Policy Controller Security and Administration

What's new in this release?

Virtual Private Networks (VPN) functionality is new for the Policy Controller for (I)SN09.

Security and administration strategy overview

The security and administrative strategy for the Policy Controller centers around the following primary activities:

- Security administration of the Policy Controller, which includes managing user IDs and passwords, and acquiring security certificates
- Operational administration and maintenance of the Policy Controller platform and applications, which includes activities surrounding managing the Policy Controller platform NCGL (Nortel Carrier-grade Linux) and hardware as well as the Policy Controller application software running on the platform
- Backing up the Policy Controller application database, which focuses on maintaining a backup strategy of the Policy Controller application database.

Tools and utilities

Security administration and operational administration of the Policy Controller is performed primarily through the two Policy Controller web interfaces and a command line interface (CLI):

- CS 2000 NCGL Platform Manager
- Policy Controller GUI

Most system and operations administrative functions and security functions are performed using these interfaces, which are accessed from a single login point.

Backup and restore functions are performed using the Policy Controller CLI-based (command line interface) console provided by the NCGL.

An online help guide is available for the CS 2000 NCGL Platform Manager GUI only. Clicking the **Help** link opens a help file.

Methods of accessing Policy Controller GUIs and CLI

There are three primary methods for accessing Policy Controller user interfaces:

- All GUI and CLI interfaces to the Policy Controller GUI can be accessed by selecting and right-clicking on the active Policy

Controller element from the Integrated EMS expanded Network Elements view, as shown below.

Accessing Policy Controller GUIs or CLI from the Integrated EMS

For more information, refer to procedure Access Policy Controller/NCGL GUIs or CLI using the Integrated EMS on page 22. For more information about using the Integrated EMS service, refer to the Integrated EMS Basics NTP, NN10329-111.

- All GUI interfaces to the Policy Controller can be accessed from a remote system known to the SSPFS proxy server (running on CS 2000 Management Tools server) on the CS-LAN. Refer to *Policy Controller Configuration Management*, NN10432-511, for more information about configuring a web proxy service on the SSPFS.

- The CLI interface can be accessed through a secure shell (SSH) connection from a remote client to the Policy Controller by way of SSH/telnet access through the SSPFS server.
- The CLI can also be accessed using a console connected to the rear of the Policy Controller active unit. In some cases, this connection is wired to a terminal box. Refer to *Policy Controller Configuration Management*, NN10432-511, for more information about using this CLI access method.

Operational administration procedures for the Policy Controller GUIs and CLI

The following operational administration procedures are available for accessing the Policy Controller GUIs and CLI.

Table 1 Policy Controller GUIs and CLI procedures

Procedure
Access Policy Controller/NCGL GUIs or CLI using the Integrated EMS on page 22
Access Policy Controller/NCGL GUIs using a proxied client on page 35
Remote login to Policy Controller using a secure shell (SSH) on page 39

Managing security certificates

A security certificate enables secure web browser-based communications for both Policy Controller GUIs and secure SIP signaling for the Policy Controller application. There are two kinds of certificates that can be provisioned on the Policy Controller: self-signed certificates and CA-signed certificates (certificates signed by a certificate authority or CA).

For security reasons, Nortel recommends using CA-signed certificates. Whenever you update or change your security certificates, you should purchase a certificate from a trusted certificate authority (CA). If you need to install new security certificates after an upgrade of the Policy Controller, because you did not keep backup copies of the certificates, it is recommended that you purchase CA-signed certificates. To update or replace your security certificates, on both Policy Controller units, refer to procedure Renewing unexpired certificates on page 5.

The following files are used in managing security certificates:

- server.crt - Only the local server certificate is in this file. In the self-signed certificate option, this file is created automatically by the tool. In the CA-signed option, this file will be provided by the customer, and placed in a temporary directory for import by the tool.
- trusted.crt - The certificate chain leading up to the root CA certificate is placed in this file. This file is provided by the customer, and placed in a temporary directory for import by the tool.
- server.key - This file contains the private key corresponding to the certificate in server.crt
- certificate.keystore - This file contains an encoded version of the server.crt, trusted.crt, and server.key file. This file is created automatically by the tool and is used by Tomcat web server.

Renewing expired CA-signed or self-signed certificates

Nortel always recommends renewing security certificates before they expire; however, if your site's CA-signed or self-signed certificates expire, then you must create new certificates to replace them. Although you can create either new CA-signed or self-signed certificates regardless of the type that expired, Nortel recommends that you replace your expired certificates with new CA-signed certificates.

- To renew expired CA-signed certificates, complete activity Creating new CA-signed certificates on page 6
- To renew expired self-signed certificates, complete activity Creating new self-signed certificates on page 7

ATTENTION

For security reasons, Nortel recommends that you always use CA-signed certificates. If your self-signed certificates expired, then they should be replaced with CA-signed certificates.

Renewing unexpired certificates

Unexpired certificates may need to be renewed or replaced when existing certificates become corrupted due to a system or database

fault. They may also need to be replaced when a system's security is compromised to an unknown extent.

- To renew unexpired CA-signed certificates, complete activity Creating new CA-signed certificates on page 6
- To renew unexpired self-signed certificates, complete activity Creating new self-signed certificates on page 7

ATTENTION
For security reasons, Nortel recommends that you always replace sign-signed certificates with CA-signed certificates.

Migrating from self-signed to CA-signed certificates

If you are currently using unexpired self-signed certificates and want to migrate your Policy Controller to using CA-signed certificates, refer to section Creating new CA-signed certificates on page 6 and complete the activity for creating new CA-signed certificates, which will replace your self-signed certificates.

Creating new CA-signed certificates

Complete the following procedures, in the order shown, to create new CA-signed security certificates

Step	Procedures
1	Back up your existing security certificates using procedure Back up security certificates on page 42.
2	Complete procedure Generate a certificate signing request on page 46.
3	Send the completed certificate signing request to a Certificate Authority for signing and certificate generation. **Note:** It can take up to several weeks to receive a signed certificate back from a Certificate Authority.
4	Once the CA-signed certificate is received, complete procedure Prepare to validate a certificate chain on page 60.
5	Validate the certificate chain by completing procedure Validate a certificate chain on page 56.
6	Complete procedure Apply security certificates on page 68 to make the new certificates available to applications and GUIs used by the Policy Controller.

Step	Procedures
7	Complete procedure Copy security certificates to the mate Policy Controller unit on page 71.
8	Back up your existing security certificates using procedure Back up security certificates on page 42.

Creating new self-signed certificates

Complete the following procedures, in the order shown, to create new self-signed security certificates

Step	Procedures
1	Complete procedure Generate self-signed security certificates on page 76.
2	Complete procedure Apply security certificates on page 68 to make the new certificates available to applications and GUIs used by the Policy Controller.
3	Complete procedure Copy security certificates to the mate Policy Controller unit on page 71.
4	Back up your existing security certificates using procedure Back up security certificates on page 42.

Using the certificate management tool

New certificates are created and managed using the Policy Controller GUI and the CLI-based *cert_mgnt* tool. The cert_mgnt tool is run on one Policy Controller unit only (usually the standby unit), and the certificate files that are created are copied to the mate unit.

The following restrictions apply to using the certificate management tool:

- You must be a root user to use the certificate management tool.
- Only PEM formatted, CA-signed certificates are supported on the Policy Controller.
- CA chain is required in PEM format in a trusted.crt file, top down with the root CA at the top
- There are additional files (cert_gen.txt and assign_cert.txt) in the /opt/base/share/ssl directory. These files are used by the cert_mgnt tool and should not be removed.

The directory /opt/base/share/ssl, where the security certificates are stored, should be backed up on a regular basis using a secure method, in a physically and logically secure environment, to help prevent unauthorized access to the private keys.

Security administration of the Policy Controller

The default security authentication mechanism for the Policy Controller is the NGCL (Nortel Carrier-grade Linux). Users of Nortel Networks operations, administration, maintenance and provisioning (OAM&P) client applications, which include the Policy Controller GUI and CS 2000 NCGL Platform Manager must belong to the primary group “succssn” for login access, and to one or more secondary user groups to specify the operations the user is authorized to perform.

Note: The CS 2000 NCGL Platform Manager GUI does not enforce group privileges when making changes. However, the Policy Controller GUI does enforce group privileges when making changes. Group privileges are set based on the group names shown in the table “Default groups.”

Replacing default HTTPS security certificates

By default HTTPS (HyperText Transport Protocol Secure) security certification is installed on the Policy Controller to enable secure web browser-based communications to the Policy Controller GUIs. For security reasons, you may want to update or change your security certificates, purchasing a certificate from a trusted certificate authority (like VeriSign). You may also need to reinstall security certificates after an upgrade of the Policy Controller NCGL platform has occurred if you did not keep backup copies of the certificates. For assistance in acquiring replacement security certificates, contact your next level of support. To update or replace your security certificates on both Policy Controller units, refer to procedure Copy security certificates to the mate Policy Controller unit on page 71.

User and authorization categories

The following table of default groups are used on the Policy Controller and their allowed operations, in similar fashion to the CS 2000 Management Tools Server SSPFS. These user groups are also

consistent with the existing Carrier VoIP user categories on other Carrier VoIP component managers.

Table 2 Allowed operations for Policy Controller User Groups

Command	User group				
	mgcadm	mgcrw	mgcsprov	mgcmtc	mgcro
Application maintenance commands (lock, unlock)	X			X	
Topology provisioning commands (add network zone, delete link layer type)	X	X			
Configuration commands (PCF/TM configuration)	X	X			
Query Commands (list provisioning data)	X	X	X	X	X
SOC command (add endpoint license file)	X	X	X	X	X
Add/delete application (Add/delete Policy Controller application)	X				

The following table describes the default user names and associated secondary groups configured on a new Policy Controller platform.

Default user IDs on a new Policy Controller installation

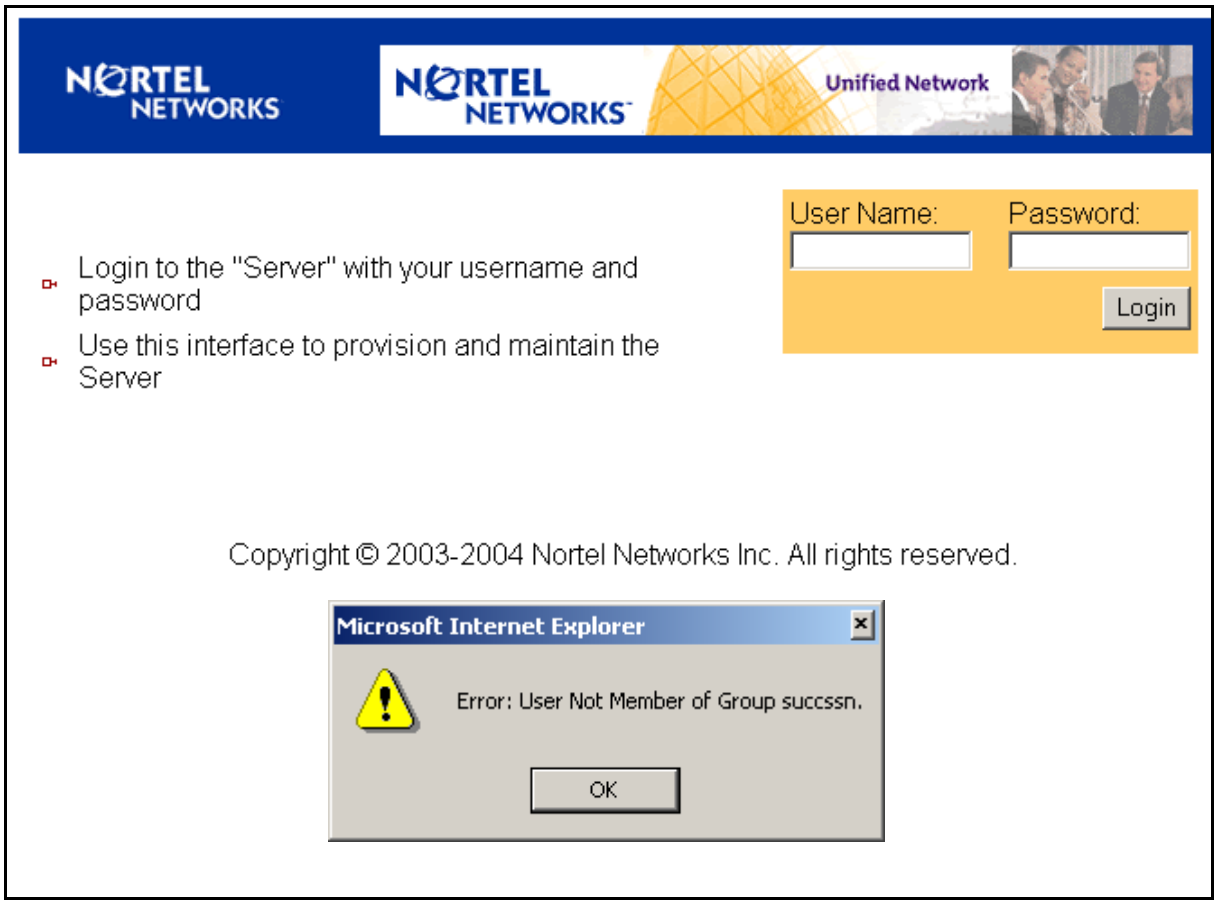
User Name	Groups	Description
root	root bin daemon sys adm disk wheel	System root user is not allowed when logging into the GUIs. Also, you cannot remotely log onto the Policy Controller console. You must log in as another user, then su (superuser) to the root user. The default root password is “sam39xts.” This password should be changed during commissioning of the Policy Controller units.
mtc	succssn users mtc mgcadm mgcrw mgcsprov mgcmtc mgcro	Policy Controller platform NCGL maintenance user. The default password for mtc user is “mtc.” This password should be changed during commissioning of the Policy Controller units. ***Note:*** The mtc user id should not be deleted. Doing so prevents command line interface (CLI) access from the Integrated EMS and web proxies. Also, the mtc user password must be a shared password account.

Using the root account for Policy Controller GUI and remote CLI access

Logging in to the Policy Controller’s GUIs is not allowed using the root account. If you attempt to log into the Policy Controller GUI as root, you receive the error message shown in the following figure. To log in as root, you must first access a command line interface at a Policy Controller console as another user type, then su to root super user. Refer to procedure Remote login to Policy Controller using a secure shell (SSH) on page 39 to perform this activity.

Note: In general, Policy Controller GUI access permissions are controlled by the mgc group type. It is unnecessary to log on to the Policy Controller GUIs as the root account. For security reasons, it is not recommended that you configure the root account to be part of the primary group “succssn” for login access.

Login screen error message when trying to use the root account



Procedures for managing user accounts and passwords

ATTENTION
User accounts and passwords are not propagated to the Policy Controller mate unit. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

The following is a list of the procedures for managing user accounts and passwords.

User account and password procedures

Procedure
Manage users on the Policy Controller platform on page 86
Manage user passwords using a Policy Controller console CLI on page 89
Manage user passwords with the Policy Controller GUI on page 91
Setting up a connection to the Topology Manager using ssh on page 1

Operational administration and maintenance of the Policy Controller platform and applications

This section provides the procedures available to manage the Policy Controller and its applications, including:

- Managing operation of the NCGL platform and hardware for each Policy Controller unit
- Managing operation of the Policy Controller application on both units to ensure uninterrupted Network VCAC call processing

The following operational administrative and maintenance activities are available to be performed on the Policy Controller platform:

- Jam and Unjam - manually prevent a switch of activity (SwAct) to the standby unit. Jam and Unjam are performed in cases where a Policy Controller unit is faulty and is about to be replaced, when configuration or maintenance activities are being performed, or when the standby unit is unavailable.
- Switch of Activity (SwAct) - switch the active unit to the standby (mate unit). Refer to section Understanding conditions for a SWACT

on page 16 for details about types of SwActs and the conditions required to perform a SwAct.

- Switch active link (Swlink) - switch the active communications links in both the active and standby Policy Controller units.
- Network ethernet link Lock and Unlock - shut down the ethernet interfaces and isolate a single Policy Controller unit from the network. Refer to section Managing Policy Controller ethernet links on page 18 for more information.

The following activities can be performed on the Policy Controller application to change its operational and administrative state:

- Taking the Policy Controller application from out-of-service to in-service - Maintenance commands *Unsuspend* followed by *Unlock*
- Taking the Policy Controller application from in-service to out-of-service - Maintenance commands *Lock* followed by *Suspend*
- Shutting down the Policy Controller application - Maintenance command *Shut Down*

Interpreting Policy Controller application states

Policy Controller application maintenance uses the CCITT X.731 state and status attributes as well as X.731 commands to be consistent with other Carrier VoIP component platforms. The following table shows the four fields that comprise the CCITT X.731 state of the Policy Controller application. The last column in the table provides a mapping to legacy DMS-style states to aid in understanding.

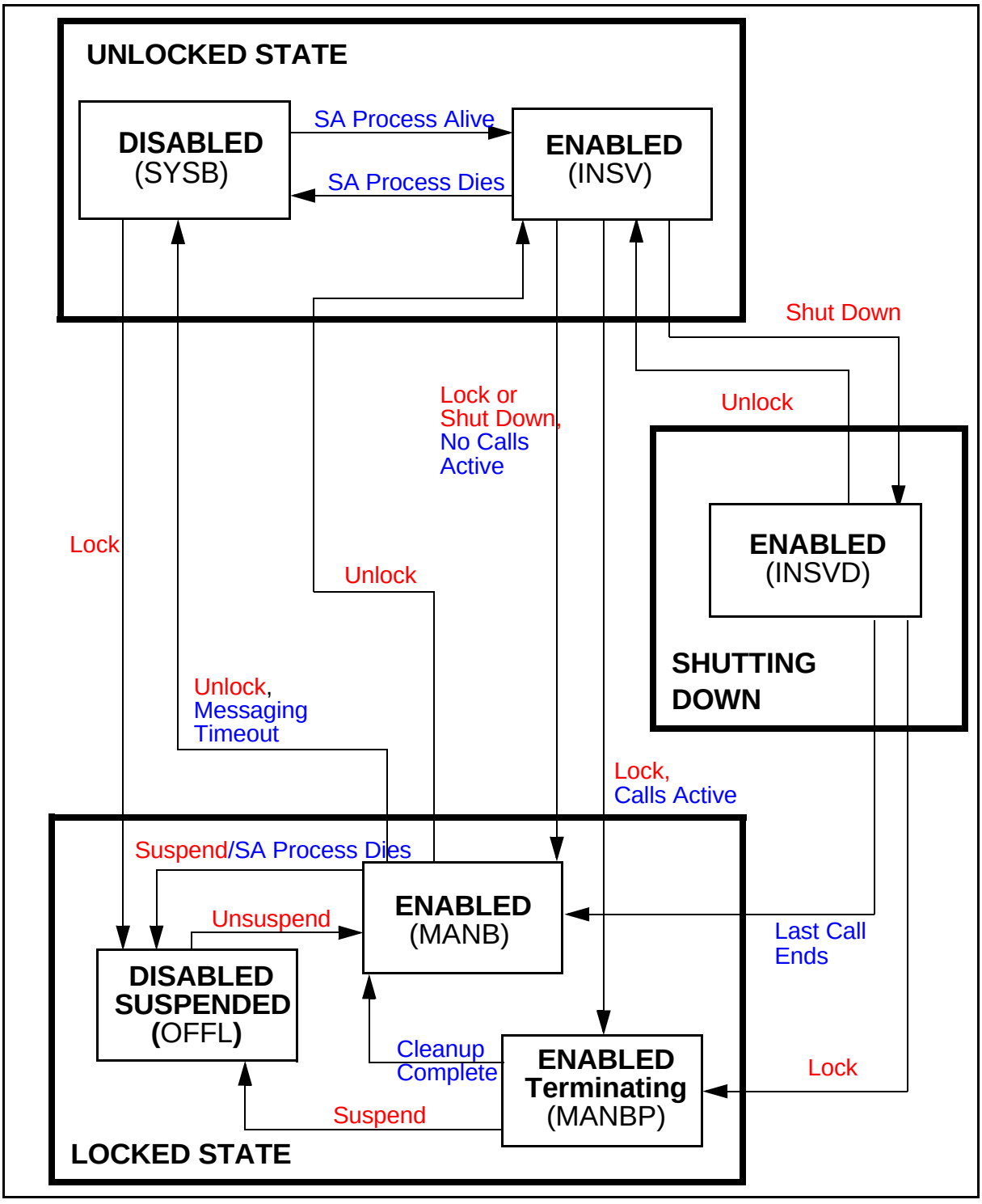
Administrative State	Operational State	Procedural Status	Control Status	DMS Style States
Locked	Disabled	-	Suspended	OFFL
Locked	Enabled	-	-	MANB
Locked	Enabled	Terminating	-	MANBP
Unlocked	Enabled	-	-	INSV
Unlocked	Disabled	-	-	SYSB
Shutting Down	Enabled	-	-	INSVD

The following table explains the controls that are allowed based on the current Admin State, Operational State, and Procedural Status of the Policy Controller application. Legacy DMS style representation is shown in parentheses to aid in understanding.

Operational State	Admin State	Procedural Status	Control Status	Allowed Controls DMS Style Commands in ()'s
Locked	Disabled	-	Suspended	Admin Control None Control Status Unsuspend (BSY)
Locked	Enabled	-	-	Admin Control Unlock (RTS) Control Status Suspend (OFFL)
Locked	Enabled	Terminating	-	Admin Control None Control Status: Suspend (OFFL)
Unlocked	Enabled	-	-	Admin Control Lock (BSYFORCE) Shut Down (BSY) Control Status None
Unlocked	Disabled	-	-	Admin Control Lock (OFFL) Control Status None
Shutting Down	Enabled	-	-	Admin Control Lock (BSYFORCE) Unlock (RTS) Control Status None

The following state diagram shows how maintenance states transition from one to the other. The legacy DMS system commands are shown in parentheses to aid in understanding. Commands that can be executed are listed in red, while messaging and state transitions are listed in blue.

Policy Controller application maintenance state diagram



Understanding conditions for a SWACT

There are three types of SwAct supported on the Policy Controller NCGL platform:

- a manual SwAct (forced or unforced)
- a system initiated SwAct
- an application requested SwAct

Swacts are executed depending on the state of the system and any failure conditions, according to the following rules:

SwActs cannot occur under the following circumstances:

- when the node is running in a simplex configuration; where the inactive unit is unavailable
- when the inactive unit is completely isolated and unreachable or is in a Jammed state
- critical failure conditions exist on the inactive unit that prevent a SwAct
- the Policy Controller application rejects a SwAct request

SwAct always occur under the following circumstance:

- a forced manual SwAct is initiated
- critical failure conditions on the active side cause a system-initiated swact.

Rules for SwActs are summarized in the following table:

Unit status		Applications accept the SWACT			
Active	**Inactive**	**Manual or Application requested SWACT**	**System Initiated SWACT**	**Application rejects SWACT**	**Manual "Force" SWACT**
Not critical	Not critical	SWACT	not applicable	no action taken	SWACT
Not critical	critical failure	no action taken	not applicable	no action taken	SWACT
critical failure	Not critical	not applicable	SWACT	no action taken	SWACT

Unit status		Applications accept the SWACT			
Active	**Inactive**	**Manual or Application requested SWACT**	**System Initiated SWACT**	**Application rejects SWACT**	**Manual "Force" SWACT**
critical failure	critical failure	no action taken	no action taken	no action taken	SWACT

In the previous table discussing rules for a SwAct, "critical failure" conditions are mentioned. Note that the conditions that would initiate a SwAct on the active side are the same conditions that would inhibit a SwAct due to a failed inactive unit. These conditions correspond to the following cases:

- a unit is not available because it has experienced a power loss, or is in the process of rebooting
- the Sanity watchdog timer times out, a kernel panic is generated or critical hardware failure occurs
- critical network monitoring-related alarms are generated, indicating that the active unit is becoming isolated or otherwise no longer responding to its mate
- one or both of the disk drives fails on a unit
- a manual SwAct is initiated to a unit which has a single disk missing/fail alarm

The following events are not included the "critical failure" conditions, even though some alarms for these events may be categorized as "critical" in the alarm view:

- major or minor alarms for connectivity and most hardware faults
- Most hardware failures, including power supply faults, voltage and temperature conditions, fan, CPU and memory
- NCGL operating system faults, including zombie processes, cpu usage and memory usage faults
- disk usage faults

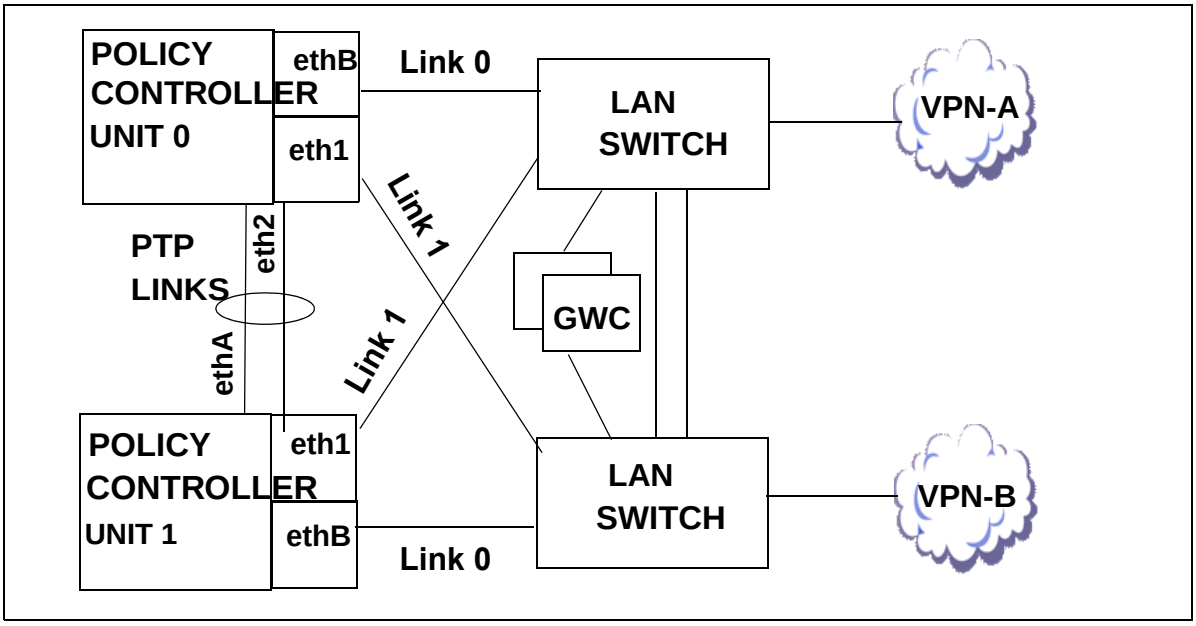
Note 1: The operating system status critical alarm is not symmetrical, in that it prevents a SwAct, but does not cause a system initiated SwAct.

Note 2: For more information about faults, alarms and fault conditions, refer to *Policy Controller Fault Management*, NN10438-911.

Managing Policy Controller ethernet links

The following figure shows each Policy Controller unit to be configured with two gigabit ethernet interfaces (shown as link 0 and link 1). These are directed to the LAN switch that routes call traffic and signalling on the customer's private central office (CO) network. In addition, two ethernet interfaces, acting as Point To Point (PTP) links, connect unit 0 to unit 1.

Map of Policy Controller ethernet ports and link configuration



Ethernet link management procedures for Policy Controller

The following table lists the link management procedures:

Operational administration procedures

Procedure
Invoke a manual switch of active links (Swlink) on page 6
Lock network ethernet link on page 11
Unlock network ethernet link on page 14

Operational administration procedures for the Policy Controller application

The following table lists administrative procedures available for controlling the Policy Controller application.

Operational administration procedures

Procedure
Invoke a maintenance SwAct of the Policy Controller platform on page 17
Invoke a manual cold SwAct of the Policy Controller application on page 22
Inhibit a system SwAct (Jam) on page 26
Enable a system SwAct (Unjam) on page 30
Lock the Policy Controller application on page 34
Unlock the Policy Controller application on page 39
Suspend the Policy Controller application on page 42
Unsuspend the Policy Controller application on page 45
Shutdown the Policy Controller application on page 48
Power-On and boot a Policy Controller unit on page 123
Power-Off a Policy Controller unit on page 121
Halt (shutdown) a Policy Controller unit on page 72
Reboot a Policy Controller unit on page 78
Query current number of calls on page 86

Performing a controlled shutdown of a Policy Controller node

Execute the procedures in the following activity to perform a controlled shutdown of a Policy Controller node. Use this activity in the event of an impending power failure at the physical site or for any other conditions requiring shutting down the entire node.

CAUTION

This is a service affecting procedure.

Step	Procedure
1	If necessary, ensure that a backup copy of the Policy Controller application database has been made using procedure Perform a manual backup of the Policy Controller database on page 195.
2	Perform procedure Lock the Policy Controller application on page 34 on the active unit.
3	Perform procedure Suspend the Policy Controller application on page 42 on the active unit.
4	Perform procedure Halt (shutdown) a Policy Controller unit on page 72 on the inactive unit. ***Note:*** The state of the Policy Controller application is saved when the unit is powered off. When the unit is powered up, the Policy Controller application initializes in the same state in which it was powered down.
5	Perform procedure Power-Off a Policy Controller unit on page 121 on the inactive unit.
6	Perform procedure Halt (shutdown) a Policy Controller unit on page 72 on the active unit. ***Note:*** The state of the Policy Controller application is saved when the unit is powered off. When the unit is powered up, the Policy Controller application initializes in the same state in which it was powered down.
7	Perform procedure Power-Off a Policy Controller unit on page 121 on the active unit.

Backing up the Policy Controller application database

Database backups secure the information stored in the Policy Controller application database. In the event that there is a complete failure of both Policy Controller units in the node or if an unrecoverable corruption in the database on the active unit occurs, a copy of the database can be restored from a backup.

Ordinarily, there is only a single backup copy of the database saved on each unit. It contains the last or most recently backed up copy (within the last 24 hours) of the database. The database on each unit is automatically backed up at 1:00 AM each day. The automatic backup file is named **solid.db** and is located at the following path on the active Policy Controller disk drive:

/opt/apps/database/solid/backup/solid.db

The time of day for the backup or the content set of the backup cannot be changed by the customer; however, the customer can perform a manual backup of the database on an as-needed basis such as when an upgrade activity is scheduled. It is recommended that manual backups be performed on the active database.

If additional security measures are required, the customer may periodically retrieve the files saved in the backup directory and store them on another system. By regularly saving copies of the backup database, a customer can maintain a history of database changes.

The following table lists the procedures available to backup the Policy Controller application database.

Database backup procedures

Procedure
Perform a manual backup of the Policy Controller database on page 195

Access Policy Controller/NCGL GUIs or CLI using the Integrated EMS

Purpose of this procedure

This procedure describes how to access the Policy Controller web-based GUIs (CS 2000 NCGL Platform Manager and CS 2000 Policy Controller GUI) or the command line interface (CLI) using the Integrated EMS.

For the inactive unit only, you can also use this procedure to access the CS 2000 NCGL Platform Manager GUI.

Limitations and Restrictions

This procedure is not a comprehensive guide to using Integrated EMS for access to the Policy Controller, for OAM&P activities. For more information refer to the *Integrated EMS Basics*, NN10329-111.

Prerequisites

The Policy Controller must be configured for access from the Integrated EMS which is installed and running on CS 2000 Management Tools.

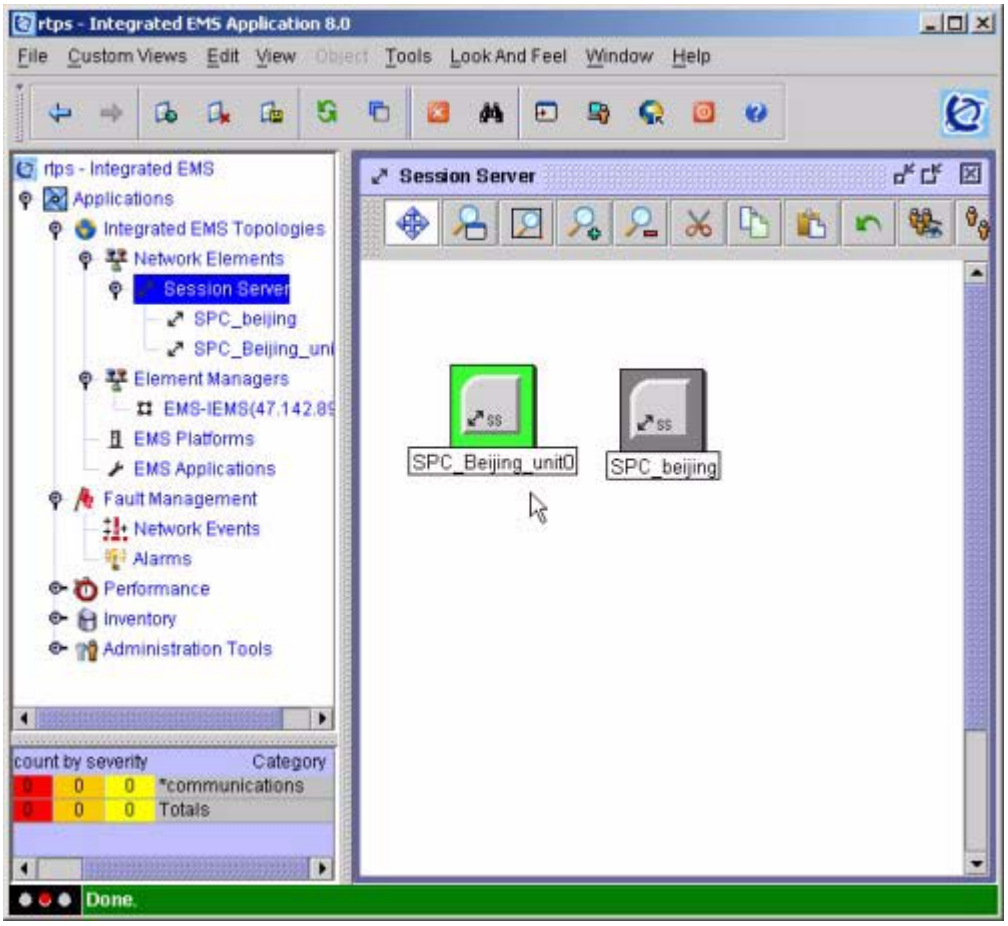
Action

At a workstation or console running the Integrated EMS client

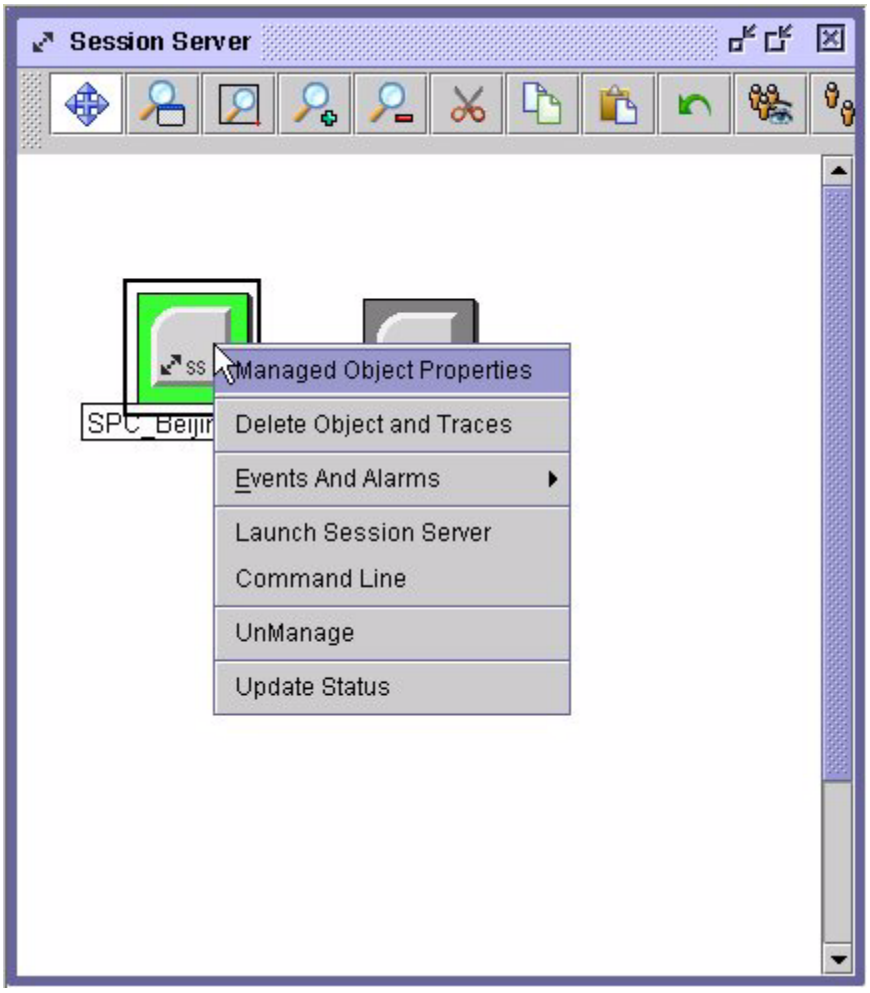
1 Use the following table to determine your next step.

If	Do
you want to access the active Policy Controller unit (the unit currently controlling the node)	step 2
you want to access the inactive Policy Controller unit	skip to section Accessing the inactive Policy Controller unit user interfaces on page 28

2 In the Network Elements view locate the Policy Controller unit icon.



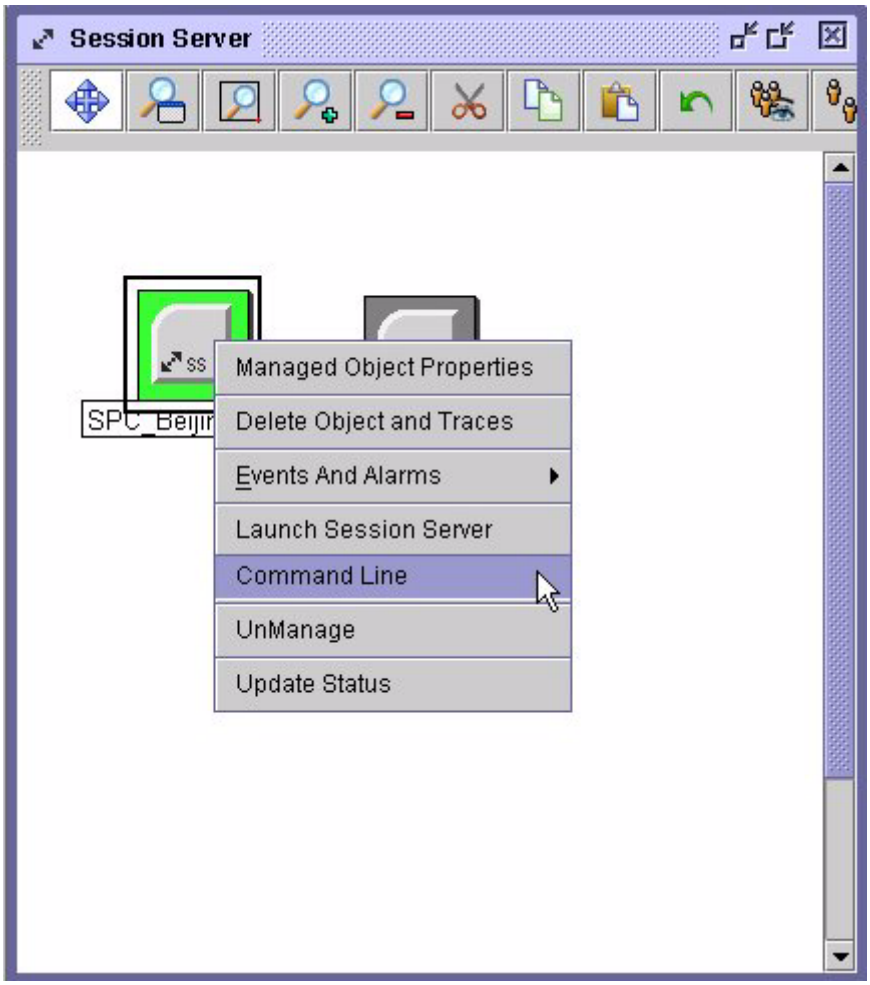
3 Right-click on the Policy Controller Node icon



4 Use the following table to determine your next step.

If	Do
you want to launch a command line session	step 5
you want to launch either the CS 2000 Platform NCGL Manager GUI or the Policy Controller GUI	step 8

5 To launch a command line session, select **Command Line** from the menu.

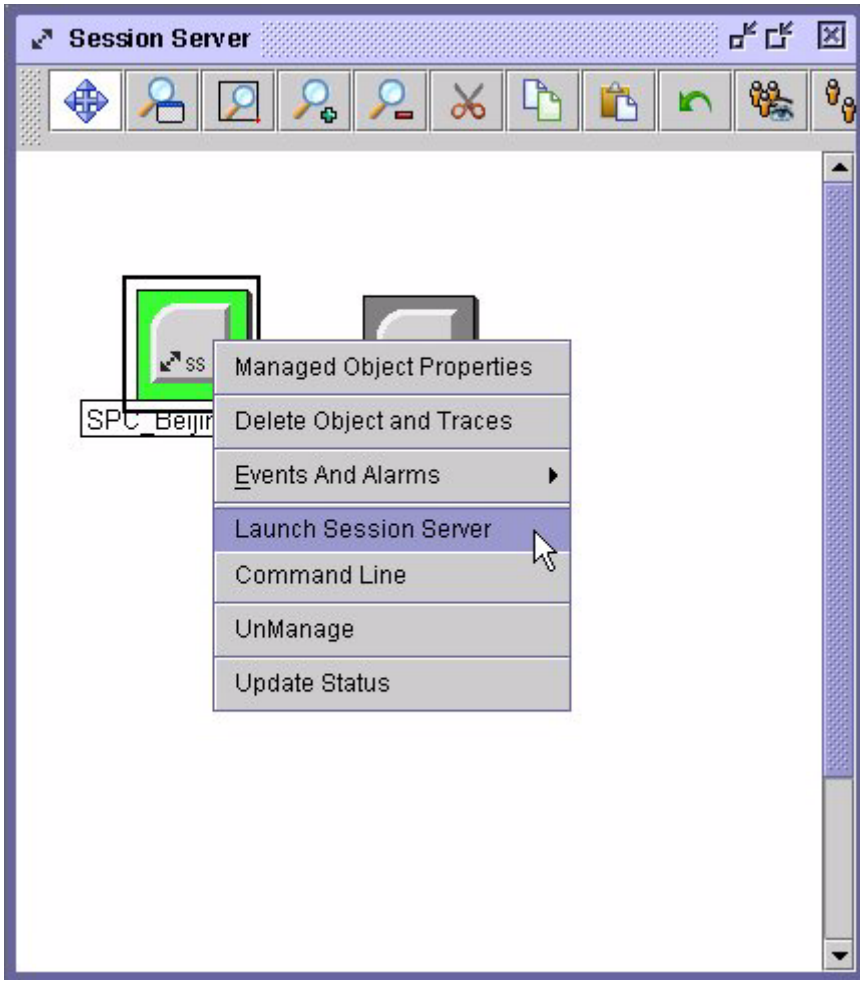


A secure shell (SSH) command line login window is presented.

