CS 2000 Management Tools Administration and Security

Overview

This section contains Security and administration procedures.

User accounts and passwords

The following table, lists the procedures available for user accounts and passwords.

User accounts and passwords procedures

Procedure
Changing the Oracle user password on a Sun server on page 5
Changing the APS Oracle account password on page 7
Setting up users on a Sun server on page 9
Changing a user password on a Sun server on page 26
Changing an expired root password on a Sun server on page 29
Deleting a user from a Sun server on page 30
Setting the Oracle Listener password on a Sun server on page 32
Changing the Oracle Listener password on a Sun server on page 34

Security

The following table, lists the procedures available for security.

Security procedures

Procedure
Changing the authentication mechanism between UNIX and DCE on page 21
Setting secure FTP proxy on page 37

Backup and restore

The following table, lists the procedures available for backup and restore.

Backup and restore procedures

Procedure
Configuring automated data backups on a Sun server on page 41
Performing a data backup on a Sun server on page 45
Performing a full backup of file systems on page 49
Performing a data restore on a Sun server on page 51
Performing a full system restore on a Sun server on page 53
Cloning the image of one node in a cluster to the other node on page 57

Client and server applications

The following table, lists the procedures available for the client and server applications.

Client and server applications procedures

Procedure
Starting the SESM server application on page 62
Starting the SAM21 Manager server application on page 65
Starting the NPM server application on page 67

Client and server applications procedures

Changing the Oracle user password on a Sun server

Application

Use this procedure to change the default Oracle passwords on a Sun server.

> ***Note:*** Refer to procedure Changing the APS Oracle account password in this document, to change the default password.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change to the Oracle user by typing

```
# su - oracle
```

and pressing the Enter key.

6 Change the password by typing

```
$ /opt/nortel/sspfs/db/pfsora_set_pwd <userID>
```

and pressing the Enter key.

Where

userID
is the user ID of the Oracle user

Example response:

```
Enter new password for user SYSTEM:
```

7 When prompted, enter the new password for the system.

Example response:

```
Re-enter new password:
```

8 When prompted, enter the password a second time to confirm the password.

Example response:

```
Please wait...
Successfully changed password for Oracle user
SYSTEM
```

Note: The command takes approximately 15 to 20 seconds to execute.

9 You have completed this procedure.

Changing the APS Oracle account password

When the APS is installed, a default password is assigned to the Oracle account. This procedure enables you to change the default password, for added system security.

Changing the APS Oracle account password

In a telnet connection to the APS server

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

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

```
getNTDBpasswd.ksh
```

The system displays the current Oracle account password.

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

```
su - oracle
```

4 Perform the following steps to change the Oracle account password:

a Enter the following command to run the script that enables you to change the password:

```
/usr/ntdb/uas/scripts/setNTDBpasswd.ksh
```

b At the prompt, enter the current APS Oracle account password.

Note: This is the password that you displayed in step 2.

c At the prompt, enter the new APS Oracle account password.

d At the prompt, reenter the new APS Oracle account password.

The system changes the password in UNIX and in the Oracle database.

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

```
exit
```

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

5 Restart the APS processes by entering the following command:

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

A message eventually displays indicating that the server is restarting.

6 Enter the following commands to complete the password change:

```
cd /
```

```
. /etc/profile
```

```
. ./.profile
```

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

```
getNTDBpasswd.ksh
```

The system displays the current Oracle account password.

8 You have completed this procedure.

Setting up users on a Sun server

Application

Use this procedure to add new users on a Sun server and assign them to user groups, or assign existing users to user groups (see User groups).

ATTENTION
User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

The default authentication mechanism is UNIX. To change the authentication mechanism from UNIX to Distributed Computing Environment (DCE), refer to procedure “Changing the authentication mechanism between UNIX and DCE” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

User groups

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

Note: If upgrading from a release prior to SN06, existing users must be assigned to primary group “succssn” for login access, and to one or more Secondary user groups to specify the operations the user is authorized to perform, as shown in step 13 of this procedure.

User groups

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

Secondary user groups

A secondary user group consists of a user group domain (see table User group domains), which defines the range of applications to which a user group applies, and a user group operation (see table User group operations), which dictates the operations a user can perform using the Nortel Networks OAM&P client applications.

User group domains

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 operations

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.
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.

User group operations

Operation	User role mapping
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

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

- Node provisioning operations
- Carrier provisioning operations
- Audit operations
- Alarm operations
- Internet transparency operations
- Trunk provisioning operations
- Trunk maintenance operations
- ADSL provisioning operations
- Line provisioning operations
- Line maintenance operations
- V5.2 provisioning operations
- CS 2000 SAM21 operations

For patching operations using the Network Patch Manager (NPM), assign users to the “emsadm” secondary user group.

Node provisioning operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
disAssocMg		x			
assocMG		x			

Node provisioning operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
changeMG		x			
querySiteInfo					x
queryGWC					x
queryMG					x
changeMGGWCEMData		x			
getPEPServerData					x
queryGWCPEPConn					x
getDQosPoliciesData					x

Audit operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
configureAudit	x				
runAudit	x				
getAuditDescription					x
getAuditConfiguration					x
getListOfRegisteredAudits					x
retrieveAuditReport					x
takeActionOnProblem	x				

Carrier provisioning operations

	User group				
Command	trkadm	trkrw	trkmtc	trksprov	trkro
addCarrier		x			
deleteCarrier		x			
getEndpoint					x
getCarrier					x
getCarrierByFilter					x

Alarm operations

	User group				
Command	emsadm	emsrw	emsmtc	emssprov	emsro
set/unset ack			x		
all other functions (query related)					x

Internet transparency operations

	User group				
Command	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
queryNAT					x
queryMP					x
ChangeAssocNAT		x			

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
getTuple					x
getTupleRange					x
getCMClli					x
addTuple		x			
replaceTuple		x			
delTuple		x			
listAllTuples	x				
suspendApplication	x				
restoreApplication	x				

Trunk maintenance operations

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

ADSL provisioning operations

	User group				
Command	lnadm	lnrw	lnmtc	lnsprov	lnro
getSubscriber					x
addSubscriber				x	
addCrossConnection				x	
modifySubscriber				x	
modifyCrossConnection				x	
deleteSubscriber				x	
deleteCrossConnection				x	

Line provisioning operations

	User group				
Command	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

	User group				
Command	lnadm	lnrw	lnmtc	lnsprov	lnro
validateLineUsingDnClli					x
validateLineUsingTidClli					x

Line maintenance operations

	User group				
Command	lnadm	lnrw	lnmtc	lnsprov	lnro
getLinePostInfo					x
bsyLine			x		
rtsLine			x		
frlsLine			x		
inbLine			x		
cancelDeload			x		
getCmClli					x
getEnpointState					x
getGwIp					x

V5.2 provisioning operations

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

V5.2 provisioning operations

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

CS 2000 SAM21 operations

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			

Prerequisites

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

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

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

6 Add the user to the primary user group “succssn” by typing

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

and pressing the Enter key.

where

userid
is a variable for the user name

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

```
# passwd <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step

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

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

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

12 Note the user groups the user currently belongs to.

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

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

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table User groups) and any other user groups you noted in step 12 to which the user already belonged (include comma between groups, but no space)

userid
is a variable for the user name

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

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

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

14 You have completed this procedure.

Changing the authentication mechanism between UNIX and DCE

Application

Use one of the following procedures to change the authentication mechanism between UNIX and Distributed Computing Environment (DCE):

- Switching from UNIX to DCE for authentication
- Switching from DCE to UNIX for authentication

The default authentication mechanism is UNIX.

Prerequisites

To perform this procedure, you need to have the root user ID and password for the CS 2000 Management Tools server, and administrative privileges for the DCE server.

Action

Perform the following steps to complete this procedure.

Switching from UNIX to DCE for authentication

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Disable the Name Service Cache daemon as follows:

a Stop the Name Service Cache daemon

```
# /etc/init.d/nscd stop
```

and pressing the Enter key.

b Move the “/etc/nscd.conf” file to a different location.

6 Add “dce” as another option for the password and group in the “/etc/nsswitch.conf” file.

The entries would look similar to “passwd: files nis dce” and ““group: files nis dce” after the change.

This enables the group information to come from DCE.

7 Enable the DCE naming service server by typing

```
# config.dce
```

and pressing the Enter key.

8 Enable the DCE PAM (Pluggable Authentication Module) by typing

