Carrier VoIP

MG 9000 Security and Administration

NN10162-611

Document status: Standard
Document version: 09.02
Document date: 20 October 2006

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

New in this release

The following sections detail what is new in *MG 9000 Security and Administration* for release (I)SN09U.

- "Features" (page 3)
- "Other changes" (page 3)

Features

See the following section for information about changes that are feature-related.

Digital signature authentication (phase 1)

This feature introduces enhancements to the way security keys are managed when used with IP Security (IPSec) on the MG 9000 gateway and its collaborating peers. It adopts Public Key Infrastructure (PKI) to manage the generation and distribution of keys used to authenticate nodes participating in an IPSec session. PKI is a widely used standard supporting the generation, distribution and redistribution of keys.

This feature addresses the reception, installation, and use of digital signatures to authenticate nodes attempting to establish an IPSec association.

Other changes

See the following list for information about changes that are not feature-related.

- requirements for window managers and mouse settings
- requirements for the configuration of the MG 9000 SPFS server as a radius client of the Integrated Element Management System (IEMS) Centralized Security Server (CSS)
- Addition of precautionary message for networks that employ IPSec using digital signature authentication. Any changes that you make to the time, date and time zone settings, or to the Network Time Protocol (NTP) server that fall outside of the validity period for certificates supporting

IP Security on call processing (CallP) and OAM connections can cause a service disruption.

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. Internet Protocol Security (IPSec) and Public Key Infrastructure (PKI) are introduced later in this document. Procedures for establishing IPSec or PKI on operations, administration, maintenance and provisioning (OAMP) communication links between the MG 9000 and the MG 9000 Manager, and for securing call control communication between the MG 9000 and the Gateway Controller (GWC) are available in *Nortel CVoIP IPSec Security Service Implementation Guide* (NN10453-100).

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 is performed through Remote Method Invocation (RMI) tunnelling. This requires certain ports to be opened on the firewall. For information on the configuration of these ports, refer to "Firewall configuration for RMI tunnelling" (page 24).

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

MG 9000 Manager user inactivity time out

The MG 9000 Manager serves as the element management system for the MG 9000 and is responsible for the fault clearing, configuration, performance monitoring, and upgrade tasks for the MG 9000. The following user inactivity time outs are configurable using the MG 9000 Manager:

- User Inactivity Timeout (Default: 10 minutes)
- User Termination Timeout (Default: 10 minutes)
- Re-Authentication Disable Timeout (Default: 30 seconds)

After the user launches the MG 9000 Manager client graphical user interface (GUI), if there is no user-initiated client-server interaction for the duration of the first timer (User Inactivity Timeout), the client is iconized and a dialog appears prompting the user to log in to the client again. Only after successful re-authentication is the GUI de-iconized.

If there is no user initiated client-server interaction for the duration of the second timer (User Termination Timeout), a warning dialog appears stating that the client is locked because of extended inactivity. When the user confirms the message, the client and the login dialog GUI are closed.

The periods of inactivity defined for the user inactivity time out functionality default to 10 minutes or are set during upgrade of the Server Platform Foundation Software (SPFS). Locking of the MG 9000 Manger client prevents all users input and provides no data output to the user. In addition, updates to the GUI and general messaging are not stopped. However, proper login authentication is required to release the application lock and make the MG 9000 Manager visible. Once re-authentication occurs, the user’s desktop view is restored with no updates lost.

> ***Note:*** For high availability (HA) cluster systems, timeout values are set independently for each side of the cluster. If timeout values have only been changed on the active side of a cluster and a switch of activity (SWACT) occurs, the timeout values will take the inactive side settings. To ensure consistent interface performance following a SWACT, when a default timeout setting is changed on the active side of the cluster, the corresponding setting should also be changed on the inactive side of the cluster. Refer to the chapter on modifying login session time outs on the CS 2000 Management Tools server, in *ATM/IP Security and Administration*, NN10402-600.

Requirements for windows managers

When evaluating idle timeout, the system treats windows focus events as client interactions. You must use the "click-tofocus" or "input focus mode = select" for the window managers.

> ***Note:*** Do not use the "focus-follows-mouse" or "input focus mode = followsmouse" settings. Such settings can cause extended idle timeout when a window is maximized.

The default behavior for windows and most Solaris Window Managers is "click-tofocus", which is supported by Nortel. Other behavioral settings resulting from user modification of windows managers are not supported.

