MG 9000 Security and Administration

Security management procedures

This document addresses security management and authentication for user access to the MG 9000 Manager and general administration information and permissions for the MG 9000 Manager. In addition, security and configuration information for the local craft interface (LCI) is presented.

Security in the MG 9000 Manager

The MG 9000 Manager uses Pluggable Authentication module (PAM) for user authentication. PAM integrates various integration technologies into system entry systems such as login, password, rlogin, telnet, and ftp. The MG 9000 Manager interacts with any pluggable authentication technology of the operating company's choosing.

A mechanism to encrypt communications between the GUI client and the mid-tier server is enabled, providing protection for userids and passwords sent between the client and the mid-tier.

Communication between the GUI client and the MG 9000 mid-tier server can traverse customer firewall configurations. This is facilitated by sending MG 9000 Manager GUI client messages to a SOCKS proxy listening port on the MG 9000 mid-tier server. The default recommended port number on the mid-tier is 10080. On the client side, the port must be configured. For information on configuring the SOCKS proxy ports, refer to .

> *Note:* The firewall must be provided by the user. The SOCKS proxy provides the tunneling capability through the firewall on configurable ports.

Authentication

The MG 9000 Manager GUI client authentication is controlled by the MG 9000 Manager mid-tier process. In a T1400 configuration, the MG 9000 Manager mid-tier process runs on a stand-alone server; however, in an N240 configuration, both the MG 9000 Manager mid-tier and EM

processes are co-resident. When a GUI client is launched, the user will be prompted to enter the userid and password. This userid and password will then be authenticated by the appropriate authentication module on the MG 9000 Manager mid-tier (T1400) or server (N240) as determined by the PAM configuration file on the mid-tier. Each authentication attempt, whether success or failure, is recorded in an MG 9000 Manager log report.

The DTA client authentication is controlled by the MG 9000 Manager server process. DTA client login and password will be authenticated by the appropriate authentication module on the MG 9000 Manager server, as determined by the PAM configuration file on the server. Some authentication modules may require userid/password to contain both upper and lower case characters. DTA clients can no longer assume the userid/password to be in uppercase.

Each time an MG 9000 Manager client attempts to log into the system, an authentication log is generated. The default location for logs is in the /var/log/securitylog directory of the SSPFS machine where the authentication took place. For example, since the mid-tier controls the GUI client authentication, all login attempts from the GUI clients will be on the mid-tier SSPFS machine. Likewise, since DTA client login is controlled by the master server, logs for DTA login attempts will be on the master server SSPFS machine.

The following figure shows the login window that appears at the element manager.

MG 9000 Manager login window

Authorization and permissions

When MG 9000 Manager PAM is in effect, all users must belong to the user group "succssn" in addition to one or more of the groups listed in the following table. The "succssn" group is a primary group that provides the same access as "emsro" group. Predefined permissions are associated with each of the groups. When a user login is created by an administrator, it can be placed in a single primary group or in a primary and multiple secondary groups. For a user login to have access to the MG 9000 Manager, the user must belong to primary group "succssn". Being in "succssn" allows the user read only privileges. If a user login is in primary group "succssn" and a secondary group of "emsro", the user still has only has read only privileges. So, there is no difference between a user in "succssn" and one that is in "succssn" and "emsro". However, a user that is just in "emsro" does not have MG 9000 Manager access.

Group and permission mapping

User groups	Privilege description	Permissions
succssn	read only	access to MG 9000 Manager
succssn, emsro	read only	nortel.ems.ro

Group and permission mapping

User groups	Privilege description	Permissions
succssn, emsadm	administration	nortel.ems.adm
		nortel.ems.iprov
		nortel.ems.mtc
		nortel.ems.sprov
		nortel.ems.ro
succssn, emsrw	infrastructure provisioning	nortel.ems.iprov
		nortel.ems.mtc
		nortel.ems.sprov
		nortel.ems.ro
succssn, emsmtc	maintenance	nortel.ems.mtc
		nortel.ems.ro
succssn, emssprov	subscriber provisioning	nortel.ems.sprov
		nortel.ems.ro

The following permissions apply as shown in the previous table:

- emsadm - has all the ems permissions
- emsrw - has all the ems permissions except the nortel.ems.adm
- all groups - have read only permissions

The MG 9000 Manager outputs an error message when an action is attempted at the MG 9000 Manager by an unauthorized user. If the user is not in the user group, the system will block the action and output the following message.

MG 9000 Manager authorization error message

The following table shows the actions mapped to user groups

MG 9000 Manager user group and actions mapping

Group	Actions	
emsadm	Delete VMG from MG 9000 and MG 9000 Manager only Maintenance - Cutover Tool SLOA - Configure Termination	In addition to all actions under emsrw, emsmtc, emssprov, and emsro groups
emsrw	Provision NE Modify NE Delete NE Import NE	Floating IP Address Manager Software Upgrade - for cards: DCC (OC-3 and DS1-IMA), ITP, ITX, ABI, and DS1 Software Download Manager - for cards: XDSL and MTA Manage Thresholds for DCC-OC3 Provision Frame Location Information

MG 9000 Manager user group and actions mapping

Group	Actions	
emsmtc	Tools Discover NE Audit NE Bandwidth Manager DTA Test Manager MTA Test Manager Fan I/Os Circuits: • Administrative state changes — lock — unlock — forcedlock — forcedunlock • Configuration state changes — online — offline • Update Port/Circuit Attributes • APS maintenance • IMA Port — Port Attribute — Port Status — Link Attribute — Link Status • Maintenance - Diagnostic • Software Download Manager • PLOA ATM Diagnostic • DTA/TL1 Commands	Cards: • Administrative state changes — lock — unlock — forcedlock — forcedunlock • Configuration state changes — online — offline — deprovision — reinitialize • Restart • Maintenance - Diagnostic • Maintenance - Swact • Maintenance - APS Provisioning • Maintenance - Carrier Test • Maintenance - Pattern Test • Edit IMA Group • Software Download Template Table • SIC I/Os • BIP I/Os Circuit listing for DCC-IMA, WLC, SAA, XDSL, and DS1 Manage Thresholds for DCC-OC3 Coefficient Table Manager for GLC In addition to all actions under emsro group