6 At the login prompt, enter your user id and password.

7 Skip to step 12.

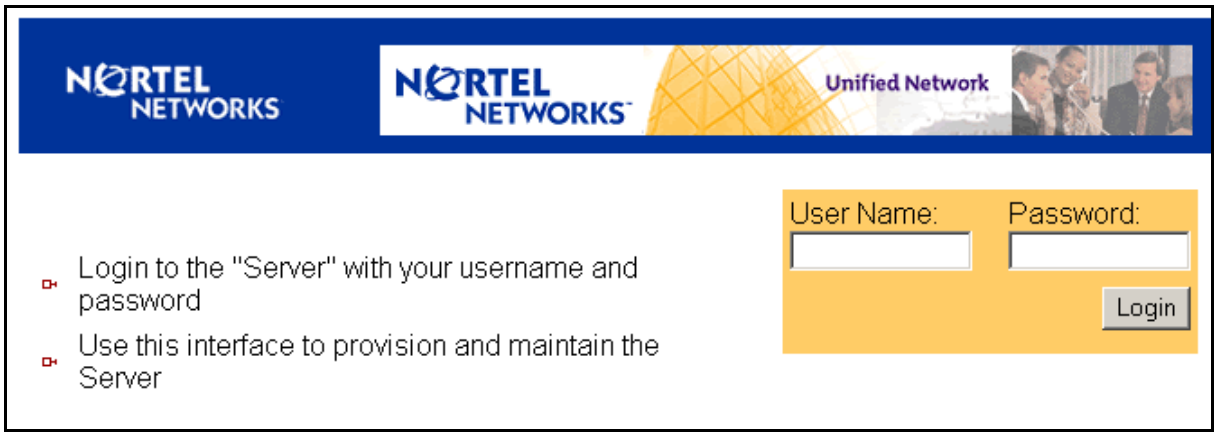
8 To launch either the CS 2000 Platform NCGL Manager GUI or the Policy Controller GUI, select **Launch Session Server** from the menu.



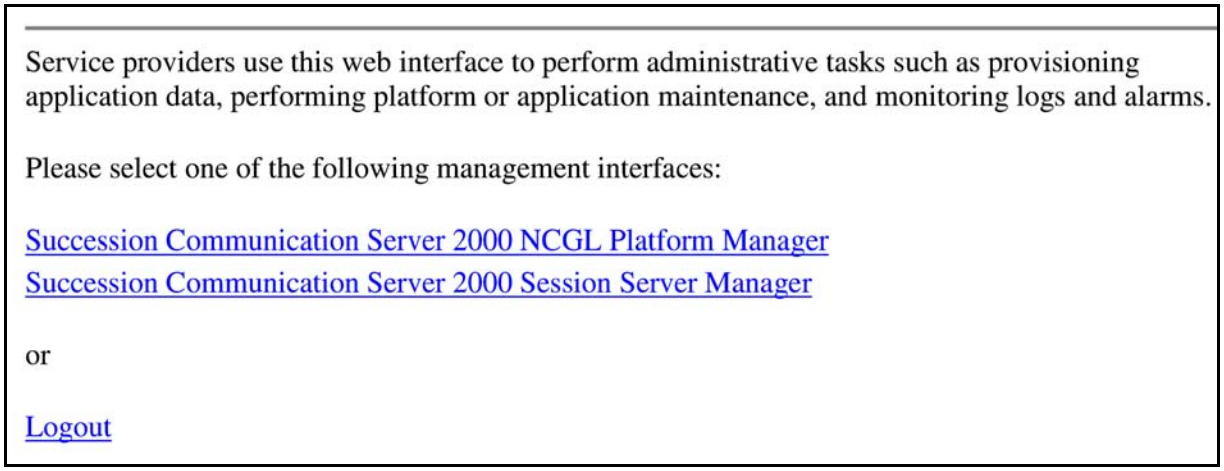
A new browser window opens and presents a login window.

9 Confirm any security alerts by clicking **Yes**.

10 At the login screen enter your user id and password, then click the **Login** button.



11 Select the GUI you want to launch from the launch point menu.



12 You have completed this procedure.

Accessing the inactive Policy Controller unit user interfaces

Use this procedure to access the CS 2000 NCGL Platform Manager GUI or Command Line Interface on the inactive unit only. Use this procedure for performing upgrade activities and other activities that require access to the inactive unit NCGL manager.

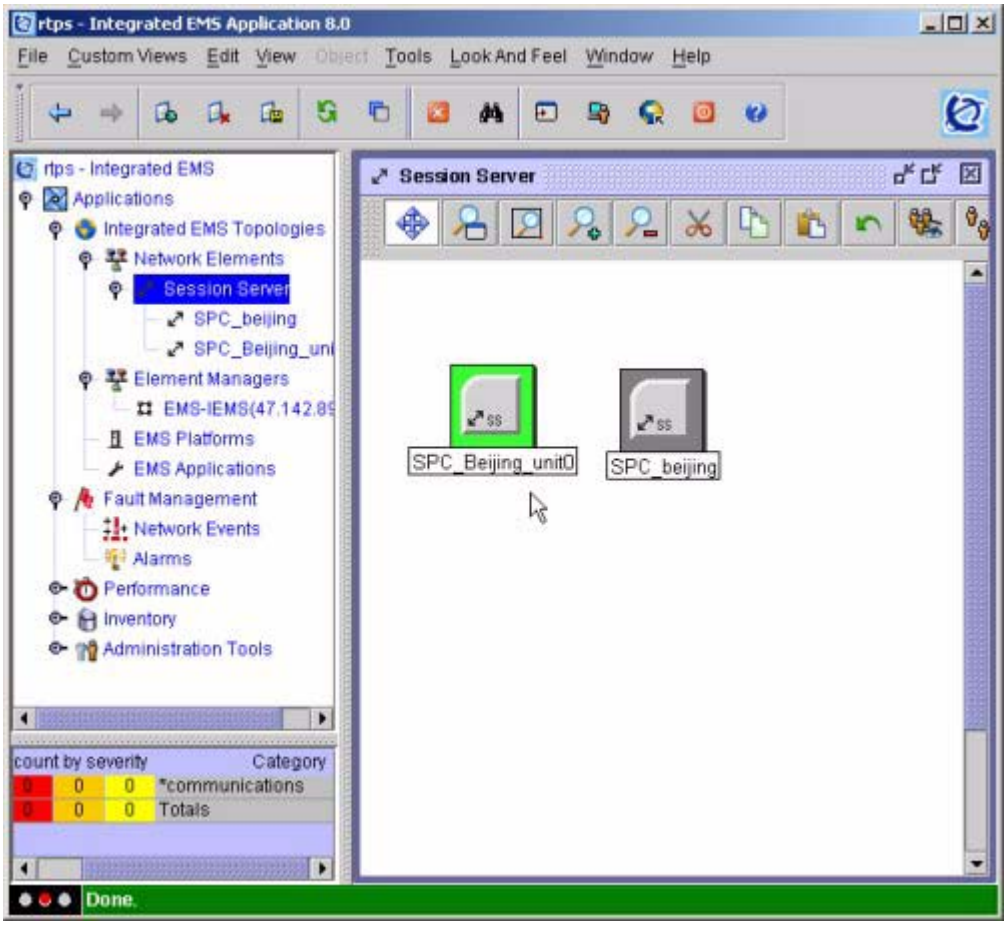
ATTENTION

You can not access the Policy Controller GUI on the inactive unit. You can only access the Policy Controller GUI on the active unit. You can always verify the activity status of the unit you are logged onto from the Policy Controller GUI by going to the Policy Controller Status panel and viewing the Policy Controller Status.

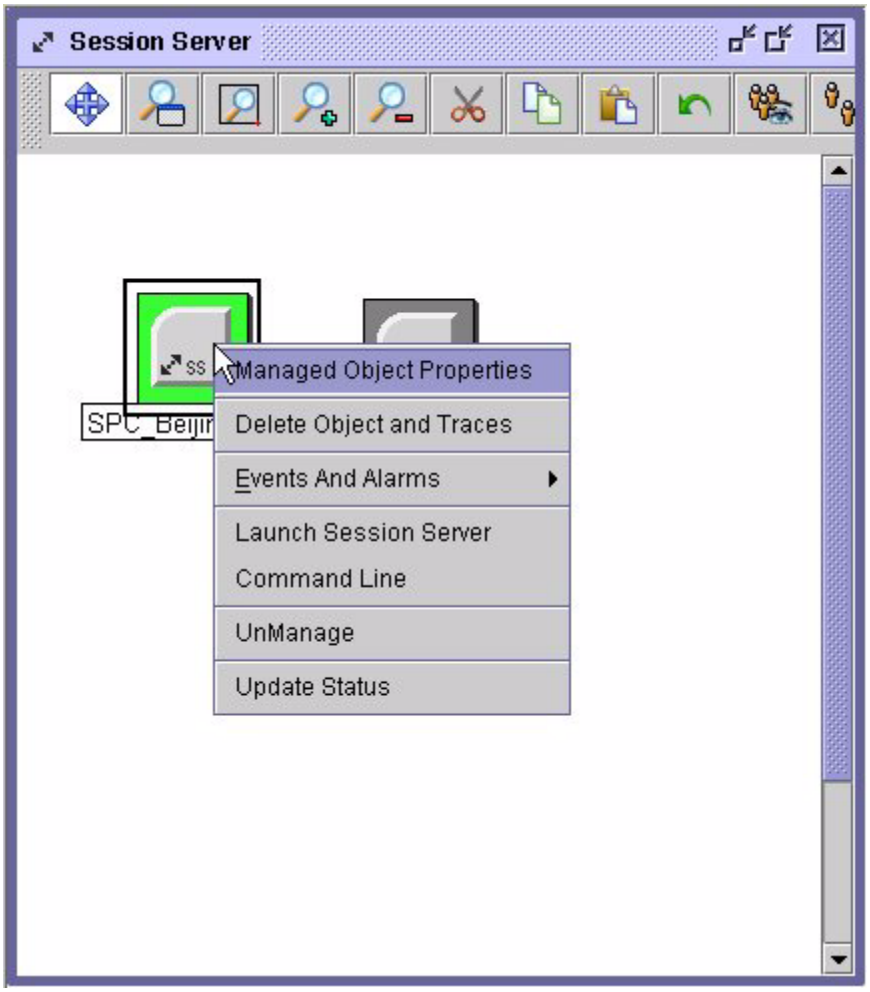
Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

At a workstation or console running the Integrated EMS client

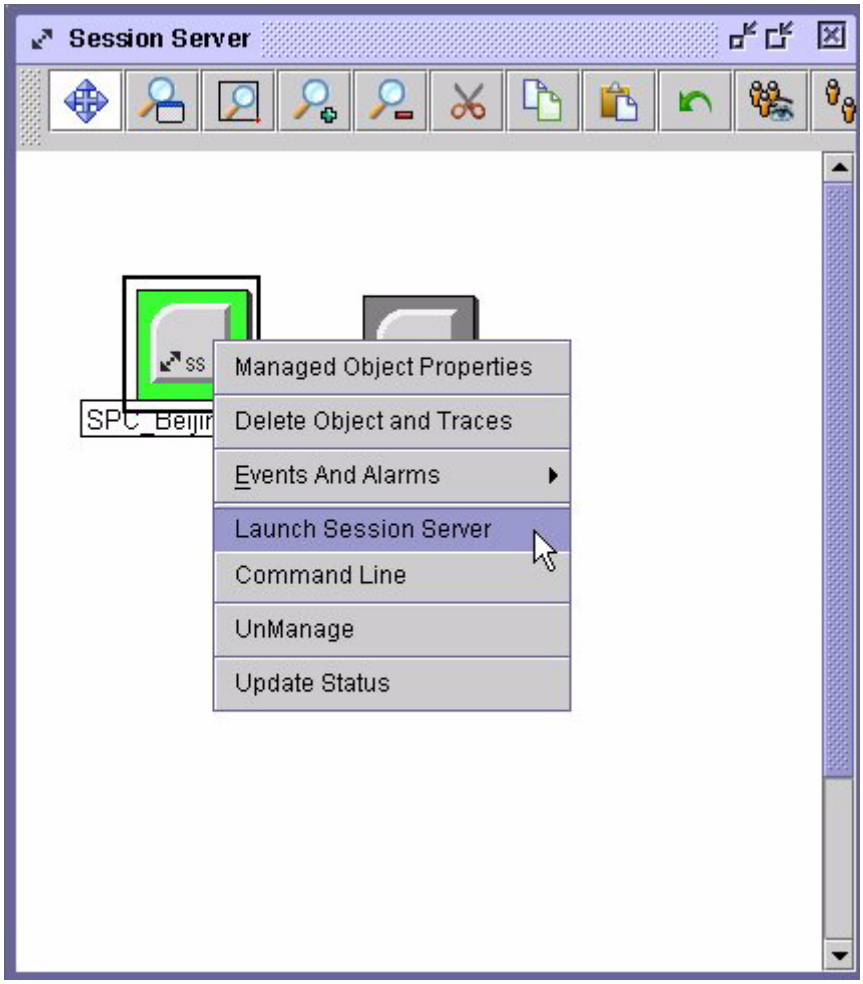
1 In the Network Elements view, locate the Policy Controller unit icons.



2 Right-click on the first Policy Controller unit icon.



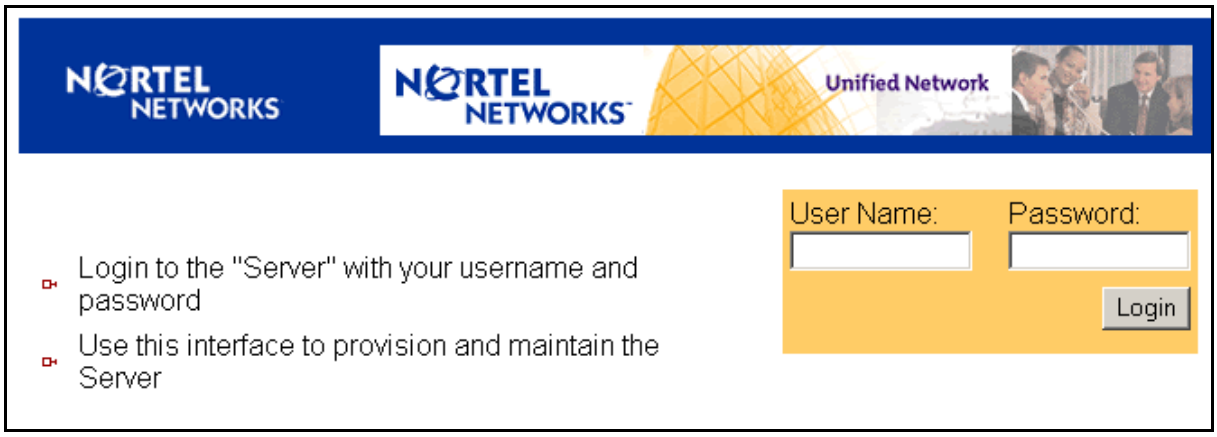
3 To launch either the CS 2000 Platform NCGL Manager GUI or the Policy Controller GUI, select **Launch Session Server** from the menu.



A new browser window opens and presents a login window.

4 Confirm any security alerts by clicking **Yes**.

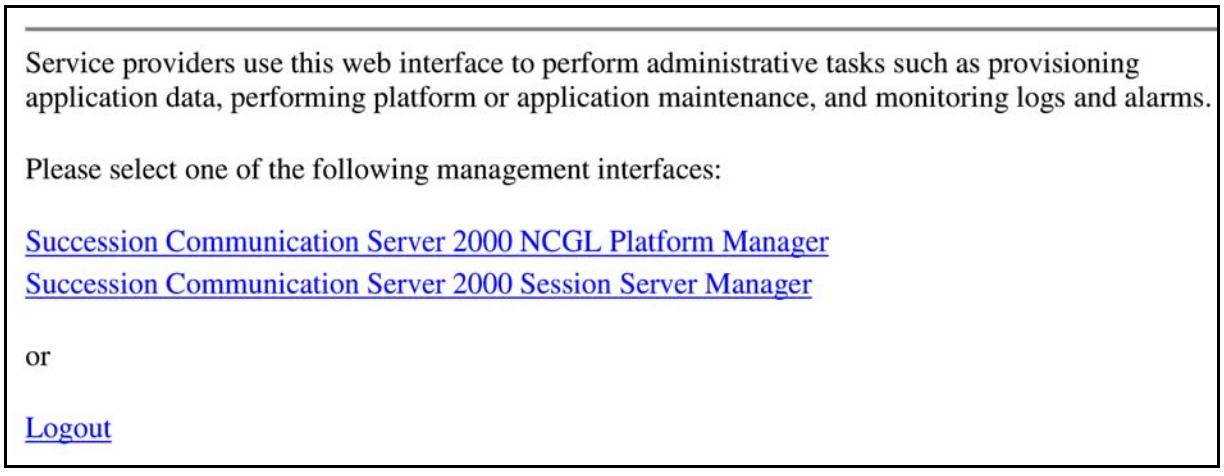
5 At the login screen enter your user id and password, then click the **Login** button.



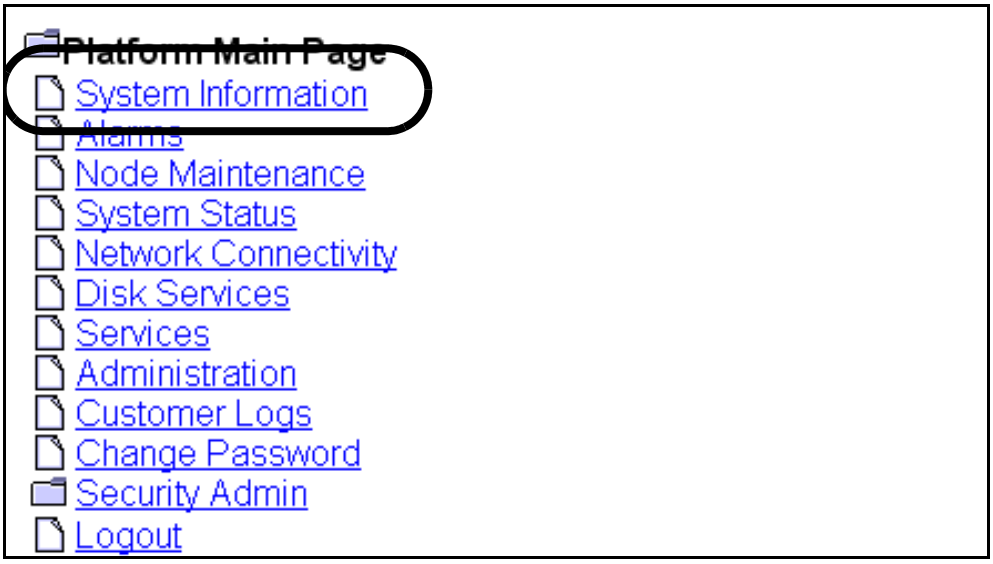
6 Select the **Succession Communication Server 2000 NCGL Platform Manger** link.

ATTENTION

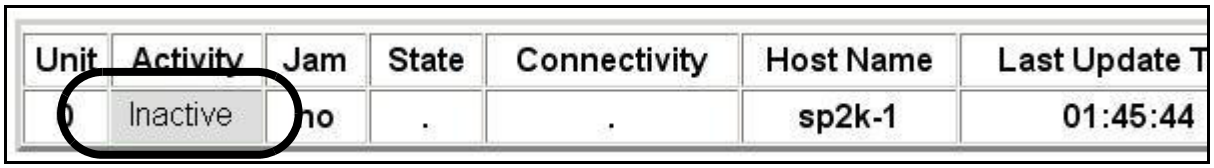
You can not access the Policy Controller GUI from the inactive unit. You can only access the Policy Controller GUI from the active unit. Clicking on the Policy Controller Manager GUI link from the *inactive* unit launch point will automatically take you to the Policy Controller GUI on the *active* unit.



7 At the Platform Main Page menu, click the **System Information** link.



8 At the System Information page, determine if the unit you have logged onto is the inactive unit by viewing the Activity field.



9 Use the following table to determine your next step.

If	Do
the unit you have logged onto is the inactive unit	you have successfully logged onto the inactive unit. Go to step 10.
the unit you have logged onto is not the inactive unit	log off from this (active) unit, return to step 4, and select the other Policy Controller unit icon.

10 You have completed this procedure.

Access Policy Controller/NCGL GUIs using a proxied client

Purpose of this procedure

This procedure describes how to access the Policy Controller web-based GUIs (CS 2000 NCGL Platform Manager and Policy Controller GUI) using a client workstation.

Limitations and Restrictions

ATTENTION

For all methods of GUI access, only HTTPS (HyperText Transport Protocol Secure) access is allowed. For security reasons, HTTP (HyperText Transport Protocol) access is not supported on the Policy Controller.

Ensure that the Policy Controller node has been configured to support GUI access through a web proxy. I you receive messages in your web browser that the access to the CS 2000 NCGL Platform Manager has been denied, your Policy Controller has not been properly configured for access through a web proxy. Refer to procedure Manage SSPFS server web proxy setup for Policy Controller, found in *Policy Controller Configuration Management*, NN10432-511, for instructions on configuring a web proxy to support access to the Policy Controller.

Prerequisites

Ensure that you are using the correct version of a web browser for accessing the GUIs. Refer to the Overview section of *Configuration Management*, NN10432-511, for this information.

Action

At a client workstation

1 Open a supported web browser.

2 In the URL address bar of the browser access the active or inactive Policy Controller unit by typing

`> https://<proxy_IP_address>/<PC_IP_address>`

and pressing the Enter key.

where

proxy_IP_address
is the IP address of the proxy server in your network

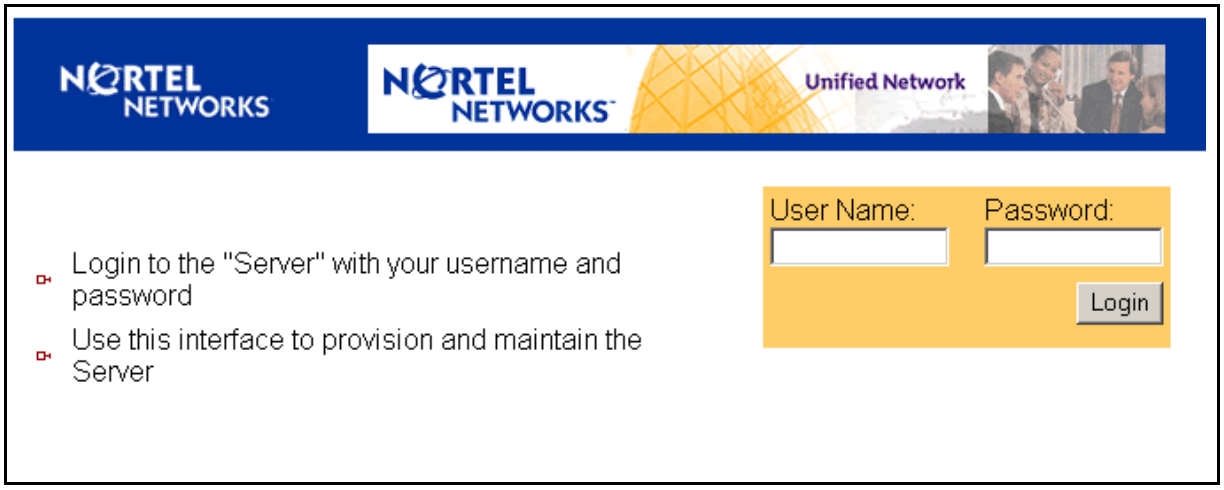
PC_IP_address
is the IP address of the Policy Controller active or inactive unit

Example
https://47.135.42.226/10.67.99.72/

3 If necessary, confirm any security alerts related to security certificates by clicking **Yes** to proceed.

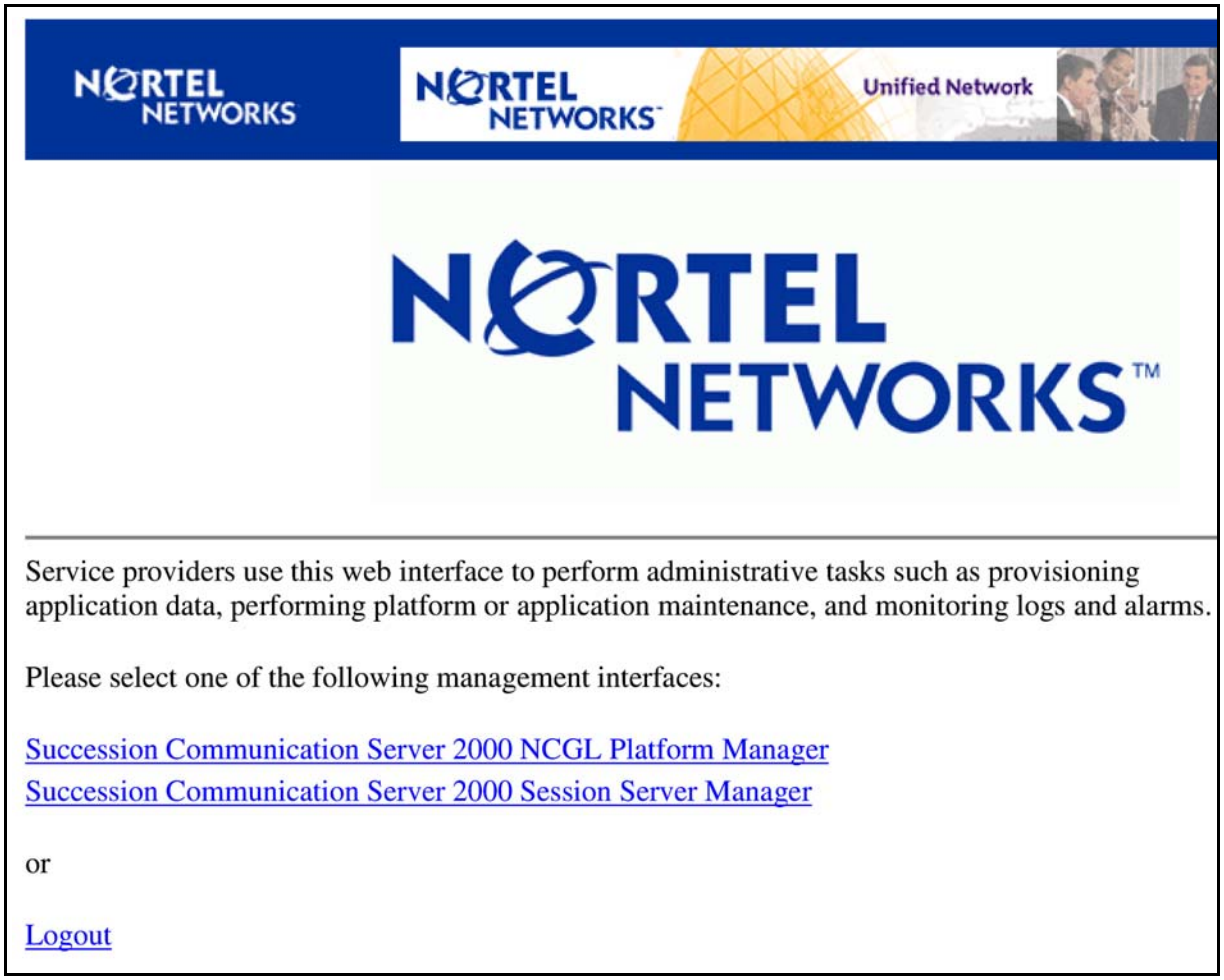
4 At the login screen enter your user id and password, then click the **Login** button.

Note: You cannot login to the Policy Controller GUIs as the root user.



5 Select the GUI you want to launch from the launch point menu.

- Select the CS 2000 NCGL Platform Manager if you want to perform maintenance or provisioning on the NCGL operating system of the Policy Controller platform
- Select the CS 2000 Session Server Manager if you want to perform maintenance or provisioning on the Policy Controller Application.
- Select Logout if you want to exit back to the login screen.



6 You have completed this procedure.

Remote login to Policy Controller using a secure shell (SSH)

Purpose of this procedure

This procedure is used to log onto a Policy Controller active unit with the CLI (command line interface from a remote client system that has access to the secure CS-LAN and has access permissions as setup on the proxy server running on the CS 2000 Management Tools server.

You can also log onto the Policy Controller with the CLI using a console connected to the rear of the Policy Controller active unit. In some cases, this connection is wired to a terminal box.

Limitations and Restrictions

ATTENTION
Due to security limitations of using telnet, Nortel Networks does not support its use, and recommends using ssh as the preferred method of accessing the Policy Controller from a remote client.

Prerequisites

The remote client must have access to the secure CS-LAN and must have access permissions as setup on the proxy server running on the CS 2000 Management Tools server.

Action

From a remote client that supports SSH on the CS-LAN

1 Open a secure shell to the Policy Controller by typing

> ssh -l <userid> <PC_IP_address>

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

PC_IP_address
is the IP address or host name of the Policy Controller

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 If applicable, change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 You have completed this procedure.

Back up security certificates

Purpose of this procedure

Use the following procedure to create backup copies of security certificates to a folder on the Policy Controller unit and make copies to a remote server location, chosen by the customer.

Use this procedure anytime new security certificates are created or when the system is changed from using self-signed certificates to CA-signed certificates. This procedure is also used as part of a major release upgrade activity.

Limitations and Restrictions

There are no limitations on performing this procedure.

Prerequisites

There are no prerequisites for this procedure.

Action

Perform the following steps to complete this procedure.

At the Policy Controller CLI or Integrated EMS client

1 Log onto either Policy Controller unit (usually the unit where the latest version of security certificates are stored), and change to root user.

2 Change directories to the /opt/base/share/ssl directory. Type

```
# cd /opt/base/share/ssl
```

and press the Enter key.

3 Create a new directory to store backup copies of the certificate files

```
$ mkdir <SNxx_ddmmyyyy>
```

and pressing the Enter key.

where

SNxx_ddmmyyyy
is the name of the new directory based on the currently installed release of the system software (for example SN09) and the current date in the format ddmmyyyy

4 Copy the certificates to the newly created backup directory by typing

 # cp * <SNxx_ddmmyyyy>

and press the Enter key.

where

SNxx_ddmmyyyy
is the name of the new backup directory

ATTENTION
Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

5 Use the following table to determine your next step:

If	Do
you want to make backup copies of the security certificates to a remote server	step 6
you do not want to make backup copies of the security certificates to a remote server	step 10

6 Secure copy the server.key file to the remote server by typing

$ scp server.key <user>@<remote_server>:</path>

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The server.key file is copied to the remote server.

7 Secure copy the certificate.keystore file to the remote server by typing

$ scp certificate.keystore <user>@<remote_server>:</path>

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The certificate.keystore file is copied to the remote server.

8 Secure copy the server.crt file to the remote server by typing

```
$ scp server.crt <user>@<remote_server>:</path>
```

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The server.crt file is copied to the remote server.

9 If you have a CA-signed certificate, secure copy the trusted.crt file to the remote server by typing

```
$ scp trusted.crt
<user>@<remote_server>:/<path>
```

and pressing the Enter key.

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The trusted.crt file is copied to the remote server.

10 You have completed this procedure.

Generate a certificate signing request

Purpose of this procedure

This procedure uses the certificate management tool to generate a certificate signing request or CSR. A CSR is sent to a certificate signing authority to generate a CA-signed certificate. This procedure should only be used as part of a high level task for updating security certificates.

A successful completion of this procedure creates a certificate signing request composed of:

- Server.csr - contains the certificate signing request

The following certificate files are returned by the certificate signing authority upon successful processing of the certificate signing request:

- Server.crt
- Trusted.crt

Limitations and restrictions

Use this procedure only for CA-signed certificates.

You must be a root user to use the certificate management tool.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At a Policy Controller command line interface (CLI)

1 Log onto the standby Policy Controller unit and change to the root user.

2 Start the certificate management tool by typing

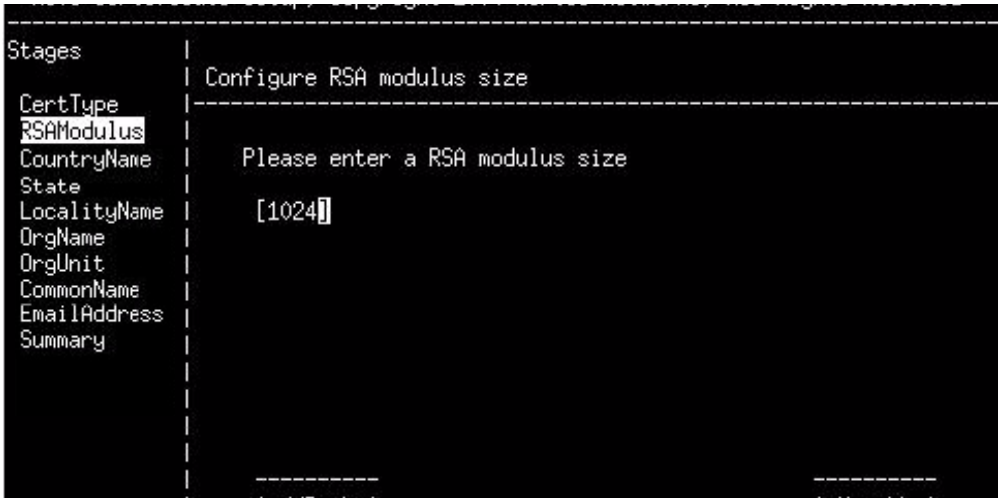
`cert_mgnt`

After a few seconds the Introduction screen is displayed.

3 Press 2 for the option to generate a certificate signing request for a signing authority, position the cursor on the **Next** button and press **Enter**.

Note: In general, use the **Tab** key or the < and > keys to navigate between fields on the screen and use **Enter** to select a field or entry.

The RSA modulus size screen appears.



4 Enter the RSA modulus (key) size, position the cursor on the **Next** button and press **Enter**. Supported values are 1024, 1536 or 2048 bits.

Note: The larger the key size, the stronger the private key. There may be a performance impact when using larger key sizes.

5 Use the following table to determine your next step:

If	Do
you receive the message that the RSA private key already exists and you do not want to reuse the key	step 6
you receive the message that the RSA private key already exists and you want to reuse the key	Press **y** and skip to step 10
you do not receive any message that an RSA private key already exists	step 10

6 If you do not want to reuse the key, press **n**.

The system prompts that the RSA key is about to be deleted.

7 Use the following table to determine your next step:

If	Do
you do not want to delete the existing RSA key	Press **n** to abort the delete operation and go to step 8
you are sure you want to proceed with deleting the existing RSA private key	Skip to step 9.

8 Press any key and return to step 4.

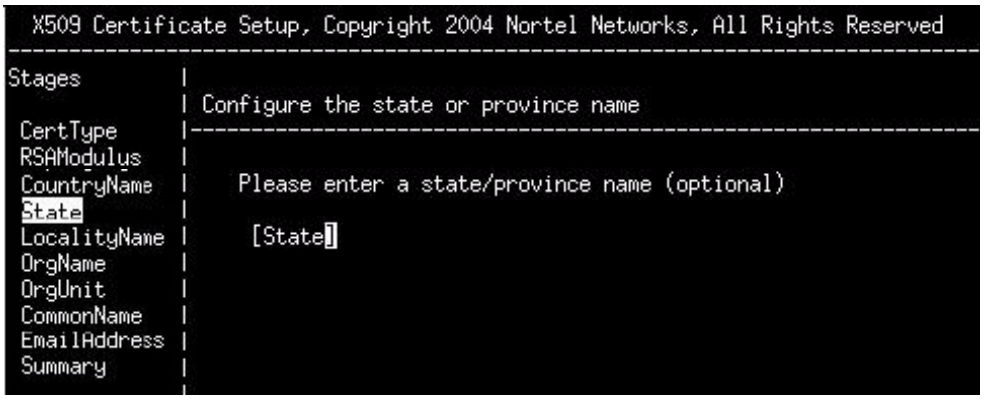
9 If you want to delete the existing RSA key, press **y**.

A backup of the existing key is made to a file in the same directory and a customer log is generated. The country name configuration screen appears.

10 If applicable, enter the optional ISO 3166-1-alpha-2 two-letter country code, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The state/province configuration screen appears.



11 If applicable, enter the optional state or province name, position the cursor on the **Next** button and press **Enter**.

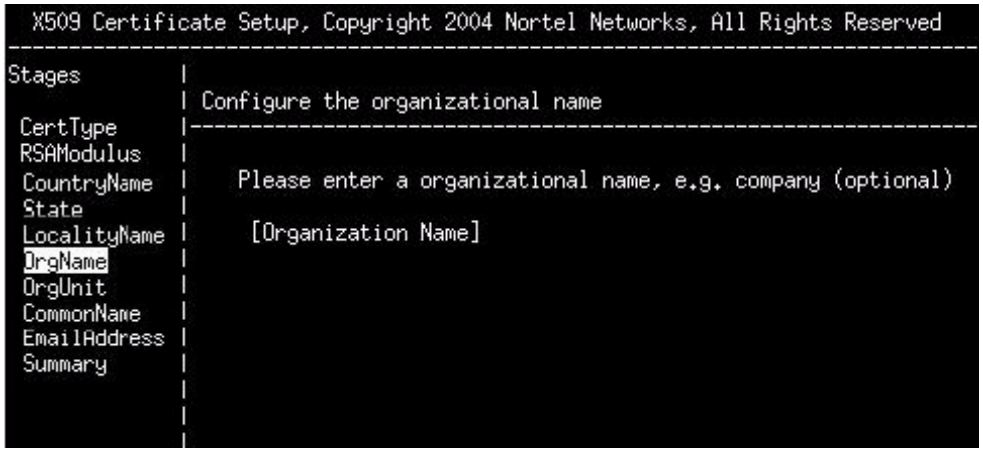
Note: This entry helps identify the Policy Controller to a remote entity.

The locality configuration screen appears.

12 If applicable, enter the optional name of the locality or city, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The organizational configuration screen appears.



13 If applicable, enter the optional name of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The organizational unit configuration screen appears.

14 If applicable, enter the optional name of the organizational unit, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The server common name configuration screen appears.

15 Enter a common name for the Policy Controller node to which this certificate applies using one of the following methods:

- use the active IP address for the Policy Controller in the format: xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. The hostname used must be in FQDN (fully-qualified domain name) format.

Note: The common name value is used for mutual authentication between the Policy Controller and the remote application server. There is no validation of the common name at this stage of the configuration operation.

16 Position the cursor on the **Next** button and press **Enter**.

An email configuration screen appears.

17 If applicable, enter the optional email address of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity. There is no validation of the email address.

A password challenge configuration screen appears.

18 Enter a password challenge phase, position the cursor on the **Next** button and press **Enter**. The challenge password may be required if you want to revoke your certificate.

Note: This entry can be up to 16 alphanumeric characters in length and can include the underscore character.

A certificate summary information screen appears.

19 Review the information summary. Position the cursor on the **Proceed** button and press **Enter**, otherwise click **Back** to make revisions.

The system responds by creating the security certificate:

```
Generating Certificate Signing Request
Creating Certificate Signing Request
Certificate Signing Request has been
successfully generated
Changing permissions on key file
```

20 The procedure is complete. The certificate signing request is ready to submit to a certificate authority, of the customer's choosing, for signing and certificate generation. This submission process may take several weeks to complete. Once the certificate authority's certificate and the signed certificate are returned to the customer site, you must validate the certificate chain using procedure Validate a certificate chain on page 56.

Validate a certificate chain

Purpose of this procedure

This procedure uses the certificate management tool to validate a certificate chain. It is part of the process for provisioning a CA-signed certificates. This procedure should only be used as part of a high level task for creating or updating security certificates.