```
# config.dce pam
```

and pressing the Enter key.

9 Change the “sesm” entry in the “/etc/pam/conf” file as “sesm auth required /usr/lib/security/$ISA/pam_dce.so.1 try_first_pass”.

10 Add users and user groups to DCE as follows:

> ***Note:*** For details on user groups, refer to procedure Setting up users on a Sun server in this document.

a Log in to DCE using the cell_admin user ID and password.

b Add a user to DCE by typing

```
dcecp> user create <userid> -group succssn
-password <password> -organization
ossaps-users -mypwd <cell_admin_password>
```

and pressing the Enter key.

where

userid
is the user ID of the user you want to add

password
is the password for the user ID you want to add

cell_admin_password
is the password for cell_admin

c Add the necessary user groups in DCE by typing

```
dcecp> group create <groupname>
```

and pressing the Enter key.

where

groupname
is each of the following groups:

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

d Add the new users to the new groups, one at a time, by typing

```
dcecp> group add <groupname> -member <userid>
```

and pressing the Enter key.

where

groupname
is each of the following groups:

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

userid
is the user ID of a new user

e Verify the user was added by typing

```
dcecp> group list <groupname>
```

and pressing the Enter key.

where

groupname
is each of the following groups:

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

11 You have completed this procedure.

Note: When the DCE authentication mechanism is selected, you must use the UNIX passwd command with the “-r” option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is “`passwd -r file <userid>`”.

Switching from DCE to UNIX for authentication

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change the “sesm” entry in the “/etc/pam/conf” file as “sesm auth required /usr/lib/security/$ISA/pam_unix.so.1”.

6 Remove “dce” as another option for the password and group in the “/etc/nsswitch.conf” file.

The entries would look similar to “passwd: files nis” and “‘group: files nis” after the change.

7 Disable the DCE naming service server by typing

```
# /etc/dcesetup unconfig.nssdce
```

and pressing the Enter key.

8 Enable the Name Service Cache daemon as follows:

a Restore the “/etc/nscd.conf” file.

b Start the Name Service Cache daemon

```
# /etc/init.d/nscd start
```

and pressing the Enter key.

9 You have completed this procedure.

Changing a user password on a Sun server

Application

Use this procedure to change a user password on a Sun server.

> **ATTENTION**
> User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change the password for a specific user by typing

```
# passwd <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user’s login identification

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

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

7 When prompted, enter the password again for verification.

8 You have completed this procedure.

Changing an expired root password on a Sun server

Application

Use this procedure to change the root password on a Sun server in the event that it has expired.

Perform this procedure when your root password failed with "su: Sorry".

> **ATTENTION**
> User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

Before you perform this procedure, ensure you entered the root password without the Caps Lock key on. Also ensure the password was not changed.

Action

Perform the following steps to complete this procedure.

At the server console

1 Log in to the Sun server through the console (port A) using the root user ID and the expired root password.

2 When prompted, enter the old (expired) password.

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

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

4 When prompted, enter the password again for verification.

5 You have completed this procedure.

Deleting a user from a Sun server

Action

Use this procedure to delete a user from a Sun server.

> **ATTENTION**
> User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

6 You have completed this procedure.

Setting the Oracle Listener password on a Sun server

Application

The Oracle Listener requires a password to perform most operations within the listener interactive command prompt. A password is required to perform operations such as "**stop**" or "**services**". This procedure demonstrates how to specify your current password.

> ***Note:*** When the system is installed, the default Oracle Listener password is set to "oracle". To change this default password, use the Changing the Oracle Listener password on a Sun server procedure.

> **ATTENTION**
> User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the Oracle Listener application by typing

```
# lsnrctl
```

and pressing the Enter key.

Example response

```
Welcome to LSNRCTL, type “help” for information.
LSNRCTL>
```

6 Initiate the password setting by typing

```
LSNRCTRL> set password
```

and pressing the Enter key.

Example response

```
Password:
```

7 Type your current password at the prompt and press the Enter key.

Example response

```
The command completed successfully
```

8 You have completed this procedure.

Changing the Oracle Listener password on a Sun server

Application

The default password for the Oracle Listener is set to “oracle” during the SSPFS installation. This procedure provides the steps to change the Oracle Listener password on a Sun server.

ATTENTION
User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the Oracle Listener application by typing

```
# lsnrctl
```

and pressing the Enter key.

Example response:

```
Welcome to LSNRCTL, type “help” for information.
```

6 Initiate the password change by typing

```
LSNRCTL> change password
```

and pressing the Enter key.

Example response

```
Old password:
```

7 When prompted, enter the old (current) password.

Example response

```
New password:
```

8 When prompted, enter the new password.

Example response

```
Reenter new password:
```

9 When prompted, enter the new password again to confirm it.

Example response

```
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=47.143.107.192) (PORT=1521)))
Password changed for LISTENER
The command completed successfully
```

10 Initiate the password setting by typing

```
LSNRCTL> set password
```

and pressing the Enter key.

Example response

```
Password:
```

11 When prompted, enter the new password.

Example response

```
The command completed successfully
```

12 Save the new password by typing

```
LSNRCTL> save_config
```

and pressing the Enter key.

Example response

```
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=47.143.107.192) (PORT=1521)))
Saved LISTENER configuration parameters.
Listener Parameter File
/opt/oracle/product/8.1.7/network/admin/listen
er.ora
Old Parameter File
/opt/oracle/product/8.1.7/network/admin/listen
er.bak
The command completed successfully
```

13 You have completed this procedure.

Setting secure FTP proxy

Application

In order to have a secure (i.e. encrypted) channel of FTP communication between the OSS/FTP clients and network elements, you need to set up SSH port forwarding. Use one of the following procedures to set secure FTP proxy using SSH port forwarding:

- Setting up SSH port forwarding on Unix
- Setting up SSH port forwarding on Windows

Once set up, SSH port forwarding establishes a port forwarding session from client to server, wherein all data forwarded are encrypted and hence secure.

Prerequisites

You need to have SSH software.

Action

Perform the following steps to complete this procedure.

Setting up SSH port forwarding on Unix

At your workstation

1 Install the SSH software.

2 Establish a port-forwarding session between your workstation and the CS 2000 Management Tools server by typing

```
# ssh -L 9999:<remote-host>:9999 <remote-host>
```

and pressing the Enter key.

The first time you run the above command on your workstation in an attempt to forward data to remote-host, you will receive the following message and prompt:

```
The authenticity of host “remote-Host
(1.2.3.4)” can’t be established. RSA key
fingerprint is <finger print information>. Are
you sure you want to continue connecting
(yes/no)?
```

SSH is verifying whether the host “remote-host” is a trusted host and whether you want to continue connecting to it.

3 When prompted, confirm you want to continue connecting by typing

```
# yes
```

and pressing the Enter key.

4 When prompted, enter your password.

Once your password is verified, a port-forwarding session is established. From this point on, all new sessions connecting to “localhost:local-port”will be forwarded to “remote-host:remote-port” in a secure channel.

Example
You set up SSH port forwarding on machine A with the following command:

```
# ssh-L 9999:CS 2000 Management Tools
host:9999 CS 2000 Management Tools host
```

To securely transmit data from machine A to the CS 2000 Management Tools server, you need to open a window logged into machine A, and type the following command:

```
# telnet localhost 9999
```

The telnet connection automatically gets secured between machine A and the CS 2000 Management Tools server.

5 You have completed this procedure.

Setting up SSH port forwarding on Windows

At your workstation

1 Install PuTTY software.

2 Launch PuTTY to display the PuTTY Configuration window.

3 Configure SSH port forwarding as follows:

a Click on ”Session” and complete the following fields:

- In the “Host Name (or IP address)” field, enter the host name or IP address of the CS 2000 Management Tools server.
- In the “Port” field, enter 22.
- Under “Protocol:” select SSH.

b Click on ”Tunnels” and complete the following fields:

- In the “Source port” field, enter any local port value, for example 9999.
- In the “Destination” field, enter <host:port>, where “host” is the host name of the CS 2000 Management Tools server, and “port” is the port number on which the CS 2000 Management Tools server listens for input (9999 is the standard port on which the CS 2000 Management Tools server listens for a client connection)
- Select “Local”, and click the Add button.
- Click the Open button.

The first time you attempt to open a session, a PuTTY Security Alert window pops up to verify whether the host you want to connect to is a trusted host and whether you want to continue connecting to it.