MG 9000 Manager user group and actions mapping

Group	Actions	
emsmtc or emssprov	The following actions may be performed by users from either the emsmtc or the emssprov group: • Persist NE • Save SLOA Services • Save PLOA Services • DCC port — lock, unlock, forcedlock, forcedunlock — onlline, offline — Capture Rx Path Trace ID • Circuit Listing for DCC-OC3	• DS1 Port — lock, unlock, forcedlock, forcedunlock — online, offline — update circuit id and port attributes — channelization — create bundles — delete bundles — lock, unlock bundles — update bundle attribute - such as, RBS mode Plus all actions under emsro group.
emssprov	• XDSL — Global Traffic Descriptors — XDSL Services Provisioning — XDSL Services Deprovisioning • PLOA — Create PLOA Services — Delete PLOA Services — Lock, Unlock PLoA Services	• SLOA — Create VMG — Delete VMG — Configure VMG — Delete Termination — Create ESA Service Code Translation — Delete ESA Service Code Translation — Enable ESA (Basic and Enhanced) — Disable ESA (Basic and Enhanced) Plus all actions under emsro group.
emsro	Refresh Subnet View Alarm Browser Performance Browser View NE Properties Refresh icon	Audit Alarm View IMA Group Query IBIP threshold attributes View PLoA Service Properties All GUI View Refresh

The following table shows the MG 9000 Manager actions and the permissions required for each action. The user group allowed to perform the action is noted by an X in the applicable user group column.

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
Subnet						
Refresh Subnet View	nortel.ems.ro	X	X	X	X	X
Global Traffic Descriptors	nortel.ems.sprov	X	X		X	
Tools	nortel.ems.mtc	X	X	X		
Alarm Browser	nortel.ems.ro	X	X	X	X	X
Performance Browser	nortel.ems.ro	X	X	X	X	X
Node						
Provision NE	nortel.ems.iprov	X	X			
View NE Properties	nortel.ems.ro	X	X	X	X	X
Modify NE	nortel.ems.iprov	X	X			
Discover NE	nortel.ems.mtc	X	X	X		
Delete NE	nortel.ems.iprov	X	X			
Audit NE	nortel.ems.mtc	X	X	X		
Refresh Icon	nortel.ems.ro	X	X	X	X	X
Audit Alarm	nortel.ems.mtc	X	X	X	X	X
Persist NE	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
Import NE	nortel.ems.iprov	X	X			