Limitations and restrictions

The private key that was generated by the certificate signing request must be the same private key currently stored in /opt/base/share/ssl. The certificate management tool will verify that the certificate provided as the user certificate matches the private key file server.key located in /opt/base/share/ssl.

Prerequisites

You must first complete procedure Prepare to validate a certificate chain on page 60.

The following certificate files are required from a signing authority and must be located in the /opt/base/share/ssl directory to complete this procedure:

- Server.crt - contains the local certificate
- Trusted.crt - contains the CA chain in top down with the root CA at the top

The following restrictions apply to migrating CA-signed certificates:

- You must be a root user to use the certificate management tool.
- Only PEM formatted, CA-signed certificates are supported on Policy Controller.
- CA chain is required in PEM format in a trusted.crt file, top down with the root CA at the top
- This procedure cannot be performed on self-signed certificates. Migrating self-signed certificates is not supported. If your site uses self-signed certificates, you must create new ones during the upgrade activity.

Action

At the Policy Controller CLI or Integrated EMS client

1 Complete procedure Prepare to validate a certificate chain on page 60.

2 Log onto the standby Policy Controller unit and change to the root user.

3 Start the certificate management tool by typing

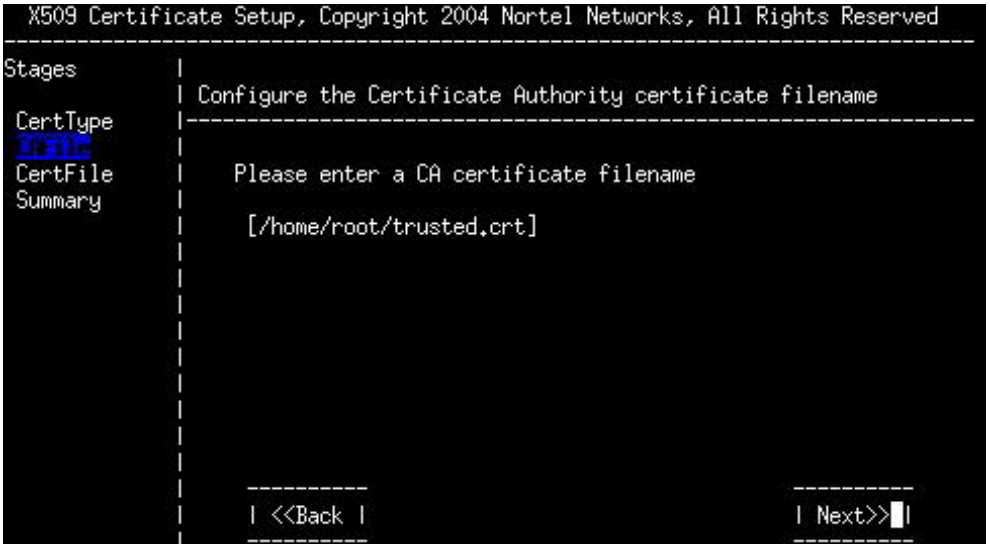
`cert_mgnt`

After a few seconds the Introduction screen is displayed.

4 Press **3** for the option to validate a certificate chain, position the cursor on the **Next** button and press **Enter**.

Note: In general, use the **Tab** key or the < and > keys to navigate between fields on the screen and use **Enter** to select a field or entry.

The configure CA-signed certificate screen appears.



5 Enter the full path and filename where the CA certificate can be found by typing

`/opt/base/share/ssl/trusted.crt`

position the cursor on the **Next** button and press **Enter**.

Note: The tool will not proceed unless the CA certificate trusted.crt file exists in the location specified.

The configure server certificate screen appears.

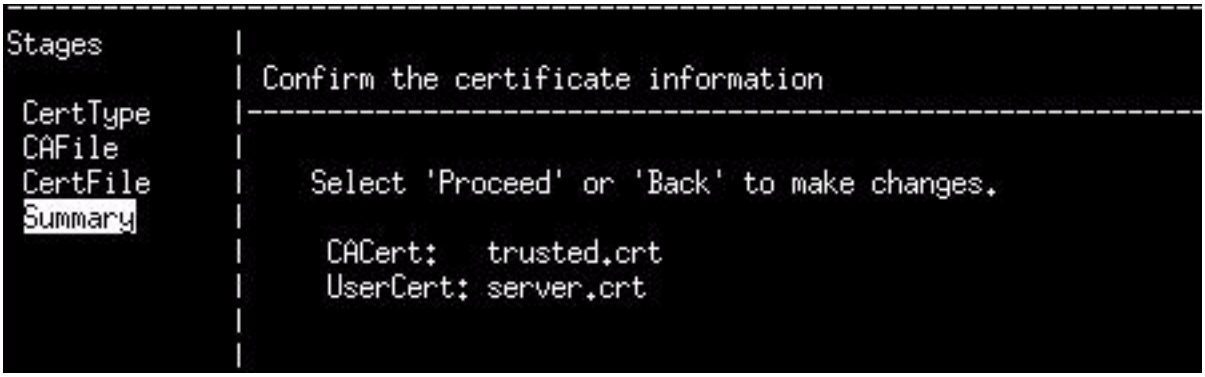
6 Enter the full path and filename where the server.crt certificate can be found by typing

`/opt/base/share/ssl/server.crt`

position the cursor on the **Next** button and press **Enter**.

Note: The tool will not proceed unless the server.crt file exists in the location specified.

The summary screen appears.



7 Review the information summary. Position the cursor on the **Proceed** button and press **Enter**, otherwise click **Back** to make revisions.

The tool validates the certificates chain and the trusted certificate files. Upon success, the tool displays the following:

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile /opt/base/share/ssl/trusted.crt
/opt/base/share/ssl/server.crt
/opt/base/share/ssl/server.crt: OK
server.crt: OK
Certificate validation succeeded
Exporting certificate/key pair to PKCS#12 keystore
Certificate/key pair has been successfully exported to PKCS#12
format
Changing permissions on key file
Changing permissions on keystore file
```

8 The procedure is complete.

Troubleshooting

The private key in the server.key file must correspond to the certificate in the server.crt file for validation to be successful. If require assistance with completing this procedure, please contact Nortel GNPS.

Prepare to validate a certificate chain

Purpose of this procedure

Use the following procedure to migrate certificate authority (CA)-signed security certificates from the current release to a new release during a major release upgrade. Use this procedure only as part of a higher level activity such as part of an upgrade or security certificate management activity.

This procedure cannot be performed on self-signed certificates. Migrating self-signed certificates is not supported. If your site uses self-signed certificates, you must create new ones during the upgrade activity.

Limitations and Restrictions

The following restrictions apply to migrating CA-signed certificates:

- Only PEM formatted, CA-signed certificates are supported on Policy Controller.
- A CA-chain is required in PEM format in a trusted.crt file, top down, with the root CA at the top. Refer to section Additional information about trusted certificates on page 62 for more information.

Prerequisites

This procedure has the following prerequisites:

- Existing CA-signed security certificates must be prepared per section Additional information about trusted certificates on page 62.

Action

Perform the following steps to complete this procedure.

At the Policy Controller CLI or Integrated EMS client

1 Log onto the inactive Policy Controller unit and change to the root user.

2 Ensure that the local server CA-signed certificate that was obtained from the certificate authority is in the file /opt/base/share/ssl/server.crt.

3 Ensure that the private key corresponding to the local server CA-signed certificate is in the file /opt/base/share/ssl/server.key.

ATTENTION

There can only be one certificate in the server.crt file and that certificate must be in PEM format.

Note: Refer to section Additional information about trusted certificates on page 62 for assistance with this task.

4 From the certificate authority, obtain the CA certificate chain, with the root CA-certificate, in top down format, in the file /opt/base/share/ssl/trusted.crt file. This chain can be obtained from the certificate authority directly.

ATTENTION

The trusted.crt certificate must be in PEM format.

5 Verify successful preparation of the certificate files by typing

```
openssl verify /opt/base/share/ssl/trusted.crt
/opt/base/share/ssl/server.crt
```

and press the Enter key.

6 If the result from step 5 is “OK”, you are ready to proceed with the upgrade preparation. If the result from step 5 is not “OK”, then there was problem with the security certificates and you must contact Nortel GNPS.

7 The procedure is complete.

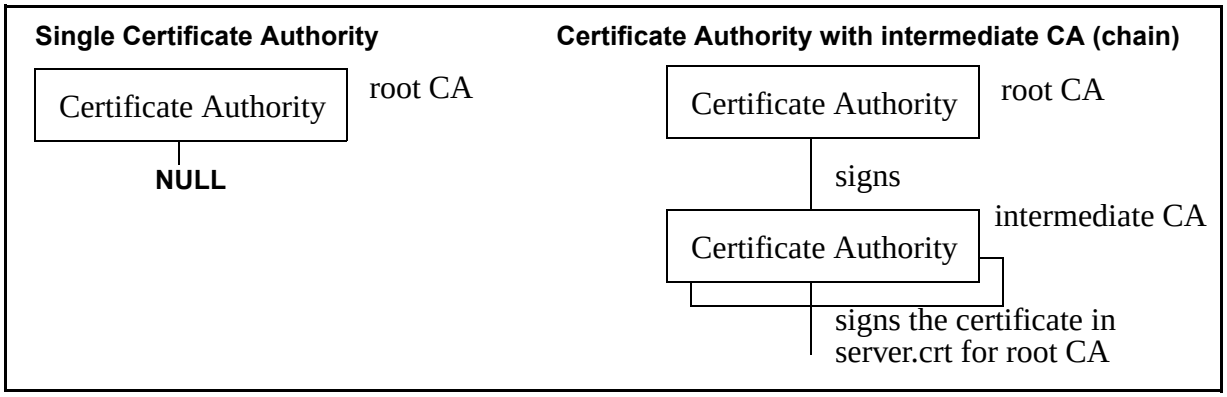
Additional information about trusted certificates

The following section provides additional information about trusted certificates and root CAs.

Root CAs that do not correspond to the local server certificate are not placed in the trusted.crt file. They are added using the CS 2000 Policy Controller Manger GUI using procedure *Manage Trusted Certificates*, found in the Policy Controller Security and Administration NTP, NN10346-611. Only the Root CA corresponding to the local certificate is placed in the trusted. crt file, followed by the CA chain. For example, if the local certificate is signed by one of the global public root certificate authorities, then that root CA certificate is placed in this file.

The following figure shows an example of the structure of a trusted.crt file. The trusted.crt on the left shows a single CA signing the root certificate. The trusted.crt on the right shows the certificate of the Certificate Authority (CA), followed by each intermediate chain CA, followed by the CA which ultimately signed the local certificate.

Structure of a trusted.crt file



The following is an example of a CA-signed trusted.crt file. In this case, it is a chain composed of a root CA, followed by 3 (three) intermediate chain CAs. At the top of the file is certificate of the root Certificate Authority (CA), followed by each intermediate chain CA, followed by that last CA which ultimately signed the local certificate.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Validity
            Not Before: Oct  8 01:14:48 2004 GMT
            Not After : Oct  8 01:14:48 2005 GMT
        Subject: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                00:bc:53:2a:bd:bf:36:87:36:5b:12:93:a7:55:84:
                 1d:3b:75:0f:d9:de:d6:34:d3:51:8d:96:c6:41:c6:
                       80:b3:08:18:e7:b1:e5:af:0a:00:1d:65:82:77:0a:
                ca:7d:74:00:79:85:d6:80:07:79:8d:ec:b0:e3:6e:
                8c:d0:a7:20:6f:c7:3b:df:09:83:93:36:9f:eb:67:
                  c1:e2:ab:a5:ed:ab:3a:d8:97:ad:83:bf:8c:11:02:
                     12:3b:dc:a9:82:0d:f3:45:d7:8a:ae:96:eb:17:26:
                  3c:de:7a:cd:91:71:b9:56:c7:e7:0c:7a:5e:57:62:
                9c:d7:3e:41:82:c9:f3:34:1d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:

90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
            X509v3 Authority Key Identifier:

keyid:90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
                DirName:/C=CA/ST=Ontario/L=Timbuktu/O=Nortel
Networks/OU=Certificate Authority
                serial:00

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        33:65:6c:d0:0d:b8:7f:58:1c:33:1c:d2:4e:e3:19:2d:36:c3:
        15:7f:b3:80:cb:22:2a:dc:eb:ba:84:50:24:7c:cc:07:49:62:
        f5:2c:f9:bc:47:04:56:ea:bd:78:de:44:43:22:e2:1c:5f:fc:
        17:91:80:70:f3:29:e2:74:46:8d:3d:ac:fa:63:f2:b4:ba:79:
        d2:22:76:6c:2e:fb:e6:55:16:6f:db:27:5f:e3:ff:32:84:5a:
        b7:a3:9c:c4:73:f9:72:c2:8b:6e:8d:4f:bf:d2:3f:b1:51:48:
        b5:4e:27:b4:bb:80:4b:87:f9:e7:18:ba:63:20:ac:6d:25:c2:
        74:1b

-----BEGIN CERTIFICATE-----
MIIDGDCCAoGgAwIBAgIBADANBgkqhkiG9w0BAQQFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
cnRlbCBOZXR3b3JrczEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTQ0OFoXDTA1MTAwODAxMTQ0OFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xETAPBgNVBAcTCFRpbWJ1a3R1MRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEF1dGhvcml0eTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvFMqvb82hzZbEpOnVYQdO3UP2d7WNNNR
jZbGQcaAswgY57HlrwoAHWWCdwrKfXQAeYXWgAd5jeyw426M0Kcgb8c73wmDkzaf
62fB4qul7as62Jetg7+MEQISO9ypgg3zRdeKrpbrFyY83nrNkXG5VsfnDHpeV2Kc
1z5BgsnzNB0CAwEAAaOByTCBxjAdBgNVHQ4EFgQUkCC8d91kUNdQVl3HP+x6MiEP
rvQwgZYGA1UdIwSBjjCBi4AUkCC8d91kUNdQVl3HP+x6MiEPrvShcKRuMGwxCzAJ
BgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMREwDwYDVQQHEwhUaW1idWt0dTEY
MBYGA1UEChMPTm9ydGVsIE5ldHdvcmtzMR4wHAYDVQQLExVDZXJ0aWZpY2F0ZSBB
dXRob3JpdHmCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQAzZWzQ
Dbh/WBwzHNJO4xktNsMVf7OAyyIq3Ou6hFAkfMwHSWL1LPm8RwRW6r143kRDIuIc
X/wXkYBw8ynidEaNPaz6Y/K0unnSInZsLvvmVRZv2ydf4/8yhFq3o5zEc/lywotu
jU+/0j+xUUi1Tie0u4BLh/nnGLpjIKxtJcJ0Gw==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Validity
            Not Before: Oct  8 01:19:20 2004 GMT
            Not After : Oct  8 01:19:20 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain1, CN=Chain1
```

```
            Subject Public Key Info:
                Public Key Algorithm: rsaEncryption
                RSA Public Key: (1024 bit)
                    Modulus (1024 bit):
                        00:c5:d9:e9:4d:aa:87:56:ce:b0:ba:17:fb:fd:78:
                        89:85:54:21:5b:2e:e8:71:e8:14:64:00:dd:b5:2e:
                        0b:2a:e5:75:71:c2:42:17:29:e7:44:79:b0:2a:82:
                        05:5b:92:c1:f3:5a:72:90:72:ee:ec:b1:77:39:cf:
                        3c:c3:92:6a:6d:49:41:43:96:4c:e9:f6:3f:c3:3a:
                        d9:79:11:ff:aa:74:ba:31:71:b3:0e:f0:f8:20:21:
                        3c:76:5b:ad:6b:b6:27:2a:27:86:99:06:3a:1c:81:
                        a5:ca:7c:68:36:cd:45:bd:2f:48:b0:5e:03:75:6e:
                        35:95:42:60:3e:6e:f5:bc:35
                    Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Basic Constraints:
                    CA:TRUE
        Signature Algorithm: sha1WithRSAEncryption
            99:56:1b:2f:2f:b0:5f:4f:a5:7b:70:ce:6c:41:d3:36:20:2c:
            31:fb:61:df:81:58:81:4c:7f:30:a8:e1:d8:c7:97:0b:ad:19:
            21:19:79:ba:90:9f:3d:38:a0:66:6d:0a:6e:47:16:7f:4c:5b:
            7d:5b:bd:21:23:bc:15:27:e9:e5:f5:ec:6b:38:67:69:4e:86:
            82:a9:c0:f5:8a:c4:39:f7:98:89:ac:45:3f:a1:c9:47:26:9b:
            54:d2:d4:9d:d2:dd:c8:4f:58:cf:7c:57:d8:10:6d:d4:3e:3e:
            0a:12:1f:54:d7:f5:38:43:3d:f7:09:8e:33:b5:a1:80:00:14:
            50:f0

    -----BEGIN CERTIFICATE-----
    MIICXjCCAcegAwIBAgIBATANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
    MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
    cnRlbCBOZXR3b3JrczEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
    DTA0MTAwODAxMTkyMFoXDTA1MTAwODAxMTkyMFowbDELMAkGA1UEBhMCQ0ExEDAO
    BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
    IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjExDzANBgNVBAMTBkNoYWluMTCBnzAN
    BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdnpTaqHVs6wuhf7/XiJhVQhWy7ocegU
    ZADdtS4LKuV1ccJCFynnRHmwKoIFW5LB81pykHLu7LF3Oc88w5JqbUlBQ5ZM6fY/
    wzrZeRH/qnS6MXGzDvD4ICE8dluta7YnKieGmQY6HIGlynxoNs1FvS9IsF4DdW41
    lUJgPm71vDUCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
    gQCZVhsvL7BfT6V7cM5sQdM2ICwx+2HfgViBTH8wqOHYx5cLrRkhGXm6kJ89OKBm
    bQpuRxZ/TFt9W70hI7wVJ+nl9exrOGdpToaCqcD1isQ595iJrEU/oclHJptU0tSd
    0t3IT1jPfFfYEG3UPj4KEh9U1/U4Qz33CY4ztaGAABRQ8A==
    -----END CERTIFICATE-----
    Certificate:
        Data:
            Version: 3 (0x2)
            Serial Number: 2 (0x2)
            Signature Algorithm: sha1WithRSAEncryption
            Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
    OU=Chain1, CN=Chain1
            Validity
                Not Before: Oct  8 01:22:23 2004 GMT
                Not After : Oct  8 01:22:23 2005 GMT
            Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
    OU=Chain2, CN=Chain2
            Subject Public Key Info:
                Public Key Algorithm: rsaEncryption
                RSA Public Key: (1024 bit)
                    Modulus (1024 bit):
                        00:bf:8a:b7:44:9c:92:b5:fd:f0:e7:d3:1c:9d:65:
                        c4:e3:8c:cb:d3:60:a0:9d:bc:d7:87:15:d1:f0:68:
                        3c:71:be:2e:8d:2f:d0:7e:f6:95:2f:f3:89:b4:9b:
                        b6:c9:bd:52:62:8d:05:e3:71:3e:d5:c1:50:27:67:
                        01:f4:8b:7e:c9:6d:4e:a5:24:ff:d7:80:37:86:09:
                        8c:0a:8d:79:cc:b2:e6:9e:d8:7d:71:db:12:e6:84:
                        7e:2f:90:17:ca:84:87:9b:63:72:4a:28:d7:75:91:
                        f1:4f:c2:6b:5e:a7:d2:2b:01:60:f7:5f:35:dd:8e:
                        92:d7:b7:f5:a4:66:f6:af:21
                    Exponent: 65537 (0x10001)
```

```
            X509v3 extensions:
                X509v3 Basic Constraints:
                    CA:TRUE
        Signature Algorithm: sha1WithRSAEncryption
            3c:0c:fa:58:1f:14:d3:3f:f1:cb:80:7b:8f:bb:f7:17:e5:18:
            21:bd:a2:77:3e:ce:5d:4c:80:a8:3e:7e:a1:9c:fe:c8:6a:d0:
            7d:67:45:b9:5a:a6:89:3a:2f:de:25:20:2f:ed:62:b5:06:8f:
            dd:a1:85:aa:a2:a3:8d:a3:6d:4c:5e:ed:e8:35:f3:50:98:26:
            99:38:1c:33:a3:99:0a:50:11:f8:0e:21:9d:fe:56:fb:ec:b9:
            55:ed:83:a7:b0:a4:26:82:7f:12:3b:35:9c:03:b9:40:02:3d:
            5c:d5:34:e2:ee:ff:91:58:9f:9d:cf:2e:91:35:9d:c8:5a:f1:
            19:59

    -----BEGIN CERTIFICATE-----
    MIICXjCCAcegAwIBAgIBAjANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
    MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
    ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMTEPMA0GA1UEAxMGQ2hhaW4xMB4X
    DTA0MTAwODAxMjIyM1oXDTA1MTAwODAxMjIyM1owbDELMAkGA1UEBhMCQ0ExEDAO
    BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
    IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjIxDzANBgNVBAMTBkNoYWluMjCBnzAN
    BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAv4q3RJyStf3w59McnWXE44zL02CgnbzX
    hxXR8Gg8cb4ujS/QfvaVL/OJtJu2yb1SYo0F43E+1cFQJ2cB9It+yW1OpST/14A3
    hgmMCo15zLLmnth9cdsS5oR+L5AXyoSHm2NySijXdZHxT8JrXqfSKwFg91813Y6S
    17f1pGb2ryECAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
    gQA8DPpYHxTTP/HLgHuPu/cX5RghvaJ3Ps5dTICoPn6hnP7IatB9Z0W5WqaJOi/e
    JSAv7WK1Bo/doYWqoqONo21MXu3oNfNQmCaZOBwzo5kKUBH4DiGd/lb77LlV7YOn
    sKQmgn8SOzWcA7lAAj1c1TTi7v+RWJ+dzy6RNZ3IWvEZWQ==
    -----END CERTIFICATE-----
    Certificate:
        Data:
            Version: 3 (0x2)
            Serial Number: 3 (0x3)
            Signature Algorithm: sha1WithRSAEncryption
            Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
    OU=Chain2, CN=Chain2
            Validity
                Not Before: Oct  8 01:24:40 2004 GMT
                Not After : Oct  8 01:24:40 2005 GMT
            Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
    OU=Chain3, CN=Chain3
            Subject Public Key Info:
                Public Key Algorithm: rsaEncryption
                RSA Public Key: (1024 bit)
                    Modulus (1024 bit):
                        00:9e:10:4a:52:3a:e3:27:cc:0f:bb:70:a0:dc:66:
                        df:27:47:17:54:4c:56:1e:f1:7c:6e:71:e6:b0:f1:
                        7e:2d:a3:32:e0:c1:a4:50:5e:3a:cf:eb:09:ac:f5:
                        00:f4:25:a5:ae:59:3d:b0:e5:02:af:ec:d8:b2:e5:
                        c3:31:35:d0:d0:14:35:7d:c9:85:ef:fc:b3:c4:05:
                        0b:06:b4:b9:67:53:4d:0b:e9:c8:f1:a0:44:ac:6f:
                        27:4c:71:6f:be:31:63:12:21:4d:4b:a8:58:97:67:
                        c0:e4:1f:bb:d2:fe:4d:d6:48:3c:19:c6:fb:db:2a:
                        4e:1d:bf:f4:b4:41:23:69:c5
                    Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Basic Constraints:
                    CA:TRUE
        Signature Algorithm: sha1WithRSAEncryption
            bd:1b:08:a2:9f:af:f4:3e:3e:b6:72:e4:ca:ec:89:c5:fe:e4:
            fd:99:b9:a4:31:b9:58:64:83:df:b5:8e:d3:97:89:c3:e8:0c:
            96:0b:9d:c2:cc:81:b1:cd:78:17:13:ad:28:e8:ae:4d:2b:0e:
            1b:b7:96:e2:74:65:23:02:5a:b1:e6:90:89:cf:9b:3c:c1:b5:
            44:6f:ac:05:0d:d7:86:cc:eb:ce:ea:36:12:5a:3b:44:ac:f9:
            0e:44:f5:c0:23:ff:55:1f:ef:1d:64:04:82:f2:7b:cc:22:25:
            49:e4:a5:74:8c:9a:1d:22:5c:a7:7e:04:12:90:c9:88:d6:f4:
            a2:b0
    -----BEGIN CERTIFICATE-----
    MIICXjCCAcegAwIBAgIBAzANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
```

```
MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMjEPMA0GA1UEAxMGQ2hhaW4yMB4X
DTA0MTAwODAxMjQ0MFoXDTA1MTAwODAxMjQ0MFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjMxDzANBgNVBAMTBkNoYWluMzCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAnhBKUjrjJ8wPu3Cg3GbfJ0cXVExWHvF8
bnHmsPF+LaMy4MGkUF46z+sJrPUA9CWlrlk9sOUCr+zYsuXDMTXQ0BQ1fcmF7/yz
xAULBrS5Z1NNC+nI8aBErG8nTHFvvjFjEiFNS6hYl2fA5B+70v5N1kg8Gcb72ypO
Hb/0tEEjacUCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQC9Gwiin6/0Pj62cuTK7InF/uT9mbmkMblYZIPftY7Tl4nD6AyWC53CzIGxzXgX
E60o6K5NKw4bt5bidGUjAlqx5pCJz5s8wbVEb6wFDdeGzOvO6jYSWjtErPkORPXA
I/9VH+8dZASC8nvMIiVJ5KV0jJodIlynfgQSkMmI1vSisA==
-----END CERTIFICATE-----
```

Apply security certificates

Purpose of this procedure

The following procedure is used to apply security certificates so that they are available to the Apache and Tomcat web services used by the Policy Controller GUIs and the Policy Controller application.

Use this procedure only as part of a higher level activity such as part of an upgrade or security certificate management activity.

Limitations and Restrictions

CAUTION

This is a service affecting procedure.

Stopping and starting the Apache and Tomcat web services, causes access to the web server to be temporarily lost. Any open web connections to the web server are dropped. When executing this procedure, ensure that provisioning or maintenance activities are not occurring on any network element using the web services. Web access to the Policy Controller GUIs returns once the Apache and Tomcat services are restarted.

Prerequisites

This procedure has the following prerequisites:

- You must have first installed or copied any new security certificates to the cd /opt/base/share/ssl directory.

Action

Perform the following steps to complete this procedure.

At your workstation CLI or Integrated EMS client

1 Log onto the inactive Policy Controller unit and change to root user.

2 Stop the Apache web server by typing

```
# /usr/local/apache/bin/apachectl stop
```

and pressing the Enter key.

3 Restart the Apache web server by typing

`# /usr/local/apache/bin/apachectl startssl`

and pressing the Enter key.

4 Stop the Tomcat web server by typing

`# /opt/apps/webint/tomcatd stop`

and pressing the Enter key.

5 Restart the Tomcat web server by typing

`# /opt/apps/webint/tomcatd start`

and pressing the Enter key.

6 The Policy Controller application must be stopped and restarted to allow it to work with the new security certificates. Execute procedures Lock the Policy Controller application on page 34, Suspend the Policy Controller application on page 42, Unsuspend the Policy Controller application on page 45 and Unlock the Policy Controller application on page 39, in the order listed, to stop and restart the application.

CAUTION

If a SIP trunk is in the INB state, performing a Suspend and Unsuspend does not cause the trunk to go to in-service state.

7 You have completed this procedure.

Copy security certificates to the mate Policy Controller unit

Purpose of this procedure

The following procedure is used to copy security certificates from one Policy Controller unit to another.

Use this procedure any time new security certificates are created, or when the system is changed from using self-signed certificates to CA-signed certificates. This procedure may also be used as part of a major release upgrade activity.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

New certificates, either self-signed or CA-signed must be installed on the inactive unit.

Action

Perform the following steps to complete this procedure.

At the Policy Controller CLI or Integrated EMS client

1 Log onto the inactive Policy Controller unit and change to the root user.

2 Change directories to the security certificates level by typing

```
# cd /opt/base/share/ssl
```

and pressing the Enter key.

3 Secure copy the server.key file to the mate Policy Controller unit by typing

```
$ scp server.key
mtc@<mate_PC_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_PC_IP_address
is the IP address of the mate Policy Controller unit

Note: For initial connections to the mate unit, confirm that you want to continue connecting by entering “yes.”

The mate unit responds by prompting for the password for the mtc user.

4 Enter the password for the mtc user at the password prompt.

The server.key file is copied to the /users/mtc directory on the mate Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.

5 Secure copy the certificate.keystore file to the mate Policy Controller unit by typing

```
$ scp certificate.keystore
mtc@<mate_PC_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_PC_IP_address
is the IP address of the mate Policy Controller unit

The mate unit responds by prompting for the password for the mtc user.

6 Enter the password for the mtc user at the password prompt.

The certificate.keystore file is copied to the /users/mtc directory on the mate Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.

7 Secure copy the server.crt file to the mate Policy Controller unit by typing

```
$ scp server.crt
mtc@<mate_PC_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_PC_IP_address
is the IP address of the mate Policy Controller unit

The mate unit responds by prompting for the password for the mtc user.

8 Enter the password for the mtc user at the password prompt.

The server.crt file is copied to the /users/mtc directory on the mate Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.

9 If you have a CA-signed certificate, secure copy the trusted.crt file to the mate Policy Controller unit by typing

```
$ scp trusted.crt
mtc@<mate_PC_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_PC_IP_address
is the IP address of the mate Policy Controller unit

The mate unit responds by prompting for the password for the mtc user.

10 If applicable, enter the password for the mtc user at the password prompt. Otherwise, skip to the next step.

The trusted.crt file is copied to the /users/mtc directory on the mate Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.

At your workstation CLI or Integrated EMS client

11 Log into to the mate Policy Controller and change to the root user.

12 Change directories to the /users/mtc level by typing

```
cd /users/mtc
```

and pressing the Enter key.

13 Move the server.key file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv server.key /opt/base/share/ssl
```

and pressing the Enter key.

14 If necessary, confirm overwriting any existing server.key file by typing **y** and pressing Enter.

15 Move the certificate.keystore file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv certificate.keystore /opt/base/share/ssl
```

and pressing the Enter key.

16 If necessary, confirm overwriting any existing certificate.keystore file by typing **y** and pressing Enter.

17 Move the server.crt file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv server.crt /opt/base/share/ssl
```

and pressing the Enter key.

18 If necessary, confirm overwriting any existing server.crt file by typing **y** and pressing Enter.

19 If you have a CA-signed certificate, move the trusted.crt file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv trusted.crt /opt/base/share/ssl
```

and pressing the Enter key.

20 If necessary, confirm overwriting any existing trusted.crt file by typing **y** and pressing Enter.

21 Change directories to the security certificates level by typing

```
# cd /opt/base/share/ssl
```

and pressing the Enter key.

22 Change the key file's owner and group to *root* by typing

```
# chown root:root server.key
```

and pressing the Enter key.

23 Change the keystore file's owner and group to *root* by typing

```
# chown root:root certificate.keystore
```

and pressing the Enter key.

24 Change the certificate's owner and group to *root* by typing

```
# chown root:root server.crt
```

and pressing the Enter key.

25 If you have a CA-signed certificate, change the trusted certificate file's owner and group to *root* by typing

```
# chown root:root trusted.crt
```

and pressing the Enter key.

26 Set the key file permissions by typing

```
# chmod 600 server.key
```

and pressing the Enter key.

27 Set the keystore file permissions by typing

```
# chmod 600 certificate.keystore
```

and pressing the Enter key.

28 Set the certificate permissions by typing

```
# chmod 644 server.crt
```

and pressing the Enter key.

29 If you have a CA-signed certificate, set the keystore file permissions by typing

```
# chmod 644 trusted.crt
```

and pressing the Enter key.

30 You have completed this procedure. If you completed this procedure as part of an upgrade activity, return to the high level activity.

Generate self-signed security certificates

Purpose of this procedure

This procedure uses the certificate management tool to generate self-signed security certificates used for both Policy Controller units. This procedure should only be used as part of a high level task for updating security certificates.

A successful completion of this procedure creates a self-signed certificate composed of the following files:

- Server.crt - contains the local certificate
- Server.key -contains the private key corresponding to the local certificate
- Trusted.crt - is an empty file if it did not already exist before the certificate management tool was run
- Certificate.keystore - contains the private key and local certificate

Limitations and restrictions

You must be a root user to use the certificate management tool.

ATTENTION

The certificate management tool sets the appropriate file permissions for when the certificate files are generated. These file permissions should not be changed.

Prerequisites

Please read the complete disclaimer, found in section Self-signed certificate security disclaimer on page 84.

Action

At the Policy Controller CLI or Integrated EMS client

1 Log onto the standby Policy Controller unit and change to the root user.

2 Start the certificate management tool by typing

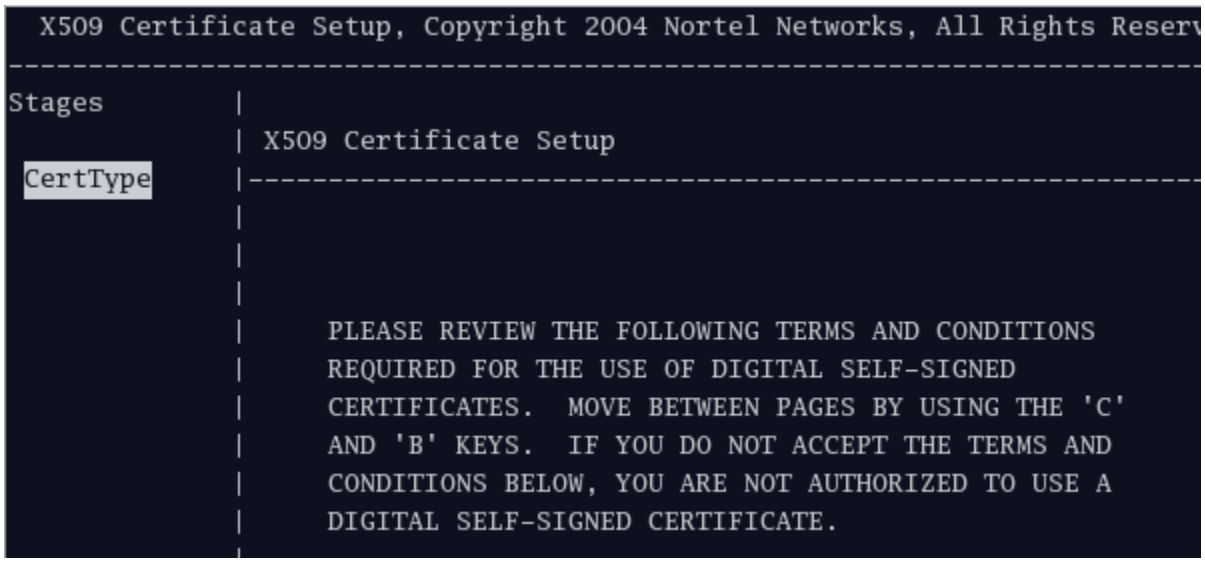
`cert_mgnt`

After a few seconds the Introduction screen is displayed.

3 Type **1** for the option to generate a self-signed certificate type, position the cursor on the **Next** button and press **Enter**.

Note: In general, use the **Tab** key or the < and > keys to navigate between fields on the screen and use **Enter** to select a field or entry.

A security disclaimer screen appears.

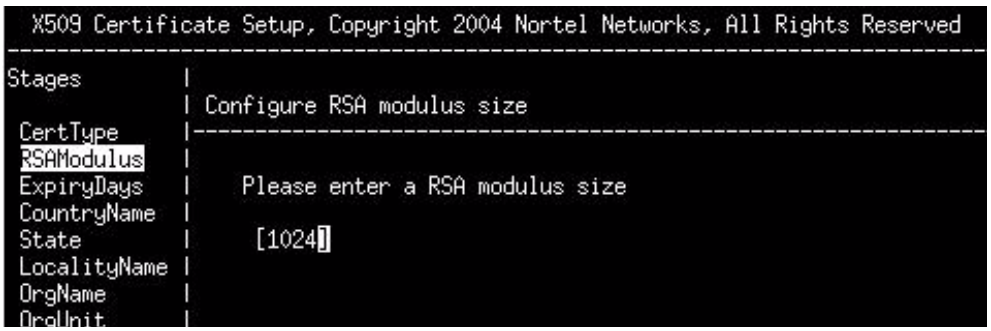


4 Carefully read the series of screens displaying the terms and conditions of the security certificate tool. Press **c** to continue to the next disclaimer page or press **b** to go back to the previous disclaimer page.

5 At the final disclaimer page, accept the terms and conditions of the security certificate tool by pressing **y**.

Otherwise you can reject the terms and conditions of the security disclaimer by pressing **n.** You are returned to the main menu.

The RSA modulus size screen appears.



6 Enter the RSA modulus (key) size, position the cursor on the **Next** button and press **Enter**. Supported values are 1024, 1536 or 2048 bits. (1024 is recommended)

Note: The larger the key size, the stronger the private key. There may be a performance impact when using larger key sizes.

7 Use the following table to determine your next step:

If	Do
you receive the message that the RSA private key already exists and you do not want to reuse the key	step 8
you receive the message that the RSA private key already exists and you want to reuse the key	Press **y** and skip to step 12
you do not receive any message that an RSA private key already exists	step 12

8 If you do not want to reuse the key, press **n**.

The system prompts that the RSA key is about to be deleted.

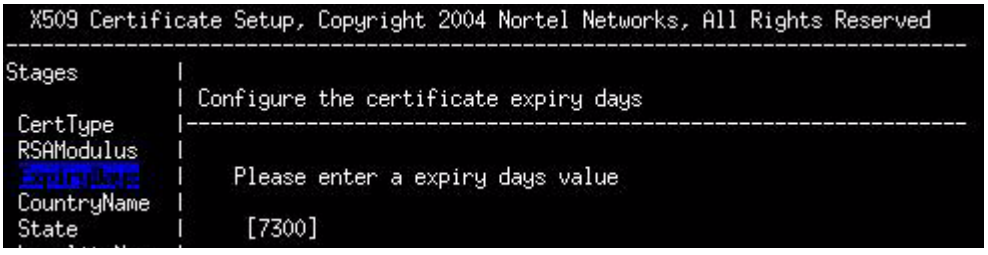
9 Use the following table to determine your next step:

If	Do
you do not want to delete the existing RSA key	Press **n** to abort the delete operation and go to step 10.
you are sure you want to proceed with deleting the existing RSA private key	Skip to step 11.

10 Press any key and return to step 6.

11 If you want to delete the existing RSA key, press **y**.

A backup of the existing key is made to a file in the same directory and a customer log is generated. The expiration configuration screen appears.



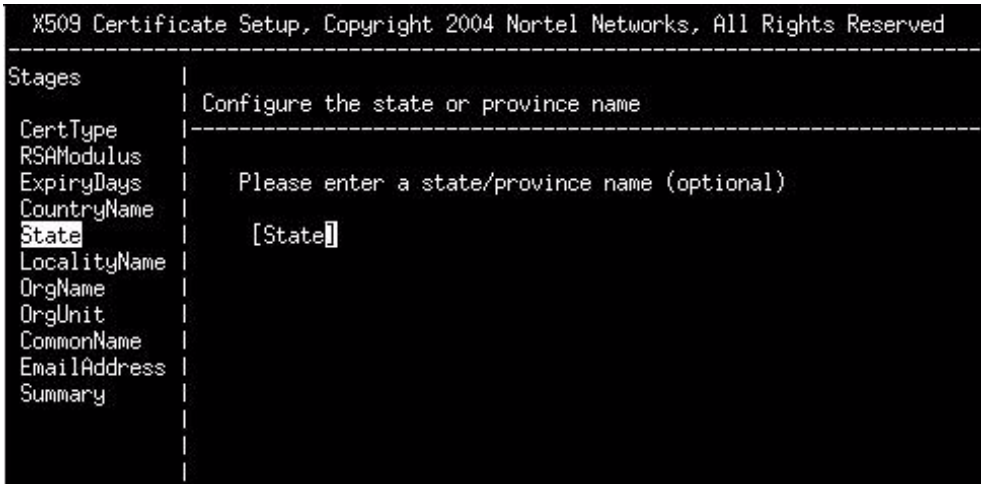
12 At the certificate expiry days screen, enter the number of days you want the certificate to be valid, position the cursor on the **Next** button and press **Enter**. Supported expiration values range from 30 (30 days from the date of creation) to 7300 (20 years from the date of creation).

The country name configuration screen appears.

13 If applicable, enter the optional ISO 3166-1-alpha-2 two-letter country code, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

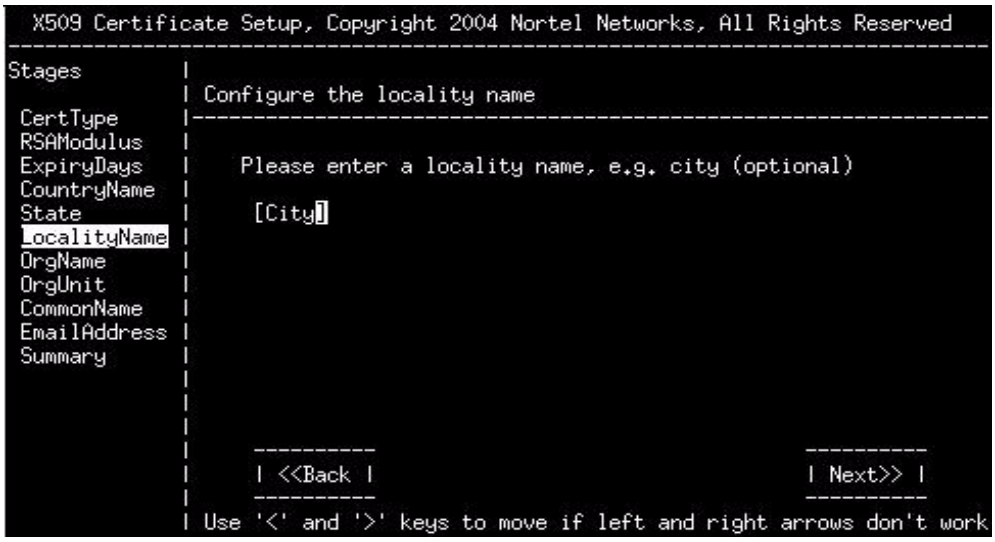
The state/province configuration screen appears.