4 Confirm you want to connect by clicking Yes in the PuTTY Security Aler window.

5 When prompted, enter your user ID and password.

This port-forwarding session is established.

You can now establish a secure connection between your workstation (client machine) and the CS 2000 Management Tools server as long as the port-forwarding session you just created exists.

6 Establish a secure connection as follows:

a Click on the computer icon in the top left-hand corner of the window.

b Select “New Session...” from the pull-down menu.

The PuTTY Configuration window opens.

c Click on ”Session” and complete the following fields:

- In the “Host Name (or IP address)” field, enter “localhost”.
- In the “Port” field, enter 9999.
- Under “Protocol:” select Telnet.

A secure session with the CS 2000 Management Tools server is established.

7 You have completed this procedure.

Configuring automated data backups on a Sun server

Application

Use this procedure to view or change the configuration settings for an automated data backup on a Sun server. The automated backup backs up Oracle and critical data.

> ***Note:*** Log SPFS320 is generated when an automated data backup fails, and when the backup failure is cleared and the backup completes successfully. Refer to the Succession Fault Management Logs Reference document, NN10275-909 for log details.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you want to configure automated data backups

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View

 2 - Configuration

 3 - Other


 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

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 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the Database Configuration option by typing

```
select - 9
```

and pressing the Enter key.

Response

```
Database Configuration
 1 - change_db (Change Database Host)
 2 - change_orabackup (Configure database
     backup)

 X - exit

select -
```

8 Select the change_orabackup option by typing

```
select - 2
```

and pressing the Enter key.

Example response

```
===Executing “change_orabackup”

Current setting:
Automated Backup Enabled N
Backup Time      6:00 Hours

Enable Automated backup (default: N):
```

9 When prompted, enter **Y** to enable automated backup or press the Enter key to accept the default value (N) to disable automated backup.

Example response

```
Set backup hour to: (default: 22):
```

10 When prompted, enter the time you want the automated backup to occur, or press the Enter key to accept the default value.

Example response

```
New settings:
Automated Backup Enabled   Y
Backup Time               22:00 Hours

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

11 Commit the changes by typing

```
ok
```

and pressing the Enter key.

Example response

```
===”change_orabackup” completed successfully
```

> ***Note:*** If enabled, automated backup will start within the first 45 seconds of the backup hour. If the backup hour is set to the current hour, automated backup will occur 24 hours from the current hour.

12 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.

13 You have completed this procedure.

Performing a data backup on a Sun server

Application

Use this procedure to perform a data backup on a Sun server.

ATTENTION
It is recommended that provisioning activities be put on hold during the time of the data backup.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS SN06.2 or greater
- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (t1400 only)
- you need one or more blank DVD-RW of 4.7 GB to store the data (Netra 240 only) - please note that the backup utility limits the storage to 2 GB per DVD-RW

ATTENTION
The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have an image of both before you proceed. Performing a restore from the Oracle database alone may cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the blank tape or DVD-RW into the drive.

At your workstation

2 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the Sun server on which you are performing the backup

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape	step 6
a DVD-RW	step 7

6 Rewind the tape by typing

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

and pressing the Enter key.

7 Backup the data by typing

```
$ /opt/nortel/sspfs/bks/bkdata
```

and pressing the Enter key.

Example response:

```
Backup Completes Successfully
```

If you are using	Do
a tape	step 8
a DVD-RW	step 9

8 Verify the backup on tape was successful as follows:

a List the content of the tape by typing

```
# gtar tvf /dev/rmt/0
```

and pressing the Enter key.

Example response:

```
-rw-rw-rw- root/other  1291264 2003-10-01
15:58 oracle.dmp
-rw-rw-rw- root/other     8192 2003-10-01
15:58 critdata.cpio
```

b Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

9 Verify the backup on DVD-RW was successful as follows:

a List the content of the DVD-RW by typing

```
# gtar tvf /cdrom/*bkdata*/current.tar
```

and pressing the Enter key.

Example response:

```
-rw-rw-rw- root/other  1291264 2003-10-01
15:58 oracle.dmp
-rw-rw-rw- root/other     8192 2003-10-01
15:58 critdata.cpio
```

b Remove the DVD-RW from the drive, label it, and store it in a safe place.

10 You have completed this procedure.

Performing a full backup of file systems

Application

Use this procedure to perform a full backup of the file systems on the CS 2000 Management Tools server.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS SN06.2 or greater
- you must perform a data backup prior to performing this procedure (refer to procedure Performing a data backup on a Sun server in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required)
- you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data (T1400 only)
- you need one or more blank DVD-RW of 4.7 GB to store the data (Netra 240 only) - please note that the backup utility limits the storage to 2 GB per DVD-RW

Action

At the CS 2000 Management Tools server

1 Insert a blank tape or DVD-RW into the drive.

At your workstation

2 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape	step 6
a DVD-RW	step 7

6 Rewind the tape by typing

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

and pressing the Enter key.

7 Backup the file systems by typing

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

and pressing the Enter key.

Example response:

```
Backup Completed Successfully
```

> ***Note:*** If you are using DVD-RW, you may be prompted to insert another blank DVD.

If you are using	Do
a tape	step 8
a DVD-RW	step 9

8 Verify the backup to tape was successful as follows:

a List the content of the tape by typing

```
# gtar tvf /dev/rmt/0
```

and pressing the Enter key.

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

9 Verify the backup to DVD was successful as follows:

a List the content of the DVD by typing

```
# gtar tvf /cdrom/*bkfullsys*/current.tar
```

and pressing the Enter key.

b Remove the DVD from the drive, label it, and store it in a safe place.

10 You have completed this procedure.

Performing a data restore on a Sun server

Application

Use this procedure to restore data from a backup tape or DVD-RW on a Sun server.

Prerequisites

You need the tape or the DVD-RW on which the data was backed up.

Action

Perform the following steps to complete this procedure.

At the Sun server

1 Insert the backup tape or DVD-RW into the drive.

At your workstation

2 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you are performing the data restore

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.

6 Stop the server applications that run on the Sun server.

On a Sun server that runs the CS 2000 Management Tools, stop the SESM, SAM21 EM, and NPM server applications. Refer to the CS 2000 Management Tools Administration and Security document, NN10172-611, if required.

On a Sun server that runs the Media Gateway 9000 Manager, stop the MG 9000 Manager server application and the mid-tier server application. Refer to the MG9000 Administration and Security document, NN10162-611, if required.

7 Restore the database by typing

```
$ /opt/nortel/sspfs/bks/rsdata
```

and pressing the Enter key.

8 Remove the backup tape or the DVD-RW from the drive, and store it in a safe place.

9 Verify the database restored properly.

10 Start the server applications that run on the Sun server.

On a Sun server that runs the CS 2000 Management Tools, stop the SESM, SAM21 EM, and NPM server applications. Refer to the CS 2000 Management Tools Administration and Security document, NN10172-611, if required.

On a Sun server that runs the Media Gateway 9000 Manager, stop the MG 9000 Manager server application and the mid-tier server application. Refer to the MG9000 Administration and Security document, NN10162-611, if required.

11 You have completed this procedure.

Performing a full system restore on a Sun server

Application

Use this procedure to perform a full system restore on a Sun server from tape on a t1400 server or DVD-RW on a Netra 240 server. Use one of the methods below according to your office configuration.

- Simplex configuration (one server)
- High-availability configuration (two servers)

> ***Note:*** Only the Simplex configuration (one server) is applicable to perform a full system restore from tape on a t1400 server.

Prerequisites

You need the backup tape or DVD-RW.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At the Sun server console

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

2 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

3 Insert SSPFS CD disk#1 into the CD/DVD drive.

4 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

5 When prompted, accept the software license restrictions by typing

```
ok
```

and pressing the Enter key.

The system reboots.

6 When prompted, insert the backup tape or Volume 1 of the backup DVD-RW into the drive.

The restore process can run for several minutes and may prompt you for additional Volumes that were generated during the full system backup to DVD-RW.

7 Restore the data. Refer to procedure Performing a data restore on a Sun server in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required. Once the data restore is complete, reboot the system by typing

```
# init 6
```

and pressing the Enter key.

8 You have completed this procedure.

High-availability configuration (two servers)

At the console connected to the inactive node

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

2 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

At the console connected to the active node

3 Log in to the active node through the console (port A) using the root user ID and password.

4 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

5 Insert SSPFS CD disk#1 into the CD/DVD drive.

6 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

7 When prompted, accept the software license restrictions by typing