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
Frame						
Provision Frame Location Information	nortel.ems.emsrw nortel.ems.emsadm	X	X			
Software Upgrade	nortel.ems.iprov	X	X			
Software Image	nortel.ems.iprox	X	X			
Save SLOA Service	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
Save PLOA Service	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
BandWidth Manager	nortel.ems.mtc	X	X	X		
Private Line Services Manager	Refer to "Private Line Services Manager" later in this table					
Switch Line Services Manager	Refer to "Switch Line Services Manager" later in this table					
DTA Test Manager	nortel.ems.mtc	X	X	X		
MTA Test Manager	nortel.ems.mtc	X	X	X		
Floating IP Address Manager	nortel.ems.iprov	X	X			
FAN I/Os	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
Shelf						
Maintenance -	nortel.ems.mtc	X	X	X		
- APS Provisioning	nortel.ems.mtc	X	X	X		
DS1-IMA -						
- View IMA Group	nortel.ems.ro	X	X	X	X	X
- Edit IMA Group	nortel.ems.mtc	X	X	X		
Cards						
DCC - OC3						
- Software Upgrade	nortel.ems.iprov	X	X			
- Manage Thresholds	nortel.ems.mtc	X	X	X		
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Maintenance - Swact	nortel.ems.mtc	X	X	X		
- Circuit Listing	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline	nortel.ems.mtc	X	X	X		
- Reinitialize	nortel.ems.mtc	X	X	X		
- Restart - current, primary	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
DCC - DS1-IMA						
- Software Upgrade	nortel.ems.iprov	X	X			
- Manage Thresholds	nortel.ems.mtc	X	X	X		
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Maintenance - Swact	nortel.ems.mtc	X	X	X		
- Maintenance - Carrier Test	nortel.ems.mtc	X	X	X		
- Maintenance - Pattern Test	nortel.ems.mtc	X	X	X		
- Circuit Listing	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline	nortel.ems.mtc	X	X	X		
- Reinitialize	nortel.ems.mtc	X	X	X		
- Restart - current, primary	nortel.ems.mtc	X	X	X		
ITP and ITX						
- Software Upgrade	nortel.ems.iprov	X	X			
- Manage Thresholds	nortel.ems.mtc	X	X	X		
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Maintenance - Swact	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline / reinitialize (ITP only) / deprov	nortel.ems.mtc	X	X	X		
- Restart - current, primary	nortel.ems.mtc	X	X	X		
ABI						
- Software Upgrade	nortel.ems.iprov	X	X			
- Manage Thresholds	nortel.ems.mtc	X	X	X		
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Maintenance - Swact	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline / reinitialize / deprov	nortel.ems.mtc	X	X	X		
- Restart - current, primary	nortel.ems.mtc	X	X	X		
WLC -						
- Software Download Template Table	nortel.ems.mtc	X	X	X		
- Circuit Listing	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- online / offline / deprov	nortel.ems.mtc	X	X	X		
GLC -						
- Coefficient Table Manager	nortel.ems.mtc	X	X	X		
- Circuit Listing	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline / deprov	nortel.ems.mtc	X	X	X		
SAA -						
- Circuit Listing	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline / deprov	nortel.ems.mtc	X	X	X		
XDSL 8x8						
- Software Download Manager	nortel.ems.iprov	X	X			
- Software Download Template Table	nortel.ems.mtc	X	X	X		
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Circuit Listing	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline / deprov	nortel.ems.mtc	X	X	X		
- Restart - cold, unconditional	nortel.ems.mtc	X	X	X		
DS1						
- Software Upgrade	nortel.ems.iprov	X	X			
- Manage Thresholds	nortel.ems.mtc	X	X	X		
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Circuit Listing	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online / offline / reinitialize / deprov	nortel.ems.mtc	X	X	X		
- Restart - current, primary, backup	nortel.ems.mtc	X	X	X		
MTA						
- Software Download Manager	nortel.ems.iprov	X	X			
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online /offline / deprov	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- Restart - current, primary	nortel.ems.mtc	X	X	X		
SIC						
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc	X	X	X		
- online/offline/deprov	nortel.ems.mtc	X	X	X		
- SIC I/Os	nortel.ems.mtc	X	X	X		
BIP - IBPAP, IBPAR, IBPDT, IBPCS						
- BIP I/Os	nortel.ems.mtc	X	X	X		
- Query	nortel.ems.ro	X	X	X	X	X
- lock/unlock	nortel.ems.mtc	X	X	X		
- online / offline	nortel.ems.mtc	X	X	X		
Circuits						
OC3 Port						
- Maintenance - APS maintenance - circuit id, circuit attributes	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- online / offline	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- Capture Rx Path Trace ID	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
STS1 Port						
- Maintenance - OC3 attributes / STS1 Path	nortel.ems.mtc	X	X	X		
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- online / offline	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
IMA Port and Link						
- Update Port Attributes	nortel.ems.mtc	X	X	X		
- Port attribute	nortel.ems.mtc	X	X	X		
- Port Status	nortel.ems.mtc	X	X	X		
- Link Attribute	nortel.ems.mtc	X	X	X		
- Link Status	nortel.ems.mtc	X	X	X		
WLC Circuit						
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Maintenance - Cutover Tool	nortel.ems.adm	X				
- lock/unlock	nortel.ems.mtc	X	X	X		
SAA Circuit						
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- Maintenance - Cutover Tool	nortel.ems.adm	X				
- Software Download Manager	nortel.ems.mtc	X	X	X		
- lock / unlock	nortel.ems.mtc	X	X	X		
XDSL - voice circuit						
- Maintenance - Diagnostic	nortel.ems.mtc	X	X	X		
- Maintenance - Cutover Tool	nortel.ems.adm	X				
- lock / unlock	nortel.ems.mtc	X	X	X		
XDSL - data circuit						
- lock / unlock	nortel.ems.mtc	X	X	X		
- XDSL Services Provisioning	nortel.ems.sprov	X	X		X	
- XDSL Services Deprovision	nortel.ems.sprov	X	X		X	
DS1 Port						
- lock / unlock / forcedlock / forcedunlock	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- online / offline	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- update circuit id and port attributes	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- channelization	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- create bundles	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- delete bundles	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- lock / unlock bundles	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- update bundle attribute - RBS mode etc.	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
Private Lines Services Manager						
- Create	nortel.ems.sprov	X	X		X	
- Delete	nortel.ems.sprov	X	X		X	
- Lock / Unlock	nortel.ems.sprov	X	X		X	
- Properties	nortel.ems.ro	X	X	X	X	X
- Diagnostic (ATM)	nortel.ems.mtc	X	X	X		
Switched Lines Services Manager						
Create VMG	nortel.ems.sprov	X	X		X	
Delete VMG	nortel.ems.sprov	X	X		X	
Configure VMG	nortel.ems.sprov	X	X		X	
Delete Termination	nortel.ems.sprov	X	X		X	
Configure Termination	nortel.ems.sprov	X				

MG 9000 Manager GUI actions/permissions user groups mapping

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
Create ESA Service Code Translation	nortel.ems.sprov	X	X		X	
Delete ESA Service Code Translation	nortel.ems.sprov	X	X		X	
Enable ESA (Basic and Enhanced)	nortel.ems.sprov	X	X		X	
Disable ESA (Basic and Enhanced)	nortel.ems.sprov	X	X		X	
All GUI View Refresh	nortel.ems.ro	X	X	X	X	X

Configuration and maintenance of SOCKS proxy

This section address the configuration and maintenance procedures related to the SOCKS proxy running on the server where the mid-tier application is running.

Configuring SOCKS   Use the following procedure to configure the SOCKS proxy.

> *Note:* SOCKS ports are initially configured with default values. If the default values are used, no action is necessary.

Configuring the SOCKS proxy

At the MG 9000 Manager mid-tier server

1   To access the command line interface to configure the SOCKS proxy, type

```
 # cli
```

The system responds:

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

 X - exit

select -
```

2   To access the configuration menu, type 2

```
> 2
```

The system responds:

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
```

```
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
X - exit
```

3   To access Security Services Configuration, type 13

     > 13

The system responds:

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

 X - exit
```

4   To access SOCKS configuration, type 1

     > 1

The system responds:

```
Socks Configuration
 1 - config_socks (Modify Socks Security
Service)
 2 - list_socks (List Socks Security Service)

X - exit
```

5   To access the config_socks script, type 1

     > 1

The system responds:

```
The changes of the server side port is a
disruptive action.
If the server side port is changed, the SOCKS
server and all dependant applications must be
restarted.

SOCKS ports in all offices must be configured to
the same port.
Misconfiguration will cause EMS clients to not
function.