14 If applicable, enter the optional state or province name, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

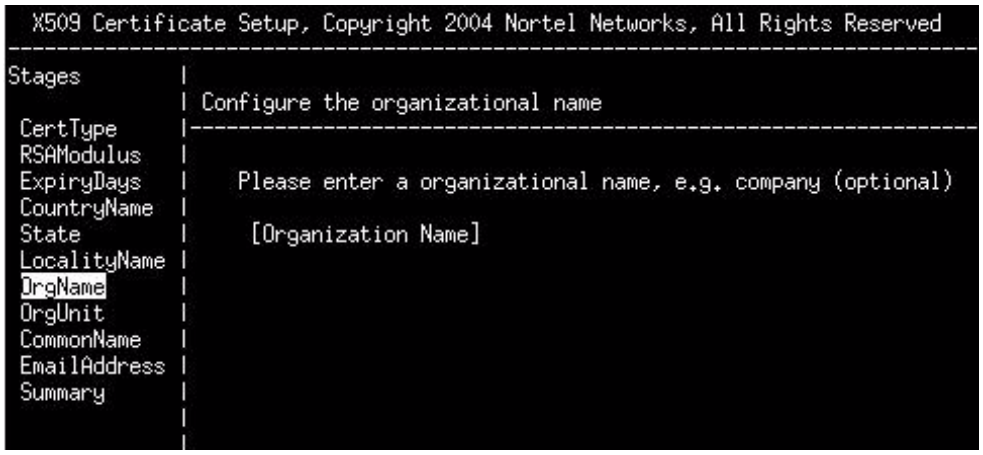
The locality configuration screen appears.



15 If applicable, enter the optional name of the locality or city, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The organizational configuration screen appears.



16 If applicable, enter the optional name of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The organizational unit configuration screen appears.

17 If applicable, enter the optional name of the organizational unit, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity.

The server common name configuration screen appears.

18 Enter a common name for the Policy Controller node to which this certificate applies using one of the following methods:

- use the active IP address for the Policy Controller in the format: xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. The hostname used must be in FQDN (fully-qualified domain name) format.

Note: The common name value is used for mutual authentication between the Policy Controller and the remote application server. There is no validation of the common name at this stage of the configuration operation.

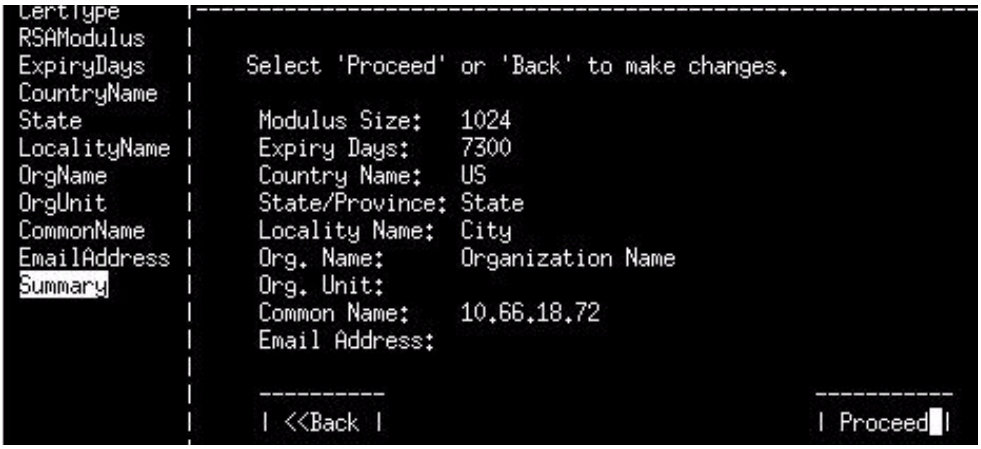
19 Position the cursor on the **Next** button and press **Enter**.

An email configuration screen appears.

20 If applicable, enter the optional email address of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Policy Controller to a remote entity. There is no validation of the email address.

A certificate summary information screen appears.



21 Review the information summary. Position the cursor on the **Proceed** button and press **Enter**, otherwise click **Back** to make revisions.

The system responds by creating the security certificate:

```
Exporting certificate/key pair to PKCS#12
keystore
Certificate/key pair has been successfully
exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

22 The procedure is complete.

Self-signed certificate security disclaimer

The following text contains the complete security disclaimer for using self-signed certificates. It is recommended that you read and understand this disclaimer before creating self-signed certificates.

“PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C' AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.”;

“DISCLAIMER OF WARRANTY: THIS DIGITAL SELF-SIGNED CERTIFICATE IS PROVIDED BY NORTEL 'AS IS' AND NEITHER NORTEL NOR ANY OF ITS SUPPLIERS MAKE, AND SPECIFICALLY DISCLAIM, ANY AND ALL REPRESENTATIONS, WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY,

ARISING BY USAGE OF TRADE OR OTHERWISE, INCLUDING WITHOUT LIMITATION, REPRESENTATIONS, WARRANTIES AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK OF THE USE OF ANY DIGITAL SELF-SIGNED CERTIFICATE SHALL BE BORNE SOLELY BY YOU.";

"LIMITATION OF LIABILITY: IN NO EVENT SHALL NORTEL OR ANY OF ITS SUPPLIERS AND THEIR RESPECTIVE, EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR BUSINESS OPPORTUNITIES, LOSS OF GOODWILL, PROFITS OR DATA, BUSINESS INTERRUPTION, LOST SAVINGS OR OTHER SIMILAR PECUNIARY LOSS, ARISING FROM OR IN CONNECTION WITH THE USE, PERFORMANCE OR NON-PERFORMANCE OF THE DIGITAL SELF-SIGNED CERTIFICATE, WHETHER ARISING IN LAW OR EQUITY, ARISING FROM CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE) OR ANY OTHER THEORY OF LIABILITY AND REGARDLESS OF WHETHER NORTEL OR ITS SUPPLIERS WERE AWARE OF THE POSSIBILITY THEREOF. BY ENTERING 'Y', YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS JUST REVIEWED. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS JUST REVIEWED, ENTER 'N' BELOW. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.";

Manage users on the Policy Controller platform

Purpose of this procedure

Use this procedure to add new users on a Policy Controller and assign them to user groups, or assign existing users to user groups. For more information about user groups refer to User and authorization categories on page 8.

Use this procedure also to delete existing users from the user database.

Limits and Restrictions

ATTENTION

Privileges for new users are only enforced on the CS 2000 Policy Controller Manager GUI, used for making provisioning changes to the Policy Controller application. However, privileges are not enforced for new users on the CS 2000 NCGL Platform Manager.

ATTENTION

User accounts and passwords are not propagated to the standby Policy Controller. Perform account management activities such as setting up users, removing users, and changing passwords, on both servers.

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

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 a secondary group, that specifies the operations a user is authorized to perform. Refer to User and authorization categories on page 8 for more information about primary and secondary user groups and user group domains.

Prerequisites

There are no prerequisites for using this procedure.

Action

At a Policy Controller console interface or command line interface

1 Open a secure shell to the Policy Controller by typing

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

PC_IP_address
is the IP address or host name on the Policy Controller

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Use the following table to determine your next step.

If you are	Do
adding a new user	step 4
deleting a user	skip to step 8
are done with this procedure	skip to step 9

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

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

and pressing the Enter key.

where

groupA
is a secondary user group. Refer to User and authorization categories on page 8 for more information about primary and secondary user groups and user group domains.

userid
is a variable for the user name

5 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.

6 When prompted, enter the password again for verification.

7 Return to step 3.

8 Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

9 Repeat this procedure on the second (mate) Policy Controller unit.

ATTENTION
User accounts and passwords are not automatically propagated to the standby Policy Controller. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

10 You have completed this procedure.

Manage user passwords using a Policy Controller console CLI

Purpose of this procedure

This procedure is used to enable, change or disable passwords for all user ids, including the root user id, on the Policy Controller using the Policy Controller platform console command line interface (CLI).

Limitations and Restrictions

ATTENTION

User accounts and passwords are not automatically propagated to the standby Policy Controller. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

Prerequisites

There are no prerequisites for this procedure.

Action

At a Policy Controller console interface or command line interface

1 Open a secure shell to the Policy Controller by typing

> **ssh -l <userid> <PC_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

PC_IP_address
is the IP address or host name of the Policy Controller on which you want to install the HTTPS certificate

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change the password for a specific user by typing

$ **passwd <userid>**

and pressing the Enter key.

where

userid
is a variable or code for the user's login identification

4 When prompted, enter a password of at least six characters.

Note: For security reasons, do not set a password with an empty value. Use a minimum of three characters.

5 When prompted, enter the password again for verification.

6 Repeat this procedure on the mate unit.

7 You have completed this procedure.

Manage user passwords with the Policy Controller GUI

Purpose of this procedure

This procedure is used to enable, change, or disable passwords for all user ids, except the root user id, on the Policy Controller using the Policy Controller GUI.

Limits and Restrictions

When performing this procedure, you can only change the password for the user ID that you logged in with. To change passwords for other user-created IDs, log into the Policy Controller using that user ID.

ATTENTION

User accounts and passwords are not automatically propagated to the standby Policy Controller. Performing account management activities such as setting up users, removing users, and changing passwords, on both units.

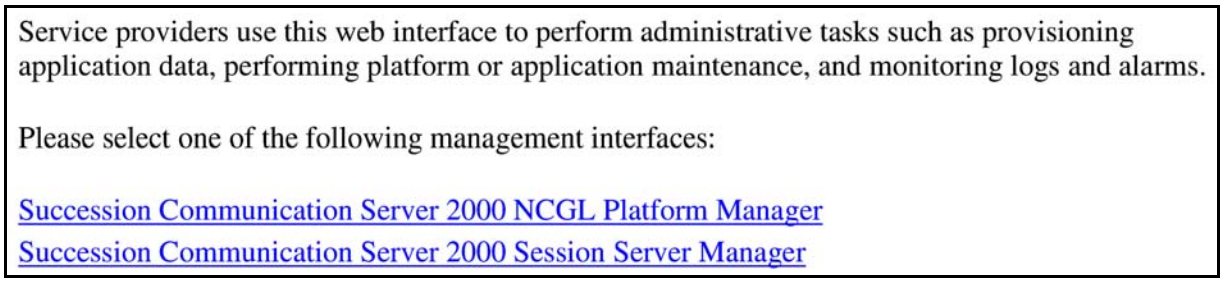
Prerequisites

There are no prerequisites for this procedure.

Action

At the Policy Controller Launch Point

1 Select either the **CS 2000 Server NCGL Platform Manager** from the launch point menu.

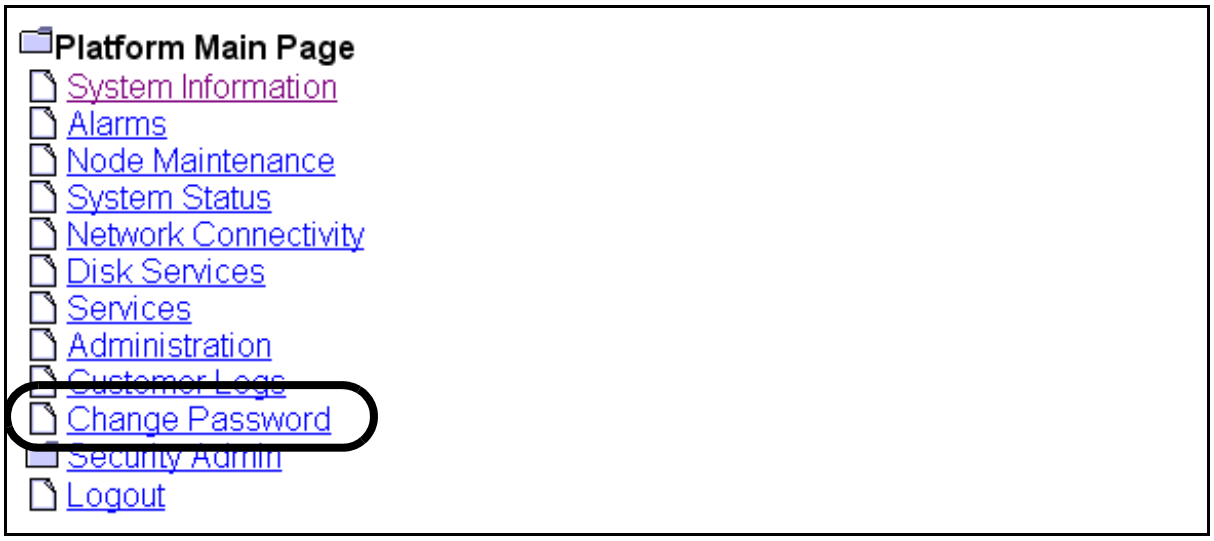

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Change Password** link.

The Change Password page is displayed.



3 Refer to the following sub-steps:

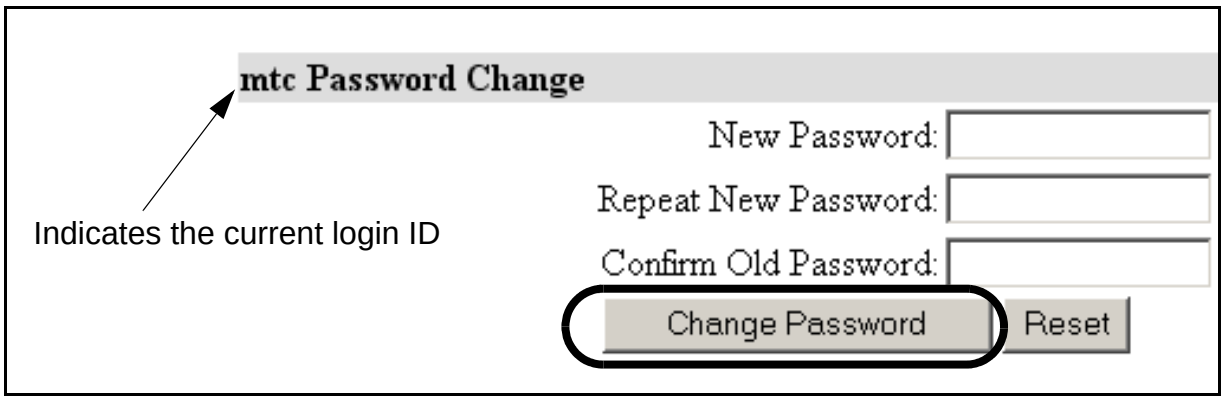
a Type the new password.

Note: For security reasons, do not set a password with an empty value. Use a minimum of six characters. Do not set the password to be the same as the user id.

b Retype the new password for verification.

c Type the old password.

d Click the **Change Password** button.



4 Repeat this procedure on the mate Policy Controller unit.

ATTENTION

User accounts and passwords are not automatically propagated to the standby Policy Controller. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

5 You have completed this procedure.

Setting up a connection to the Topology Manager using ssh

Purpose of this procedure

This procedure is used to enable users to access the Topology Manager using ssh. The OSS only has access to the OAM&P LAN, but the Policy Controller resides in the CallP LAN. In order to have a secure (encrypted) channel of communication between the OSS and the Policy Controller, SSH port forwarding must be done through Integrated EMS.

Limitations and restrictions

This procedure has the following limitations:

- The port forwarding should only be configured on either the Integrated EMS server or the Policy Controller, not both.
- The SSH port forward must be reconfigured in the event of an Integrated EMS or Policy Controller server reboot.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At a Policy Controller command line interface

1 Determine if you will set up the port forward on the Integrated EMS server or Policy Controller server.

If you will be using the	Do
Integrated EMS server	step 2
Policy Controller server	step 8

2 Open a secure shell with root privilege to the Integrated EMS server by typing

`>ssh -l root <EMS_IP_address>`

and pressing the Enter key.

where

EMS_IP_address
is the IP address or host name of the Integrated EMS server

Example
ssh -l root 46.128.66.43

3 When prompted, enter the root password and press the Enter key.

4 Set up port forward by typing

#ssh -NF -L <ems_local_port>:<pc_host>:<pctm_port> username@spc-host

and pressing the Enter key.

where

ems_local_port
is the IP address or host name of the Integrated EMS server

pc_host
is the IP address or host name of the Policy Controller

pctm_port
is the port to which the Topology Manager is configured to listen (typically 18023)

5 The first time this command is run on IEMS/SSPFS in an attempt to forward data to spc-host, the user will be prompted with information as shown here:

```
The authenticity of host spc-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 with the user whether the host spc-host is a trusted host and whether the user wants to continue connecting to it. The user should enter "yes".

6 Next the user will be prompted for a password for the user. Once the entered password is verified, a successful port forwarding session is established. This means that all new sessions by the user connecting to localhost:local-port on the Integrated EMS server will be forwarded to pc-host:pctm-port in a secure channel.

7 Go to step 14.

8 Open a secure shell to the Policy Controller by typing

>ssh -l <userid> <PC_IP_address>

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

PC_IP_address
is the IP address or host name of the Policy Controller

Example
ssh -l mtc 45.128.12

9 When prompted, enter your password.

10 If applicable, change to the root user by typing

```
$su -root
```

and pressing the Enter key.

11 When prompted, enter the password.

12 Set up the port forward by typing

```
#ssh -Nf -R
<pctm_port>:<ems_host>:<ems_local_port>
username@iems-host
```

where

pctm_port
is the port to which the Topology Manager is configured to listen (typically 18023)

ems_host
is the IP address or host name of the Integrated EMS server

ems_local_port
is any valid port number; however, higher numbers like 2000 and above are preferred

13 Open a secure shell with root privilege to the Integrated EMS server by typing

```
>ssh -l root <EMS_IP_address>
```

and pressing the Enter key.

where

EMS_IP_address
is the IP address or host name of the Integrated EMS server

Example
ssh -l root 46.128.66.23

14 Create a shell script named *auto_pc_login* by typing

```
#!/bin/sh
telnet localhost1 <EMS_IP_address>
```

and pressing the Enter key.

where

EMS_IP_address
is the IP address or host name of the Integrated EMS server

15 Add a new user in Integrated EMS, specifying the default login shell as *auto_pc_login*.

Refer to *Integrated EMS Security and Administration*, NN10336-611.

16 The procedure is complete.

Invoke a manual switch of active links (Swlink)

Purpose of this procedure

This procedure provides a service-impacting recovery routine. It forces a switch of link activity on the Policy Controller units regardless of call activity on the active unit.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a determining if a network ethernet link is faulty.

Links on either the active or standby Policy Controller units can be switched.

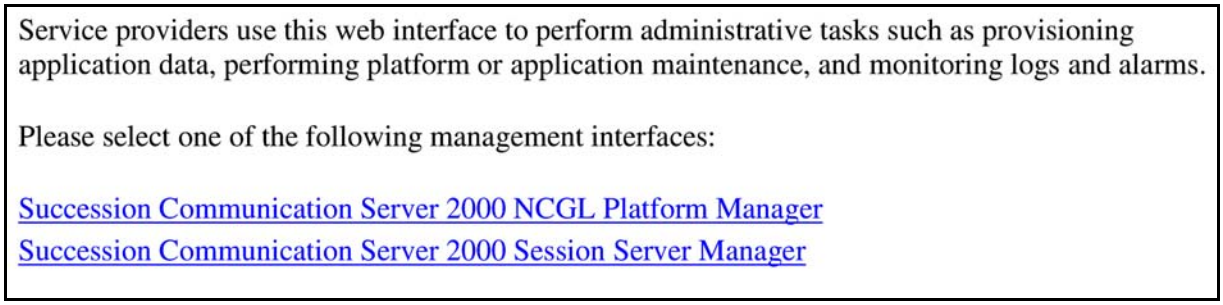
Prerequisites

There are no prerequisites to using this procedure.

Action

At the Policy Controller Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

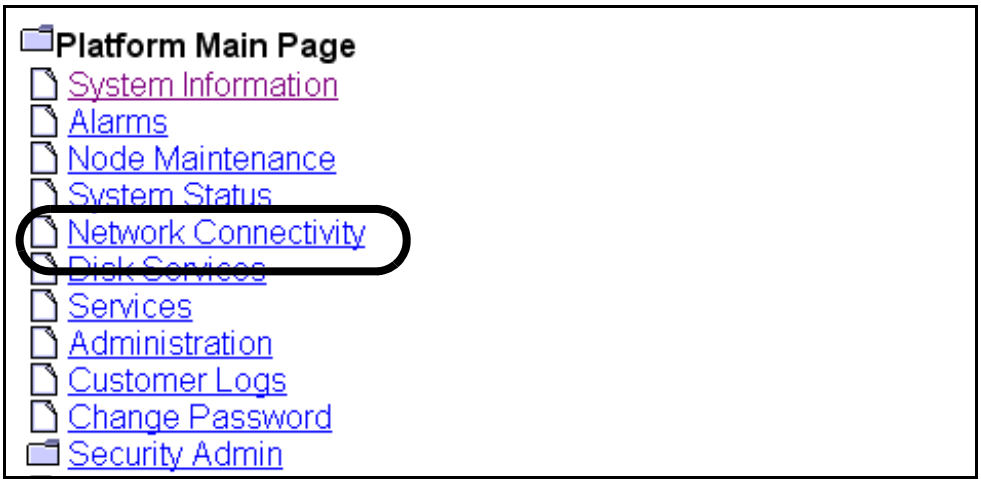

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

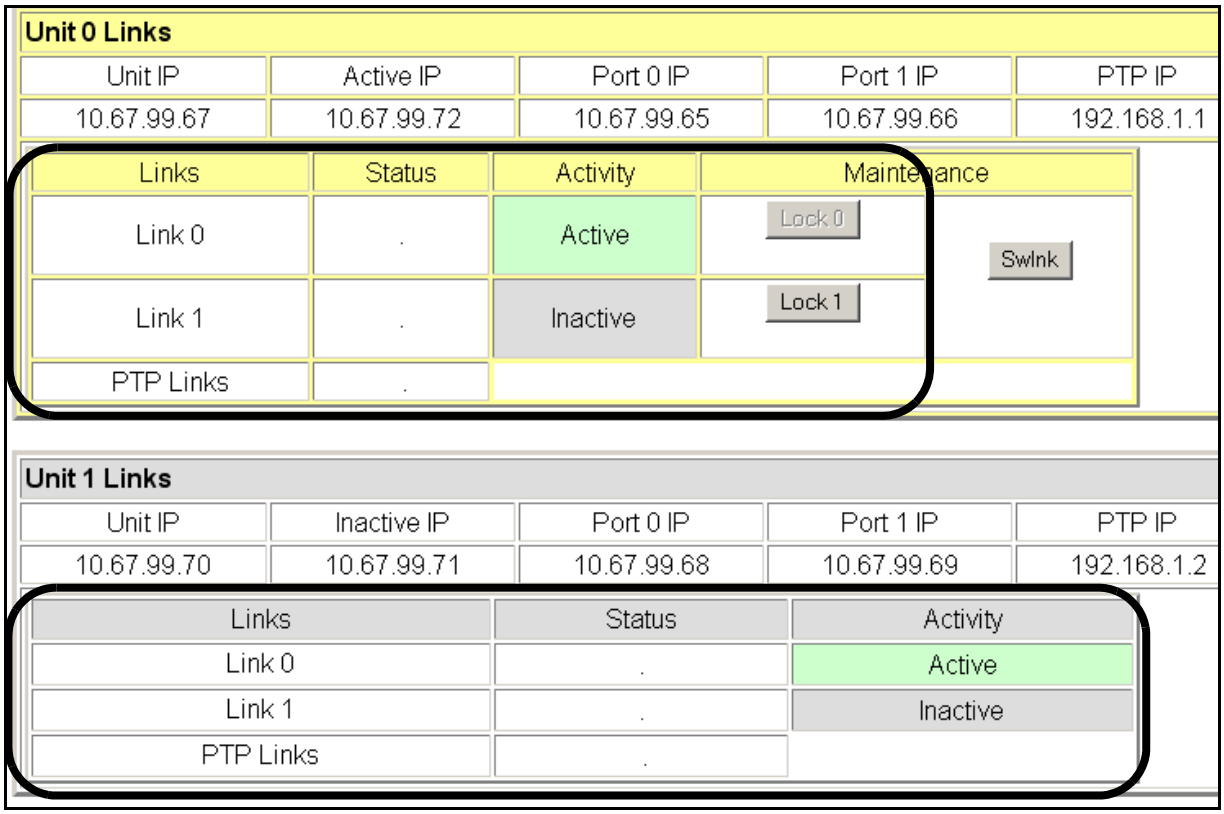
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Network Connectivity** link.

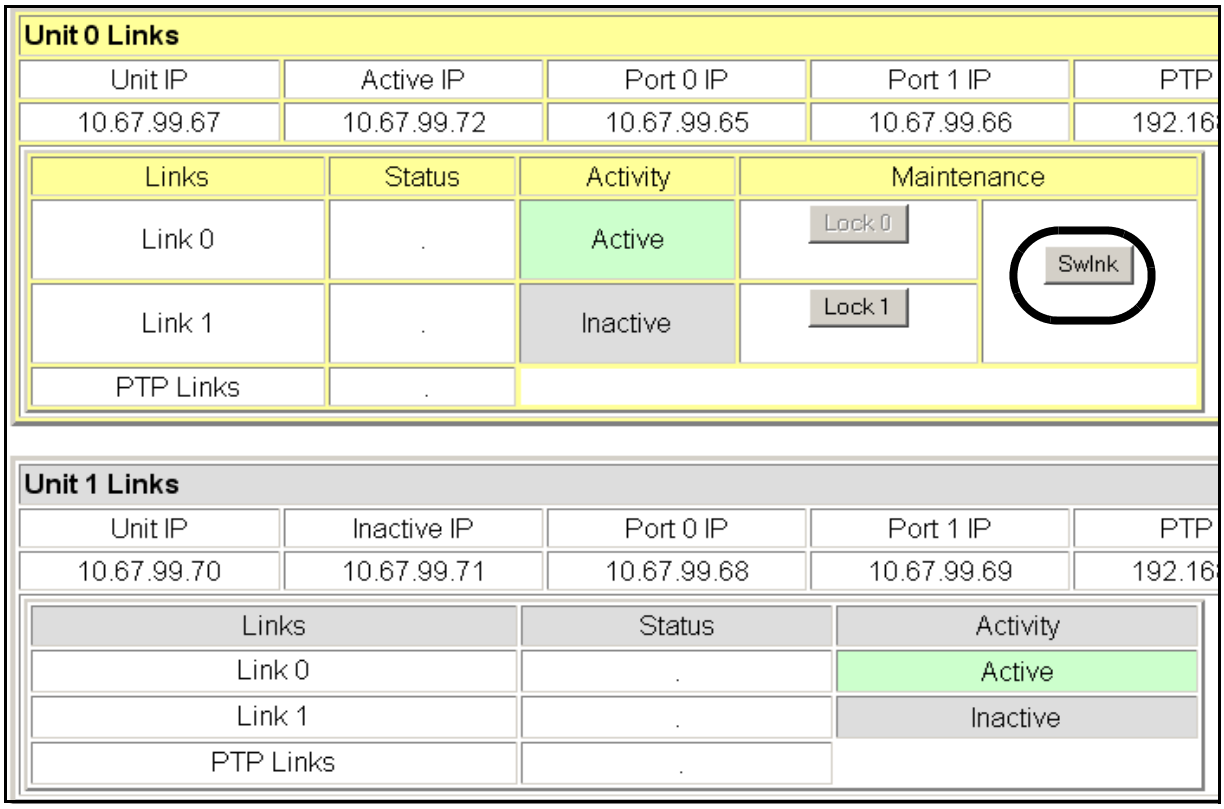
The Network Connectivity page is displayed.



3 Review the link state of both Policy Controller units.



4 Click the **Swlink** button for the active link on the active unit.

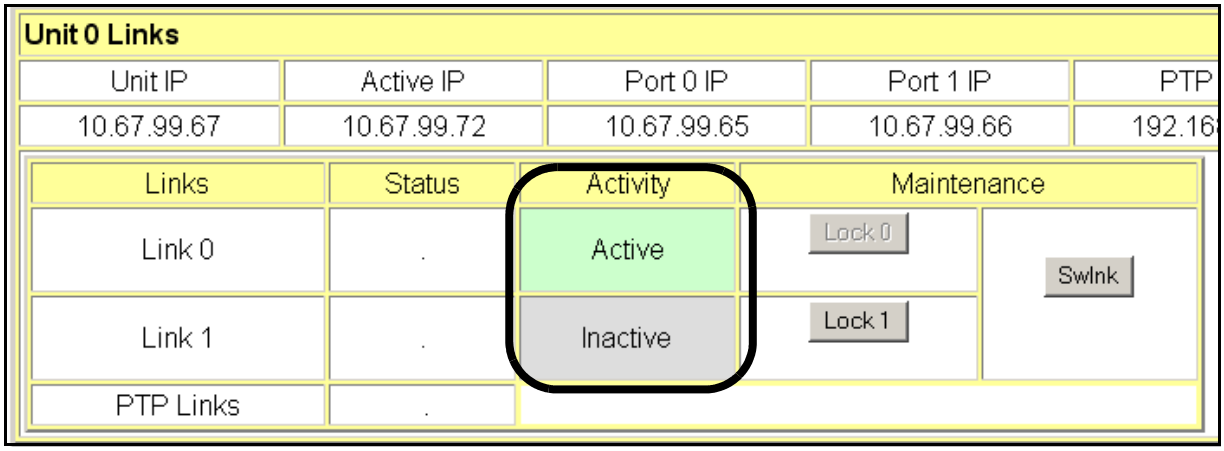


The system responds:

```
Are you sure you wish to switch link activity?
Click OK to confirm or cancel to abort.
```

5 Click **OK** to confirm the switch link activity.

6 Ensure that the state of the links swaps.



7 This procedure is complete.

Lock network ethernet link

Purpose of this procedure

This procedure is used to lock (shut down) the inactive ethernet link on a Policy Controller unit, preventing a switch of link activity (Swlnk) to the inactive link. These links allow the Policy Controller to communicate with other components in the network.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities.

CAUTION

This procedure prevents the Policy Controller node from operating in a fully fault-tolerant mode.

Prerequisites

There are no prerequisites to using this procedure.

Action

At the Policy Controller Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

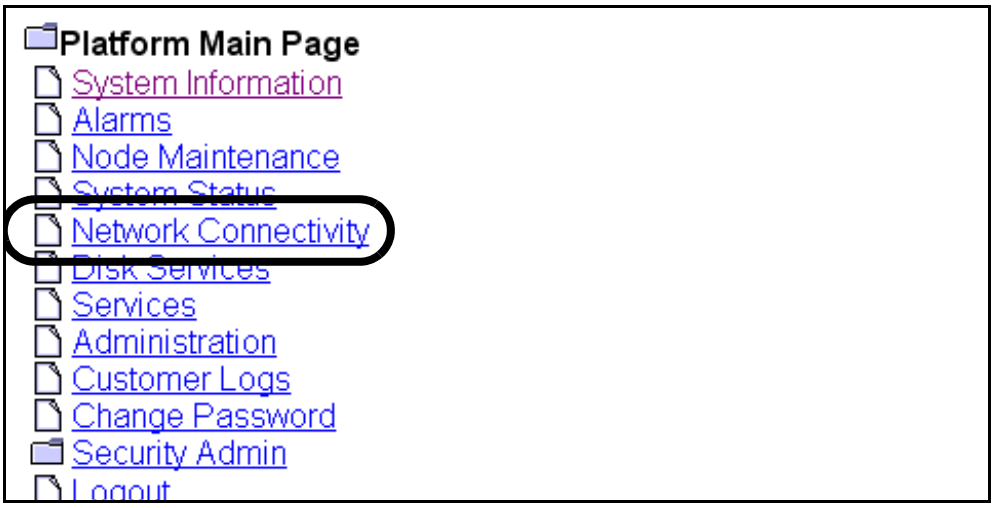
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

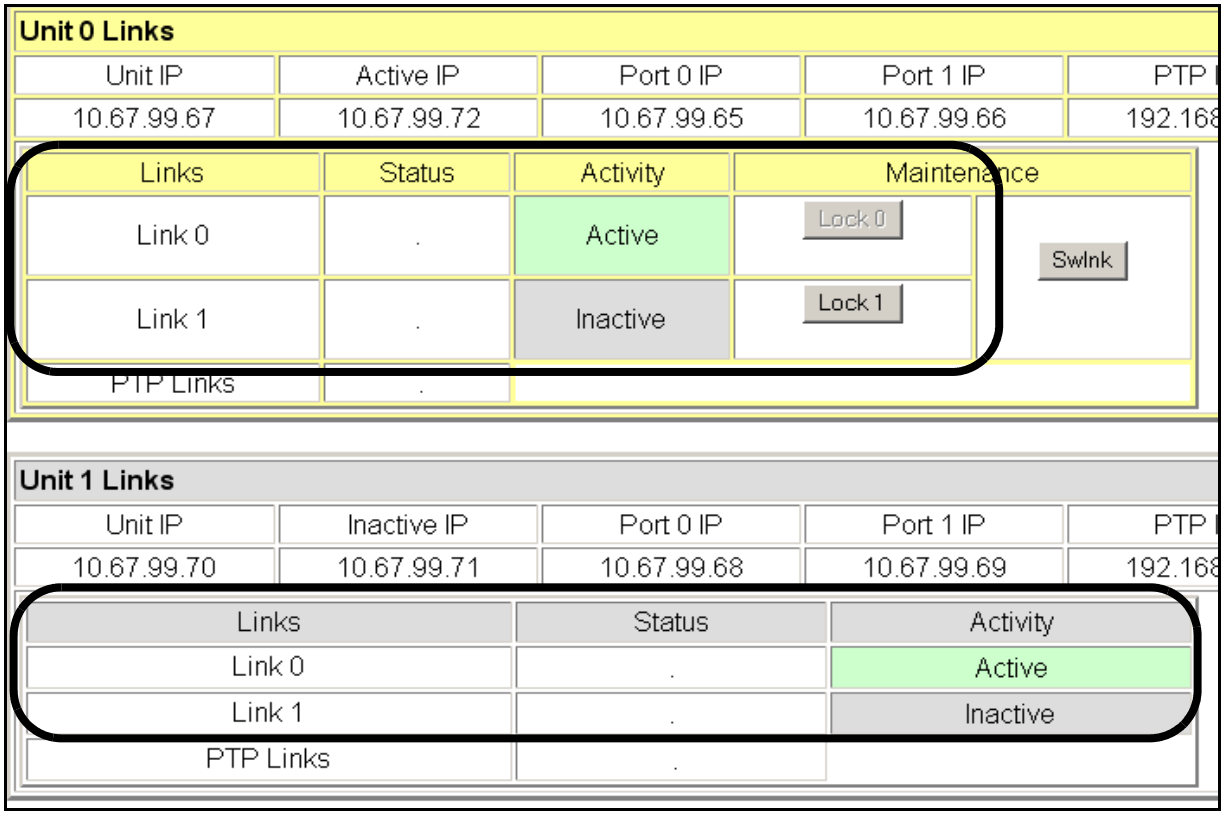
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Network Connectivity** link.

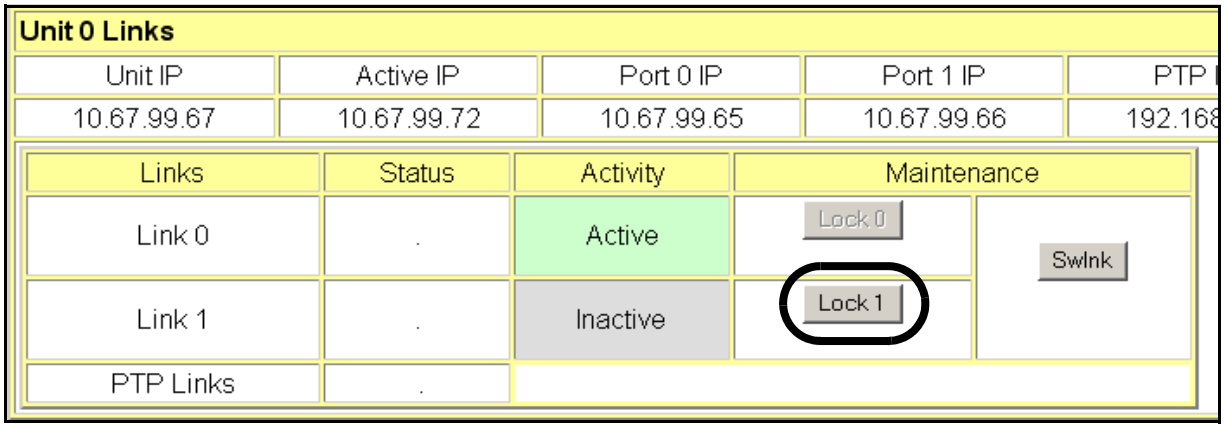
The Network Connectivity page is displayed.



3 Review the link state of the Policy Controller units.



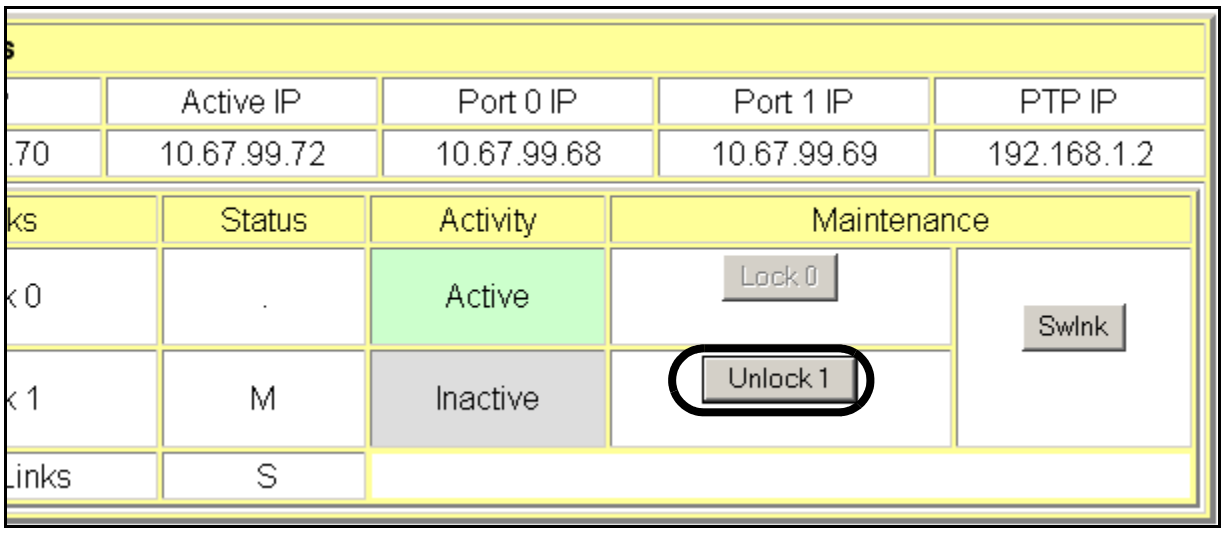
4 Click the **Lock** button for the inactive link on the active unit.



The system responds:

```
Info: Lock Link X - Command passed.
```

5 Ensure that the **Lock** button for the inactive link transitions to **Unlock**.



6 This procedure is complete.

Unlock network ethernet link

Purpose of this procedure

This procedure is used to unlock (start) a Policy Controller unit's inactive (locked) ethernet link.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities.

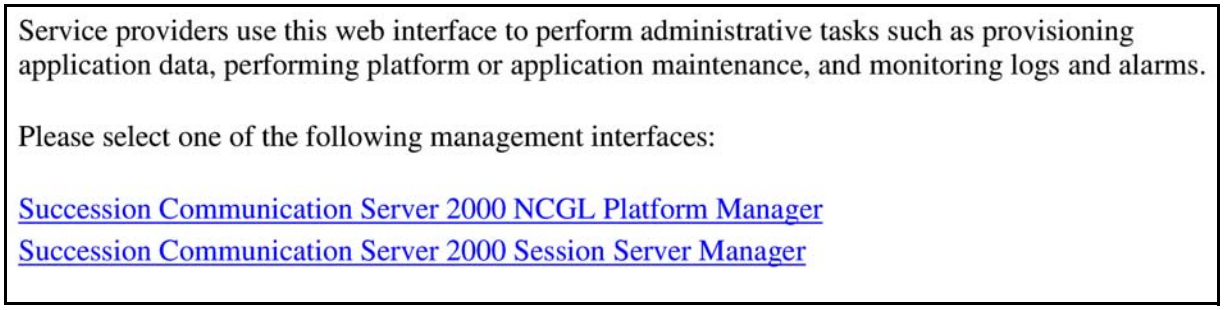
Prerequisites

The unit's inactive ethernet link must already be in a locked state.