```
ok
```

and press the Enter key.

The system reboots.

8 When prompted, insert Volume 1 of the backup DVD-RW into the drive.

The restore process can run for several minutes and may prompt you for additional Volumes that were generated during the full system backup to DVD-RW.

9 Restore the data. Refer to procedure Performing a data restore on a Sun server in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required. Once the data restore is complete, reboot the system by typing

```
# init 6
```

and press the Enter key.

10 Re-image the inactive node using the active node's image. Refer to procedure "Cloning the image of one node in a cluster to the other node" in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required.

11 You have completed this procedure.

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

Application

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

Prerequisites

You need the root user ID and password.

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

Action

Perform the following steps to complete this procedure.

At the console connected to the active node

1 Log in to the active node through the console (port A) using the root user ID and password.

2 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
PSE                      RUNNING
PROP_SRV                 RUNNING
WEBSERVER                RUNNING
DATABASE                 RUNNING
SAM21EM                  RUNNING
SESMService              RUNNING
CORBA                    RUNNING
ORA_ARCHIVE_ROTATOR      RUNNING
OMPUSH                   RUNNING
BOOTB                    RUNNING
WEBSERVICES              RUNNING
ORA_AUTO_BACKUP          RUNNING
APS                      RUNNING
NPM                      RUNNING
```

3 Use the following table to determine your next step.

If	Do
all applications are running	step 6
one or more applications are not running	step 4

4 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

5 Use the following table to determine your next step.

If	Do
one or more applications do not start	contact your next level of support
all applications are running	step 6

6 Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

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

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

  SESM APPLICATION STATUS: All Applications ready
```

7 Use the following table to determine your next step.

If the SESMService is	Do
not fully functional	contact your next level of support
fully functional	step 9

At the console connected to the inactive node

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

9 Bring the system to the OK prompt by typing

```
# init 0
```

and press the Enter key.

10 At the OK prompt, display the Ethernet address of the inactive node 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.
```

11 Take note of the Ethernet address that is displayed.

At the console connected to the active node

12 Start the cloning process by typing

```
# startb
```

and press the Enter key.

Example response:

```
Please enter the ethernet address for the other
unit:
```

13 When prompted, enter the Ethernet address of the inactive node you noted in step 11.

Example response:

```
SSH public private key pair present
d99: Soft Partition is setup
exporting / to unit1-priv0
exporiting /var to unit1-priv0
exporting /opt to unit1-priv0
exporting /opt/nortel to unit1-priv0

Enter the command “boot net - image” at the “ok”
prompt of unit1-priv0
```

The system response progresses on the active node once you enter the command in step 14.

At the console connected to the inactive node

14 When prompted, boot the inactive node from the image of the active node by typing

```
OK boot net - image
```

and press the Enter key.

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

Example response:

```
SC Alert: Host System has Reset


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


Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

15 Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

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.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

16 Once the cloning process is complete, stop and start the PSE server application as follows:

a Stop the PSE server application by typing

```
# servstop PSE
```

and pressing the Enter key.

b Start the PSE server application by typing

```
# servstart PSE
```

and pressing the Enter key.

17 You have completed this procedure.

Starting the SESM server application

Application

Use this procedure to start the SESM server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, start the SESM server application as follows:

a Start the SESM server by typing

```
# ptmctl -f start
```

and pressing the Enter key.

b Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

c Verify the SESM server application started by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS --------------------------------

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

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

SESM APPLICATION STATUS: All Applications
ready
```

7 For the SN06.2 or greater release, start the SESM server application as follows:

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

a Start the SESM server application by typing

```
# servstart SESMService
```

and pressing the Enter key.

b Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

c Verify the SESM server application started by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

8 You have completed this procedure.

Starting the SAM21 Manager server application

Application

Use this procedure to start the SAM21 Manager server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, start the SAM21 Manager server application as follows:

a Start the SAM21 Manager server application by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl start
```

and pressing the Enter key.

b Verify the SAM21 Manager server application started by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl status
```

and pressing the Enter key.

7 For the SN06.2 or greater release, start the SAM21 Manager server application as follows:

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

a Start the SAM21 Manager server application by typing

```
# servstart SAM21EM
```

and pressing the Enter key.

b Verify the SAM21 Manager server application started by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

8 You have completed this procedure.

Starting the NPM server application

Application

Use this procedure to start the Network Patch Manager (NPM) server application.

Prerequisites

Both CORBA and the database must be installed.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, start the NPM server application as follows:

a Start the NPM server application by typing

```
# npmsrvr start
```

and pressing the Enter key.

b Verify the NPM server application started by typing

```
# npmsrvr status
```

and pressing the Enter key.

Example response:

```
The NpmServer is running
```

Note: Wait approximately 1 min. before using the NPM.

7 For the SN06.2 or greater release, start the NPM server application as follows:

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

a Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

b Verify the NPM server application started by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

Note: Wait approximately 1 min. before using the NPM.

8 You have completed this procedure.

Launching CS 2000 Management Tools client applications

Application

Use this procedure to launch any one of the following CS 2000 Management Tools client application graphical user interfaces (GUIs):

- Trunk Maintenance Manager
- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

  Note: The Network Patch Manager also has a command line user interface (CLUI). Refer to procedure Accessing the Network Patch Manager CLUI in this document.

- Batch Configuration Monitor

This procedure offers the following four methods to launch a CS 2000 Management Tools client application:

- Launching applications from a web browser. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching applications from a desktop icon or Start menu (Windows only).

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching specific applications using a URL.

Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section “Client workstation requirements” in the CS 2000 Management Tools Basics document, NN10020-111.

> **ATTENTION**
>
> If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you may experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following URL: http://developer.java.sun.com/developer/bugParade/bugs/4713003.html. A workaround for this issue is to download the latest ATI graphics driver from the following web site http://mirror.ati.com/support/driver.html. Contact your IT support team if you need assistance.

You need the IP address or host name of the CS 2000 Management Tools server, and a valid user name and password to launch an application.

Note: Users of the CS 2000 Management Tools client applications must belong to the primary user group “succssn” for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

You must have Java^{TM} 2 Runtime Environment (JRE) version 1.4.1_02 and Java^{TM} Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.1_02.

Action

Launching applications from a web browser

At your workstation

1 Launch your web browser.

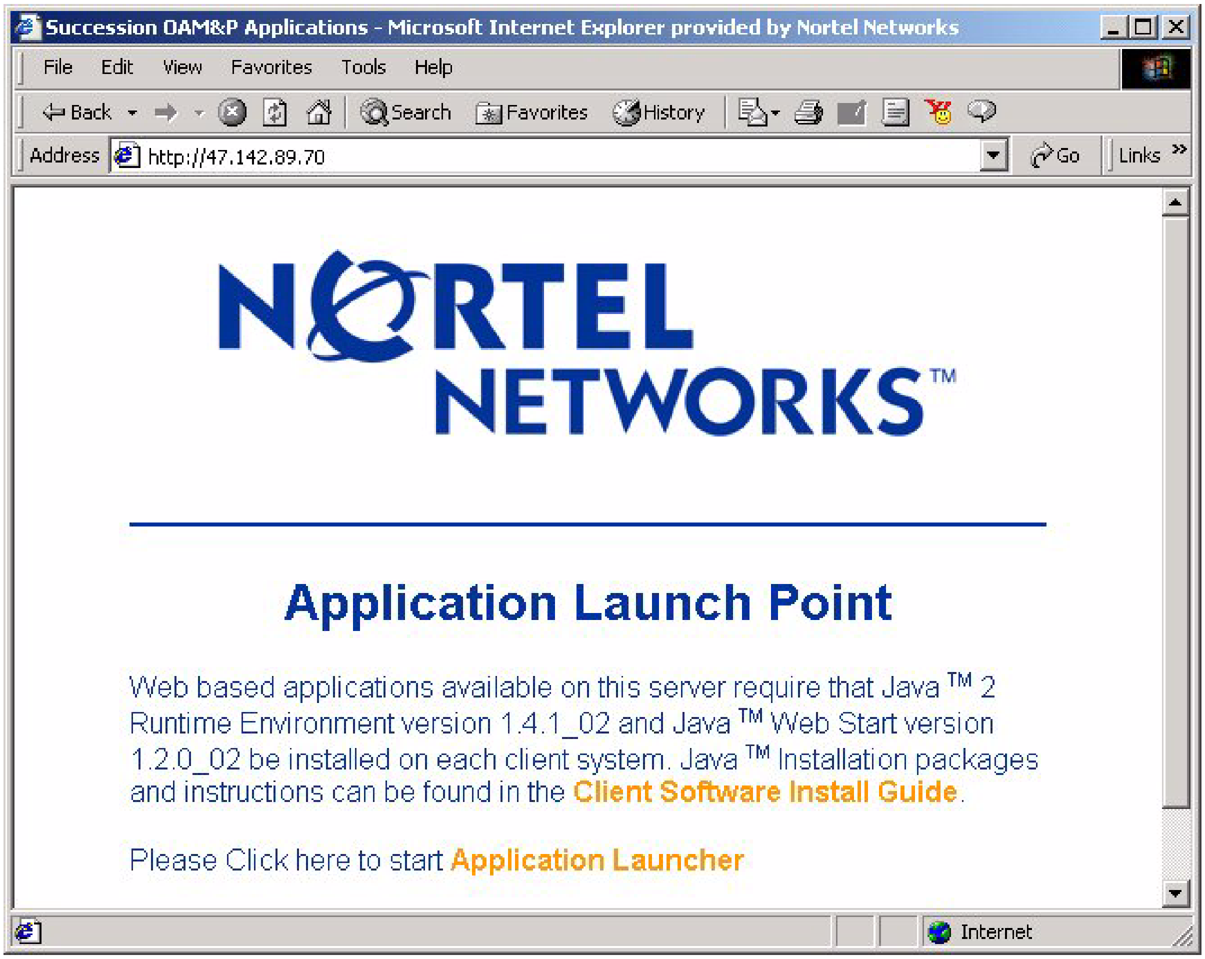
2 Access the CS 2000 Management Tools server by typing