Proceed with caution.
```

```
Enter the port the Server side SOCKS Proxy will
listen on. Value must be
within [1025 - 65535].
Current value 10080[?,q]
```

6   Use the information in the following table to determine the next step.

If	Do
default values are used for the SOCKS ports	step 7
non-default values are used for the server and the client SOCKS proxy ports	step 8
configuring only the server side SOCKS proxy port	step 12
configuring only the client side SOCKS proxy port	step 14
the SOCKS configuration values are to be listed	step 17

7   To use the default SOCKS port values, respond to the system as follows.

Press the Enter key.

The system responds:

```
Leaving SERVER port at 10080
```

```
Enter the port the Client side SOCKS Proxy will
listen on. Value must be
within [1025 - 65535]. Current Value - 10090
[?,q]
```

Press the Enter key.

The system responds:

```
Leaving CLIENT port at 10090.
SOCKS is currently configured to:
        Server side SOCKS Proxy port: 10080
        Client side SOCKS Proxy port: 10090

=== "config_socks" completed successfully
```

Go to step 18.

8   To enter non-default values for the server and client SOCKS proxy ports, respond to the system as follows.

Enter the non-default server server side SOCKS proxy port number. For example,

```
> 2334
```

The system responds:

```
WARNING: Configuring the SOCKS server side port
requires a restart of the SOCKS server all
dependent applications, are you sure you want to
change the configuration? [y] [y,n,?,q]
```

9 To continue with changing the configuration, type Y

```
> Y
```

The system responds:

```
Enter the port the Client side SOCKS Proxy will
listen on. Value must be
within [1025 - 65535]. Current Value - 10090
[?,q]
```

10 Enter the new client side SOCKS proxy port number. For example,

```
> 3445
```

The system responds:

```
Warning: Clients already running Succession
GUI's must be restarted to use
this new port, are you sure you want to change
the configuration?
[y] [y,n,?,q]
```

Enter y

```
Configuring ports to:
          Server side SOCKS Proxy port to 2334
          Client side SOCKS Proxy port to 3445
```

```
WARNING: Configuring the Server Side socks port.
This will cause disruption of
service. Do you want to continue? [y] [y,n,?,q]
```

11 To continue with changing the configuration, type Y

```
> Y
```

The system responds:

```
Stopping NTSocks on Thu Jan 29 05:32:41 EST 2004
```

```
#####/tcp
```

```
SOCKS started successfully
```

```
The Server side SOCKS Proxy port has been
configured to 2334.
```

```
The Client side SOCKS Proxy port has been
configured to 3445.
```

```
=== "config_socks" completed successfully
```

Go to step 18.

12   To configure only the server SOCKS proxy port, respond to the system as follows.

Enter the new server SOCKS proxy port number. For example,

> 5555

The system responds:

```
WARNING: Configuring the SOCKS server side port
requires a restart of the
SOCKS server and all dependent applications, are
you sure you want to change
the configuration?  [y] [y,n,?,q]
```

13   To change the configuration, type Y.

> Y

The system responds:

```
Enter the port the Client side SOCKS Proxy will
listen on. Value must be within [1025 - 65535].
Current Value - 10090 [?,q]
```

Press the Enter key.

The system responds:

```
Leaving CLIENT port at 10090.
```

```
Configuring ports to:
```

```
Server side SOCKS Proxy port to 10080
```

```
Client side SOCKS Proxy port to 10090
```

```
WARNING: Configuring the Server Side socks port.
This will cause disruption of service. Do you
want to continue? [y] [y,n,?,q]
```

Enter Y.

The system responds:

```
Stopping NTSocks on Thu Jul 1 13:35:57 EDT 2004
```

```
10080/tcp
```

```
SOCKS started successfully
```

```
The Server side SOCKS Proxy port has been
configured to 10080.
```

```
=== "config_socks" completed successfully
```

14   To configure only the client side SOCKS proxy port, respond to the system as follows.

Press the Enter key.

The system responds:

```
Leaving SERVER port at 10080
```

```
Enter the port the Client side SOCKS Proxy will
listen on. Value must be within [1025 - 65535].
Current Value - 10090 [?,q]
```

15   To change the client side SOCKS proxy port number, enter the new port number. For example:

```
> 4445
```

```
Warning: Clients already running Succession
GUI's must be restarted to use this new port,
are you sure you want to change the
configuration? [y] [y,n,?,q]
```

16   To change the configuration, type Y.

```
> Y
```

The system responds:

```
Configuring ports to:
        Server side SOCKS Proxy port to 10080
         Client side SOCKS Proxy port to 4445
4445/tcp
The Client side SOCKS Proxy port has been
configured to 4445.
```

```
=== "config_socks" completed successfully
```

Go to step 18.

17   To list the SOCKS configuration, type 2.

> **> 2**

The system responds:

```
The ports configured for use by socks are:
    The Client side SOCKS Proxy will listen on
port 10090
    The Server side SOCKS Proxy will listen on
10080