Action

At the Policy Controller Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

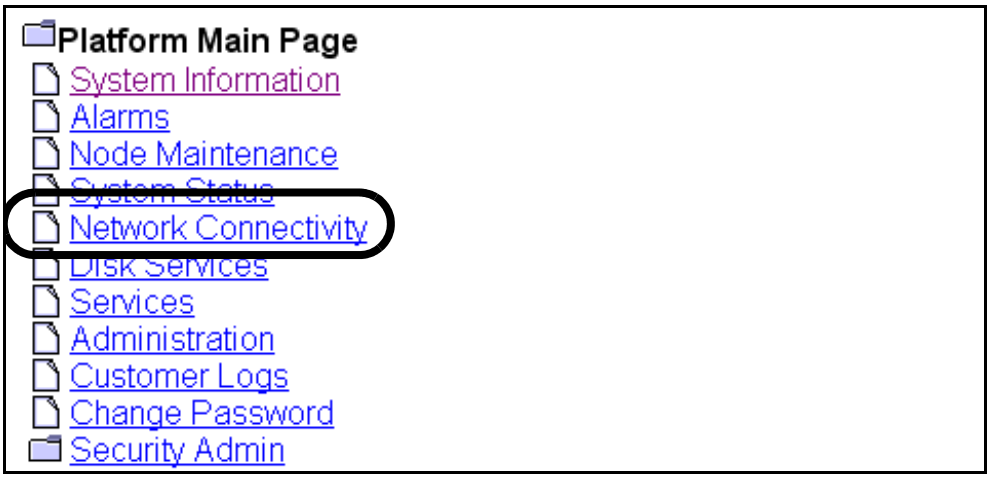

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

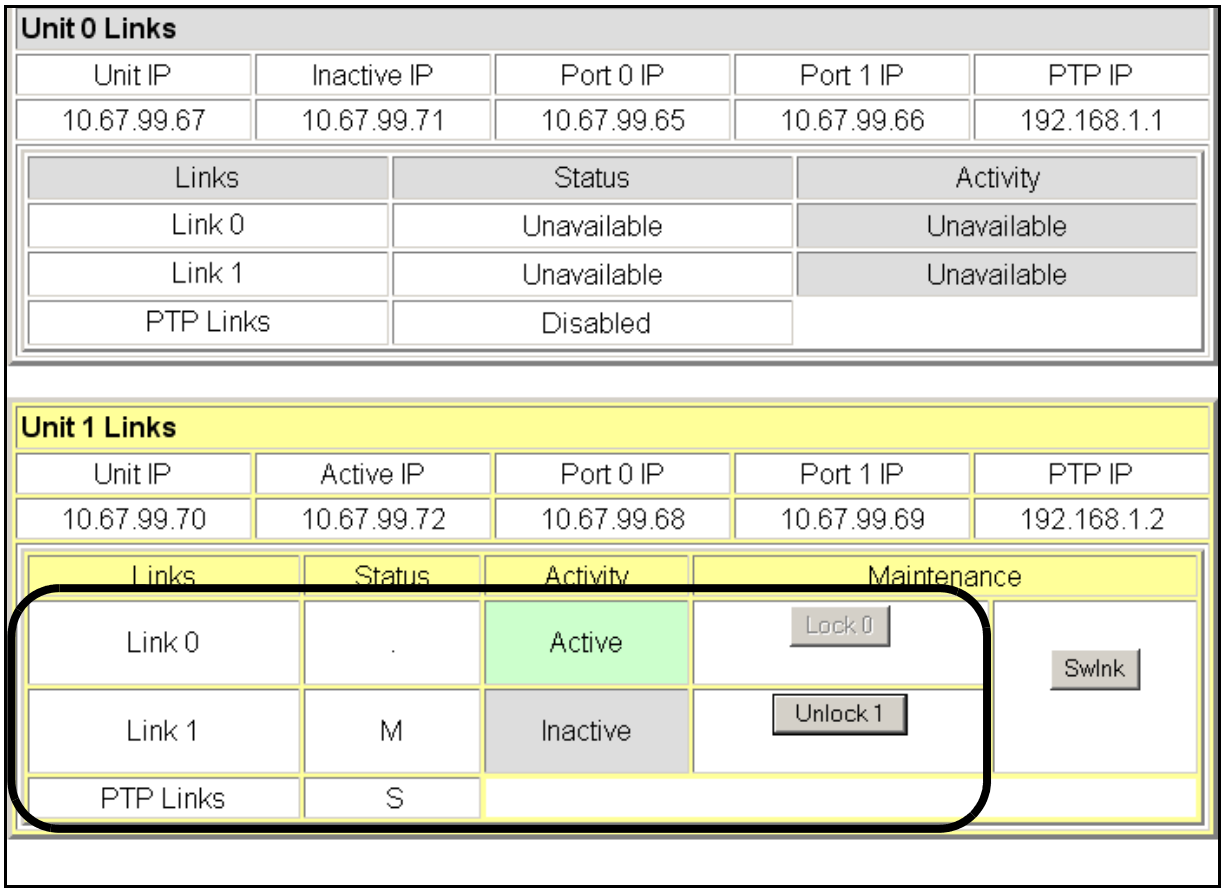
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Network Connectivity** link.

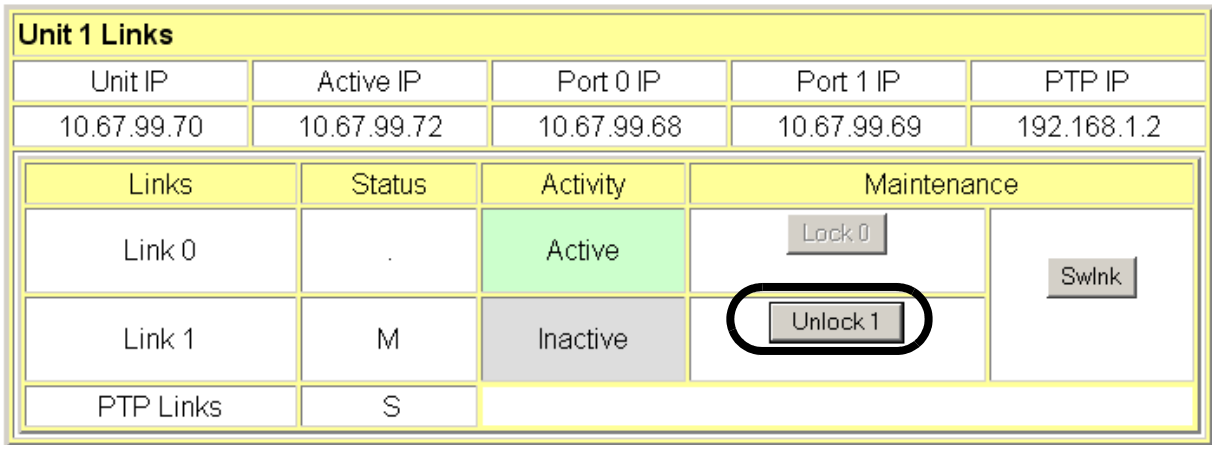
The Network Connectivity page is displayed.



3 Review the link state of the active Policy Controller unit.



4 Click the **Unlock** button for the inactive link on the active unit.



The system responds:

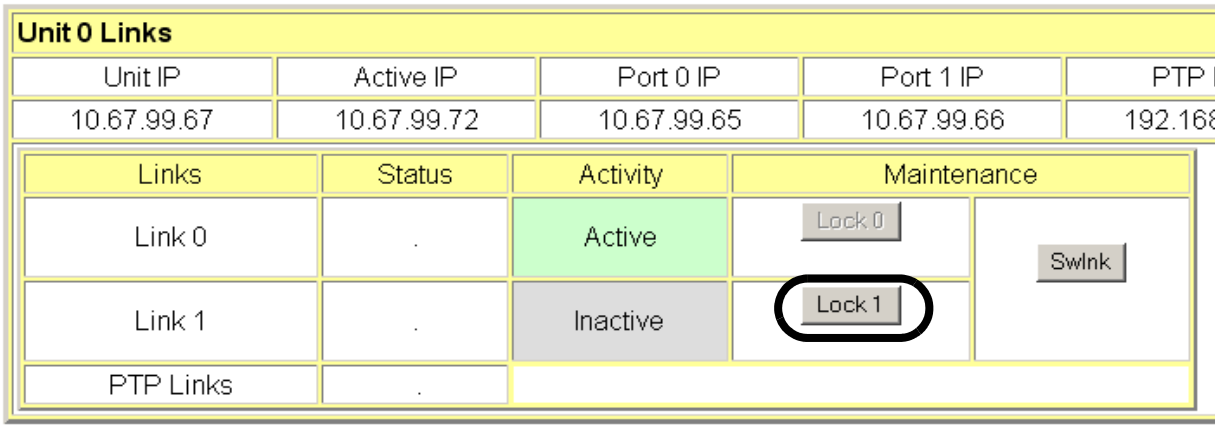
```
Are you sure you wish to Lock link X?
Click OK to confirm Lock or cancel to abort.
```

5 Click **OK** to confirm the unlock.

The system responds:

```
Info: Unlock Link X - Command passed.
```

6 Ensure that the **UnLock** button for the inactive link transitions to **Lock**



7 This procedure is complete.

Invoke a maintenance SwAct of the Policy Controller platform

Purpose of this procedure

This procedure manually performs a maintenance SwAct (switch of activity) of the Policy Controller platform. A SwAct gracefully transitions call processing activity from the active Policy Controller unit to the standby unit without first reloading and re-initializing the Policy Controller application on the standby unit. All call data and Bandwidth resource usage counters for the Policy Controller Application will be maintained during the SwAct.

Use this procedure as a standalone task or as part of a maintenance or fault clearing activity like replacing a faulty standby unit or a high-level activity such as upgrading a standby unit.

Note: An automatic failover SwAct can be initiated by the platform NCGL in cases of critical faults on the active unit. For more information about conditions required for a SwAct, refer to section Understanding conditions for a SWACT on page 16.

Limits and Restrictions

ATTENTION
A maintenance SwAct should only be performed when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot SwAct Policy Controller units if the active unit Jam state is *jammed*. If the unit Jam state is jammed, refer to procedure Enable a system SwAct (Unjam) on page 30 to unjam the unit.

ATTENTION
Logins to the Policy Controller do not survive a platform SwAct.

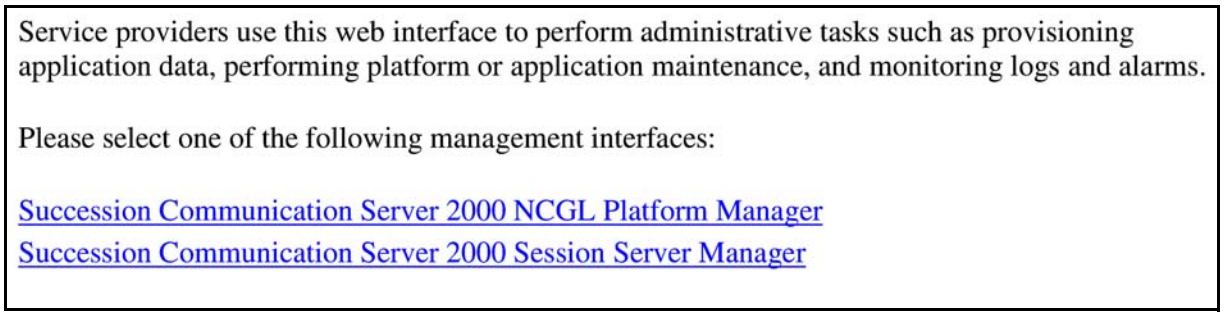
Prerequisites

If you are executing a Forced SwAct, confirm that there are no alarm conditions.

Action

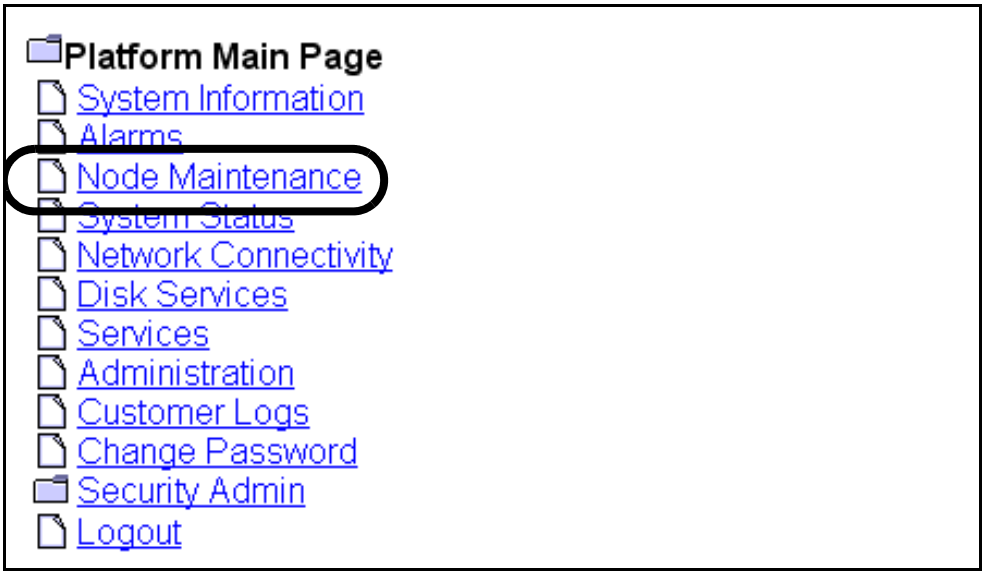
At the Policy Controller Launch Point

1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

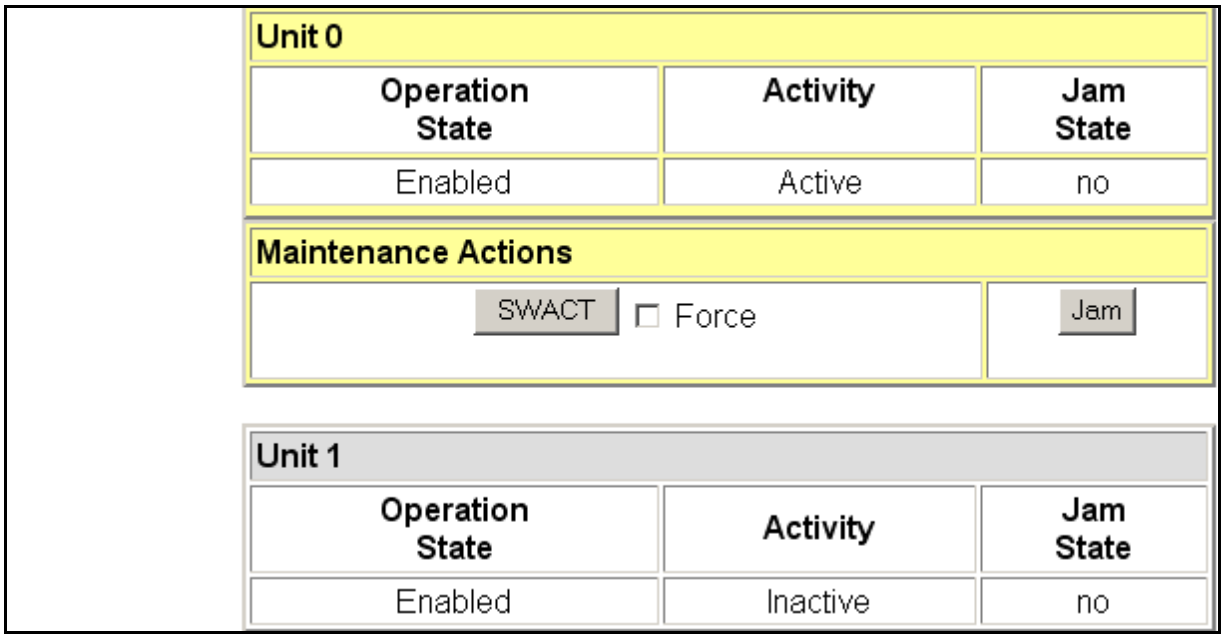


2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Refer to the table in section Additional status information on page 20 to review the description of the various fields of the Node Maintenance page.



Unit 0

Operation State	Activity	Jam State
Enabled	Active	no

Maintenance Actions

SWACT ☐ Force Jam

Unit 1

Operation State	Activity	Jam State
Enabled	Inactive	no

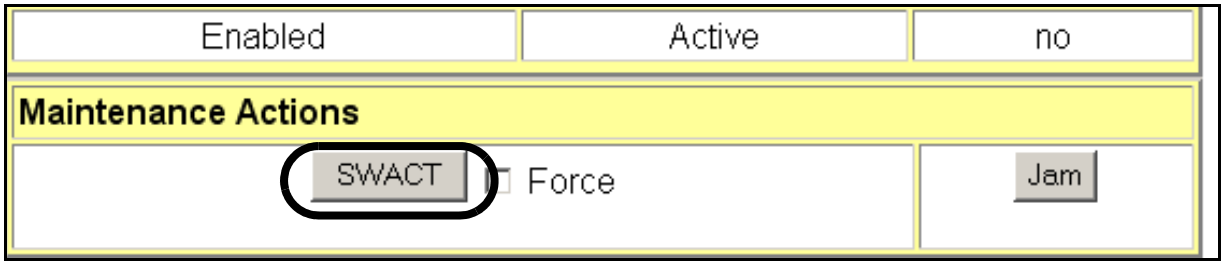
4 To SwAct the Policy Controller units, click the **SWACT** button.

or

To override any pre-SwAct queries, first click the **Force** check box, then click the **SWACT** button. Refer to section To SWACT or Force a SWACT? on page 21 for details regarding which type of SWACT to chose.

CAUTION

Due to the risk for loss of data and service outage, it is recommended that the Forced SWACT option not be used except when instructed by your Nortel customer support representative.



The system responds:

```
Are you sure you wish to swact? This may cause
a service interruption to applications running
on this server. Click OK to confirm server swact
or cancel to abort.
```

5 Click **Yes** to confirm either the SwAct or forced SwAct.

6 Observe the *Activity* field for each unit. Each unit's activity status (whether Active or Inactive) swaps.

7 The procedure is complete.

Additional status information

The following table describes the various fields of the Node Maintenance panel.

Field	Description
Operation State (unit 0 or 1)	The operational state of the platform software, either enabled or disabled.
Activity (unit 0 or 1)	The activity state of the platform software, either active or inactive.
Jam State (active unit only)	Indicates whether or not the unit has been "jammed", preventing the standby unit from being able to become active, regardless of any failures on the active unit. States are either jammed, where a SwAct is disabled, or unjammed, where a SwAct is enabled.
Maintenance Actions (active unit only)	Maintenance panel for performing node SWACT activity and to jam or unjam node activity switches.

To SWACT or Force a SWACT?

A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT pre-checks monitor the inactive unit for critical faults on the platform that should prevent a SWACT. In addition, the pre-check ensures that the Policy Controller application is in-sync. A SWACT force may result in a full service outage on the Policy Controller node if the inactive unit is not in-sync. There is potential for loss of provisioned data if a SWACT to an unstable unit is completed.

Invoke a manual cold SwAct of the Policy Controller application

Purpose of this procedure

This procedure performs a manual switch of activity (SwAct) from the active to the standby Policy Controller unit. It also forces a reload and re-initialization of the Policy Controller application on the standby unit before switching callP activity from the active unit to the standby unit. During this re-initialization all call data will be reset, and also Bandwidth resource usage counters will be reset to zero, for the Policy Controller Application.

This procedure is used for fault clearing activities, and when a problem has been detected with Policy Controller call processing as determined by the alarm panel.

Limits and Restrictions

ATTENTION

Do not use this procedure to request a platform SwAct. Only proceed with this procedure if a platform SwAct has already occurred, and a problem has been detected with Policy Controller call processing.

ATTENTION

You cannot cold SwAct the Policy Controller application if the inactive (standby) Policy Controller unit is out of service. A SIP cold SwAct can only be performed when both the active and standby Policy Controller platform units are operationally enabled.

You cannot cold SwAct the Policy Controller application if the active unit's communications mode is in a jammed state. If the active unit is jammed, refer to procedure Enable a system SwAct (Unjam) on page 30 to unjam the unit.

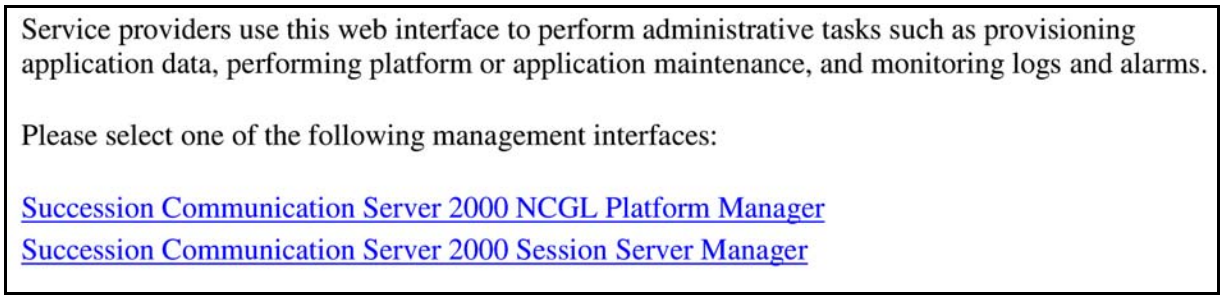
Prerequisites

There are no prerequisites for performing this procedure.

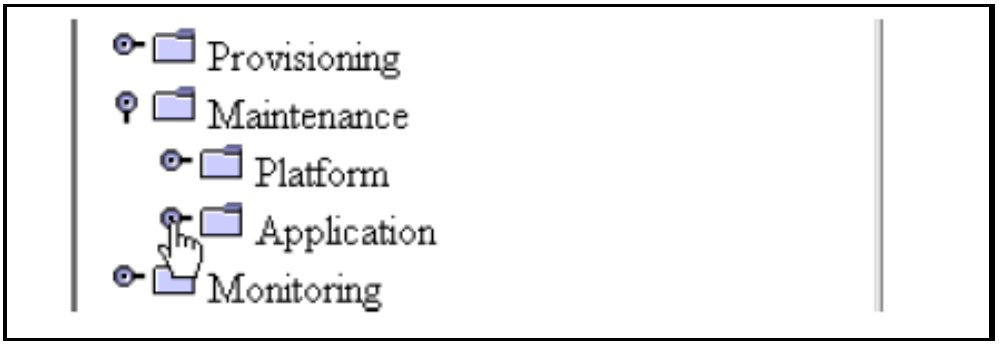
Action

At the Policy Controller Launch Point

1 Select ***Succession Communication Server 2000 Policy Controller Manager*** from the launch point menu.



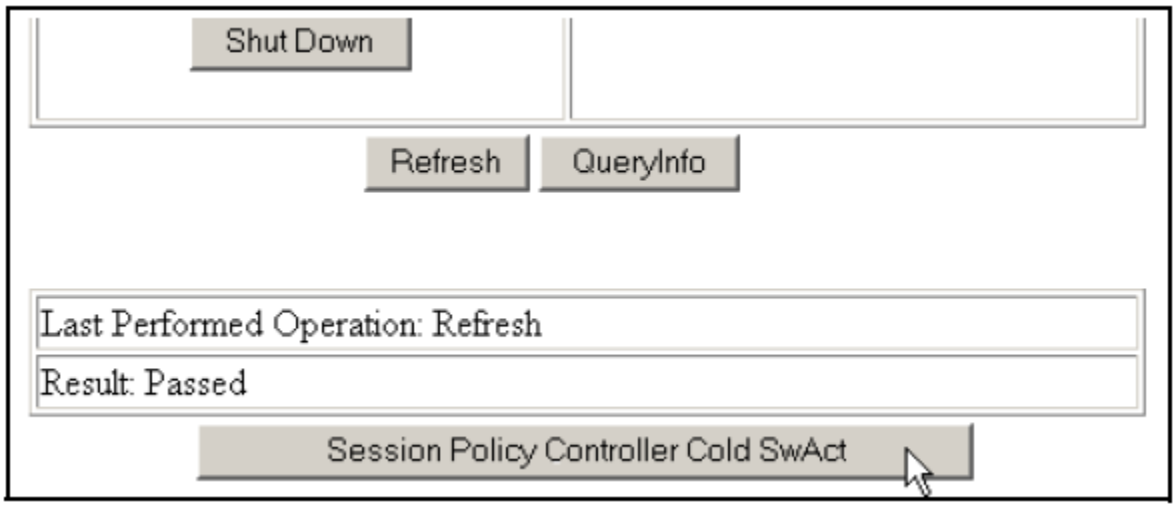
2 At the Policy Controller folder, click the **Maintenance** folder**,** then click the **Application** folder.



3 Click on the **Policy Controller** folder to open it.

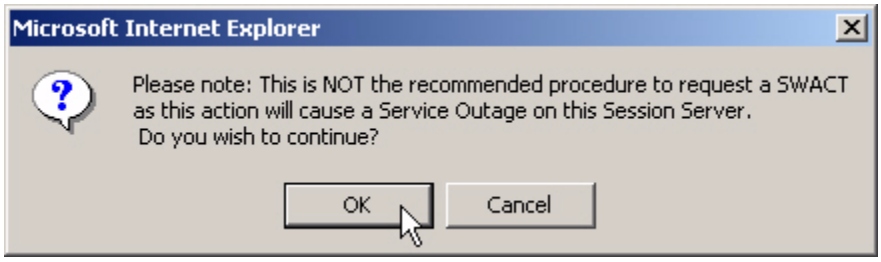
4 Determine whether both the active and standby units are operationally enabled and that the **Session Policy Controller Cold SwAct** button is not disable (shaded out).

5 To cold SwAct the Policy Controller application, click the **Session Policy Controller Cold SwAct** button.



A dialog box appears to verify if the user wants to proceed with a Policy Controller cold SwAct.

6 Confirm that you want to proceed with the Policy Controller cold SwAct by clicking on the **OK** button.



7 Observe the Message field for details about the SwAct transaction status.

If the result of the cold SwAct request is anything but Passed, refer to *Policy Controller Fault Management*, NN10438-911, to troubleshoot the failure using logs and alarms and consult your next level of support.

For more information about determining the status of the Policy Controller application, refer to procedure View the operational status of the Policy Controller application on page 42.

8 The procedure is complete.

Inhibit a system SwAct (Jam)

Purpose of this procedure

The jam command is used to manually prevent a SwAct (switch of activity) of the active and stand-by units by inhibiting the toggling of operational states of both units, thereby preventing the stand-by unit from going active.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a replacing a faulty standby unit or upgrading the software for a standby unit.

ATTENTION

This procedure can only be performed from the active unit. You cannot Jam the active unit if the inactive unit is out of service.

CAUTION

This procedure prevents the Policy Controller node from operating in a duplex, fault-tolerant mode and prevents the Policy Controller application from being able to SwAct between Policy Controller units as needed. Keep a jam in effect only as long as is necessary.

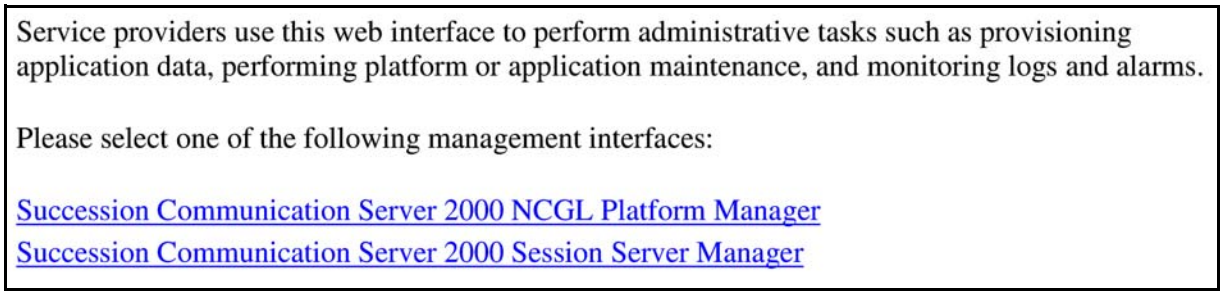
Prerequisites

There are no prerequisites for performing this procedure.

Action

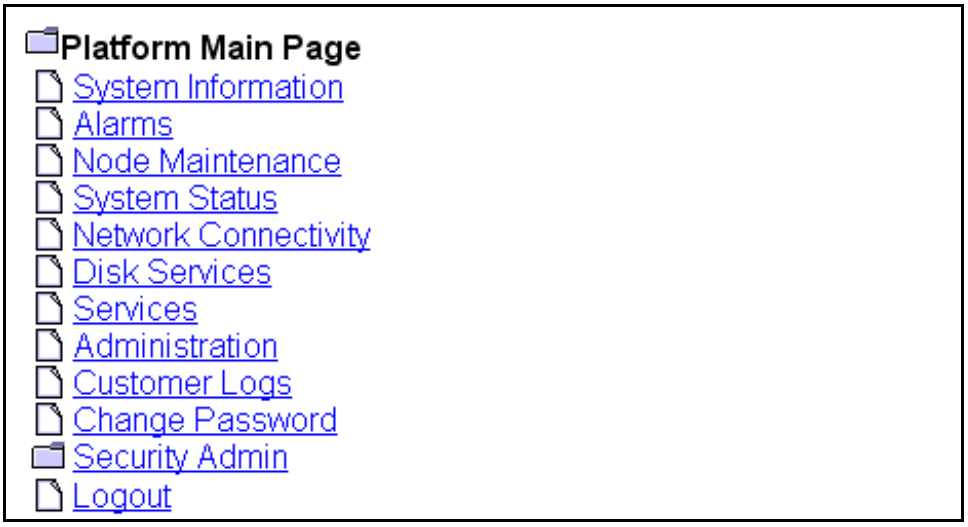
At the Policy Controller Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

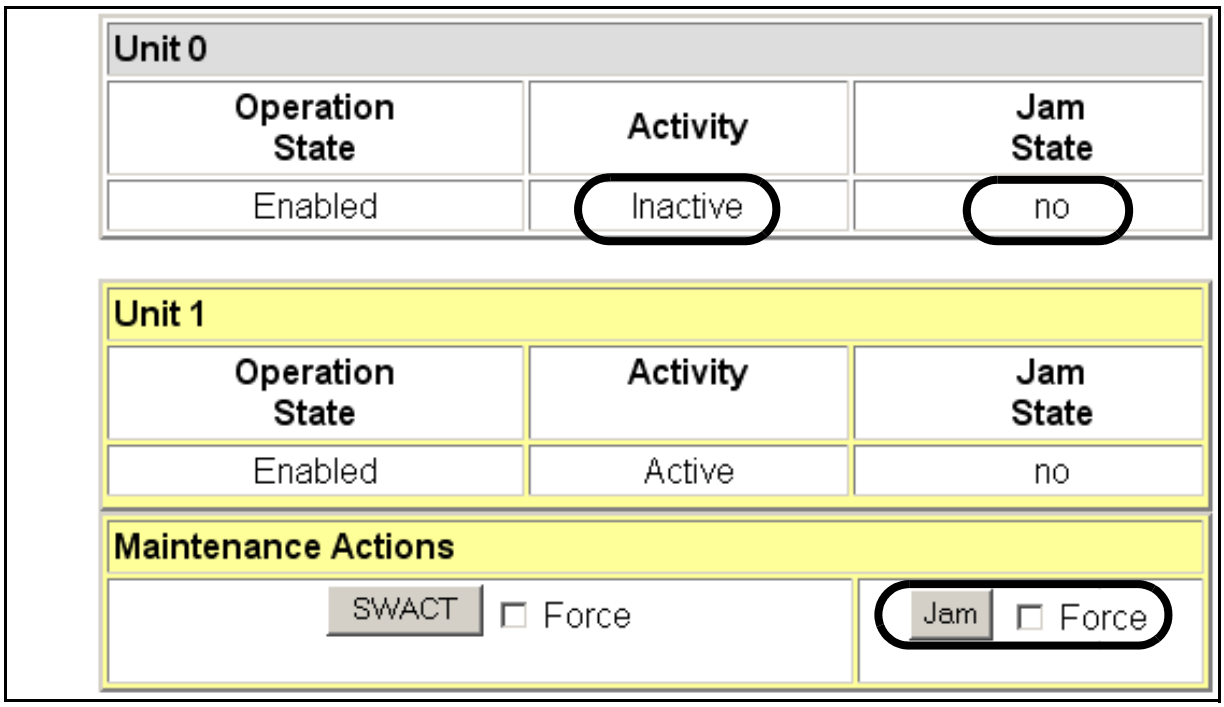


2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Determine if the Jam State of the standby unit is Yes or No. If it is Yes, then the unit is already jammed and you are done with this procedure; skip to the last step. If it is No, then continue with the next step.



Note: Refer to procedure Enable a system SwAct (Unjam) on page 30 to unjam a standby Policy Controller unit.

4 Click the **Jam** button.

or

If you want to override any pre-Jam queries, first click the **Force** check box, then click the **Jam** button.

The system responds

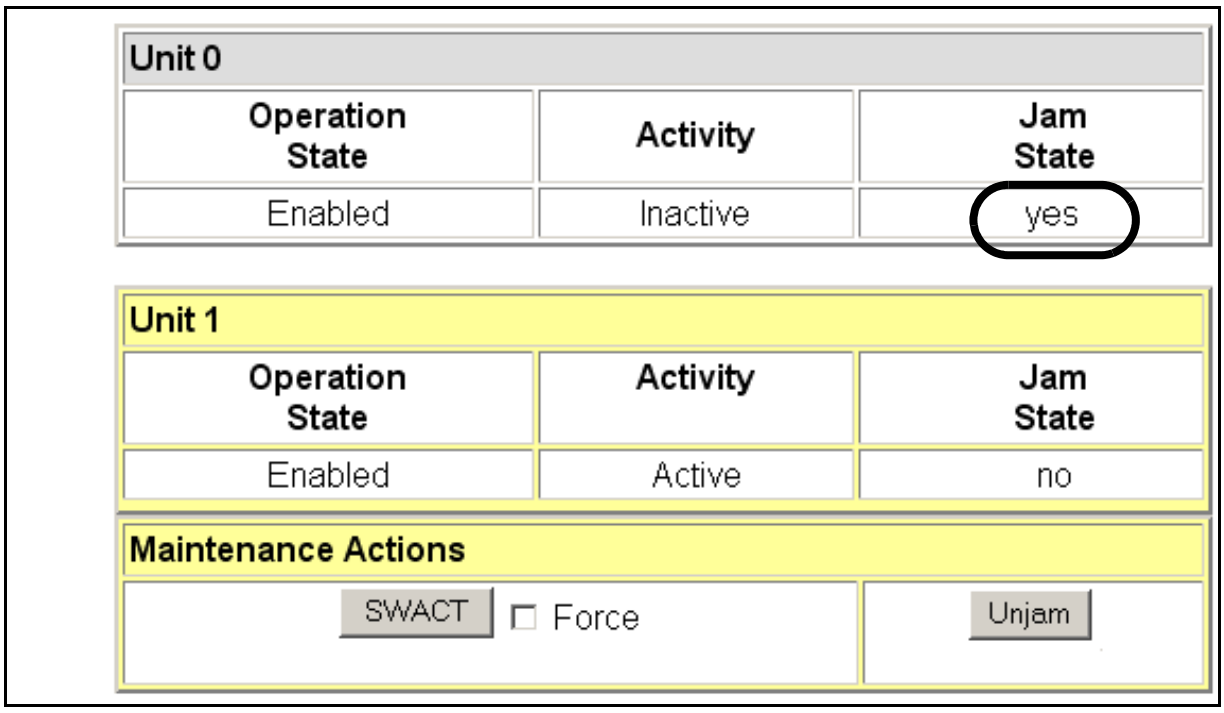
```
Are you sure you wish to perform jam action?

This will prevent the switch of activity to the
inactive node.
Click OK to confirm node jam or cancel to abort.
```

5 Click **OK** to proceed with the jam activity.

The system responds:

```
Info: Jam - Command passed.
```

6 Observe the Jam state for the standby Policy Controller unit transitions from No to Yes.



7 This procedure is complete.

To Jam or Force Jam?

The Jam action does not work if critical faults exist on the active unit. Using the Jam command with the Force option overrides any pre-checks. A Forced Jam forces a Jam of the inactive unit even if critical faults exist on the active unit, in which case, a full service outage could occur on the Policy Controller node if the active unit fails.

Enable a system SwAct (Unjam)

Purpose of this procedure

The Unjam command is used to manually enable a SwAct (switch of activity) of the active and stand-by units by allowing the two units to toggle their operational states.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as replacing a faulty standby unit or upgrading a standby unit.

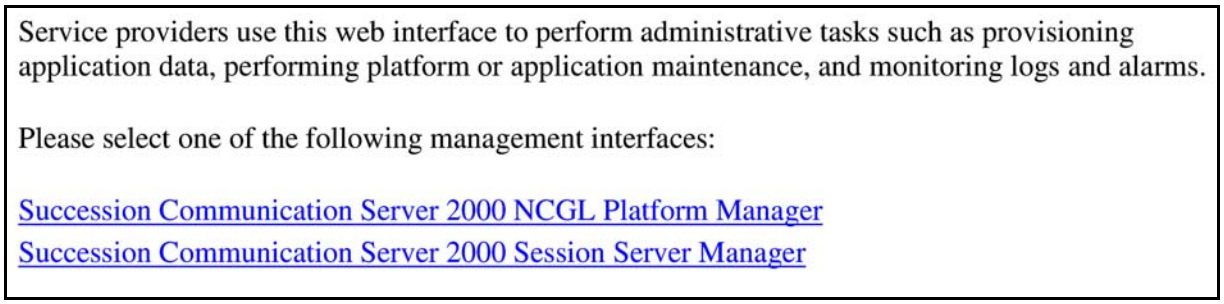
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Policy Controller Launch Point

1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

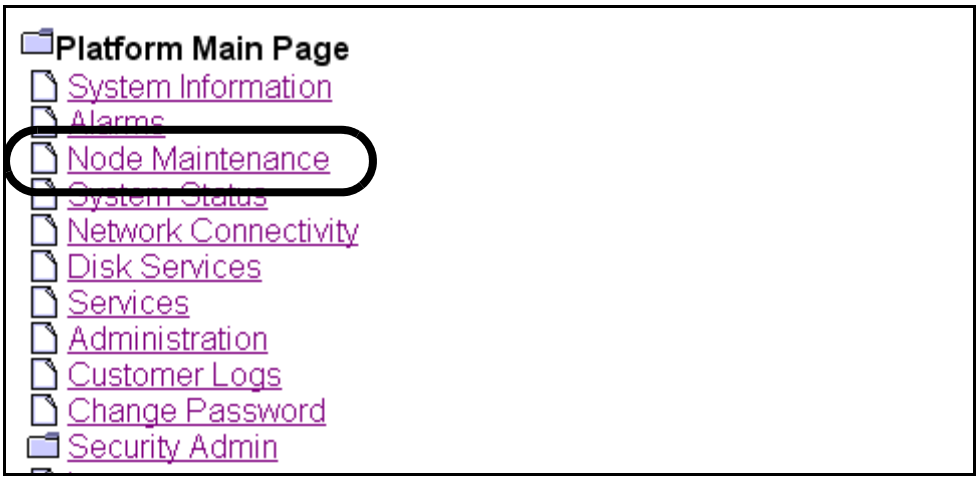

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

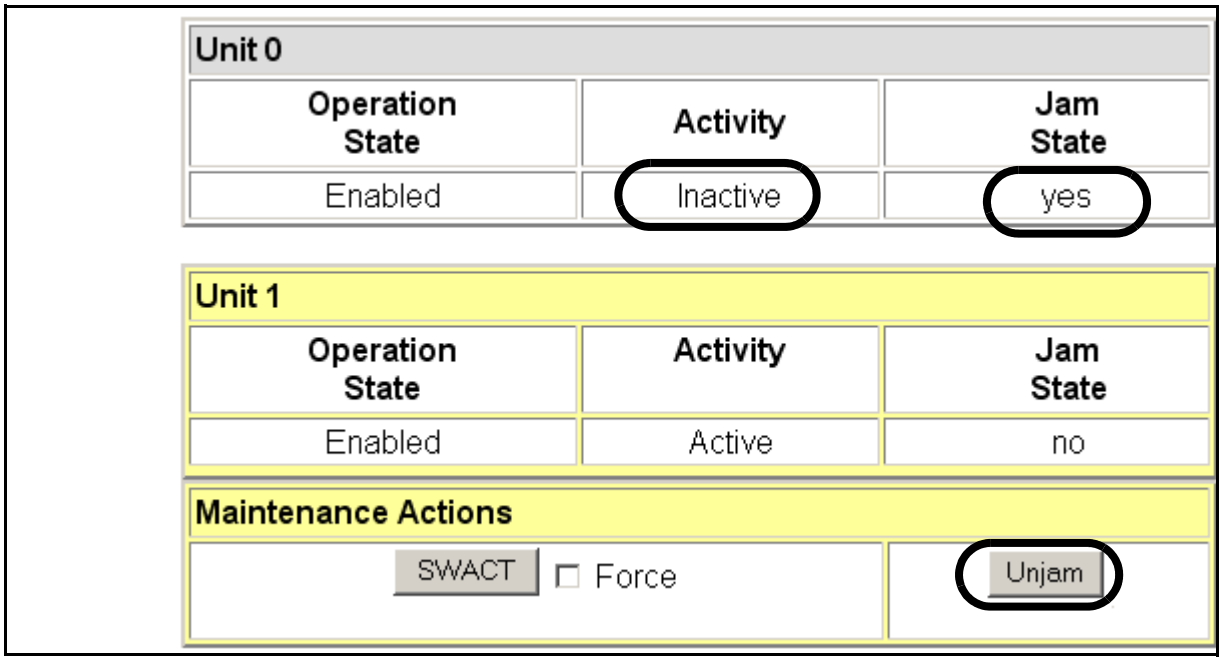
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Determine if the Jam State of the standby unit is Yes or No. If it is No, then the unit is already unjammed and you are done with this procedure. If it is Yes, then continue with step 4.