>http://<host>

where

<host>
is the name or IP address of the CS 2000 Management Tools server where the CS2M software package is installed

The “Application Launch Point” page appears.



Succession OAM&P Applications - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.142.89.70
Go Links
NORTEL NETWORKS™
Internet

Application Launch Point

Web based applications available on this server require that Java ™ 2 Runtime Environment version 1.4.1_02 and Java ™ Web Start version 1.2.0_02 be installed on each client system. Java ™ Installation packages and instructions can be found in the Client Software Install Guide.

Please Click here to start Application Launcher

3 Refer to the following table to determine your next step.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 4
you do not know which version of JRE and JWS you have	step 4

4 Click **Client Software Install Guide** and follow the instructions under “How to check version” to verify your client setup.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 5

5 Click **Java 2 Runtime Environment Install Guide** under “Microsoft Windows” or “Sun Solaris” for system requirements and installation instructions.

6 Once you have read through the “Java 2 Runtime Environment Install Guide”, click the **Back** button to return to the “Client Software Installation” page.

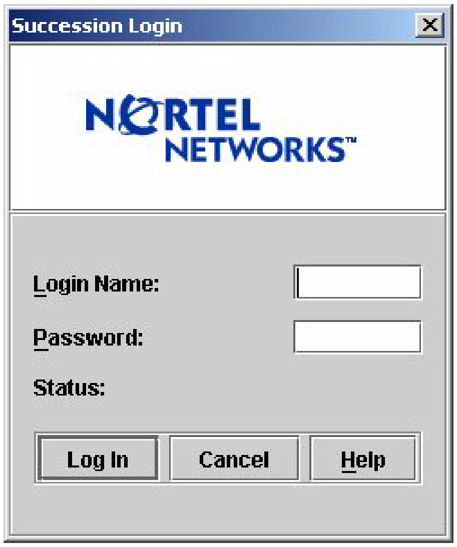
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

8 Click the **Back** button to return to the “Application Launch Point”.

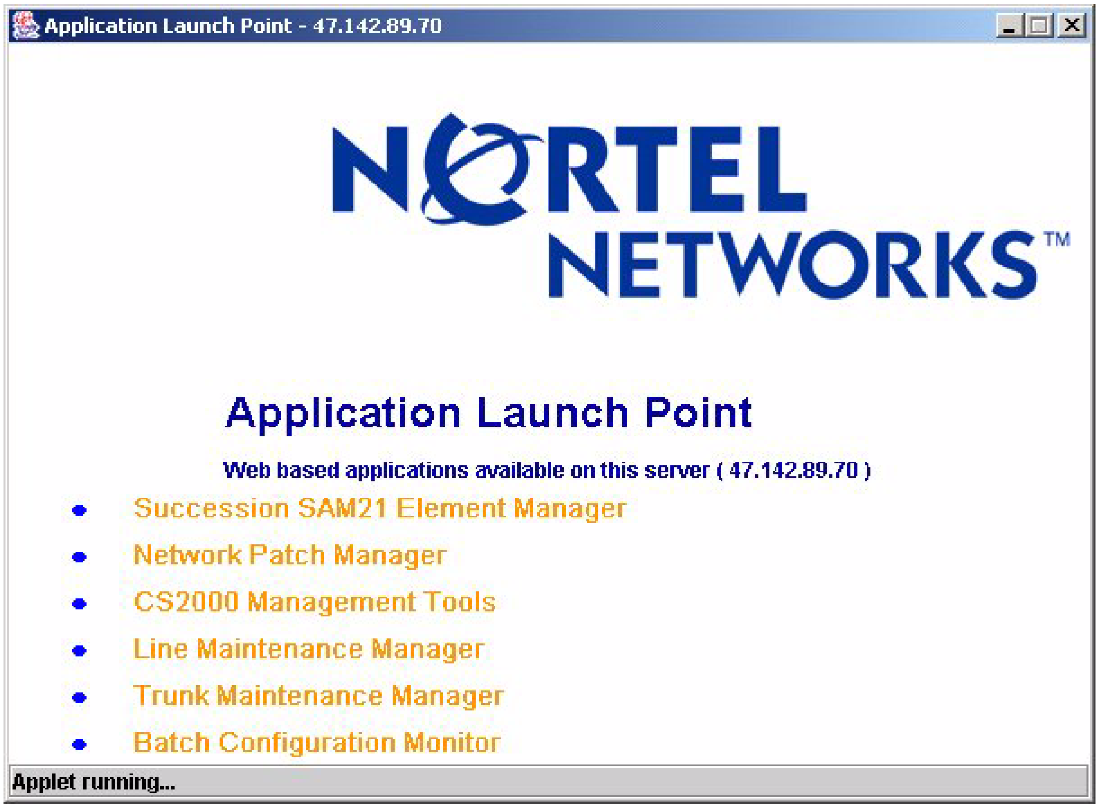
9 Click **Application Launcher**.

The Login window appears.



10 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.


Application Launch Point - 47.142.89.70
NORTEL NETWORKS
Application Launch Point
Web based applications available on this server (47.142.89.70)
Succession SAM21 Element Manager
Network Patch Manager
CS2000 Management Tools
Line Maintenance Manager
Trunk Maintenance Manager
Batch Configuration Monitor
Applet running...

11 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

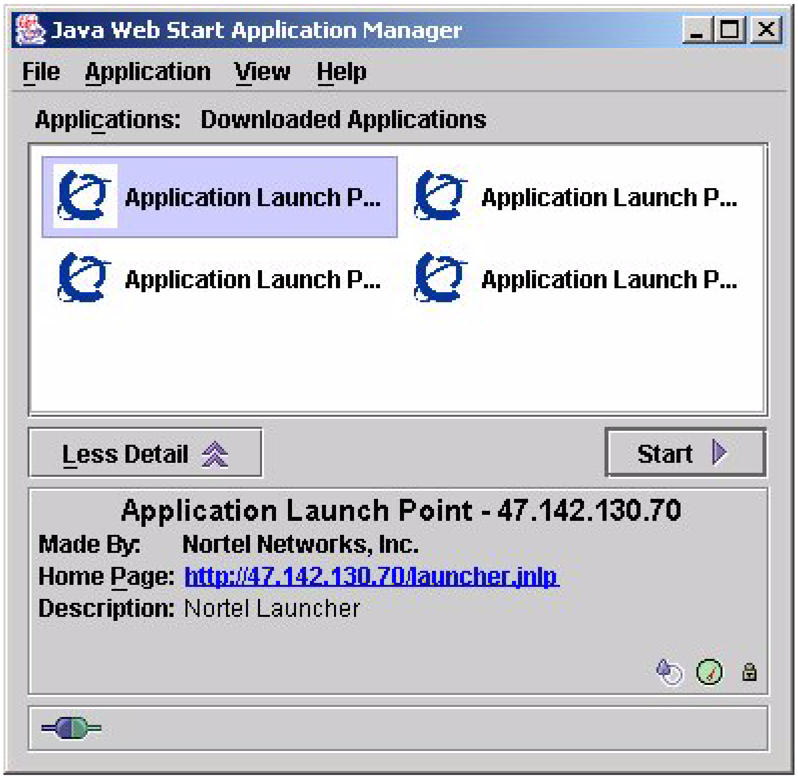
12 You have completed this procedure.