=== "list_socks" completed successfully
```

18   This procedure is complete.

Troubleshooting SOCKS configuration errors   Use the information in the following table to resolve socks configuration errors.

SOCKS configuration errors

Error	Symptom	Solution
Client port binding error	If the port on the client machine is already bound to another process, the GUI client will fail to start. If the port is already bound to another process, and client will not start successfully, a Port contention message appears.	Free the port in the client machine. Closing the application will free the port.

SOCKS configuration errors

Error	Symptom	Solution
SOCKS Proxy is not running	The server side SOCKS proxy is not running. An error message identifying this condition appears.	Start the server side SOCKS proxy by performing a boot command on the server system running the MG 9000 mid-tier process. When the system has fully recovered, re-launch the application.
Server configuration error	If there are server side configuration differences between offices there will be a failure of the GUI to connect to the server machine. If office A is configured for the server to listen on port 10080, and office B is configured for the server to listen on port 10090. If there are only GUI's launched to communicate with either office A or office B, there will be no problems. If GUI's are launched to communicate with both office A and B, then there will be a failure to communicate with one of the offices. The GUI that is launched to communicate with one office, say office A will work. If there are other GUI's launched to communicate with office A, those will also work. If there is a GUI launched to communicate with office B, those communications will fail.	Verify that there is a configuration error. If there is a configuration error, there are two ways to get the GUI's to launch correctly. • If the GUI to server B, described previously needs to be launched, and the desire is to not reconfigure the server, then the GUI's launched that are communicating with office A need to be closed. After all the GUI's have been closed, re-launch the GUI to office B. • Reconfiguring the server is the best solution to this problem. Configure all the server side ports to the same value on all offices. Refer to Configuring the SOCKS proxy to reconfigure the server side ports.

MG 9000 Manager user administration procedures

User authentication at the client is controlled by the mid-tier application. When the client is launched, the user is prompted for the userid and password. The userid and password are authenticated by the mid-tier PAM authentication file.

The digital test access (DTA) client authentication is controlled by the MG 9000 Manager server process. DTA client login userid and password are authenticated by the MG 9000 Manager server.

The PAM configuration file is located in the /etc/pam.conf file. The pam.conf entry that specifies the authentication module for the MG 9000 Manager is sesm.

The default authentication module is Unix, but the customer may choose a different authentication module by changing the PAM configuration file. More information on updating the PAM configuration file is available using the man pages for pam.conf.

> *Note:* If a non-Unix PAM configuration is chosen, such as an LDAP server, to provide the user credential information, the /etc/nsswitch.conf file should be reconfigured to use the alternative Name Service mechanism. Refer to the man page for details.

The description and procedures that follow are for the Unix approach to administering user accounts.

When using PAM, the users who are allowed to connect to the MG 9000 Manager must belong to the user group "succssn" on the server. In addition to being in the user group "succssn", the user also needs to belong to the appropriate user group to obtain the desired authorization level. Refer to the Group and permission mapping table. The system administrator at the operating company sites is typically responsible for creating the user group "succssn" and adding / removing users in the system.

The following procedures are used to perform these administration tasks.

Creating user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To create the user group "succssn", type

   groupadd succssn

3   This procedure is complete.

Adding a new user to user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To add a user to the system and to user group "succssn", type

   useradd –g succssn <user login>

3   This procedure is complete.

Registering an existing user to user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To identify the existing user groups to which the user is registered (in this example the user name is "johnsmith"), type

   groups johnsmith

   The system responds with

   others groupA groupB

3   To add user "johnsmith" to user group "succssn", type

   usermod –g other –G groupA,groupB,succssn johnsmith

   Note 1: If the user has only one user group registered, assuming for example, the one group is "others," the command to be entered is as follows:
   "usermod -g others -G succssn johnsmith"

   Note 2: Failure to add all the groups in this step will automatically unregister the user from groups that are excluded in the command.

4   This procedure is complete.

Verifying a user is added to user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To verify a user is added to user group "succssn", type

```
groups <username>
```

3   Ensure group name "succssn" is one of the groups displayed in the system response.

4   This procedure is complete.

Setting or modifying user password

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To set or modify the user password, type

```
passwd <username>
```

3   Enter user password when prompted.

4   Re enter user password for validation.

5   This procedure is complete.

Showing a list of users added to user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To show a list of users added to user group "succssn", type

```
logins -g succssn
```

3   This procedure is complete.

Unregistering a user from user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To identify the existing user groups to which the user is registered (in this example the user name is "johnsmith"), type

```
groups johnsmith
```

The system responds with

```
others groupA groupB succssn
```

3   To remove user "johnsmith" from user group "succssn" (leaving out "succssn" from the command), type

    `usermod -g other -G groupA,groupB johnsmith`

    Note 1: If the user has only two user groups registered, assuming for example, they are "others" and "succssn," the command to be entered is as follows:
"usermod -g others johnsmith"

    Note 2: Failure to add all the groups in this step will automatically unregister the user from groups that are excluded in the command.

4   This procedure is complete.

Removing a user from system

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To remove user from the system, type

    `userdel <username>`

    Note: After this step the user is completely remove from the server. The user is not allowed to access the server until they are added to the system again.

3   This procedure is complete.

Removing user group "succssn"

At the MG 9000 Manager workstation serving as mid-tier or master server

1   Login as root or as a user with Administration privileges.

2   To list all users registered to the user group "succssn," type

    `logins -g succssn`

3   Unregister all users from the user group by performing the [Unregistering a user from user group "succssn"](#) procedure.

4   To remove the user group "succssn" from the system, type

    `groupdel succssn`

5   This procedure is complete.

Logging into the MG 9000 Manager
The following procedures provide steps for logging into the MG 9000 Manager.

Starting the MG 9000 Manager server

At the MG 9000 Manager

1   Log on to the MG 9000 server

```
>telnet <MG_9000_server_IP address>
login: <user id>
password: <user password>
```

2   Start the MG 9000 server.

```
 >servstart MG9KSERVER_07
```

3   This procedure is complete.

Starting the MG 9000 Manager mid-tier

At the MG 9000 Manager

1   Log on to the MG 9000 server

```
>telnet <MG_9000_mid-tier_IP address>
login: <user id>
password: <user password>
```
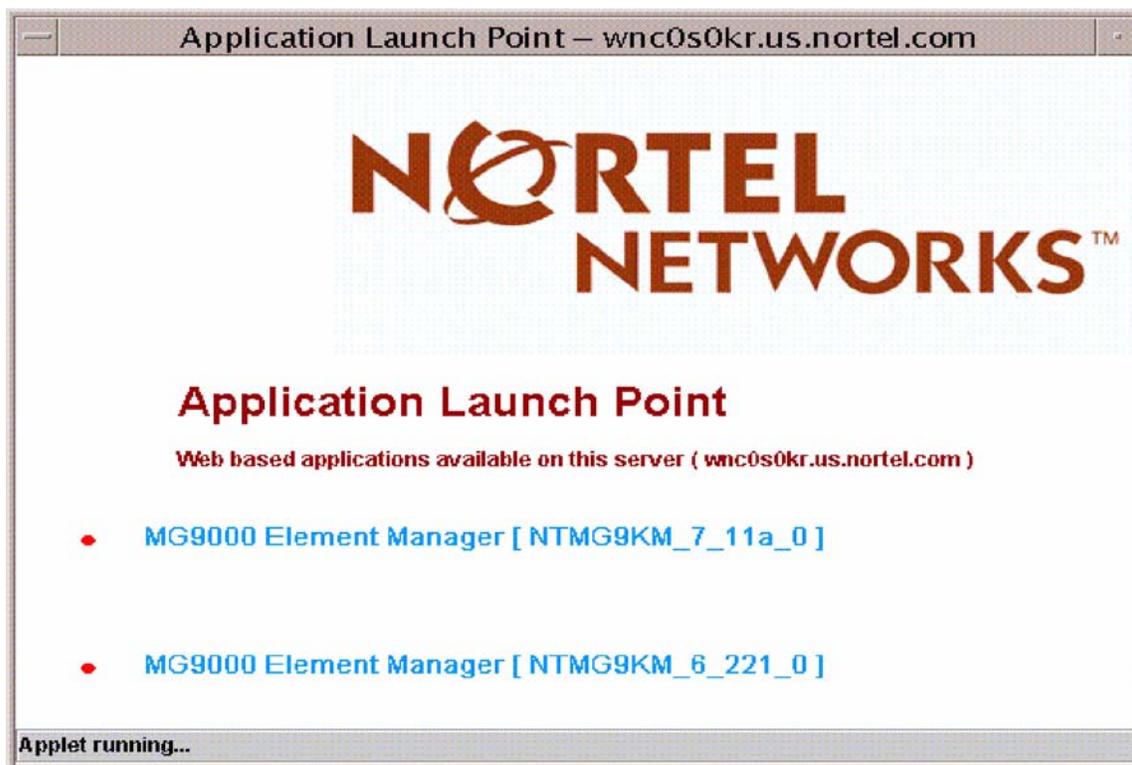
2   Start the MG 9000 mid-tier.