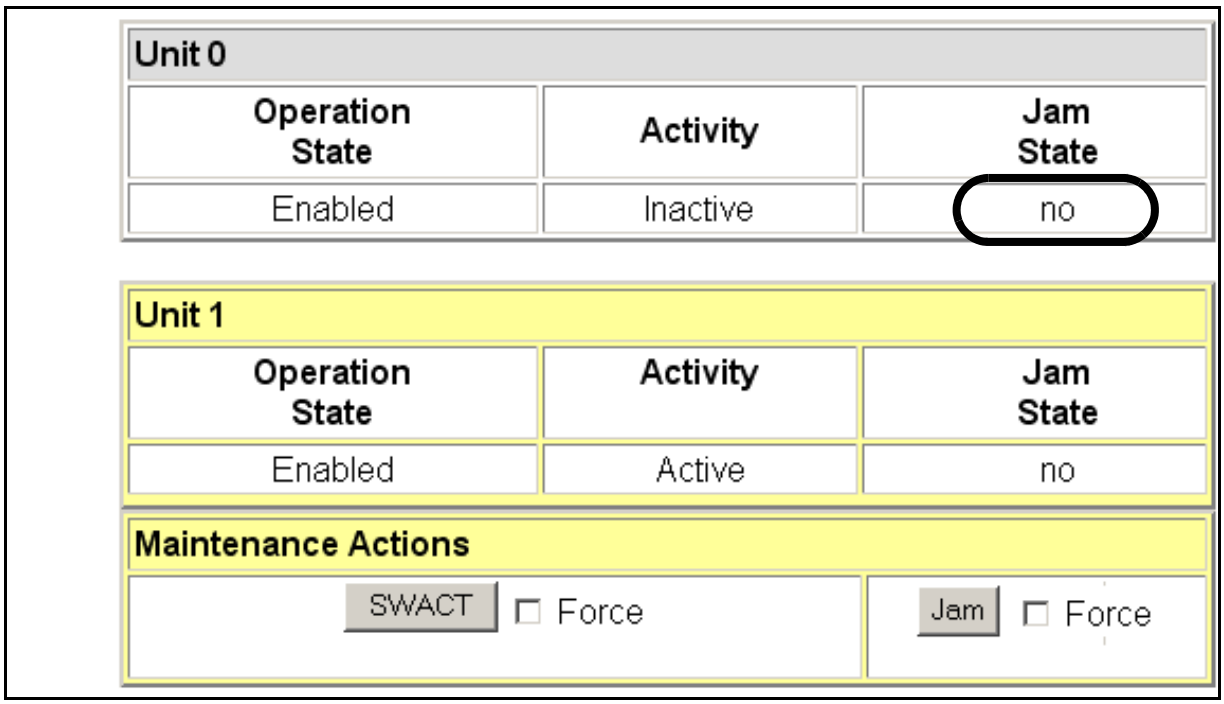


4 Click the **UnJam** button.

The system responds:

```
Info: Unjam - Command passed.
```

5 Observe the Jam state for the standby Policy Controller unit transitions from Yes to No.



6 This procedure is complete.

Lock the Policy Controller application

Purpose of this procedure

Use the following procedure to change the administrative status of the Policy Controller application to Locked. This will cause all call data to be reset, and will also automatically reset Bandwidth resource usage counters to zero, for the Policy Controller Application.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section of *Policy Controller Security and Administration* NTP, NN10434-611.

Limitations and restrictions

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure View the operational status of a Policy Controller NCGL platform on page 1.

CAUTION

This is a service affecting procedure. Locking the Policy Controller application prevents any lines configured for Virtual Call Admission Control to make or receive calls using the Policy Controller. Existing calls regardless of call state will not be released by this procedure. However, once Locked the Policy Controller Application will not be able to process any new VCAC requests.

Note: The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Locked State.

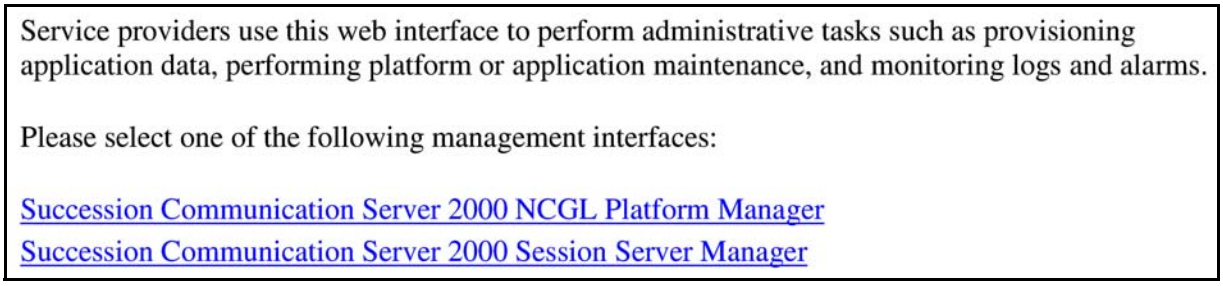
Prerequisites

There are no prerequisites for this procedure.

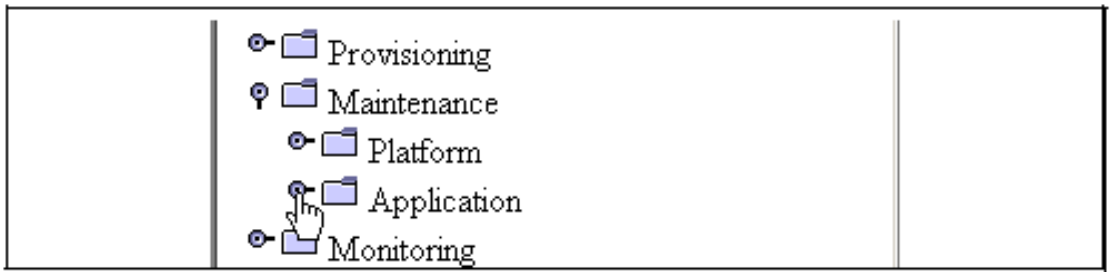
Action

At the Policy Controller Launch Point

1 Select Succession Communication Server 2000 Policy Controller Manager from the launch point menu.

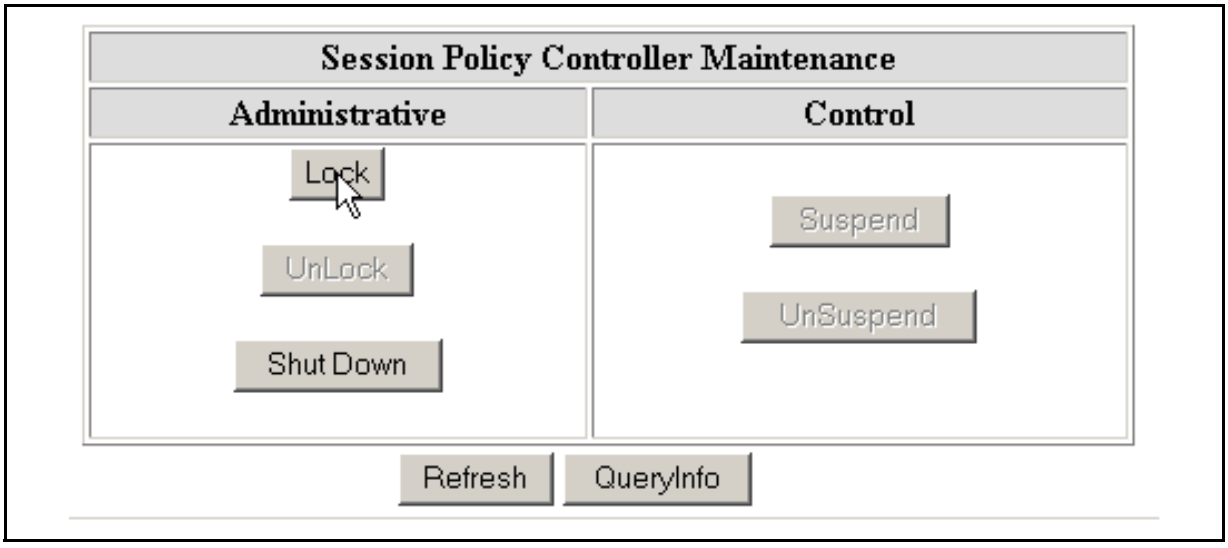


2 At the Policy Controller folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click on the **Policy Controller** folder to open it.

4 In the Policy Controller panel click the **Lock** button.



The system responds:

```
This action will block all call resource
requests to the Session Policy Controller. This
will cause a SERVICE OUTAGE on this Session
Policy Controller and subsequent call attempts
will be denied.
```

5 Click **OK** to confirm locking the Policy Controller application.

CAUTION

This is a service affecting procedure. Locking the Policy Controller application prevents any lines configured for Virtual Call Admission Control to make or receive calls using the Policy Controller. Existing calls regardless of call state will not be released by this procedure. However, once Locked the Policy Controller Application will not be able to process any new VCAC requests.

Note: The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Locked State.

6 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Administrative State changes to **Locked**

Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-

Note: The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise, manually refresh the page by clicking on the **Refresh** button.

7 The procedure is complete.

Unlock the Policy Controller application

Purpose of this procedure

Use the following procedure to change the administrative status of the Policy Controller application to Unlocked, bringing the application into service and enabling callP to begin.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section of the *Policy Controller Security and Administration*, NN10434-611.

Limitations and restrictions

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure View the operational status of a Policy Controller NCGL platform on page 1.

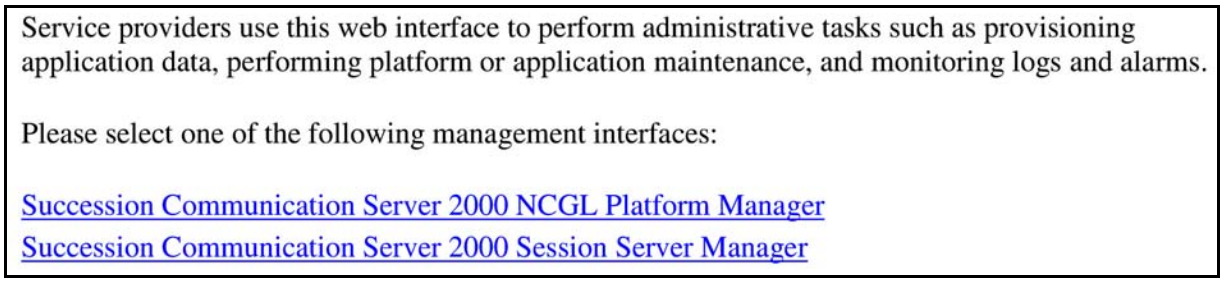
Prerequisites

The active Policy Controller unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the Policy Controller application on page 34.

Action

At the Policy Controller Launch Point

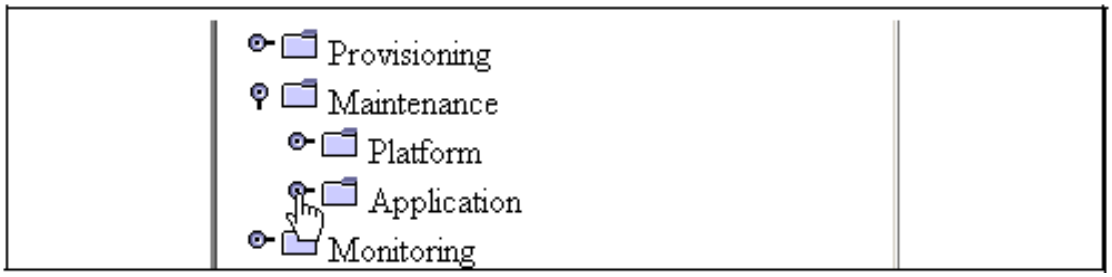
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

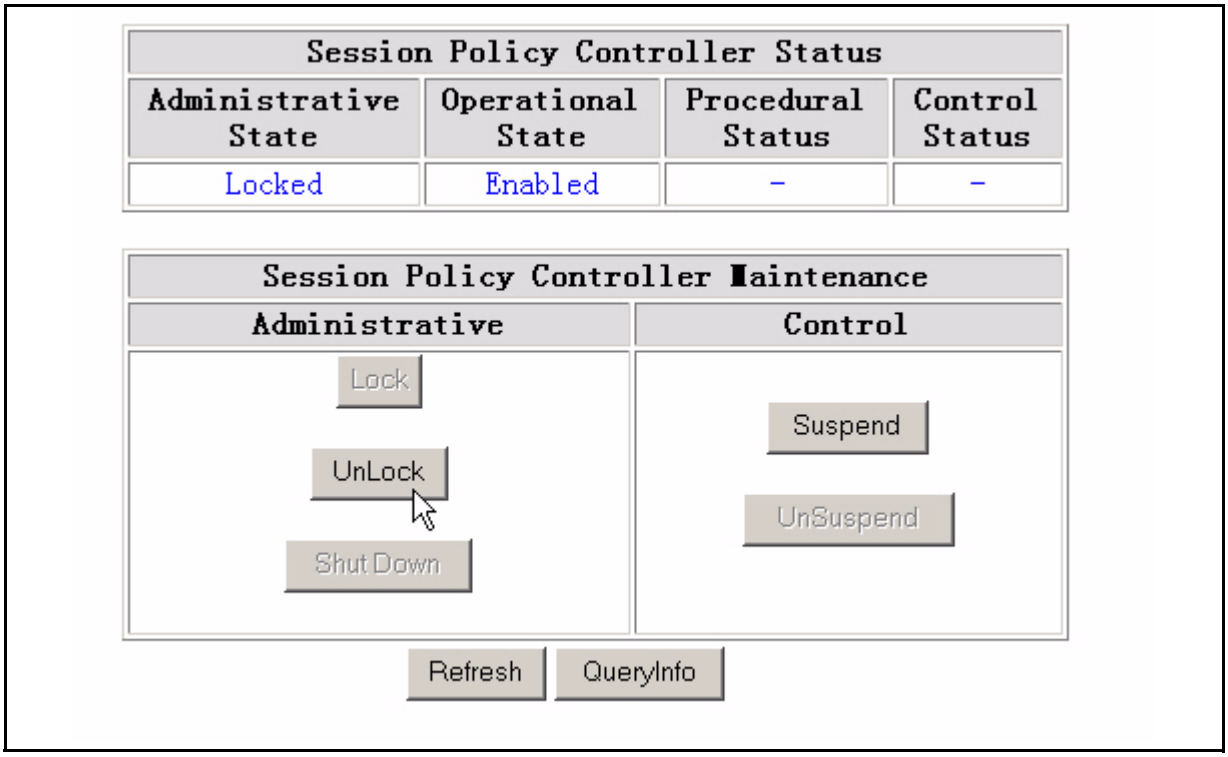
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 At the Policy Controller folder, click the **Maintenance folder,** then click the **Application** folder.



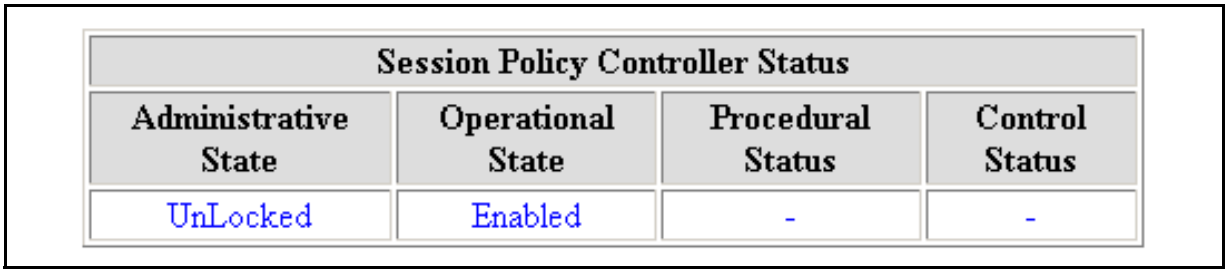
3 Click on the **Policy Controller** folder to open it.

4 In the Policy Controller panel click the **Unlock** button.



5 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Administrative State changes to **Unlocked**



Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

Note: The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise, manually refresh the page by clicking on the **Refresh** button.

6 The procedure is complete.

Suspend the Policy Controller application

Purpose of this procedure

Use the following procedure to temporarily take the Policy Controller application out of service.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section "Interpreting Policy Controller application states" in the *Policy Controller Security and Administration*, NN10434-611.

Limitations and restrictions

This procedure can only be performed when the Policy Controller application is in the following service states:

- the Operational State is **Enabled**
- the Administrative State is **Locked**

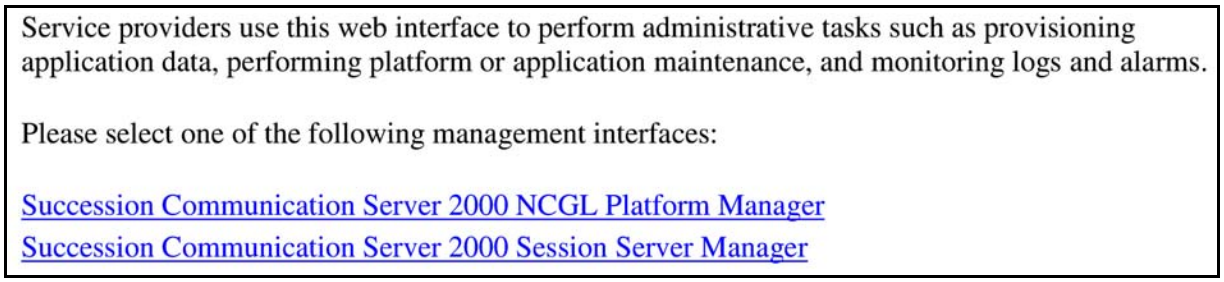
Prerequisites

The Policy Controller application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the Policy Controller application on page 34.

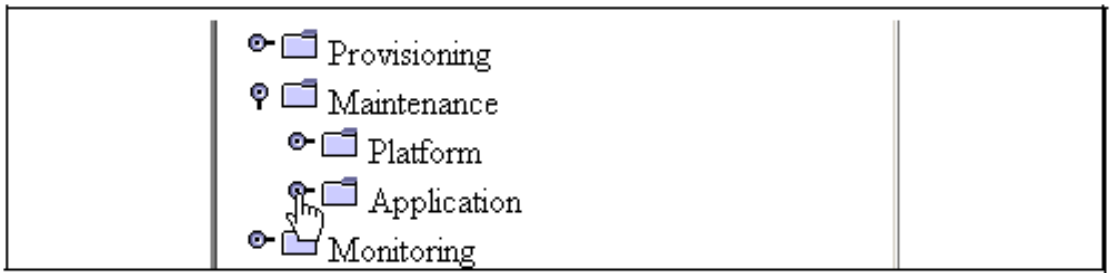
Action

At the Policy Controller Launch Point

1 Select Succession Communication Server 2000 Policy Controller Manager from the launch point menu.

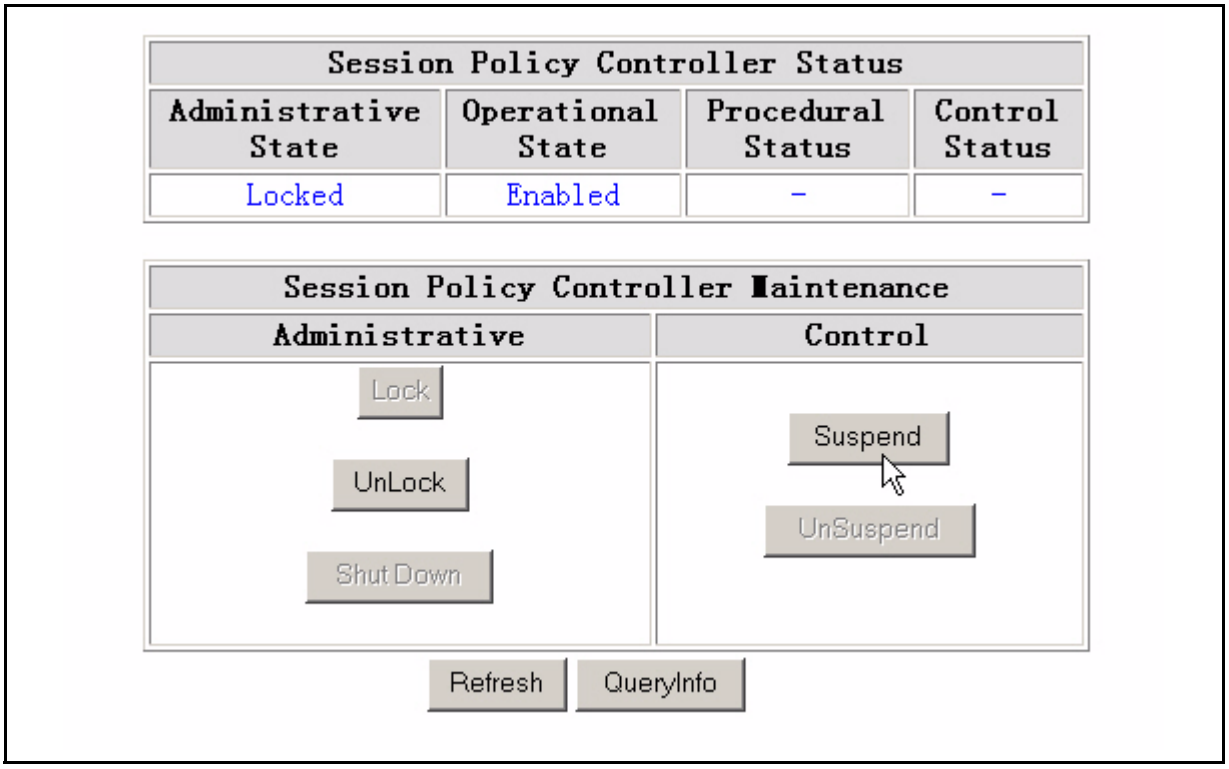


2 At the Policy Controller folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click on the **Policy Controller** folder to open it.

4 In the Policy Controller panel click **Suspend**.



5 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Operational State changes to **Disabled**

Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Disabled	-	Suspended

6 If applicable, restart the Policy Controller application by executing procedure Unlock the Policy Controller application on page 39.

7 The procedure is complete.

Unsuspend the Policy Controller application

Purpose of this procedure

Use the following procedure to bring the Policy Controller application back into service without restarting callP activity.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section *Interpreting Policy Controller application states,* in *Policy Controller Security and Administration*, NN10346-611.

Limitations and restrictions

This procedure can only be performed when the Policy Controller application is in the following service states:

- the Operational State is **Disabled**
- the Administrative State is **Locked**

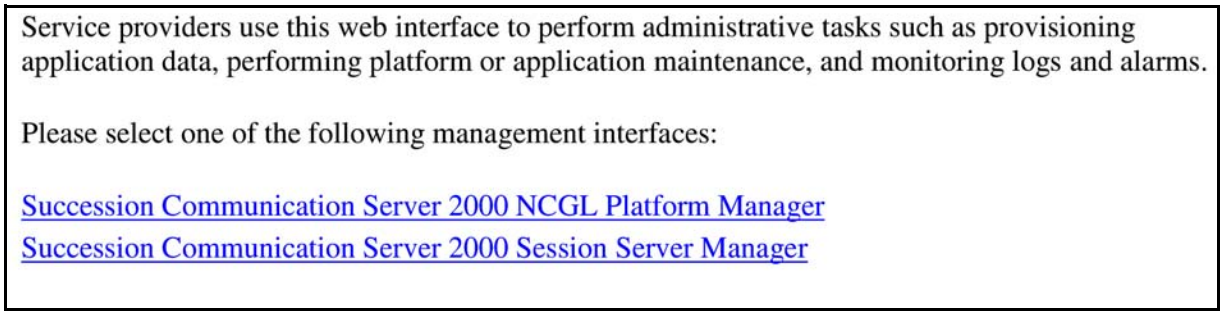
Prerequisites

The Policy Controller application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure Suspend the Policy Controller application on page 42.

Action

At the Policy Controller Launch Point

1 Select **Succession Communication Server 2000 Policy Controller Manager** from the launch point menu.

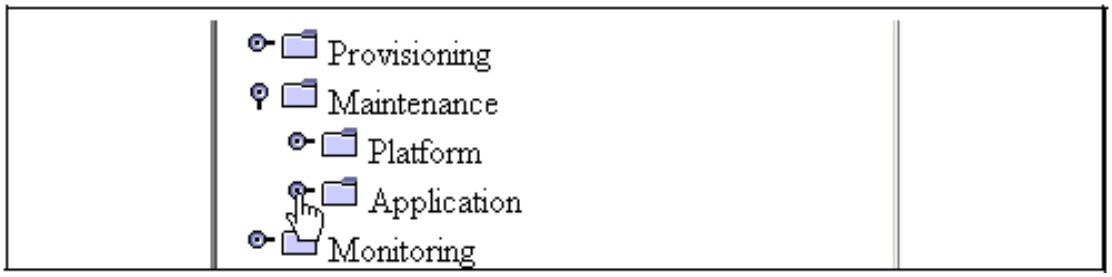

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager

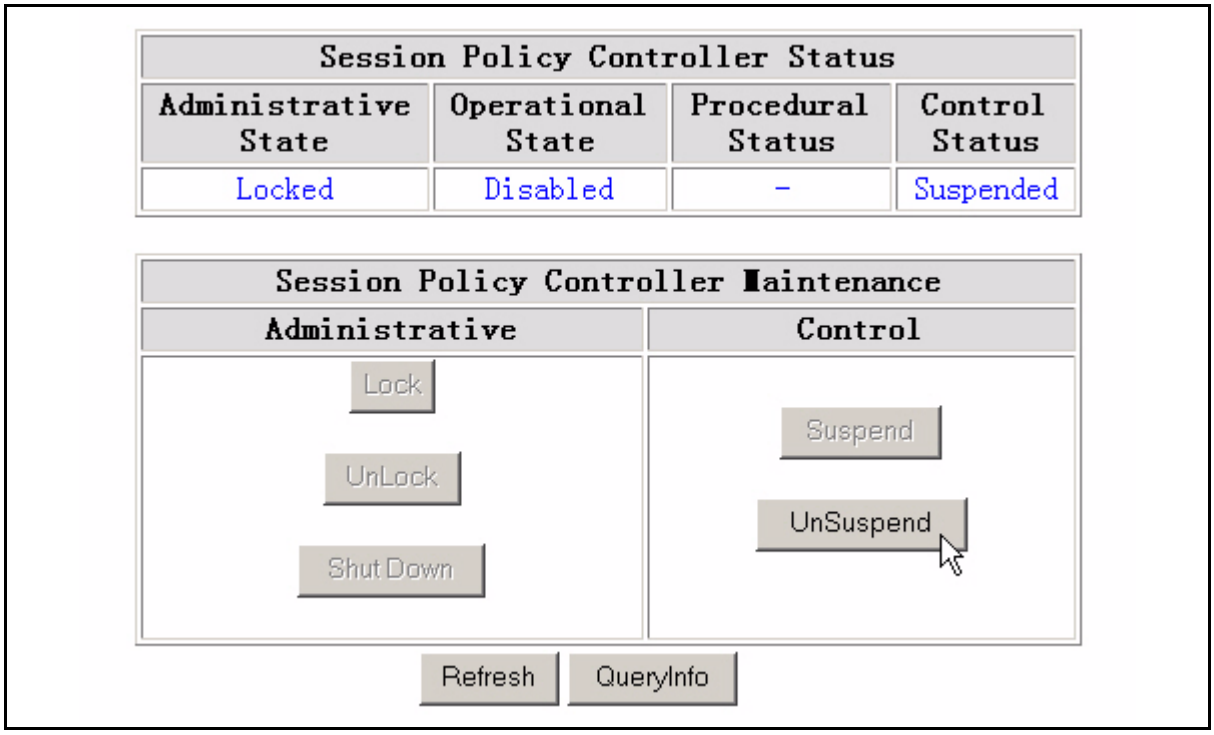
Succession Communication Server 2000 Session Server Manager

2 At the Policy Controller folder, click the **Maintenance folder,** then click the **Application** folder.



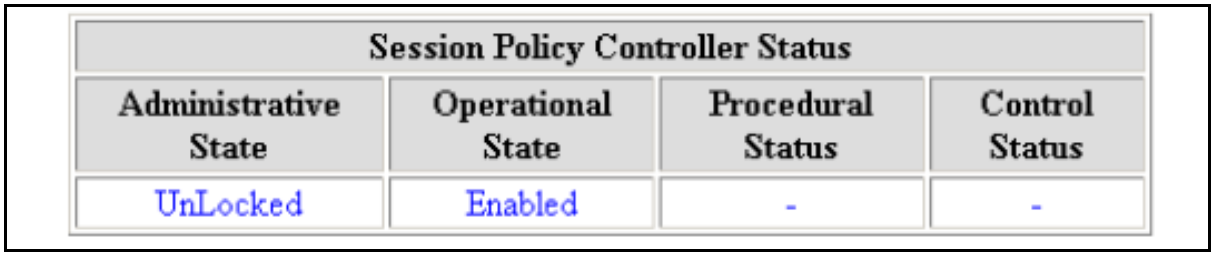
3 Click on the **Policy Controller** folder to open it.

4 In the Policy Controller panel click **Unsuspend**.



5 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Operational State changes to **Enabled**
- the Control status changes to **-**



Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

6 If necessary, bring the Policy Controller application back into service by executing procedure Unlock the Policy Controller application on page 39.

7 The procedure is complete.

Shutdown the Policy Controller application

Purpose of this procedure

Use the following procedure to gracefully transition the administrative state of the Policy Controller application to Locked, blocking new resource requests and only accepting messages for calls that existed prior to the Shut Down command.

The shutdown command, unlike the Lock command, does not reset Bandwidth resource usage and call data until all Virtual Call Admission Control calls on the CS 2000 have cleared down. It is a more graceful method but it will prevent the Policy Controller from processing new Virtual Call Admission Control requests whilst shutting down and locked. During the Shutting Down state the Bandwidth resource usage held by the Policy Controller will only be changed if a call release message is received.

Note: For more detailed information about Policy Controller application states and administrative functions, refer to Interpreting Policy Controller application states on page 13.

Limitations and restrictions

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure View the operational status of a Policy Controller NCGL platform on page 1.

While the Policy Controller is Shutting Down it has an Administrative state of "Shutting Down" and an operational state of "enabled". However, it is also possible to issue the Lock or Unlock command whilst the Policy Controller is Shutting Down. If the Lock command is issued then the Policy Controller will cause all call data to be reset, and will also automatically reset Bandwidth resource usage counters to zero immediately. During the Lock operation the Policy Controller will transition from "Shutting Down Enabled" to "Locked Enabled Terminating" and finally to "Locked Enabled". Alternatively, if the Unlock command is issued the Policy Controller will return to Unlocked Enabled and will thereafter start processing any new Virtual call Admission Control requests. Since Bandwidth resource usage and call data is not automatically reset during the shut down state the Policy Controller still maintains an accurate view of the Bandwidth resource usage after the Unlock operation.

Refer to the Policy Controller application maintenance state diagram on page 15 for valid transition states.

CAUTION

This is a service affecting procedure. Shutting Down the Policy Controller application prevents any lines configured for Virtual Call Admission Control to make or receive calls using the Policy Controller. Existing calls regardless of call state will not be released by this procedure. However, while the Policy Controller is Shutting Down, it is only capable of receiving call release requests from the CS 2000 in order to release the existing calls. While Shutting down and Locked the Policy Controller Application will not be able to process any new VCAC requests

Note: The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Shutting Down state.

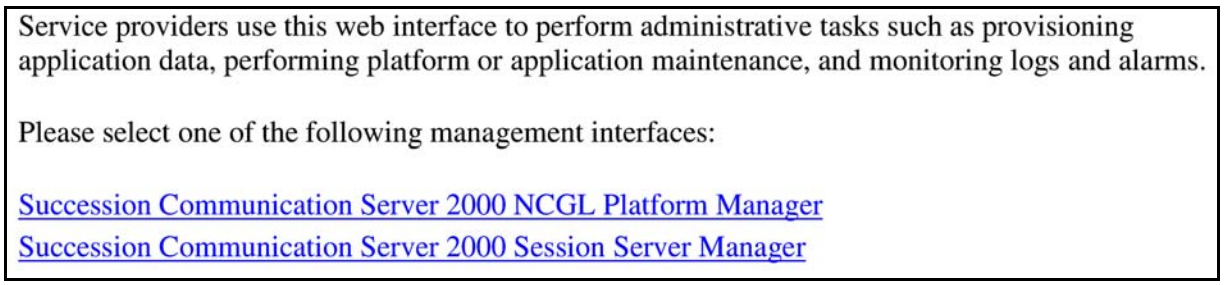
Prerequisites

There are no prerequisites for this procedure.

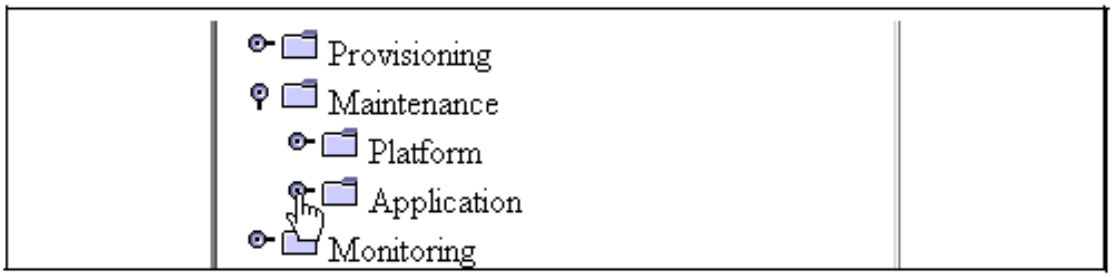
Action

At the Policy Controller Launch Point

1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

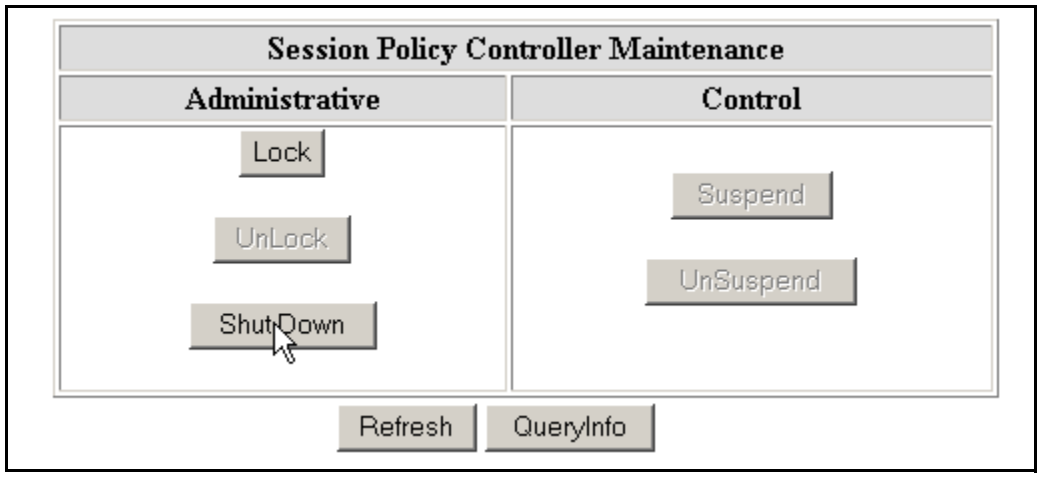


2 At the Policy Controller folder, click the **Maintenance** folder, then click the **Application** folder.



3 Click the **Policy Controller** folder to open it.

4 In the Policy Controller panel click the **Shutdown** button.



The system responds:

```
This action will block all call resource
requests to the Session Policy Controller.  This
will cause a SERVICE OUTAGE on this Session
Policy Controller and subsequent call attempts
will be denied.
```

5 Click **OK** to confirm locking the Policy Controller application.

CAUTION

This is a service affecting procedure. Shutting Down the Policy Controller application prevents any lines configured for Virtual Call Admission Control to make or receive calls using the Policy Controller. Existing calls regardless of call state will not be released by this procedure. However, while the Policy Controller is Shutting Down, it is only capable of receiving call release requests from the CS 2000 in order to release the existing calls. While Shutting down and Locked the Policy Controller Application will not be able to process any new VCAC requests

Note: The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Shutting Down state.

6 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Administrative State changes to **Locked**

Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-

Note: The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise manually refresh the page by clicking on the **Refresh** button.

7 This procedure is complete.

Power-On and boot a Policy Controller unit

Purpose of this procedure

This procedure is used to power on a Policy Controller unit that has been installed as a replacement, or was shutdown for any other reason.

This procedure may be used as a standalone task or as part of a higher level activity such as part of a dead office recovery activity or software upgrade activity.

Limitations and restrictions

There are no restrictions on using this procedure.

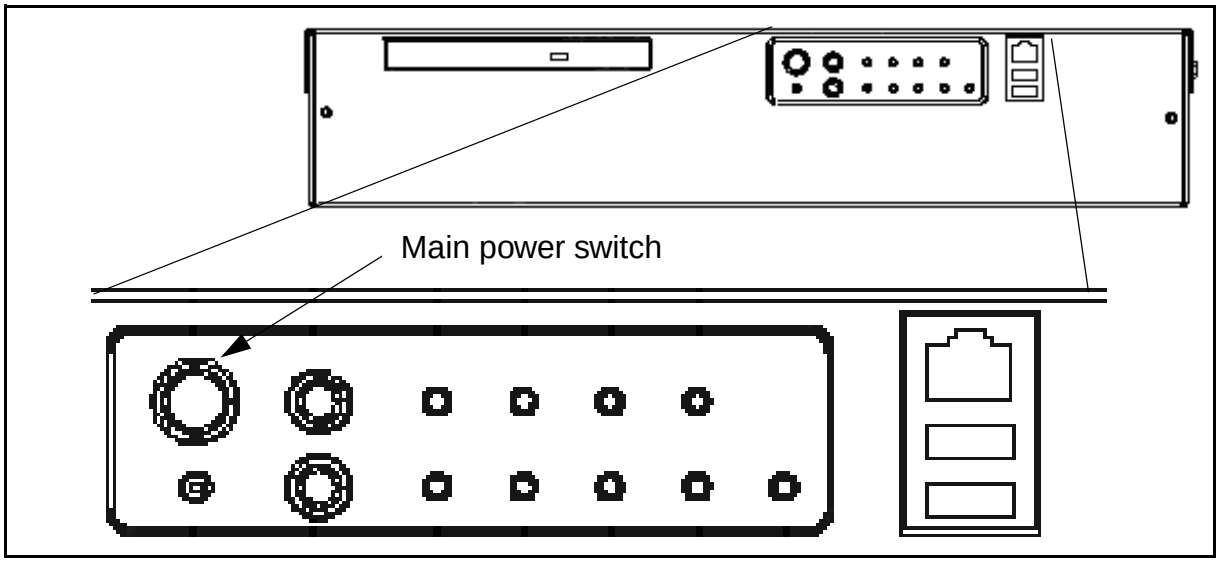
Prerequisites

If the unit was a replacement unit recently installed, ensure that all power cabling connections have been properly installed and secured at the rear of the chassis and SAM-F frame.

Action

At the front panel of the Policy Controller unit

1 If necessary, power on the Policy Controller using the main power switch located on the front panel.



2 If desired, at the Policy Controller console, monitor the boot progress of the unit.

3 The procedure is complete.

Power-Off a Policy Controller unit

Purpose of this procedure

This is used to power off a Policy Controller unit.

This procedure may be used as a standalone task or as part of a higher level activity such as a part of a controlled shutdown activity or part of a software upgrade activity.

Limitations and restrictions

CAUTION

This is a service affecting procedure. Powering off a Policy Controller unit prevents the node from operating in a fault-tolerant manner. Ensure that the unit you are powering off is not the active unit. Failure to do so may result in loss of call processing.

Prerequisites

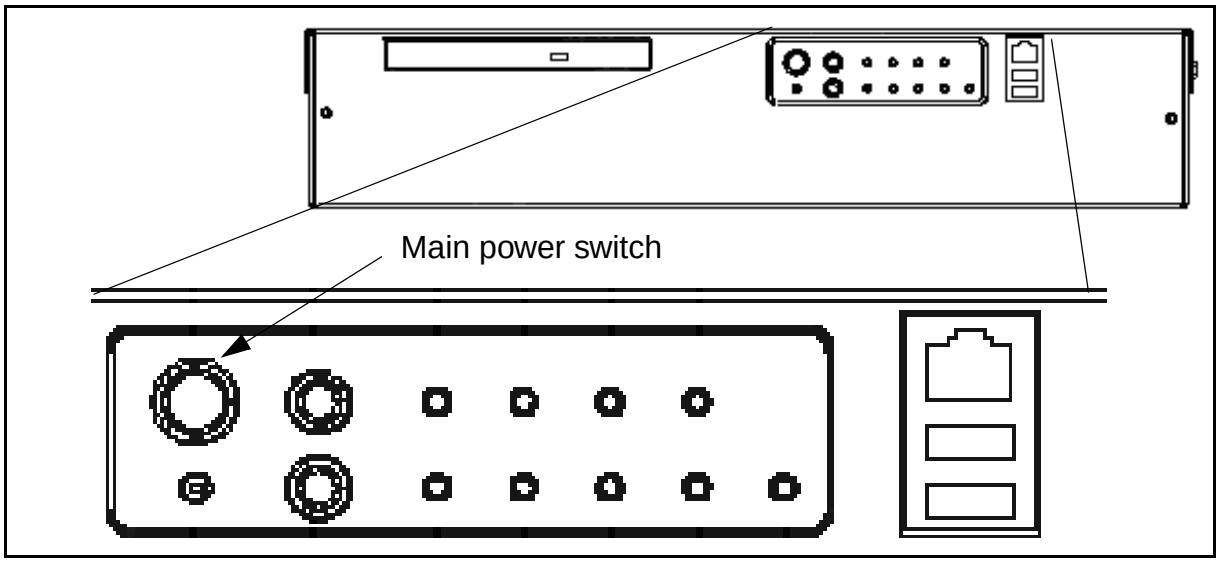
Refer to procedure “View the operational status of a Policy Controller NCGL platform” in Policy Controller Fault Management, NNxxxxx-911 to verify that the unit to be shut down is not active.