Launching applications from the JWS Application Manager

> **ATTENTION**
> You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Launch the Java Web Start Application Manager.



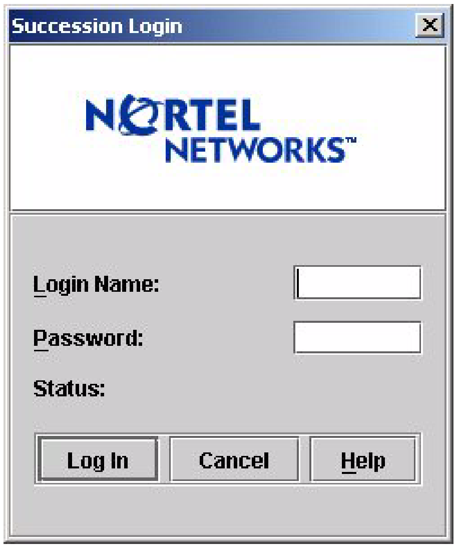
Application Launch Point - 47.142.130.70
Made By: Nortel Networks, Inc.
Home Page: http://47.142.130.70/launcher.jnlp
Description: Nortel Launcher

Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

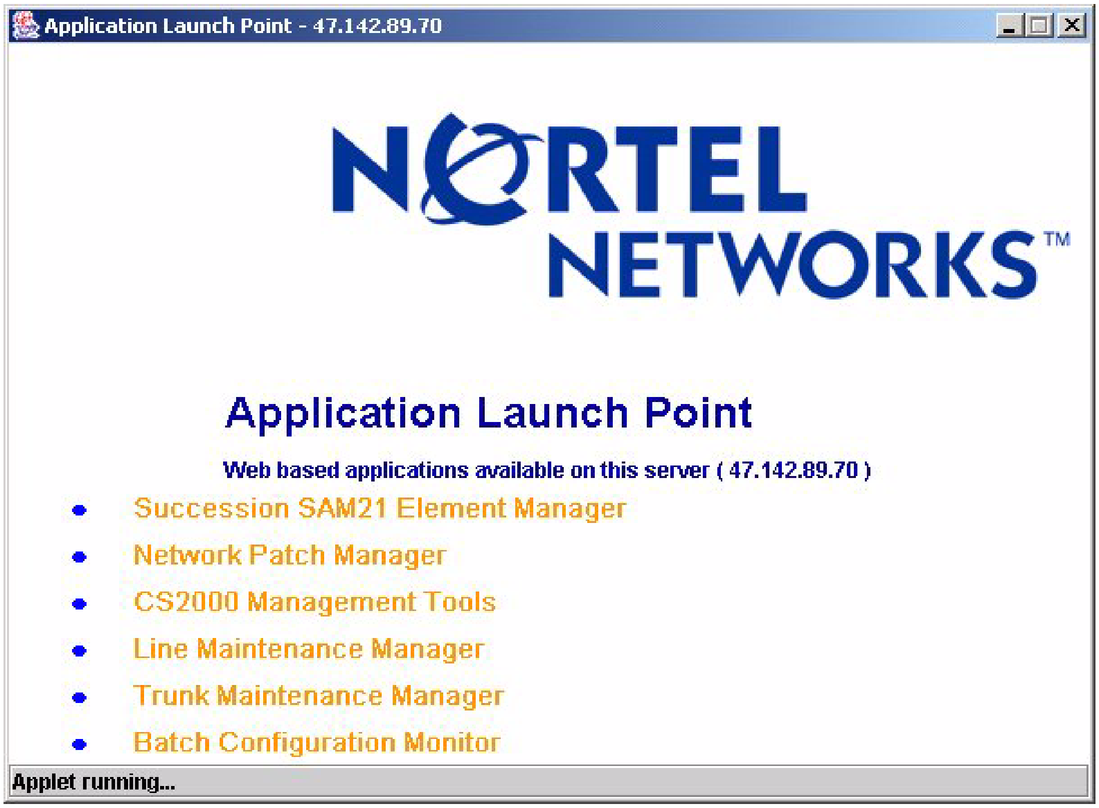
2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

The Login window appears.

3 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



Application Launch Point

Web based applications available on this server (47.142.89.70)

- Succession SAM21 Element Manager
- Network Patch Manager
- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor

Applet running...

4 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

5 You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

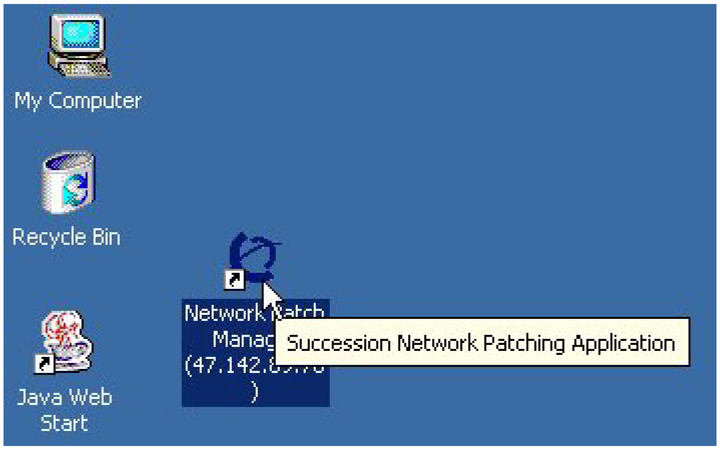
ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Perform step a to launch an application from a desktop icon, or b to launch an application from the Start menu.

a Locate the short-cut icon on your desktop, and double click on it to start the application.

Note: For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.

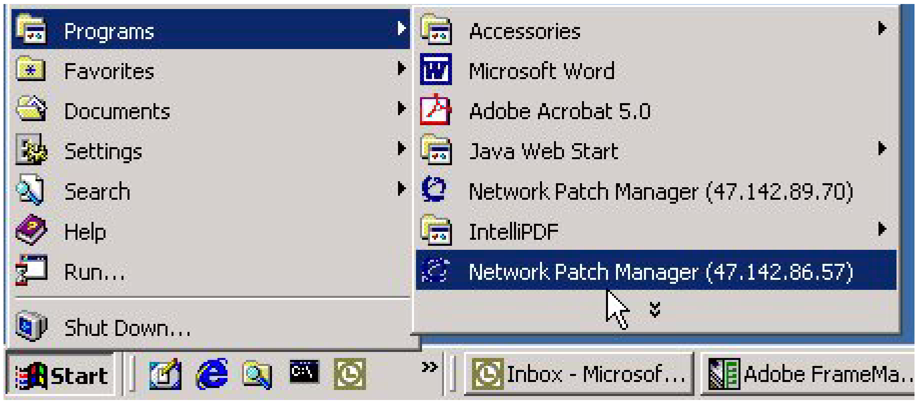

My Computer
Recycle Bin
Java Web Start
Network Patch Manag (47.142.
)
Succession Network Patching Application

The Login window appears.

Proceed to step 2.

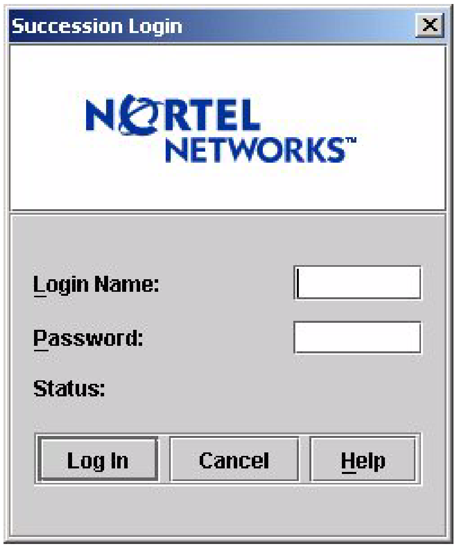
OR

b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click on the CS 2000 Management Tools client application you want to launch.