```
 >servstart MG9KMIDTIER_07
```

3   This procedure is complete.

Starting the MG 9000 Manager client at a PC or Sun workstation

At the Windows PC or Sun workstation

1   Start the browser.

2   In the URL address field, enter the hostname or IP Address of the mid-tier server to be connected and press Enter. The following figure shows the browser Application Launch Point.

3   Click on the Application Launcher link to start the application. The Login dialog box appears.

> *Note:* When starting the MG 9000 Manager from a Microsoft Windows platform, Windows may ask for a Security Certificate Approval. Windows does not display the Security Certificate Approval window on top of all other open windows. It may become necessary to iconify all open windows to see the Security Certificate Approval window. The security settings in the browser determine if the user will be asked for certificate approval.

4   Enter the login name and password.

5   Select the appropriate application MG 9000 link from the Application Launch Point. The Subnet View appears.

> *Note:* A Client Side SOCKS proxy dialog appears identifying that the SOCKS proxy is being launched as shown in the following figure.

6   This procedure is complete.

Launching the MG 9000 Manager client from the PC desktop and Start Menu shortcut

By default in JWS, when launching the JWS application for the second time on a Windows platform, the following dialog box appears.

JWS dialog box

If Yes is selected, a shortcut to launch the MG 9000 Manager application will be created on the PC desktop and in the Start Menu under Start->Programs. Users can later use these shortcuts to launch the MG 9000 Manager applications without using any internet browser.

Users can choose whether to create a shortcut or not. There is no functional impact to the MG 9000 Manager client applications if a shortcut is used or not.

Modifying default preferences for shortcuts

At the Windows PC desktop

1   Double-click on the Java Web Start icon to access the Java Web Start Application Manager.

2   Select File->Preferences from the menu bar.

3   Select the Shortcut Options tab. Modify the default preferences for shortcut creation. The following figure shows the Java Web Start - Preferences view with the Shortcut Options tab selected.

Java Web Start - Preferences with Shortcut Options tab
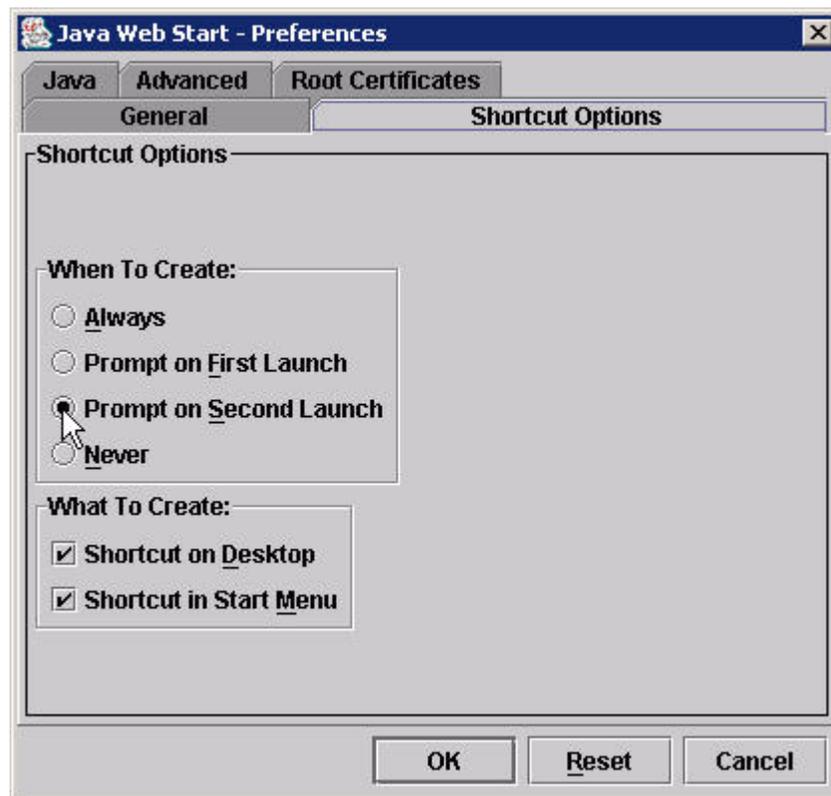
4   Click OK to apply the changes.

5   This procedure is complete.

Launching MG 9000 Manager client from JWS Application Manager

The MG 9000 Manager client can also be launched from Java Web Start Application Manager, if the MG 9000 Manager client has been launched from that server before and Java Web Start cache is not cleared.

Launching MG 9000 Manager client from JWS Application Manager on a Windows PC

At the Windows PC desktop

1   Double-click on the Java Web Start icon on the desktop to access the Java Web Start Application Manager.

2   Select View->Downloaded Applications from the menu bar.

3   Double click an Media Gateway 9000 Manager application icon to launch the client. The Home Page field identifies the MG 9000 Manager server from which the client application is launched.

> *Note:* If the Media Gateway 9000 Manager icon does not appear in the Java Web Start Application Manager, it means the MG 9000 Manager application has never been launched from this PC after JWS is installed, or JWS cache was manually cleared or automatically deleted because of a JWS upgrade. Users can still launch the MG 9000 Manager client using the internet browser.

The Login dialog box appears.

4   Enter the login name and password.

5   Select the appropriate application MG 9000 link from the Application Launch Point. The Subnet View appears

6   This procedure is complete.

Launching MG 9000 Manager client from JWS Application Manager on a Sun workstation

At the Sun workstation

1   From within the home directory, navigate to the subdirectory containing the javaws executable. Execute javaws.

2   Select View->Downloaded Applications from the menu bar.

3   Double click an Media Gateway 9000 Manager application icon to launch the client. The Home Page field identifies the MG 9000 Manager server from which the client application is launched.

> *Note:* If the Media Gateway 9000 Manager icon does not appear in the Java Web Start Application Manager, it means the MG 9000 Manager application has never been launched from this workstation after JWS is installed, or JWS cache was manually cleared or automatically deleted because of a JWS upgrade. Users can still launch the MG 9000 Manager client using the internet browser.

