
the above mentioned libraries to be available
in the system.
other password required  pam_dhkeys.so.1
```

```
other password requisite pam_authtok_get.so.1
other password requisite pam_authtok_check.so.1
other password required  pam_authtok_store.so.1
server_policy
#
# Support for Kerberos V5 authentication
# (Uncomment to use Kerberos)
#rlogin auth optional pam_krb5.so.1 #try_first_pass
#login auth optional  pam_krb5.so.1
#try_first_pass
#other auth optional  pam_krb5.so.1
#try_first_pass
#cron  account  optional pam_krb5.so.1
#other account  optional pam_krb5.so.1
#other session  optional pam_krb5.so.1
#other password optional pam_krb5.so.1
#try_first_pass
#
# Begin NTLogin Additions
# Support for NTLogin security enhancements
sesm auth required
/usr/lib/security/$ISA/pam_unix.so.1
try_first_pass
sesm account required
/usr/lib/security/$ISA/pam_unix.so.1
sesm session required
/usr/lib/security/$ISA/pam_unix.so/1
sesm password required
/usr/lib/security/$ISA/pam_unix.so.1
# END NTLogin additions
```

—End—

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

All users are authorized to perform this procedure.

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

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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

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

Step	Action
	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.

—End—

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

You must be a user in a role group authorized to perform accounting-manage actions.

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

Procedure
Logging in to the CBM
Displaying actions a role group is authorized to perform

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

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.

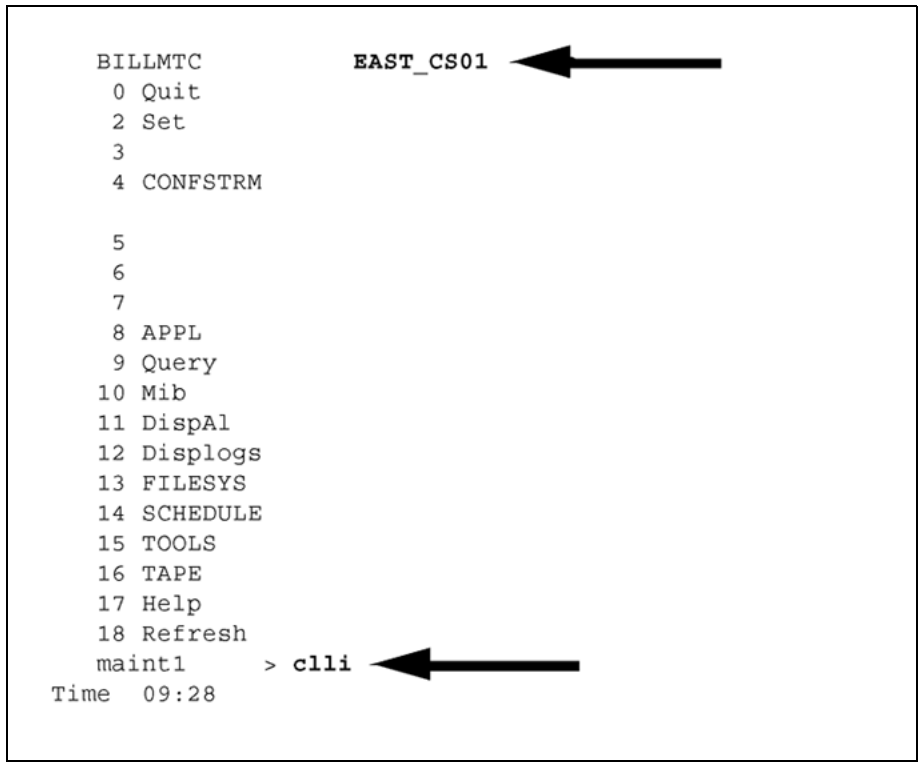
Procedure

Step	Action
	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



4 You have completed this procedure.

—End—

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.

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)" (page 203)
"Removing IPSec from the OSS (Solaris 5.9 machine)" (page 204)

Configuring IPSec on the OSS (Solaris 5.9 machine)

Step	Action
	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 When IPSec and IKE are configured on an 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 SPFS-based server. The information in these two files can be used to update the files shown in the preceding.

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.

—End—

If the SPFS software load for release (I)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 an SPFS-based server" located in *ATM/IP Solution-level Security and Administration*, NN10402-600.

Removing IPSec from the OSS (Solaris 5.9 machine)

Step	Action

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.

—End—

If the SPFS software load for release (I)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 an SPFS-based server" located in *ATM/IP Solution-level Security and Administration*, NN10402-600.

Configuring IPSec and IKE on an SPFS-based server

Application

Use this procedure to configure IP Security (IPSec) and Internet Key Exchange (IKE) on a 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.

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.

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" (page 206)
"Procedure to add an IPSec rule" (page 209)
"Procedure to delete an IPSec rule" (page 212)
"Procedure to list an IPSec rule" (page 212)
"Procedure to add an IKE rule" (page 213)
"Procedure to delete an IKE rule" (page 215)
"Procedure to list IKE entries" (page 216)
"Procedure to change a preshared key for an IKE entry" (page 216)

Procedure to access CLI in order to perform IPSec and IKE configuration

Step	Action
	At your workstation
1	Telnet to the server:

telnet <server>

where

server is the IP address or host name of the 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" (page 209)
you wish to delete an IPSec rule	"Procedure to delete an IPSec rule" (page 212)
you wish to list all IPSec rules	"Procedure to list an IPSec rule" (page 212)

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" (page 213)
you wish to delete an IKE entry	"Procedure to delete an IKE rule" (page 215)
you wish to list IKE entries	"Procedure to list IKE entries" (page 216)
you wish to change a preshared key for an IKE entry	"Procedure to change a preshared key for an IKE entry" (page 216)

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.

—End—

Procedure to add an IPSec rule

Step	Action

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 in the following.

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 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
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
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.

—End—

Procedure to delete an IPSec rule

Step	Action

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 in the following.

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.

—End—

Procedure to list an IPSec rule

Step	Action

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 in the following.

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.

—End—

Procedure to add an IKE rule

Step	Action

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 in the following.

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.

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

Field	Entry	Explanation
Authentication Method	Preshared	authentication method used for IKE phase 1
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.
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.

—End—

Procedure to delete an IKE rule

Step	Action
	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 in the following.

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.

—End—

Procedure to list IKE entries

Step	Action

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 in the following.

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.

—End—

Procedure to change a preshared key for an IKE entry

Step	Action

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 in the following:

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.

—End—

Carrier VoIP

Core and Billing Manager 850 Security and Administration

Publication: NN10358-611
Document status: Standard
Document version: 04.04
Document date: 20 October 2006

To provide feedback or report a problem in this document , go to **http://www.nortel.com/documentfeedback**

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.