Action

At the front panel of the Policy Controller unit.

1 Complete procedure Halt (shutdown) a Policy Controller unit on page 72 in before powering off the unit.

2 Once the operating system has been halted, disconnect the power to the unit using the main power switch located on the front panel.



3 The procedure is complete.

Halt (shutdown) a Policy Controller unit

Purpose of this procedure

This procedure is used to perform a graceful shut down a Policy Controller platform NCGL operating system. Use this procedure only as part of a high-level activity such as part of a controlled shutdown activity or part of a software upgrade activity. Included at the end of this procedure is an alternate CLI method for halting a unit.

Limitations and Restrictions

This procedure does not cause the Policy Controller unit to power-off.

Ensure that the Policy Controller unit you are shutting down is not performing call processing activities.

CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit, and prevents the Policy Controller node from operating in a fault-tolerant mode.

Prerequisites

Use procedure "View the operational status of a Policy Controller NCGL platform" in Policy Controller Fault Management, NNxxxxx-911, to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

Action

At the CS 2000 Policy Controller Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

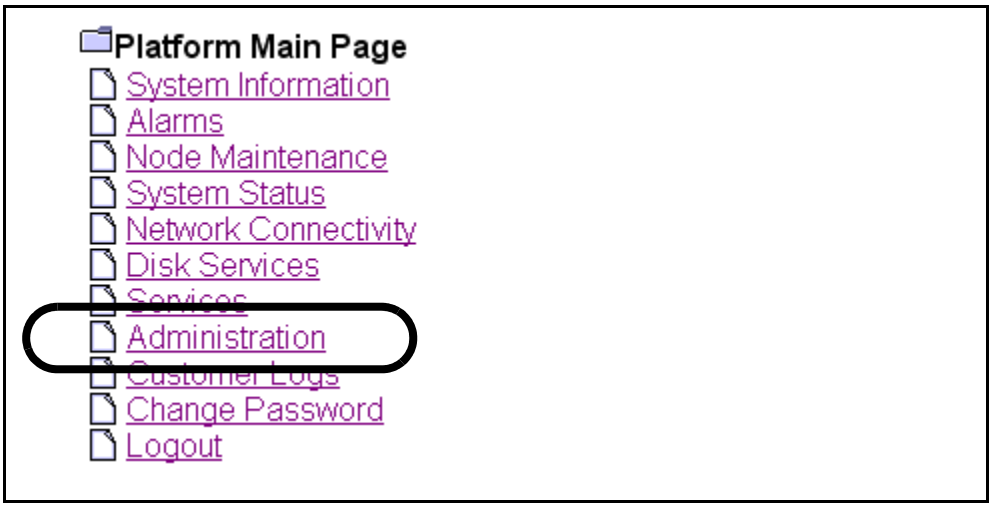
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

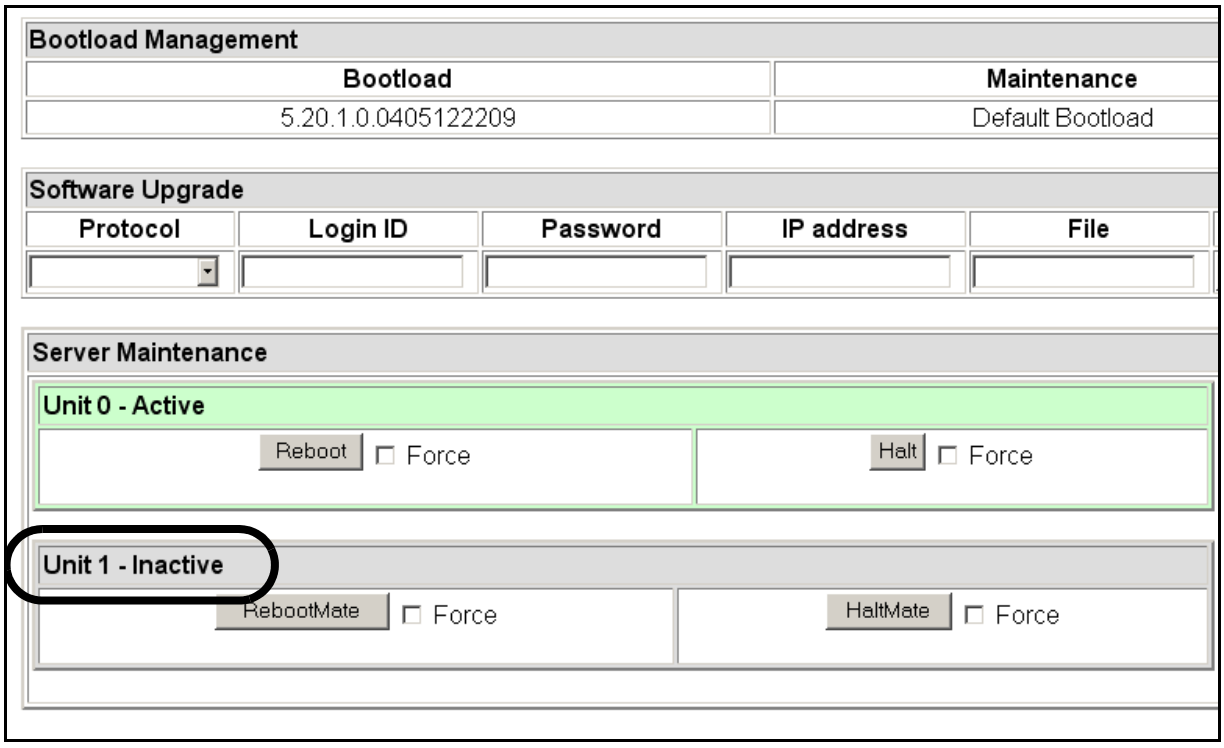
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Administration** link.

The Administration page is displayed.

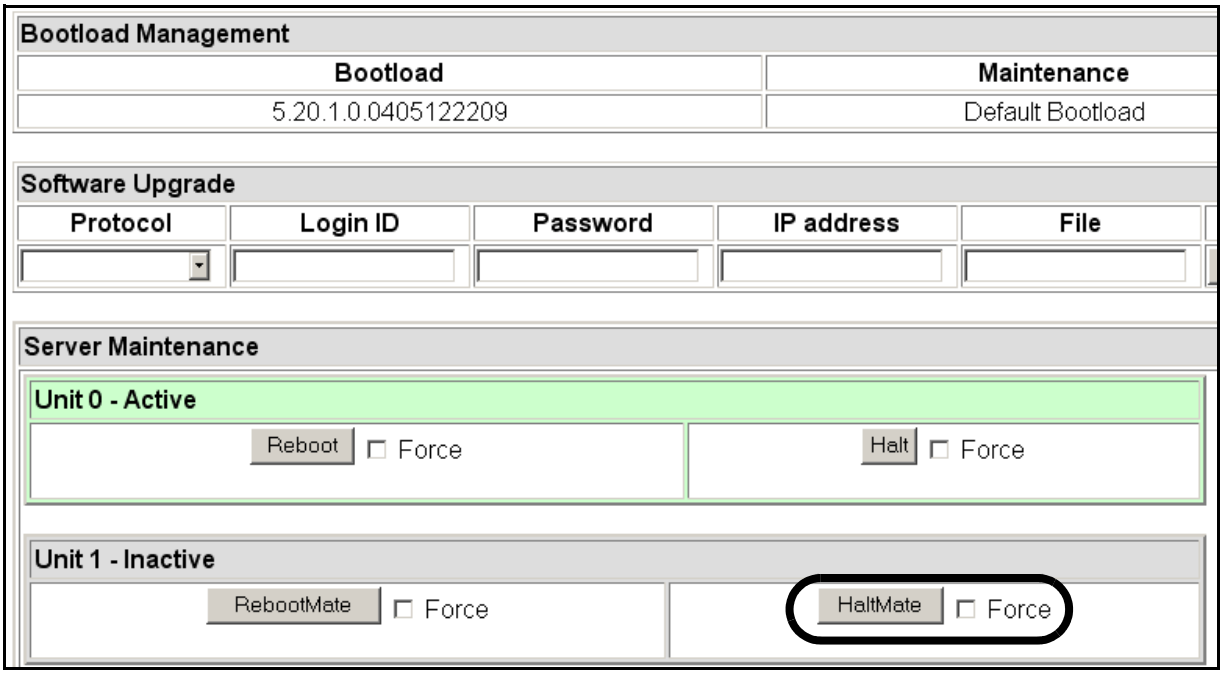


3 Review the status of the unit you want to halt. If it is unavailable, the **Halt** or **HaltMate** buttons are not accessible.



4 Click the **Halt** or **HaltMate** button for the Policy Controller unit you want to halt the NCGL operating system for.

Note: To override any pre-halt (shutdown) queries, click the **Force** check box before clicking the **Halt** or **HaltMate** button.



The system responds:

```
Are you sure you wish to halt?
This may cause an extended service outage to any
clients currently using this server. Click OK to
confirm server halt or cancel to abort.
```

5 Click **OK** to confirm the halt operation.

The NGCL and all call activity on the affected Policy Controller begins the process of halting. This can take several minutes.

6 If you receive the following message, you must halt the unit using the Force option in step 4.

```
Error: Command failed. Reason: Mate not
available.
```

7 If applicable, complete procedure Power-Off a Policy Controller unit on page 121 to disconnect power from the unit.

8 This procedure is complete.

To Haltmate or Force Haltmate?

The Haltmate action does not work if the SIP Gateway application database on the active unit is out of sync with the database on the inactive unit. Using the Haltmate command with the Force option overrides any pre-checks for this condition and forces a Halt of the inactive unit regardless of the sync state of the active unit database.

Alternate command line interface (CLI) method

ATTENTION
All prerequisites and restrictions shown on page 72 apply to using this procedure.

At the Policy Controller console interface

1 Log onto a Policy Controller unit using a secure shell by typing

> **ssh -l <userid> <PC_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

PC_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 Shutdown the Policy Controller unit by typing

 # halt

and pressing the **Enter** key.

6 If applicable, complete procedure Power-Off a Policy Controller unit on page 121 to disconnect power from the unit.

7 You have completed this procedure.

Reboot a Policy Controller unit

Purpose of this procedure

Use this procedure to perform a graceful shut down and reboot of the NCGL operating system running on a Policy Controller unit. Use this procedure only as part of a high-level activity such as maintenance or fault clearing activities or as part of a software upgrade activity.

ATTENTION

This procedure causes a 3-4 minute service interruption of the affected unit and should only be used when recommended by Nortel support personnel.

Limitations and Restrictions

ATTENTION

Nortel recommends performing this procedure only on the standby unit.

CAUTION

If both active and inactive units are rebooted, the reboot procedure prevents the Policy Controller from performing Virtual Call Admission Control processing. If the inactive unit alone is rebooted then this prevents the Policy Controller node from operating in a fault-tolerant state.

Note: The CS 2000 will continue to process calls without Network VCAC if it determines the Policy Controller is unreachable.

Prerequisites

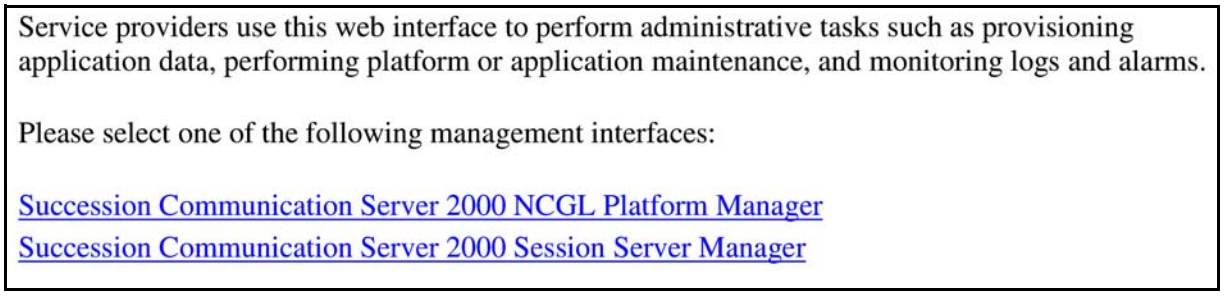
Use procedure View the operational status of a Policy Controller NCGL platform on page 1 to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

Ensure that you have your bootable software installation DVD disk available, in case you have trouble rebooting the unit.

Action

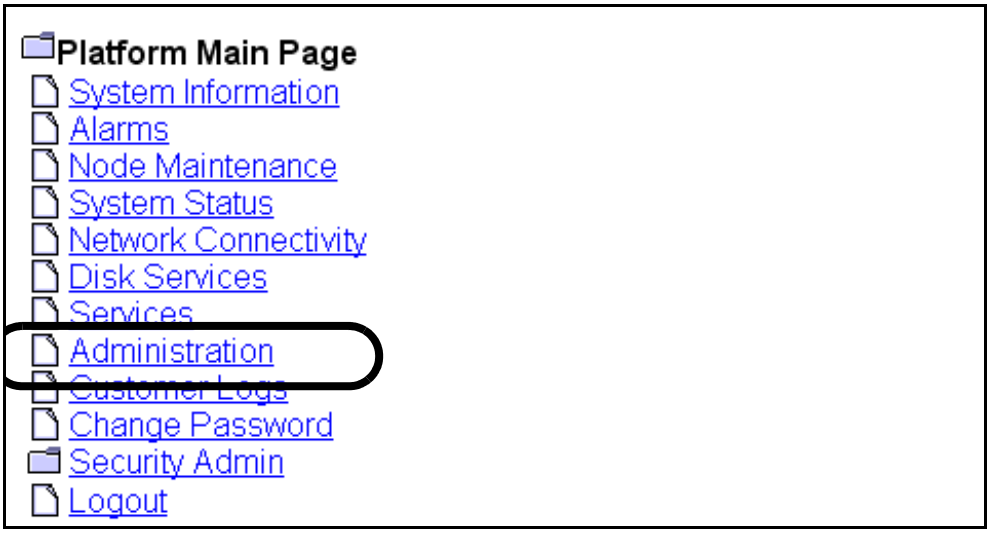
At the Policy Controller GUI or IEMS client for the active unit

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

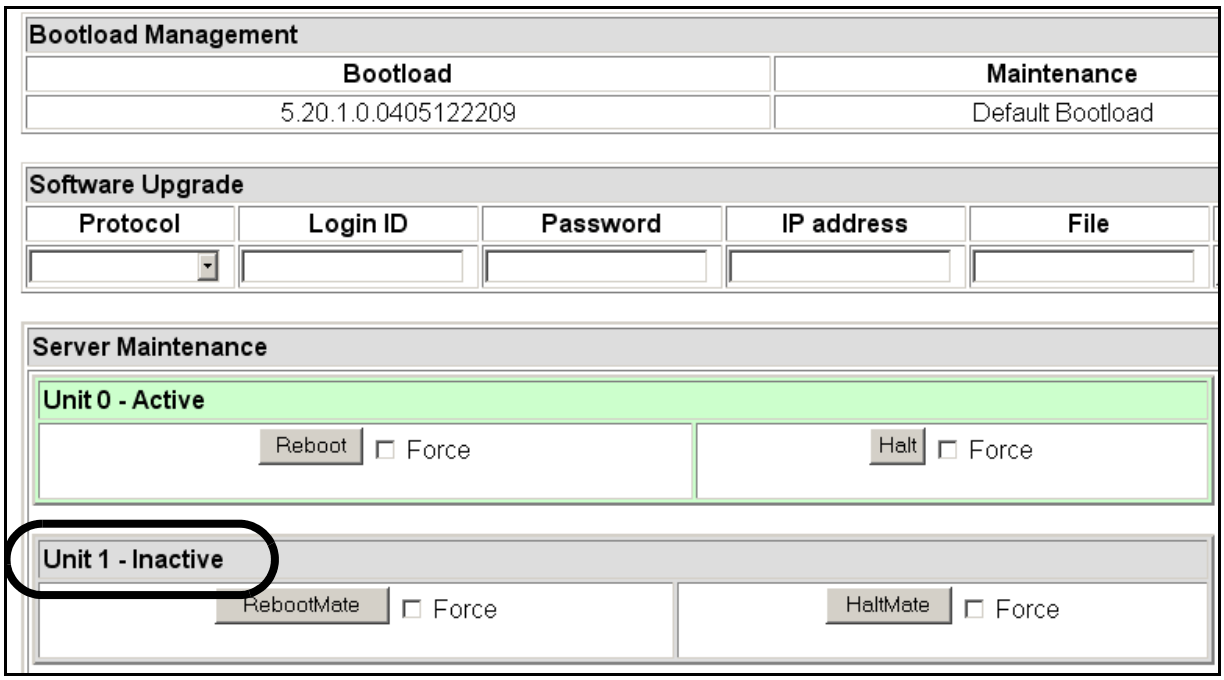


2 Click the **Administration** link.

The Administration page is displayed.



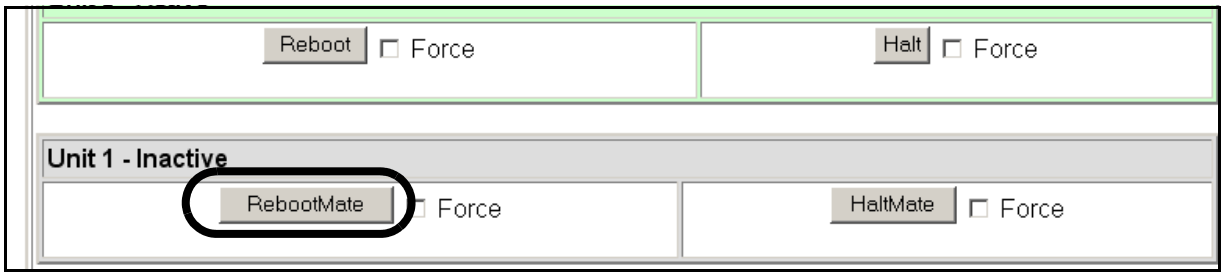
3 Review the status of the unit you want to reboot. If it is available, the **Reboot** or **RebootMate** buttons are accessible.



4 Click the **Reboot** button (for the active unit) or **RebootMate** button (for the inactive unit) for the Policy Controller unit you want to reboot.

Note 1: If you want to override any pre-reboot queries including a pre-check by applications running on the unit, click the **Force** check box before clicking the **Reboot** or **RebootMate** button.

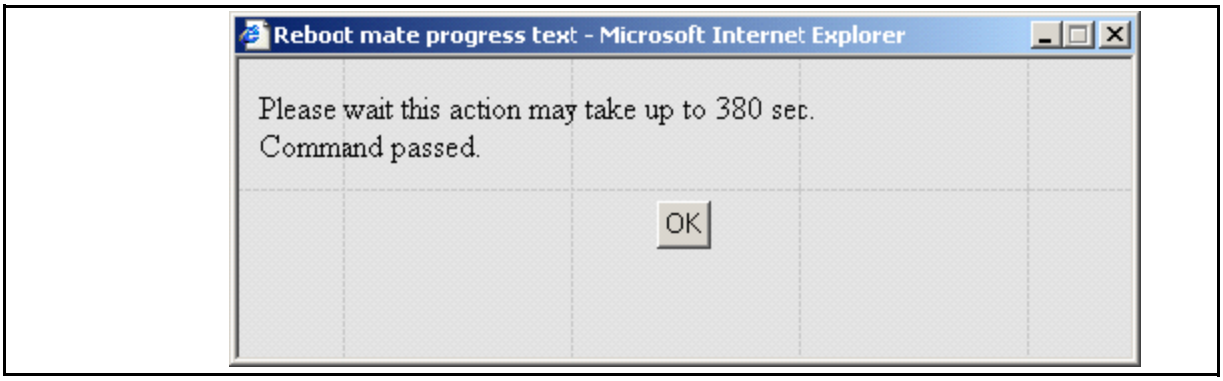
Note 2: In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be rebooted using RebootMate or a Forced RebootMate. A Reboot or Forced Reboot can only be performed if the system is operating in simplex mode.



The system responds with the following message box:

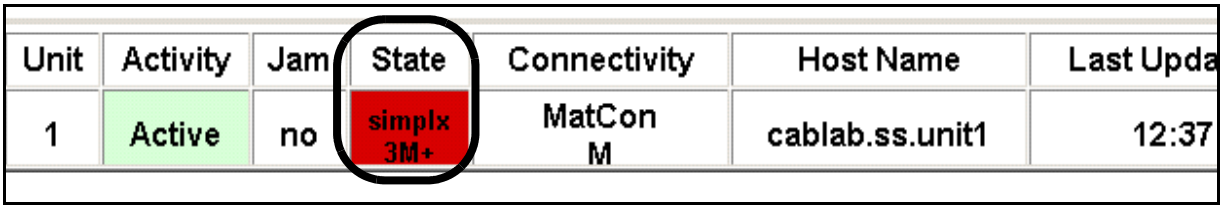
5 Click **OK** to confirm the reboot operation.

The NGCL and all call activity on the affected unit is shutdown and the unit begins to reboot. The system responds with the following message box:



6 Click **OK** to close the dialog box.

7 Monitor the recovery of the rebooting unit using procedure View the operational status of a Policy Controller NCGL platform on page 1 to confirm the recovery of the unit after reboot. Continue monitoring the active unit until you see the State field in the alarm panel change back to duplex.



Unit	Activity	Jam	State	Connectivity	Host Name	Last Upda
1	Active	no	simplx 3M+	MatCon M	cablab.ss.unit1	12:37

8 This procedure is complete.

Troubleshooting reboots

The following possible error messages received during a reboot attempt and their meaning are described:

Error: Command failed. Reason: Mate not available.
You must reboot the unit using the Alternate command line interface (CLI) method on page 83.

Error: Reboot - Command rejected. Reason: Mate is available.
You have attempted to reboot the active server when the inactive server is available.

Error: Halt - Command rejected. Reason: Mate is available.
You have attempted to halt the active server when the inactive server is available.

Error: Command failed. Reason: PRECHECK FAILED: application rejected request.
The user has attempted a rebootmate or haltmate command and the application rejected the request. The user should check /var/log/designlog to determine the name of the application that rejected the maintenance command.

Actions:

- Using the Force option overcomes a pre-check failure by any application running on the unit.
- Try the operation again later. If the problem persists, then contact Nortel Networks support personnel for assistance.

Alternate command line interface (CLI) method

ATTENTION
All prerequisites and restrictions shown on page 78 apply when using this procedure.

At Policy Controller CLI or Integrated EMS client

1 Log onto the either Policy Controller unit and change to the root user.

2 Reboot the Policy Controller unit by typing

```
# reboot
```

and pressing the **Enter** key.

3 Use procedure View the operational status of a Policy Controller NCGL platform on page 1 to confirm the recovery of the unit after reboot.

4 You have completed this procedure.

Query current number of calls

Purpose of this procedure

Use this procedure to determine how many Network VCAC calls are currently being processed by the Policy Controller node.

Limitations and restrictions

Only active Network VCAC calls are reported, including calls in ringing and answered state.

The Policy Controller application must be in one of the following states to report the number of active calls:

- In service (Unlocked, Enabled, -, -)
- In service but shutting down (Shutting Down, Enabled, -, -)
- Locked or ManB In-progress (Locked, Enabled, Terminating, -)

Session Policy Controller Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

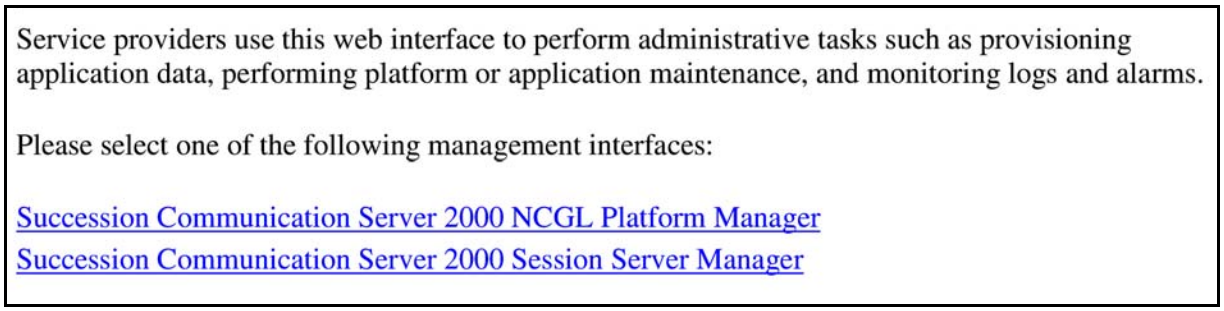
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Policy Controller Launch Point

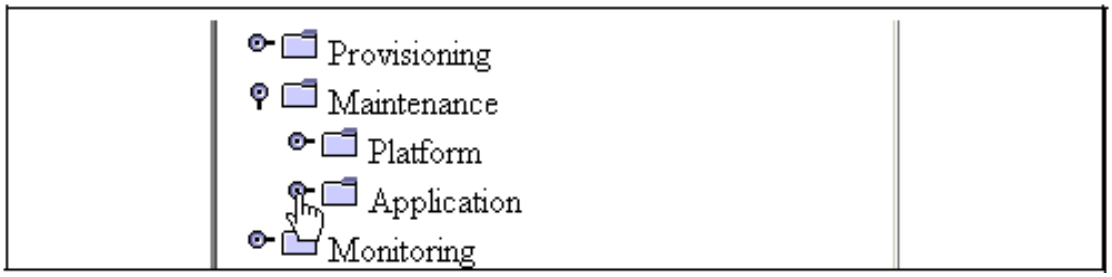
1 Select ***Succession Communication Server 2000 Policy Controller Manager*** from the launch point menu.


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

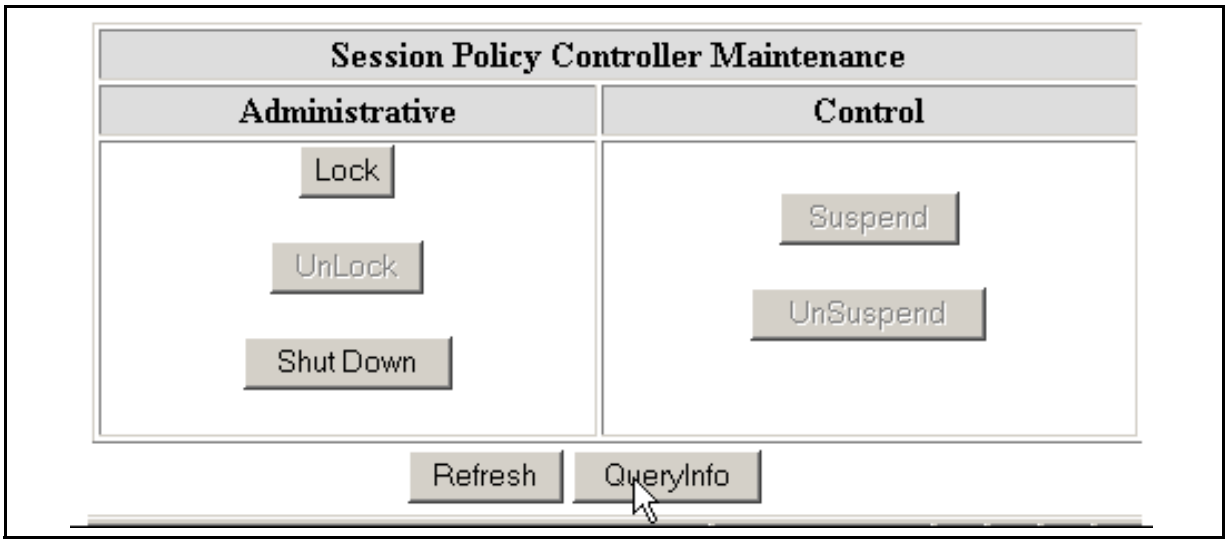
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 At the Policy Controller folder, click the **Maintenance folder,** then click the **Application** folder.



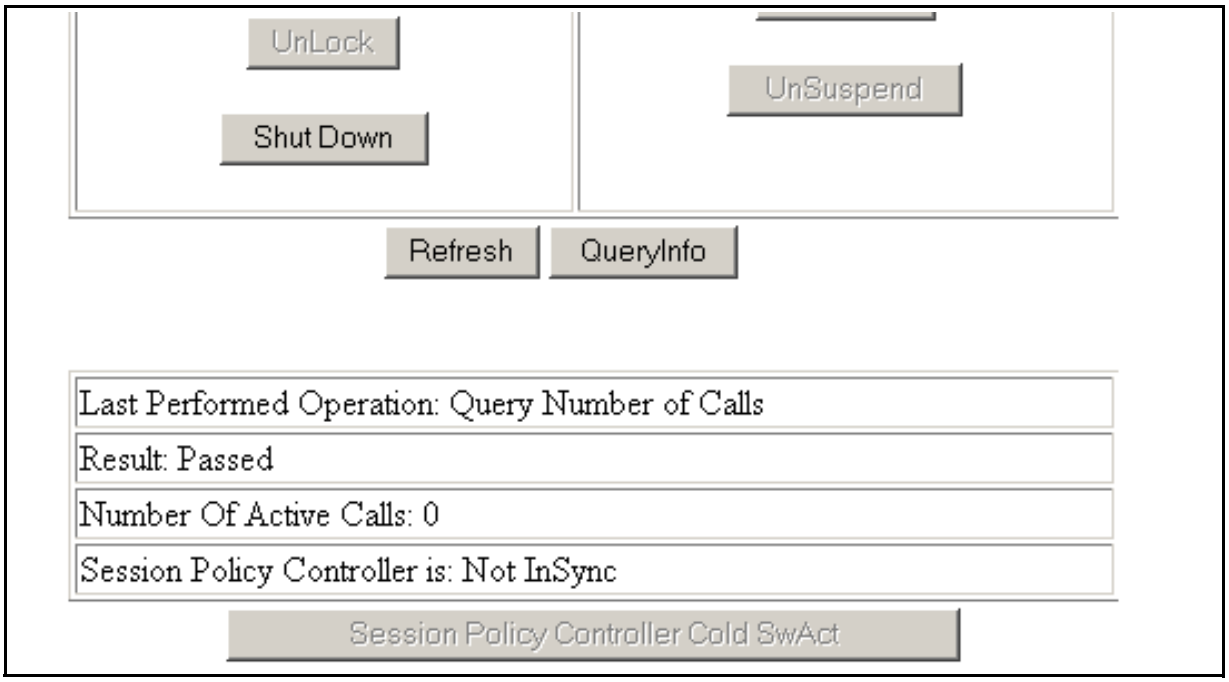
3 Click on the **Policy Controller** folder to open it.

4 At the bottom of the Policy Controller Maintenance panel, locate and click the **QueryInfo** button.



5 The number of currently active calls is displayed in the table below the **QueryInfo** button.

Note: The status panel is refreshed according the value shown in the drop down box at the bottom of the status panel. When refresh occurs, the info box disappears. If necessary, to increase the refresh rate, select a larger value from the drop down menu and click the **Refresh Rate** button.



6 The procedure is complete.

Perform a manual backup of the Policy Controller database

Purpose of this procedure

Use this procedure to perform a backup of the active Policy Controller unit Policy Controller application database. Use this procedure to make regular backup copies of the database or as a precautionary activity before starting any type of upgrade to the Policy Controller application. This procedure may be used as a standalone task or as part of a higher level upgrade activity.

Limitations and Restrictions

ATTENTION

If you perform provisioning changes during this procedure, it can lead to database corruption and possible system outages. To ensure that you create an accurate and complete copy of the active unit database, verify that all provisioning changes are stopped before continuing this procedure.

Prerequisites

ATTENTION

The Policy Controller database and the CS 2000 database must always be in sync. CS 2000 core images, CS 2000 GWC Manager Oracle database backups, and the Policy Controller application backups must always be maintained in sync for emergency recovery. To ensure they are in sync, perform images and backups at the same time.

Action

At the Policy Controller command line interface

1. Log onto the active Policy Controller unit and change to the root user.
2. Change directory to the database directory by typing

   `# cd /opt/apps/database/solid/dbfiles`

   and pressing the Enter key.

3 Put a copy of the database for the active unit in the backup directory by typing

```
# cp solid.db  /opt/apps/database/solid/backup
```

and pressing the Enter key.