The Login dialog box appears.

4   Enter the login name and password.

5   Select the appropriate application MG 9000 link from the Application Launch Point. The Subnet View appears

6   This procedure is complete.

Setting up an MG 9000 Manager client application log debug file

To aid in debugging, MG 9000 Manager client application logs can be saved in a log file and sent to Nortel Networks support for investigation. Use the following procedure to set up the log file.

Logs generated from all applications in the JWS application manager are written to the same log file. It is recommended that users using this functionality, delete the file as needed. If the file is deleted, the JWS application manager creates a new log file the next time a JWS application is launched.

>   *Note:* The JWS logging system is not able to retrieve and save MG 9000 Manager client application logs that were generated before the Log Output option is enabled as presented in the following procedure.

Saving MG 9000 Manager client application logs in a debug file

At the MG 9000 Manager client Windows PC or Sun workstation

1   Access the Java Web Start Application Manager.

2   Select File->Preferences from the menu bar.

3   Click on the Advanced tab.

4   Select the Log Output option and type in a name for the log file. The following figure shows the Java Web Start - Preferences view.

Java Web Start - Preferences view
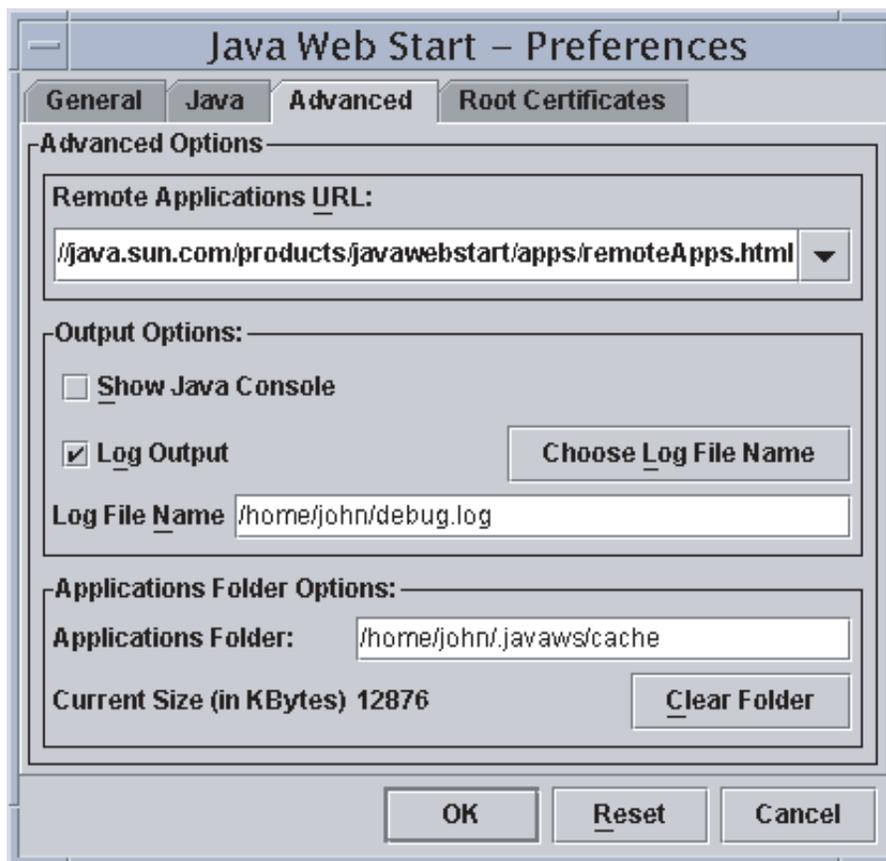
5   Click OK. The changes will take effect the next time the application is launched.

6   This procedure is complete.

Clearing JWS cache

Use the following procedure to clear the JWS cache.

>   *Note:* To remove a single application from JWS cache, go to the Removing an MG 9000 Manager JWS application from cache.

Clearing JWS cache

At the MG 9000 Manager client PC

1   Access the Java Web Start Application Manager.

2   Select File->Preferences from the menu bar.

3   Click on the Advanced tab.

4 Click on Clear Folder in the Applications Folder Options pane of the window.

> *Note:* Deleting the cache clears out all the downloaded applications from the application manager. Use this with caution only when all applications from the JWS need to be removed.

5 This procedure is complete.

Use the following procedure to remove an individual application from the JWS application manager.

Removing an MG 9000 Manager JWS application from cache

At the MG 9000 Manager client PC

1 Access the Java Web Start Application Manager.

2 Select View->Downloaded Applications from the menu bar.

3 Select an MG 9000 Manager JWS application to be deleted as shown in the following figure.

Java Web Start Application Manager

4   Select Application->Remove Application from the menu bar.

5   This procedure is complete.

Security in the local craft interface

The local craft interface (LCI) provides one userid/password pair which provides full access to the LCI functionality.

The LCI should be directly connected to the data control card (DCC) using a CAT5 Ethernet cable. Connection over a network is not recommended.

Configuring the Local Craft Interface (LCI)

Each gateway controller (GWC) must establish communication with the gateway (MG 9000). If provisioning multiple GWCs, use the following procedural overview.

Procedural overview

Order of procedures
Bring the first GWC into service using SAM21 Shelf Controller view. Refer to *SAM21 Shelf Controller Configuration Management*.
Perform the local craft interface setup and access procedures
Bring the second GWC into service. Refer to *SAM21 Shelf Controller Configuration Management*.
Perform the local craft interface setup and access procedures

The Data Control Card (DCC), NTNY45AA/CA (OC-3) or NTNY45BA (DS1-IMA), has a factory installed IP address of 10.0.0.1. Set the PC Ethernet Adapter to an address in the same subnet, such as 10.0.0.2. The PC Ethernet Adapter should be set to a factory default subnet mask of 255.255.255.0. Connect the LCI through a cross-over Ethernet cable or an Ethernet hub between the PC and the DCC card.

LCI setup and access

From a laptop PC installed with LCI software and a Windows operating system:

1   Turn on the PC.

2   Click on Start.

3   Select Settings and chose Control Panel.

4   Select Network from the Control Panel screen.

5   Scroll down the selection window and select the TCP/IP controller for the PCMCIA card.