Mouse settings

The following procedures are recommendations regarding how to configure your mouse settings. See the vendor documentation for complete information on how to configure your mouse settings.

Linux users

Step	Action
1	Go to **Preferences > Look & Feel > Window Behavior > Focus Policy**.
2	From the menu, select **Click to focus**.
3	Click **OK**.

—End—

Sun Users

Step	Action
1	Go to **Style Manager > Window Behavior**.
2	Click in the window to make the window active.
3	Click **OK**.

—End—

IEMS client session monitor

The Client Session Monitor (CSM) launched from the Integrated Element Management System (IEMS) tracks and records authentications, client starts, and client stops of users within the MG 9000 Manager. The CSM allows end security users to view reports that display which client application sessions are currently active and for which user. For more information on the CSM, refer to *IEMS Basics* (NN10329-111). To launch the CSM, refer to "Launching Client Session Monitor" in *IEMS Basics* (NN10329-111).

Radius client communication with the IEMS server

A secure hypertext protocol (HTTPS) certificate must be installed and Domain Name Service (DNS) must be enabled on the following SPFS platforms:

- IEMS
- CS 2000 Management Tools
- MG 9000 Element Manager

When configuring the MG 9000 SPFS server as a radius client of the IEMS Centralized Security Server (CSS), DNS must be enabled. The MG 9000 Manager SPFS server must be able to resolve the fully qualified domain name (FQDN) of the IEMS SPFS server to enable communication with the IEMS CSS. For additional details on DNS configuration, see *CS 2000 Management Tools Configuration Management* (NN10106-511). For details on IEMS configuration, see *IEMS Configuration* (NN10330-511).

IEMS/Radius authentication

To allow the IEMS/Radius server to provide central authentication of the MG 9000 userid and password, the same MG 9000 Manager-level userid and password must be entered at the IEMS/Radius server and at the MG 9000 Manager GUI. The userid and password are configured on each MG 9000 Manager for each MG 9000 network element. If Radius is not available, when the MG 9000 Manager communicates with the MG 9000, the network element (NE) level userid and password are used for authentication instead of the MG 9000 Manager level userid and password. If Radius is available, there will not be an attempt to authenticate using the NE-level userid and password.

The same userid and password must be configured on the MG 9000 Manager and Radius. At the MG 9000 Manager, the userid and password are configured using the User Id and Password GUI. A warning message appears informing the user that the MG 9000 Manager-level userid and password will be used instead of the NE-level userid and password. The MG 9000 Manager-level userid and password are stored in the Oracle database. Use the following procedure to change the MG 9000 Manager userid and password to match the IEMS/Radius server central userid and password.

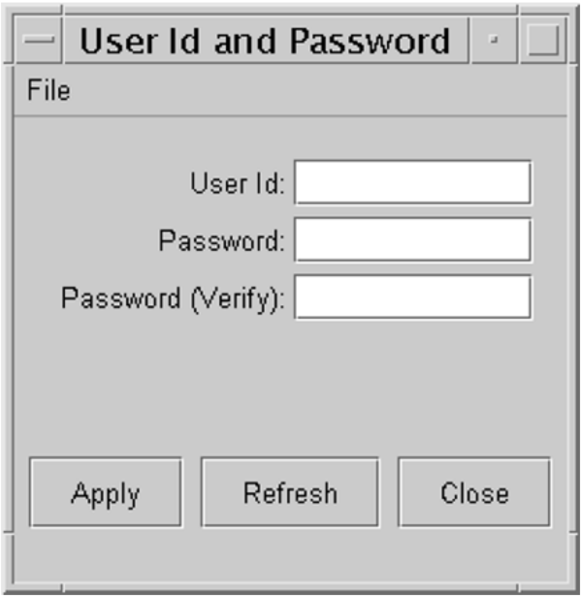
Changing the MG 9000 Manager level userid and password to match the Radius central userid and password

Step Action

At the MG 9000 Manager

1 From the Subnet View, select the MG 9000 NE for the User Id and Password are to be changed by clicking once on the NE icon.

2 Select **Configuration->Central User Id and Password GUI** from the menu bar. The User Id and Password GUI appears.



User Id and Password

Use the information in the following table when entering your userid and password information:

> ***Note:*** To allow the IEMS/Radius server to provide authentication, the User Id and Password entered in this GUI must match that entered at the IEMS/Radius server.