Note: If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

Example

```
# cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

4 For security purposes, ensure that a backup copy of the database file is transferred to a secure location.

Use the unix **scp** command to make a secure copy of the backup database file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the Policy Controller application database become necessary, such as during an upgrade rollback. A root password for the remote server may be required.

5 You have completed this procedure.

View the operational status of a Policy Controller NCGL platform

Purpose of this procedure

Use the following procedure to view the service status of the Policy Controller platform hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. This procedure may be used as a standalone task or as part of a high-level activity.

Limitations and restrictions

Although some activities described in this procedure can be accomplished using the Policy Controller GUI, they are described instead using the more complete CS 2000 NGCL Platform Manager.

This procedure does not describe how to change platform or NCGL settings such as changing BIOS settings or platform provisioning. Refer to the appropriate procedures in the Policy Controller Configuration Management NTP, NN10432-511, for changing these settings.

This procedure does not describe how to view customer logs, alarms or how to change the root password. For instructions on how to change the platform root password, refer to the Policy Controller Security and Administration NTP, NN10434-611.

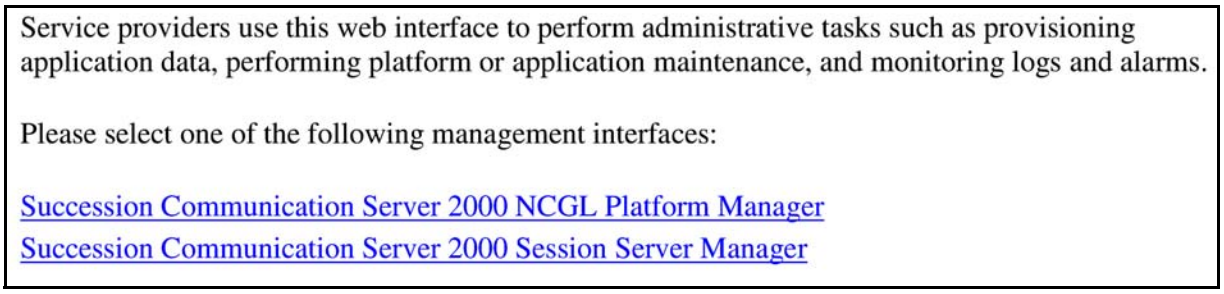
Prerequisites

None

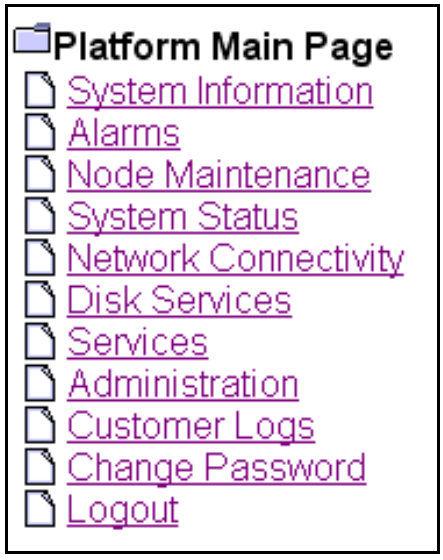
Action

At the CS 2000 Policy Controller Launch Point

1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.



The Platform Main Page menu is displayed.

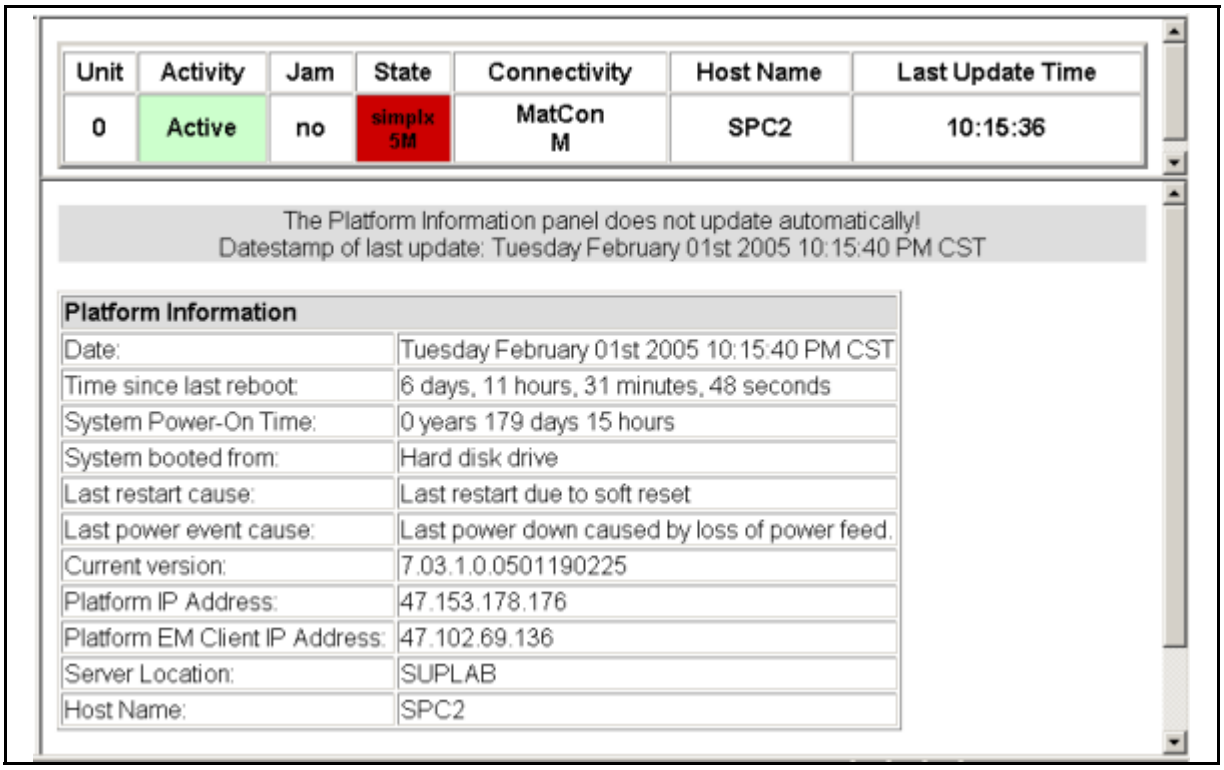


2 Use the following table to determine your next step:

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the **System Information** link and go to step 3.
you want to review existing platform alarms	Skip to step 17 and go to procedure *View Policy Controller Alarms* in NTP 10432-911.
you want to review node maintenance status	Click the **Node Maintenance** link and go to step 5.
you want to review the status of system processes, CPU load and memory or related alarm thresholds	Click the **System Status** link and go to step 7.
you want to review the connectivity status of the network links. To perform link management activities, refer to the Policy Controller Security and Administration NTP, NN10434-611	Click the **Network Connectivity** link and go to step 9.
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the **Disk Services** link and go to step 10.
you want to review details about platform services including the network time protocol servers	Click the **Services** link and go to step 12.
you want to review platform version information only	Click the **Administration** link and go to step 14.
you want to review customer logs	Skip to step 17 and go to procedure *View Policy Controller logs* in NTP 10432-911.
you want to change root passwords	Skip to step 17 and go to procedure "Manage user passwords with the Policy Controller GUI" in the Policy Controller Security and Administration NTP, NN10434-611.
you are done reviewing information and want to logout from the GUI	step 16.

3 Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page:

Note: The Platform (System) Information panel does not update automatically. Click the **System Information** link again to update it.



Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
0	Active	no	simplx 5M	MatCon M	SPC2	10:15:36

The Platform Information panel does not update automatically!
Datestamp of last update: Tuesday February 01st 2005 10:15:40 PM CST

Platform Information	
Date:	Tuesday February 01st 2005 10:15:40 PM CST
Time since last reboot:	6 days, 11 hours, 31 minutes, 48 seconds
System Power-On Time:	0 years 179 days 15 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	7.03.1.0.0501190225
Platform IP Address:	47.153.178.176
Platform EM Client IP Address:	47.102.69.136
Server Location:	SUPLAB
Host Name:	SPC2

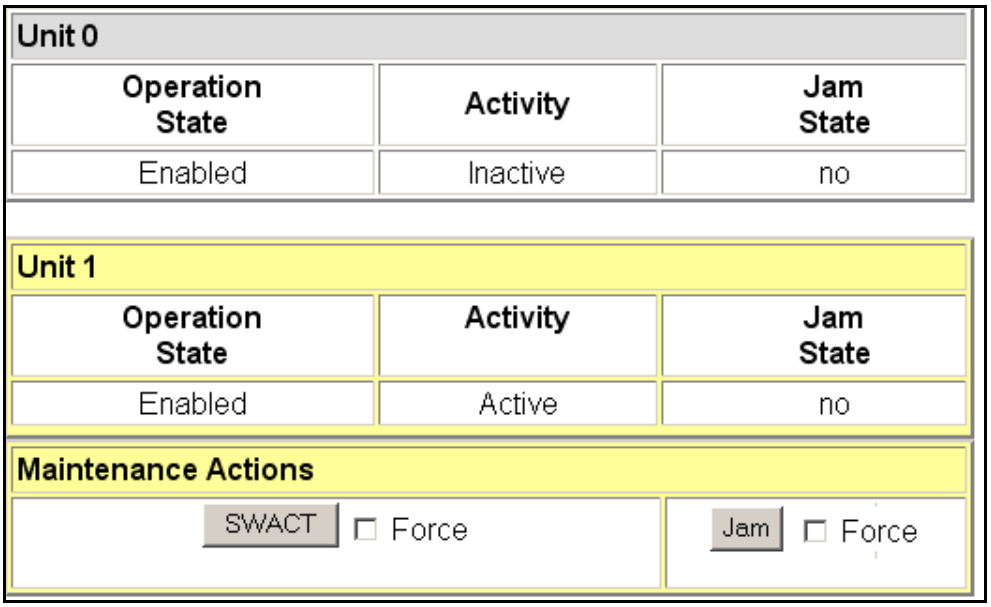
Field	Description
Unit	The Unit number of the Policy Controller in the node that is active. This is the unit you are logged into using your GUI.
Activity	Indicates the activity of the unit (either active or standby).
Jam	Indicates if an activity Jam has occurred on the active Policy Controller unit. This prevents the standby unit from becoming active, regardless of any failures on the active unit.
State	Indicates if the Policy Controller node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line).

Field	Description
Connectivity	Indicates the state of the network links on the node.
Host Name	Indicates the name of the Policy Controller unit (not node).
Date	Indicates the system date as maintained by the network time protocol (NTP) server.
Time since last reboot:	Indicates the amount of time that has elapsed since the Policy Controller was last rebooted for any reason.
System Power-On Time:	Indicates the recorded system time that the Policy Controller was powered up.
System booted from:	Indicates whether the Policy Controller is currently booted from the hard drive, or DVD-ROM drive.
Last restart cause:	Indicates any event that forced a platform reboot (manual or system generated).
Last power event cause:	Indicates any event that affected the power supply subsystem of the unit chassis.
Current version:	Indicates the installed version of the Policy Controller platform software. (Does not include the SIP Gateway application or other co-resident applications.) Refer to the Policy Controller Upgrades NTP, NN10431-461, for more procedures on acquiring version information.
Platform IP Address:	Indicates the IP address of the Policy Controller platform.
Platform EM Client IP Address:	Indicates the IP address of the Policy Controller client web interface. This is the IP address of the PC or Unix client from which the GUI was launched. When a web proxy is used, IP address is prefixed with the SSPFS proxy IP address.
Server Location:	Indicates the physical location of the Policy Controller.
Host Name:	Indicates the hostname of the Policy Controller node.

4 When you have completed reviewing System Information page, return to step 2.

5 Review the Node Maintenance page and use the following table to review the description of the various fields of the Node Maintenance page:

Note: The Node Maintenance panel is refreshed every 45 seconds.



Field	Description
Operation State (unit 0 or 1)	Indicates the operational state of the platform software.
Activity (unit 0 or 1)	Indicates the activity state of the platform software.
Jam State (active unit only)	Indicates whether or not an activity jam has been requested.
Maintenance Actions (active unit only)	Maintenance panel for performing node SwAct activity and to unjam node activity. Refer to the Policy Controller Security and Administration NTP, NN10434-611, for procedures on performing a SwAct or Jam/unJam of the active unit.

6 When you have completed reviewing the Node Maintenance page, return to step 2.

7 Review the System Status page and use the following table to review the descriptions of the various fields of the System Status page:

Note: The Chassis Information panel is not automatically refreshed.

Chassis Information

Self Test	Chassis Subsystems
Self tests passed.	Chassis subsystems OK.

CPU Load

1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.02	0.01	0.00	10.00	20.00	40.00

CPU Utilization

5 mins. Utilization average	20 mins. Utilization average	30 mins. Utilization average	Minor alarm threshold 5 min.	Major alarm threshold 20 min.	Critical alarm threshold 30 min.
0.77	0.62	0.62	95.00%	99.00%	99.00%

Process Information

Number of processes	Number of zombie process(es)	Zombie		
		Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
165	0	5	10	15

Memory Information

Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)
3,787.31	2,951.86	3,539.29	500.00	250.00	100.00

Field	Description
Chassis information: Self Test	Indicates the status of the self test performed on the platform at boot up.
Chassis information: Chassis Subsystems	Indicates the status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections.
CPU Information: load average	Indicates the 1, 5 and 15 minute load averages for the CPU utilization.
CPU information: load average threshold values	Indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
Chassis Utilization: Utilization average	Indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.
Chassis Utilization: alarm threshold values	Indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.
Process Information: Number of Processes	Indicates the total number of processes (non-threaded) that are running on the Policy Controller Platform.
Process Information: Number of zombie processes	Indicates the number of defunct or terminated NCGL zombie processes. ***Note:*** A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources.
Process Information-zombie: minor alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded.

Field	Description
Process Information-zombie: major alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded.
Process Information-zombie: critical alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded.
Memory Information: Total Memory (MB)	The total amount of RAM installed on the motherboard of each Policy Controller unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	The amount of memory available unallocated for use.
Memory Information: Available memory (MB)	The amount of memory available for programs.
Memory Information: minor alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised.
Memory Information: major alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised.
Memory Information: critical alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised.

8 When you have completed reviewing the System Status, return to step 2.

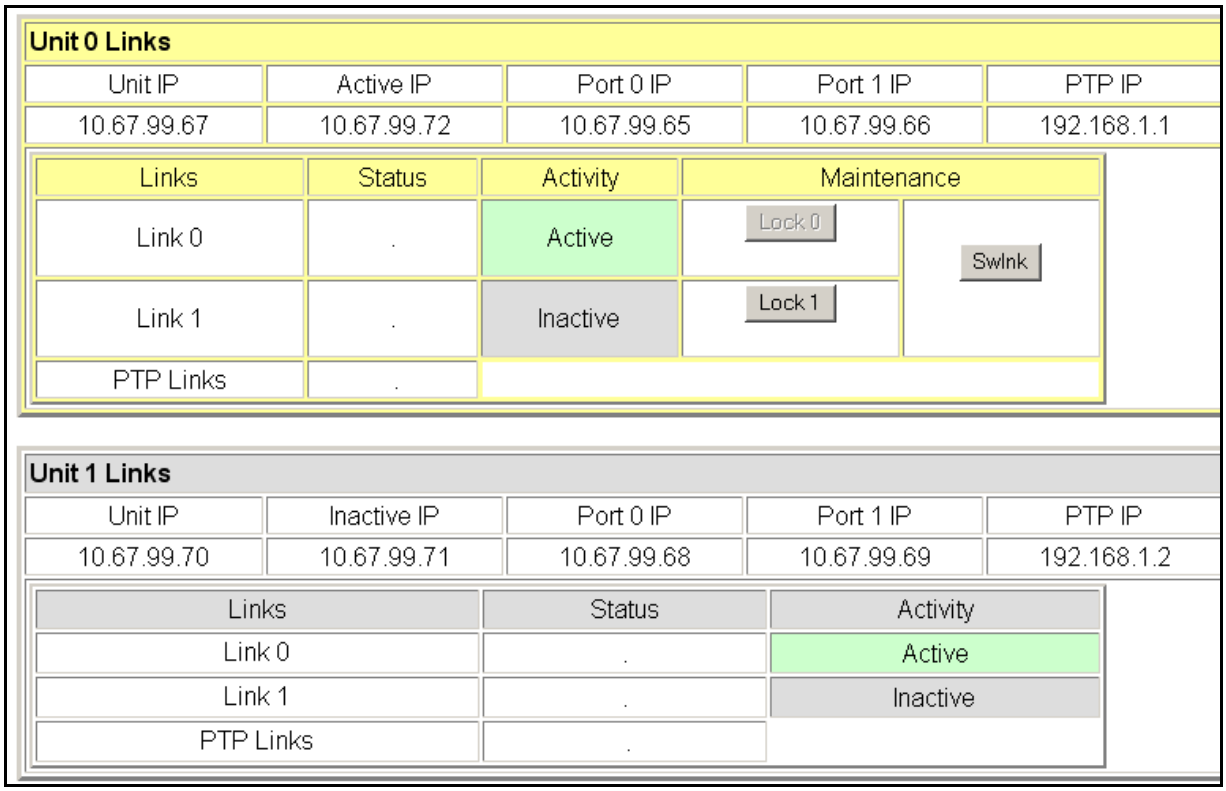
9

ATTENTION

Do not perform link management activities such as Lock, Suspend or Swlink using this procedure. Refer to the Policy Controller Security and Administration NTP, NN10434-611, to perform these activities.

Review the Network Connectivity page and use the following table to review the description of the various fields of the Network Connectivity page:

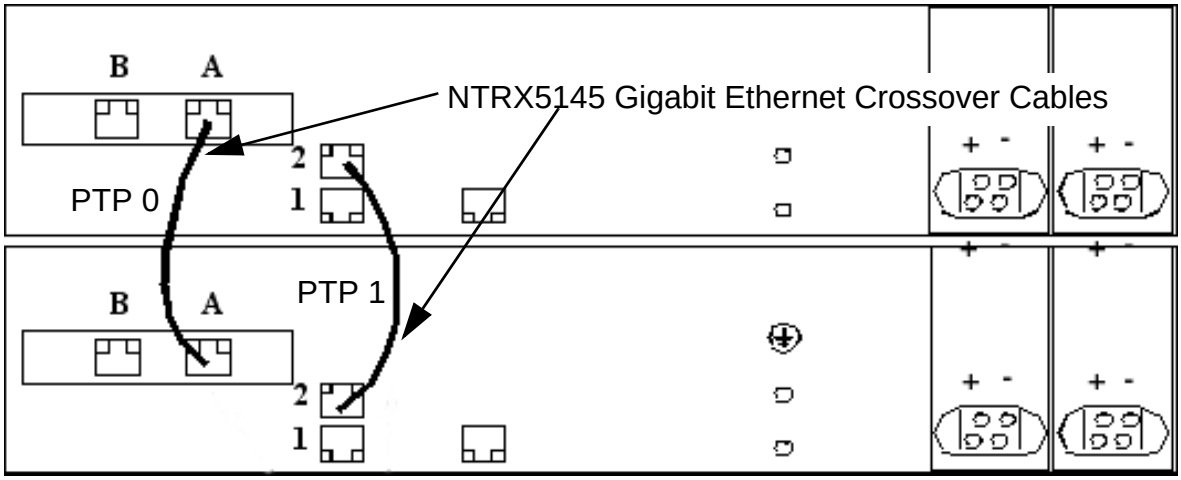
Note: The Network Connectivity panel is refreshed every 45 seconds.



Field	Description
Unit 0,1 Links	Indicates which ethernet IP links are installed on the Policy Controller units (each unit has two links).
Unit 0,1 Status	Indicates the status of the ethernet links.

Field	Description
Unit 0,1 Activity	Indicates the activity status of the ethernet links; either active or inactive.
Unit 0,1 Maintenance	Indicates the maintenance actions that can be performed on the ethernet links; either Lock, Unlock or Swlink. Refer to the Policy Controller Security and Administration NTP, NN10434-611, to perform link management.
Unit 0,1 PTP Links status	Indicates the status of the PTP links between both units in the node.
Unit IP	The network IP address of the Policy Controller unit.
Active IP	The IP address of the local (active) Policy Controller unit.
Inactive IP	The IP address of the mate (inactive) Policy Controller unit.
Port 0 IP	The IP address of the active or inactive ethernet port 0.
Port 1 IP	The IP address of the active or inactive ethernet port 1.
PTP IP	The IP address of the active or inactive PTP link.

Crossover and LAN ethernet cable connections for Policy Controller units



Ethernet Ports:

Ports 1 and B (both sets) go to CS-LAN Switch

Ports 2 (PTP1) and A (PTP0) are point-to-point connections between Session Server units

10 Review the Disk Services page and use the following table to review the description of the various fields of the Disk Storage page:

Note 1: The Disk Services panel does not update automatically. Click the **Disk Services** link again to update it.

Note 2: To create and remove file systems, refer to applicable procedures in the Policy Controller Configuration Management NTP, NN10432-511.

RAID Array Status

Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	.	.	.	Array is operating normally
ntvg	68.26	.	.	.	Array is operating normally

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	68.37	.	Remove
1	68.37	.	Remove

Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Minor Alarm Threshold (%)	Major Alarm Threshold (%)	Critical Alarm Threshold (%)
	/	.	61.47	58.29	100.00	0.00	0.00	85.00	90.00	95.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-	-
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85.00	90.00	95.00
No	/opt/apps	.	507.31	314.31	62.00	193.00	38.00	-	-	-
Yes	/tmp	.	123.31	0.31	1.00	123.00	99.00	85.00	90.00	95.00
Yes	/var/log	.	507.31	9.61	2.00	497.71	98.00	85.00	90.00	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-	-
No	/opt/apps/webint	.	1,494.00	209.78	15.00	1,284.22	85.00	-	-	-
No	/opt/apps/database	.	10,006.00	48.19	1.00	9,957.81	99.00	-	-	-
No	/opt/apps/logs	.	507.31	206.34	41.00	300.98	59.00	-	-	-
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	-	-	-

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

Volume Group Information

Volume Group Name	Volume Group Size (GB)	Total Space Allocated (GB)	Total Space Allocated (%)	Total Space Available (GB)	Total Space Available (%)
ntvg	68.22	23.84	34.95	44.38	65.05

Field	Description
RAID Array Status: Name	Indicates the name of each RAID-1 array in the system.
RAID Array Status: Size (GB)	Indicates the size of the partition in gigabytes.
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. -Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	Indicates the service status of disk 0.
RAID Array Status: Disk 1	Indicates the service status of disk 1.
RAID Array Status: Status	Indicates the status of the array. Values are: - The array is operating normally - Missing - Failed - Rebuild.
Disk Maintenance: Disk Number	Indicates the disk number in the array; 0 or 1.
Disk Maintenance: Disk Size (GB)	Indicates the total capacity of the disk drive in gigabytes.
Disk Maintenance: Disk State	Indicates the installation state of the disk.
Disk Maintenance: Disk Action	Indicates whether a hard disk can be inserted into the operating system. For more information about the **Remove** and **Insert** commands, refer to *Upgrading the Policy Controller*, NN10431-461.
Filesystem Information: Monitor	Indicates the status of individual filesystems on the disk array. For more information about the **Monitor** command, refer to procedures in the *Policy Controller Configuration Management*, NN10432-511.
Filesystem Information: Filesystem Name	Indicates the name of the filesystem on the disk array. Some filesystem names are reserved.

Field	Description
Filesystem Information: Test Results	Indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.
Filesystem Information: Total Space (MB)	Indicates the total amount of disk space (in MB) allocated for this filesystem.
Filesystem Information: Total Space Used (MB)	Indicates the total amount of disk space (in MB) in use on this file system.
Filesystem Information: Total Space Used (%)	Indicates the total amount of disk space (in %) in use on this file system.
Filesystem Information: Total Space Available (MB)	Indicates the percent of total disk space (in MB) free for use on this filesystem.
Filesystem Information: Total Space Available (%)	Indicates the amount of disk space (in %) available for use by platform processes and applications.
Filesystem Information: Minor Alarm Threshold (%)	Indicates the maximum amount of disk space (in percent) that can be utilized before a minor alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Major Alarm Threshold (%)	Indicates the maximum amount of disk space (in percent) that can be utilized before a major alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Critical Alarm Threshold (%)	Indicates the maximum amount of disk space (in percent) that can be utilized before a critical alarm is raised indicating that the set threshold has been exceeded.
Volume Group Information: Volume Group Name	Indicates the name of the volume group in the array.
Volume Group Information: Volume Group Size (GB)	Indicates the total size of the volume group in the array.
Volume Group Information: Total Space Allocated (GB)	Indicates the amount of volume group space, in gigabytes, currently allocated to filesystems.
Volume Group Information: Total Space Allocated (%)	Indicates the amount of volume group space (in %) currently allocated to filesystems.

Field	Description
Volume Group Information: Total Space Available (GB)	Indicates the amount of unallocated volume group space, in gigabytes, available for filesystems.
Volume Group Information: Total Space Available (%)	Indicates the amount of unallocated volume group space (in %) available for filesystems.

11 When you have completed reviewing the Disk Services page, return to step 2.

12 Review the Services page and use the following table to review the description of the various fields of the Platform Services page:

Note: The Services panel does not update automatically. Click the **Services** link again to update it.

Network Services

Number of Active Command Line Sessions	Number of Clients with Active Web Sessions
3	2

NTP Information

Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.162.68 in sync	undefined	undefined	1	1	1

Field	Description
Network Services: Number of Active Command Line Sessions	Indicates the number of command line interface (CLI) sessions (both remote and local) on the Policy Controller.
Network Services: Number of Clients with Active Web Sessions	Indicates the number of clients running one or more web GUI sessions.
NTP Information: Server1 - Server 3	Indicates the IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection.

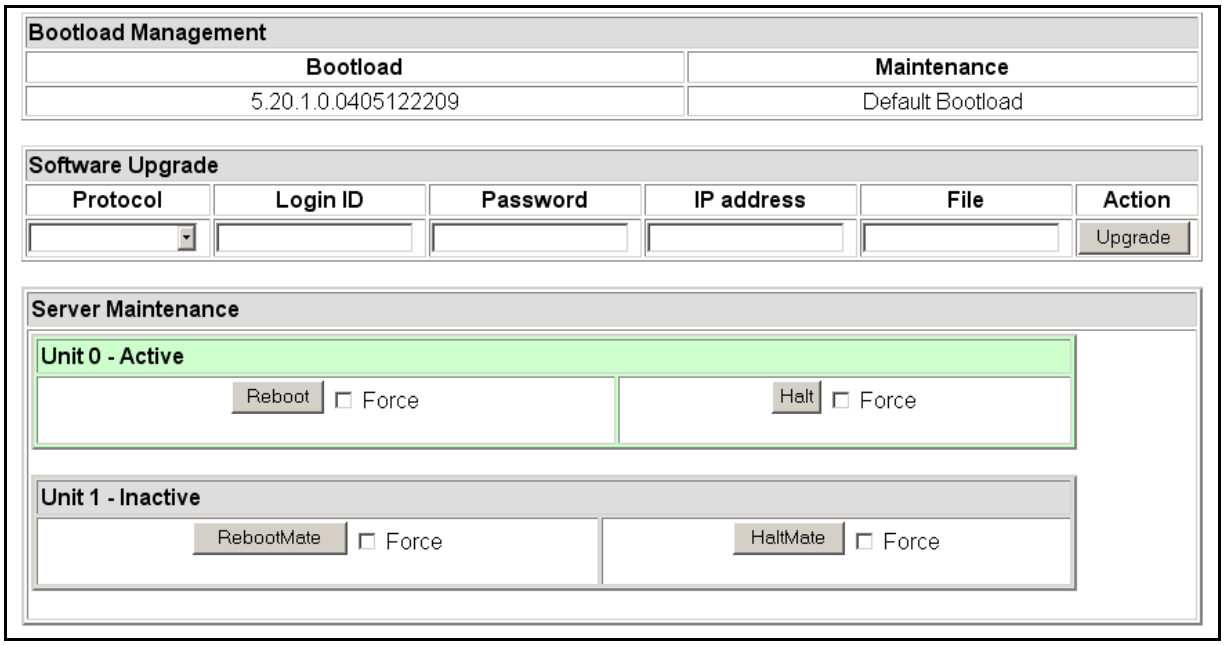
Field	Description
NTP Information: Total Number of Servers	Indicates the number of NTP servers registered with the CS-LAN network.
NTP Information: Accessible Servers	Indicates the number of NTP servers accessible to the Policy Controller.
NTP Information: Synchronized Servers	Indicates the number of NTP servers to which the Policy Controller is synchronized.

13 When you have completed reviewing Platform Services status, return to step 2.

14

ATTENTION
To perform software upgrades to the NCGL platform, refer to *Upgrading the Policy Controller*, NN10431-461.

Review the Administration page and use the following table to review the description of the various fields of the Platform Admin page:



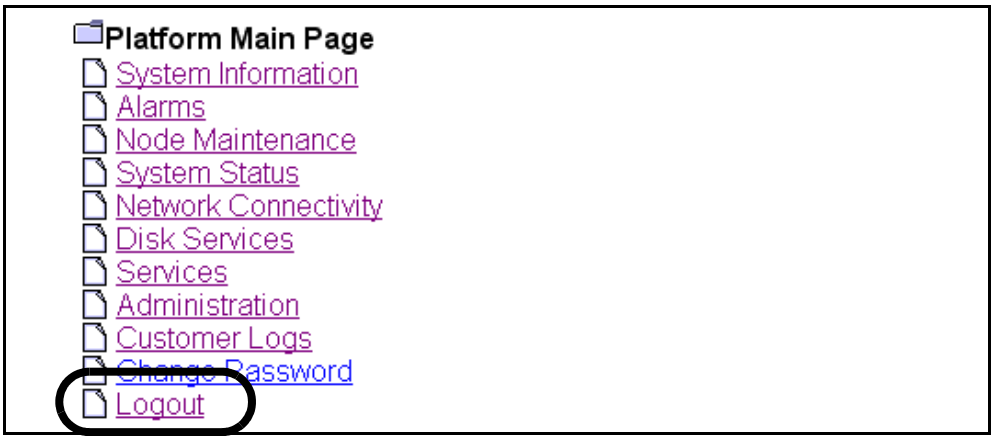
Field	Description
Bootload Setting: Bootload	Indicates the load ID for the NCGL platform software load.
Bootload Setting: Maintenance	Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.
Software Upgrade: Protocol	Indicates the file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM.
Software Upgrade: Login ID	If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.
Software Upgrade: Password	If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.
Software Upgrade: IP Address	If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.
Software Upgrade: File	The target upgrade load path and filename is entered here.
Software Upgrade: Action Upgrade button	The **Upgrade** button initiates a platform NCGL upgrade. Refer to *Upgrading the Policy Controller*, NN10431-461, for instructions on using this function.
Server Maintenance (active and inactive units)	To execute the **Reboot**, **Halt**, **Rebootmate** and **Haltmate** functions, refer to the applicable procedures in *Policy Controller Security and Administration*, NN10434-611.

Note: The Administration panel does not update automatically. Click the link again to update it.

15 When you have completed reviewing Platform Admin page, return to step 2, or continue with step 16.

16 If you want to logout from platform GUI, click the **Logout** button.

You are returned to the login page



17 The procedure is complete.

View the operational status of the Policy Controller application

Purpose of this procedure

Use the following procedure to view the service status of the Policy Controller application. This procedure may be used as a standalone task or as part of a high-level activity.

Limitations and restrictions

This procedure provides instructions for determining the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure *View the operational status of a Policy Controller NCGL platform* in NTP 10432-911.

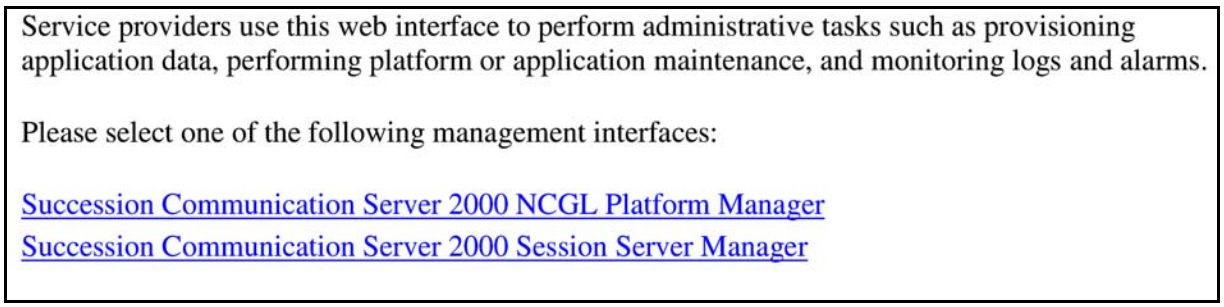
Prerequisites

There are no prerequisites for this procedure.

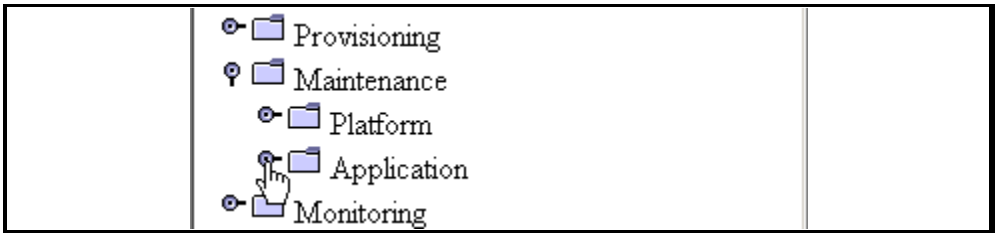
Action

At the Policy Controller Launch Point

1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

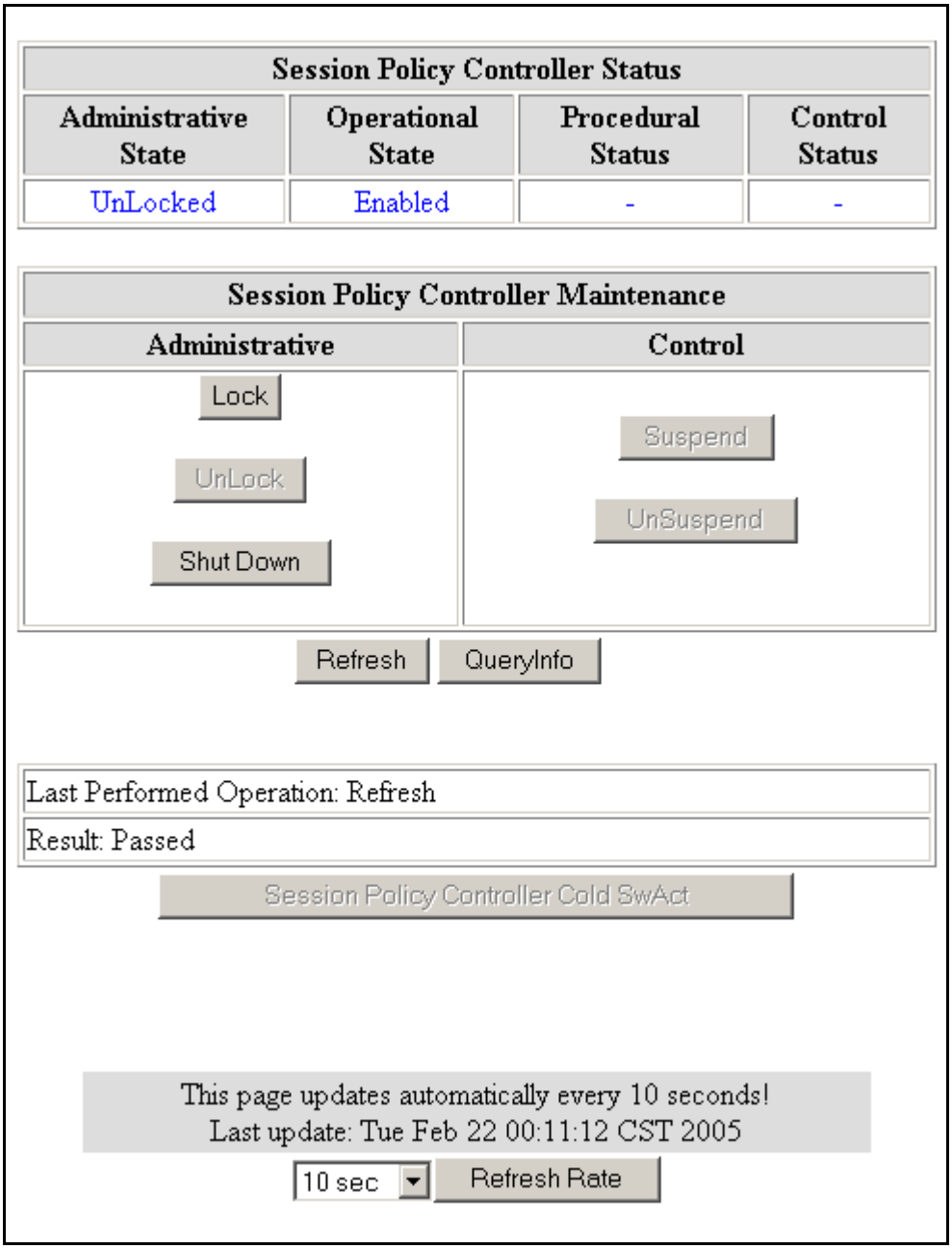


2 At the Policy Controller folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click on the **Session Policy Controller** folder to open it.

4 Monitor the status of the Policy Controller application on the active Policy Controller node from this view.



Note: This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button or manually refresh the page by clicking the **Refresh** button.

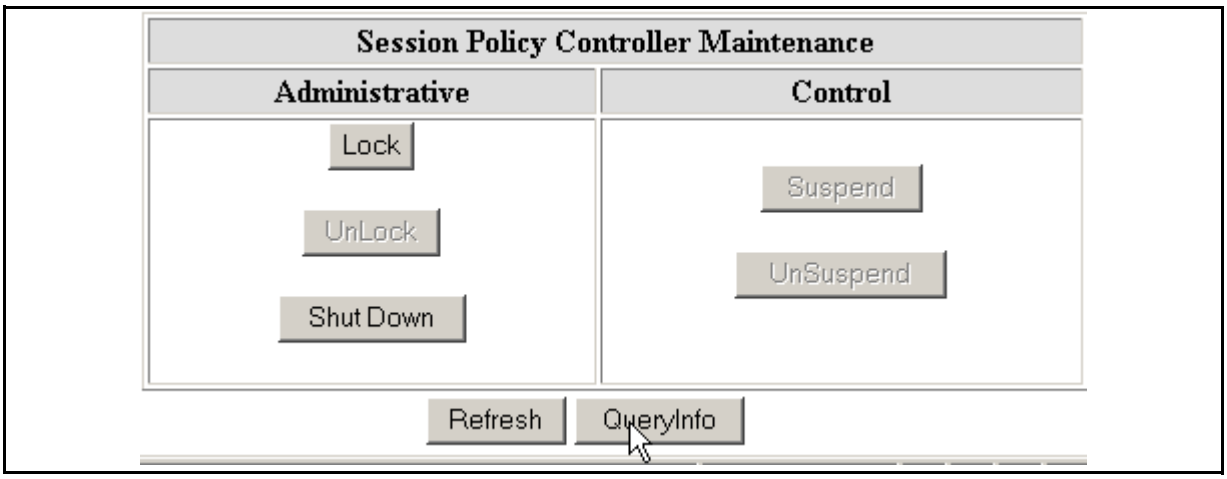
5 Refer to section Interpreting Policy Controller application status and maintenance fields on page 45 to review the description of the various fields of this view.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to *Policy Controller Security and Administration*, NN10434-611.

6 To perform available Policy Controller application maintenance activities, refer to the following procedures found in *Policy Controller Security and Administration*, NN10434-611:

- Lock the Policy Controller application
- Unlock the Policy Controller application
- Suspend the Policy Controller application
- Unsuspend the Policy Controller application
- Shutdown the Policy Controller application
- Cold SwAct the Policy Controller application

7 To view the number of active calls currently being handled by the application and the sync status of the Policy Controller units, click the **QueryInfo** button.



8 The procedure is complete.

Interpreting Policy Controller application status and maintenance fields

Use the following table to assist you in interpreting the Policy Controller Status area.

Policy Controller node status field descriptions

Field	Description
Unit Connection Status Bar	Indicates which Policy Controller unit in the node the CS 2000 Policy Controller Manager is connected to.
Unit Number	indicates the units in the Policy Controller node, (labeled 0 and 1) and a maximum of one node on the Call Server-LAN
Activity State	indicates which unit is Active and which is Inactive (standby), also an indirect indicator of fault-tolerant status, assuming both units are operational.
Operational State	indicates the service status of each Policy Controller unit (either Enabled or Disabled).

Use the following table to assist you in interpreting the Policy Controller status area.

Policy Controller application Status field descriptions

Field	indication
Administrative State	Locked, Unlocked, ShuttingDown
Operational State	Enabled or Disabled
Procedural Status	Terminating or -
Control Status	Suspended or -

Use the following table to assist you in interpreting the Policy Controller area's CCITT X.731-style and related DMS-style status indicators:

Policy Controller Maintenance field descriptions and interpretation of service states

Administrative State	Operational State	Procedural Status	Control Status	DMS style Service States
Locked	Disabled	-	Suspended	Offline (OFFL)
Locked	Enabled	-	-	Manual Busy MANB)
Locked	Enabled	Terminating	-	Manual Busy Transitioning (MANBP)
Unlocked	Enabled	-	-	In Service (INSV)
Unlocked	Disabled	-	-	System Busy (SYSB)
Shutting Down	Enabled	-	-	Going out of service (INSVD)

Note: (-) indicates a status of in-service

Verify synchronization status of Policy Controller units

Purpose of this procedure

Use this procedure to determine the synchronization status of the Policy Controller units. This procedure may be used as a standalone task or as part of a higher level activity.

Limitations and restrictions

There are no restrictions for performing this procedure.

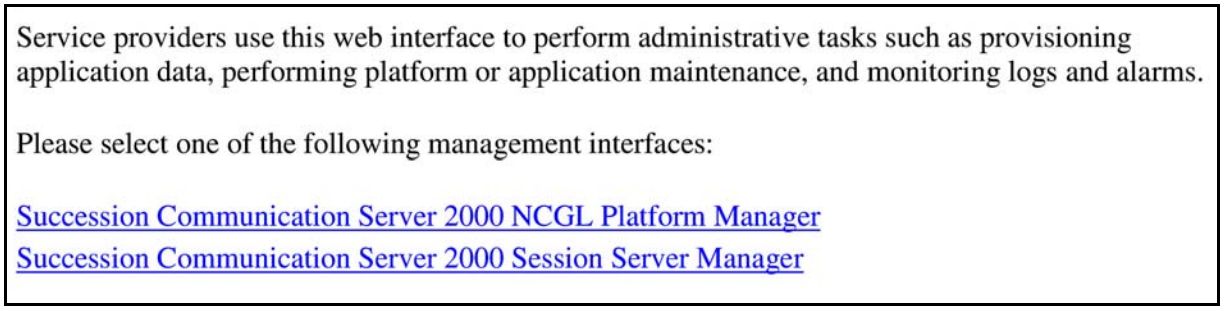
Prerequisites

None

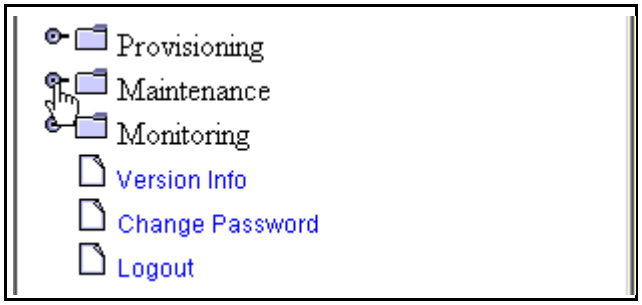
Action

At the CS 2000 Policy Controller Launch Point

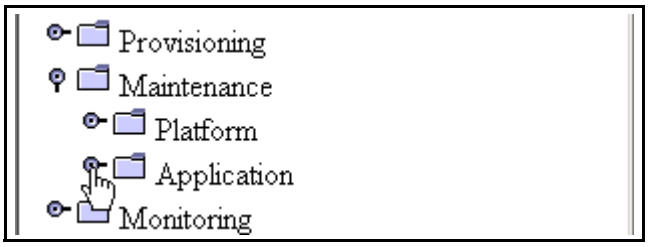
1 Select ***Succession Communication Server 2000 Policy Controller Manager*** from the launch point menu.



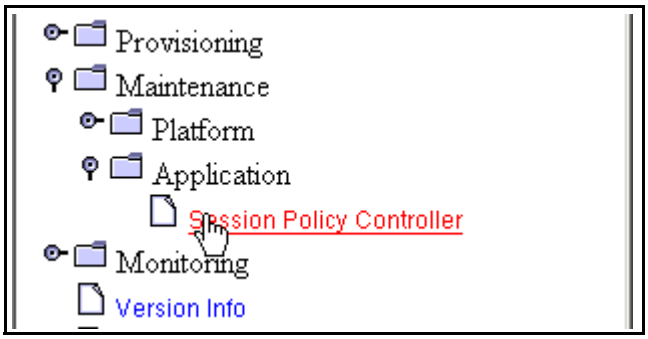
2 At the Policy Controller folder, click the **Maintenance** folder.



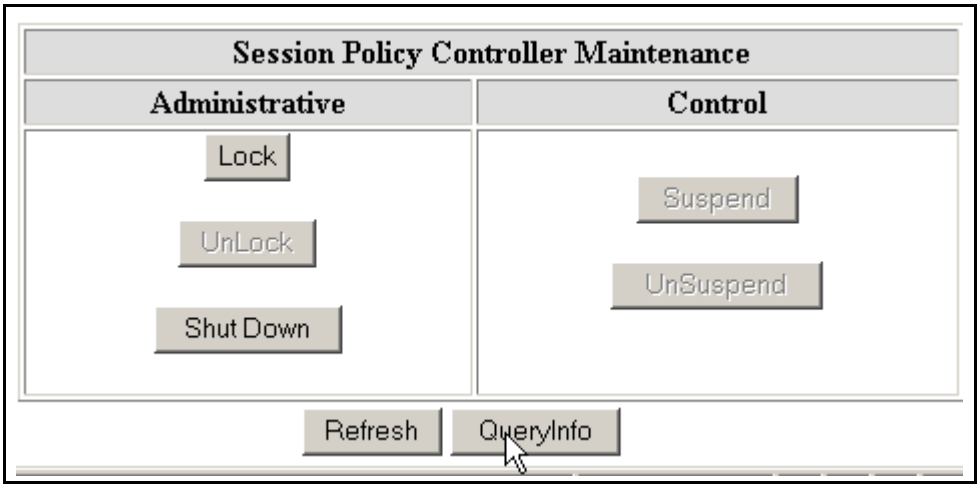
3 Next click the **Application** folder.



4 Click on the **Session Policy Controller** folder to open it.

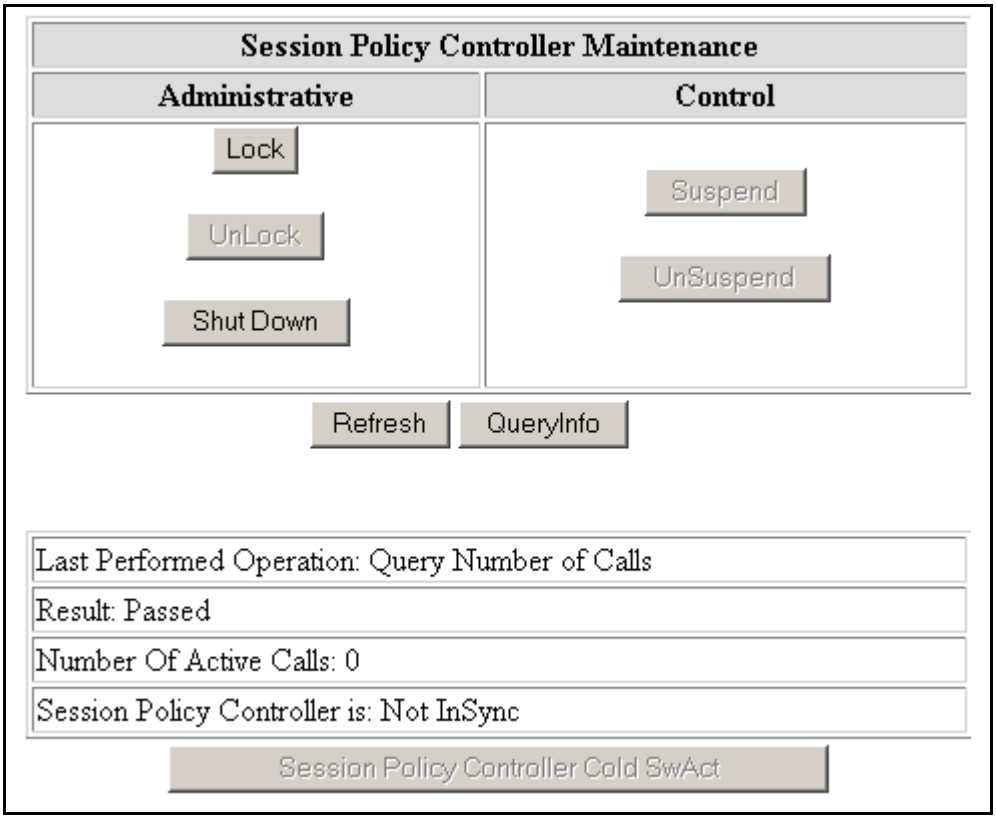


5 At the bottom of the Session Policy Controller Maintenance panel, locate and click the **QueryInfo** button.



6 The synchronization status of the units is displayed at the bottom of the query results panel.

If the units are not in sync, execute procedure *View Policy Controller alarms* in NTP 10432-911.



7 The procedure is complete.