6   Click on Properties.

7   Select the Tab for IP Address.

8   Select Specify an IP address and ensure that the IP Address field is set to 10.0.0.2.

9   Set the Subnet mask field to 255.255.255.0

10   Select the Gateway tab.

11   Add 10.0.0.1 as the Gateway to support software loading.

> ***Note:*** To support software downloading from the laptop PC to the MG 9000 using the LCI, an SFTP daemon application must be loaded onto the PC and running in the background before attempting the download. The daemon application is an SFTP utility that must accept requests from userid: admin, passwd: n0rtel.

12   Click on OK to exit.

13   Insert the Ethernet Crossover cable to the Ethernet port on the PC.

14   Insert the other end of the Crossover cable into the Ethernet port on the active DCC.

15   Start the browser (Netscape 4.7 on a Windows95 platform or Netscape 7.0 and above, or Microsoft Internet Explorer 5.5 and above on the Windows2000 platform) on the PC.

16   Click Edit, then Preferences.

17   Configure the preferences according to the settings listed in the following table.

LCI Browser Configuration

Menu path	Setting
[Netscape] Edit-->Preferences--> Appearance-->Fonts [Explorer] Tools-->Internet Options-->General-->Fonts	• Fonts for Encoding/Fonts for: Western (NN4.7 & NN7.0) • Variable Font =Times New Roman, Size = 10 (NN4.7), Proportional: Serif, Size = 12, Serif: Times New Roman, Sans-serif: Arial (NN7.0) • Fixed Font/Monospace = Courier New, Size = 10 (NN4.7 & NN7.0) • Select: use my default fonts, overriding document-specified fonts (NN4.7) • Uncheck: Allow documents to use other fonts: (NN7.0) • Language Script: Latin Based, Web page font: Times New Roman, Plain text font: Courier New (IE5.5)
[Netscape] Edit-->Preferences--> Advanced [Explorer] Tools-->Internet Options-->Advanced	• Select: Automatically load images (NN4.7) • Select: Enable Java (NN4.7 & NN7.0) • Select: Enable JavaScript (NN4.7) • Select: Enable style sheets/SXLT (NN4.7 & NN7.0) • Select: Restore Defaults (IE5.5)
[Netscape] Edit-->Preferences--> Advanced-->Cache [Explorer] Tools-->Internet Options-->General-->Temporary Internet Files-->Settings	• Memory Cache = 0 (NN4.7 & NN7.0) • Disk Cache = 0 (NN4.7 & NN7.0), Amount of disk space to use: Set to minimum value (IE5.5) • Select: Document in cache is compared to document on network: Every time (NN4.7 & NN7.0) • Check for newer versions of stored pages: Every visit to the page (IE5.5)
General	If any toolbars are installed (such as, Google toolbar or Yahoo toolbar), ensure the pop-up blocker is disabled on all of them.

18   Click OK to close the Preferences window.

19   In the Location field type: https://10.0.0.1 and press Enter.

20   At the popup window use the following logon parameters:

- User Name = admin

- Password = n0rtel

Click OK.

21   Click on the Nortel Networks MG 9000 logo to open the LCI window.

22   From the LCI window, select the Maintenance button on the upper, right, portion of the window.

> *Note:* A graphical shelf appears with 21 empty slots. To the left of the shelf is a list of all the frames and shelves currently available in the system. The first frame and shelf displayed is Frame #1 Shelf #0, the master shelf.

23   Select the frame/shelf link located in the box underneath Select a shelf view below.

> *Note 1:* Auto discovery updates the shelf display with all the cards in communication with the DCC card. All of those cards should be in a locked state. A padlock icon designates a card as locked.

> *Note 2:* Wait several minutes for autodiscovery complete. However, if auto discovery fails, reseat the DCC card and repeat Step 23. If discovery still fails there is no communication to the ITP card. Replace the DCC card with a spare and repeat Step 1.

24   This procedure is complete.

Recovering communication between the DCC and the LCI

Occasionally, when moving the laptop cross-over cable between DCC cards, communication can be lost. Use the following procedure to restore communication.

Recovering communication with the DCC

At the laptop computer

1   Move the cross-over Ethernet cable to the other DCC card.

2   To clear the ARP table, wait 5 minutes for the ARP table to clear or manually clear the ARP table in the laptop by typing the following command at an MS-Dos prompt

```
arp -d <dcc_card_IP_address>
```

where dcc_card_IP_address is the IP address set in the DCC card. The default IP address set at the factory is10.0.0.1.

3   This procedure is complete.