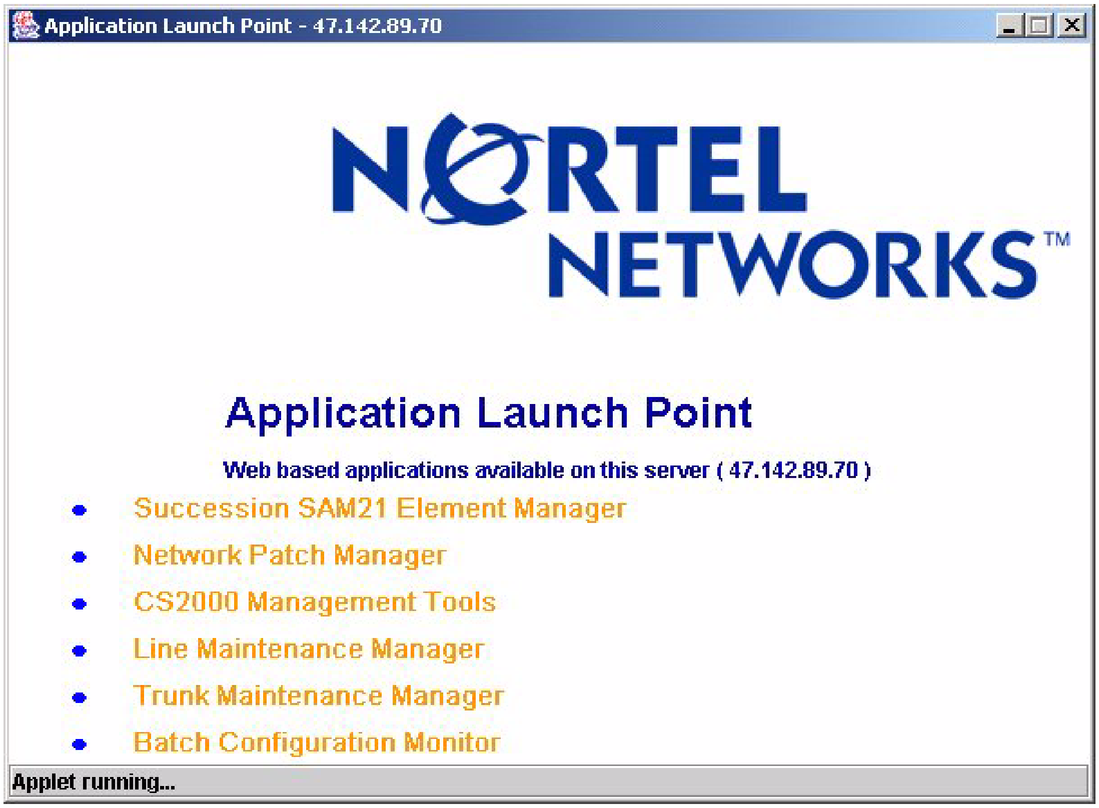


The Login window appears.

2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



Application Launch Point - 47.142.89.70

Application Launch Point

Web based applications available on this server (47.142.89.70)

- Succession SAM21 Element Manager
- Network Patch Manager
- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor

Applet running...

3 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

4 You have completed this procedure.

Launching specific applications using a URL

ATTENTION
You must have Java^{TM} 2 Runtime Environment (JRE) version 1.4.1_02 and Java^{TM} Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure Launching applications from a web browser.

At your workstation

1 Launch your web browser.

2 In the Address field, enter one of the following URLs for the application you want to launch:

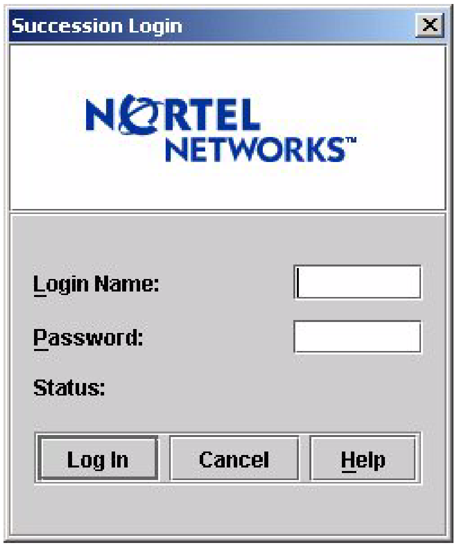
- CS2000 Management Tools - http://<host>/sesm/sesm.jnlp
- Line Maintenance Manager - http://<host>/sesm/lmm.jnlp
- Trunk Maintenance Manager - http://<host>/sesm/tmm.html
- Batch Configuration Monitor - http://<host>/sesm/bpt.html
- CS2000 SAM21 Manager - http://<host>/sam21em/sam21em.jnlp
- Network Patch Manager - http://<host>/npm/npm.jnlp

Where

host
is the host name or IP address of the CS 2000 Management Tools server

The Login window appears.

3 Enter your user name and password, then click **Log In**.



The interface for the application you launched, is displayed.

4 You have completed this procedure.

Accessing the Network Patch Manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

> ***Note:*** The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure Launching CS 2000 Management Tools client applications in this document.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter ‘npm’ commands, help
or quit to exit.

npm>
```

5 You have completed this procedure.

Starting the batch provisioning tool

Application

Use this procedure to start the batch provisioning tool.

Prerequisites

You must have a valid user ID and password.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Start the batch provisioning tool by typing

```
$ bpt
```

and pressing the Enter key.

4 When prompted, enter your username and password.

Example response:

```
Login in progress...

You are currently logged in as : rtps!

==========
Main Menu:
==========

     (1) Execute Batch File
     (2) Display Output
     (3) Display Logs
     (4) Delete Output or Log Files
     (h) Help

     (1) Exit

Selection: [1/2/3/4/h/x:1]
```

5 You have completed this procedure.

Connect to OSSGate

Application

Use this procedure to connect to OSSGate.

Prerequisites

You must have a telnet client that supports line mode and can implicitly add a Carriage Return (CR) to any data coming from the OSSGate server.

Action

Perform the following steps to complete this procedure.

From the telnet client

1 Connect to the OSSGate using the OSSGate Server name and the port number.

Example

```
> telnet <host_name> <port_number>
```

where

host_name
is the name of the CS 2000 Management Tools server

port_number
is the port number (default 10023)

Note: The entry of this command depends on your telnet client.

2 When prompted, enter your username and password separated by a space, and press the Enter key.

Example

```
Enter username and password
```

```
> ossuser osspassword
```

3 You have completed this procedure.

Changing modes within OSSGate

Application

Use this procedure to change between CI and XML mode in OSSGate. OSSGate supports two modes: Command Interface (CI) and XML. The default mode is CI for Lines.

Prerequisites

You must be logged in to OSSGate.

Action

Perform the following steps to complete this procedure.

From the OSSGate user interface

1 Change to Control mode by pressing the Control key and the B key (Ctrl+B) at the same time.

```
> ^B
```

and pressing the Enter key.

> ***Note:*** Based on the terminal settings, the Ctrl+B character may not be displayed on the screen.

2 At the prompt, enter the mode to change to by typing

```
? mode <new_mode>
```

and pressing the Enter key.

where

new_mode
is the mode (ci or xml) to change to

Example

```
> mode xml
```

The system responds with a confirmation of the mode change. The following example is for a mode change to XML.

```
Mode is XML.
```

3 You have completed this procedure.

Stopping the SESM server application

Application

Use this procedure to stop the SESM server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05	step 6
SN06 or SN06.1	step 7
SN06.2 or greater	step 8

6 For the SN05 release, stop the SESM server application by typing

```
# /opt/nortel/NTptm/bin/ptmctl stop
```

and pressing the Enter key.

7 For the SN06 or SN06.1 release, stop the SESM server application as follows:

a Stop the SESM server application including the Proxy Agent by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl -f stop
```

and pressing the Enter key.

b Verify the SESM server application stopped by typing

```
# /opt/nortel/NTsesm/admin/bin/ptmctl status
```

and pressing the Enter key.

Example response (without stopping Proxy Agent):

```
SESM STATUS --------------------------------

  COMPONENT                    STATUS
  ---------                    ------
 Proxy Agent                   NOT RUNNING
 RMI Registry                  NOT RUNNING
 Snmpfactory                   NOT RUNNING
 MI2 Server                    NOT RUNNING

Current number of SESM processes running: 0
(of 4)

SESM APPLICATION STATUS: No Applications are
ready
```

8 For the SN06.2 or greater release, stop the SESM server application by typing

> ***Note:*** In a two-server configuration, perform the steps that follow on the active side.

```
# servstop SESMService
```

and pressing the Enter key.

9 Verify the SESM server application stopped by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

10 You have completed this procedure.

Stopping the SAM21 Manager server application

Application

Use this procedure to stop the SAM21 Manager server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, stop the SAM21 Manager server application as follows:

a Stop the SAM21 Manager server application by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl stop
```

and pressing the Enter key.

b Verify the SAM21 Manager server application stopped by typing

```
# /opt/nortel/sam21em/bin/sam21emCtrl status
```

and pressing the Enter key.

7 For the SN06.2 or greater release, stop the SAM21 Manager server application as follows:

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

a Stop the SAM21 Manager server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

b Verify the SAM21 Manager server application stopped by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

8 You have completed this procedure.

Stopping the NPM server application

Application

Use this procedure to stop the Network Patch Manager (NPM) server application.

Prerequisites

All users of the NPM CLUI and GUI should exit before stopping the NPM server application.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If the release you are running is	Do
SN05, SN06 or SN06.1	step 6
SN06.2 or greater	step 7

6 For the SN05, SN06, or SN06.1 release, stop the NPM server application as follows:

a Stop the NPM server by typing

```
# npmsrvr stop
```

and pressing the Enter key.

b Verify the NPM server application stopped by typing

```
# npmsrvr status
```

and pressing the Enter key.

7 For the SN06.2 or greater release, stop the NPM server application as follows:

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

a Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

b Verify the NPM server application stopped by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

8 You have completed this procedure.

Disconnect from OSSGate

Application

Use this procedure to disconnect from OSSGate.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

From the OSSGate user interface

1 Change to Control mode by pressing the Control key and the B key (Ctrl+B) at the same time.

```
> ^B
```

and pressing the Enter key.

> ***Note:*** Based on the terminal settings, the Ctrl+B character may not be displayed on the screen.

2 Log out by typing

```
? logout
```

and pressing the Enter key.

You are returned to the input (‘>’) prompt.

3 Change to Control mode by pressing the Control key and the B key (Ctrl+B) at the same time.

```
> ^B
```

and pressing the Enter key.

> ***Note:*** Based on the terminal settings, the Ctrl+B character may not be displayed on the screen.

4 End the session by typing

```
? clearconv
```

and pressing the Enter key.

5 You have completed this procedure.

Starting and stopping the PM Poller

Application

Use this procedure to start the PM poller on a network element, or stop the PM poller after you have collected the required data on the network element.

Prerequisites

The SSPFS must be installed and running the SN06 or later load.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change to the PM poller directory by typing

```
# cd /opt/nortel/snmp-poller/bin
```

and pressing the Enter key.

6 Use the following table to determine your next step.

If you want to	Do
start the PM poller	step 7
stop the PM poller	step 9

7 Start the PM poller as follows:

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

a Start the PM poller by typing

```
# servstart SNMP_POLLER
```

and pressing the Enter key.

b Verify the PM poller started by typing

```
# servman query -status -group SNMP_POLLER
```

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status
-group SNMP_POLLER.
pmfadm -c snmpp -n 5 -t 60
/opt/nortel/snmp-poller/bin/snmpp -c
/opt/nortel/snmp-poller/config/poller-config.xml
     retries: 0
     owner:   root
     pids:    23853
The poller process is running.
```

8 Use the following table to determine your next step.

If you want to	Do
leave the PM poller running	you have completed this procedure
stop the PM poller	step 9

9 Stop the PM poller as follows:

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

a Start the PM poller by typing

```
# servstop SNMP_POLLER
```

and pressing the Enter key.

Example response

```
SNMP_POLLER stopped
```

b Verify the PM poller stopped by typing

```
# servman query -status -group SNMP_POLLER
```

and pressing the Enter key.

Example response

```
Wed 19 Mar 2003 09:36:08 AM EDT: status poller
command.
pmfadm: “snmpp” No such <nametag> registered

The poller process is not running.
```

10 You have completed this procedure.

Starting and stopping the QoS Collector Application

Application

Use this procedure to start or stop the QoS Collector Application (QCA) on the CS 2000 Management Tools server.

You need to stop and restart the QCA after you performed procedure “Configuring the QoS Collector Application” in the Configuration Management document.

Prerequisites

None

Action

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify the status of QCA by typing

```
# /opt/nortel/qca/query_qca
```

and pressing the Enter key.

6 Use the following table to determine your next step.

If you want to	Do
start QCA	step 7
stop QCA	step 8

7 Start QCA by typing

```
# /opt/nortel/qca/qca_server
```

and pressing the Enter key.

Response

```
Attempting to register QCA as Qca with PMFADM.
```

If a QCA instance has not already been started with the `qca_server` script, the following message is displayed:

```
Registration as Qca was ok. QCA started.

QCA has been started with the following
properties...
MaxFileSize=1 (Range is 1 to 100)
MaxFileTime=15 (Range is 1 to 240)
recycleToD=0 (Range is 0 to 23)
portNumber=20000 (Range is 20000 to 20004)
RetainFileTime=5 (Range is 1 to 30)
fileExt=xml (Default is xml)
nodeName=QCA (Default is QCA)
closedFileCompression=true (Default is 'True')
oldFileCompression=true (Default is 'True')

Please check /var/log/customerlog if any of the
above properties are out of range.
```

If a QCA instance has already been started with the `qca_server` script the following message is displayed:

```
pmfadm: Request "Qca" already queued.
Could not register QCA as Qca with PMFADM, this
suggests a QCA instance is already running.
If a second QCA instance is required please use
the qca_server2 script.
```

> ***Note:*** Only use the `qca_server2` script when a second QCA instance is required for a single host in-service upgrade.

When you start QCA, the values in the configuration file (qca.properties) are validated. If a value in the configuration file is invalid or missing, the default value is used. When this occurs, a log is generated to inform you that a default value is being used. If using default values is unacceptable, you can stop QCA at this point, and change the values.

If	Do
a log is generated and you want to stop QCA	step 8
a log is generated but you do not want to stop QCA	you have completed this procedure
no log is generated	you have completed this procedure

8 Stop QCA by typing

```
# /opt/nortel/qca/stop_qca
```

and pressing the Enter key.

Response

```
Are you sure you want to stop the QCA? Have you
checked the port number in qca.properties? [no
or yes].
```

Note: If a second instance of QCA was started, stop QCA using “stop_qca2”.

If you	Do
checked the port number	step 10
did not check the port number	step 9

9 Check the port number in qca.properties, and repeat step 8.

10 Confirm you checked the port number by typing

yes

and pressing the Enter key.

Example response

```
Attempting to unregister QCA as Qca fro PMFADM.
Attempting to stop local QCA on port : 20001
QCA stopped successfully.
```

11 You have completed this procedure.

Starting the OMPUSH server application

Application

Use this procedure to start the OMPUSH server application.

> ***Note:*** The OMPUSH server application is automatically started with SSPFS.

Prerequisites

The Succession Server Platform Foundation Software (SSPFS) must be at release SN06.2 or higher.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where SSPFS is installed

2 When prompted, enter your user ID and password.

3 Determine the status of the OMPUSH server application by typing

```
$ ompush_ctl -status
```

and pressing the Enter key.

If the OMPUSH server application	Do
is not running	step 4
is running	you have completed this procedure

4 Start the OMPUSH server application by typing

```
$ ompush_ctl -start
```

and pressing the Enter key.

Example response:

```
Tue May 22 19:13:38 2003: start ompush command.
The OMPUSH start command was sent.
```

5 You have completed this procedure.

Stopping the OMPUSH server application

Application

Use this procedure to stop the OMPUSH server application.

Prerequisites

The Succession Server Platform Foundation Software (SSPFS) must be at release SN06.2 or higher.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where SSPFS is installed

2 When prompted, enter your user ID and password.

3 Determine the status of the OMPUSH server application by typing

```
$ ompush_ctl -status
```

and pressing the Enter key.

If the OMPUSH server application	Do
is running	step 4
is not running	you have completed this procedure

4 Stop the OMPUSH server application by typing

```
$ ompush_ctl -stop
```

and pressing the Enter key.

Example response:

```
Tue May 22 19:13:38 2003: start ompush command.
The OMPUSH stop command was sent.
```

5 You have completed this procedure.