Field	Explanation and action
User Id	1-32 alphanumeric characters
Password	1-128 alphanumeric characters. The data you enter will not be visible.
Password (Verify)	1-128 alphanumeric characters. The data you enter will not be visible. This field must match what is entered in the Password field and is used to verity that the same password has been entered in both fields.

3 Click **Apply**.

4 This procedure is complete.

—End—

The central userid and password for the Radius server must not be the same as the default EM central userid and password, which is hard coded in the EM application. This restriction is applicable from SN09 onwards.

Authentication

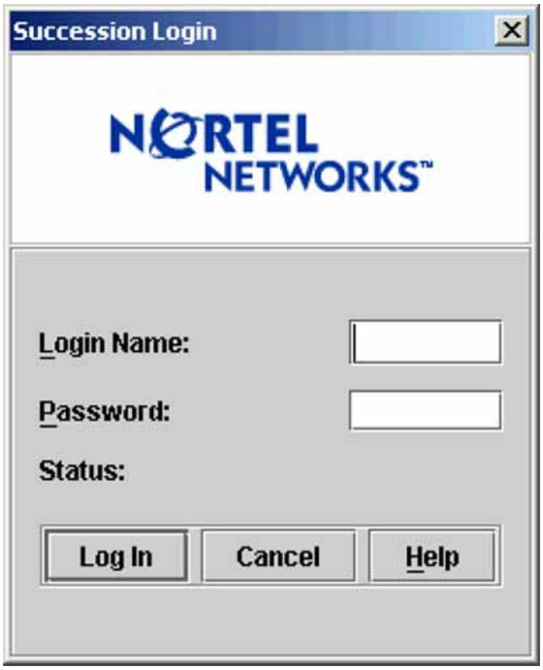
The MG 9000 Manager GUI client authentication is controlled by the MG 9000 Manager mid-tier process. In a T1400 configuration, the MG 9000 Manager mid-tier process runs on a stand-alone server; however, in an N240 configuration, both the MG 9000 Manager mid-tier and EM processes are co-resident. When 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 digital test access (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 SPFS 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 SPFS machine. Likewise, since DTA client login is controlled by the master server, logs for DTA login attempts will be on the master server SPFS 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

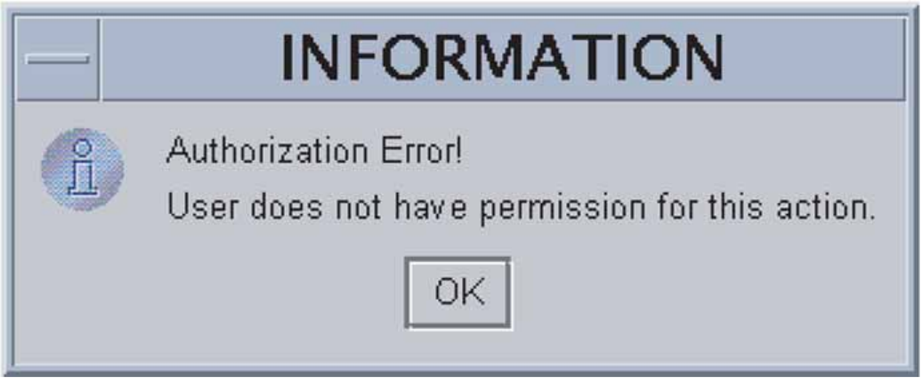
User groups	Privilege description	Permissions
succssn, emsadm	administration	nortel.ems.adm nortel.ems.iprov nortel.ems.mtc nortel.ems.sprov nortel.ems.ro
succssn, emsrw	infrastructure provisioning	nortel.ems.iprov nortel.ems.mtc nortel.ems.sprov nortel.ems.ro
succssn, emsmtc	maintenance	nortel.ems.mtc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



Authorization Error!

User does not have permission for this action.

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 Download certificates for an NE Set up or modify PKI-related options 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 Configure Collection Interval Download certificates for an NE Set up or modify PKI-related options	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

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	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

Group	Actions	
	• PLOA ATM Diagnostic • DTA/TL1 Commands	
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 • Set up or modify PKI-related options	• 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	Audit Alarm
	Alarm Browser	View IMA Group
	Performance Browser	Query IBIP threshold attributes

Group	Actions	
	View NE Properties	View PLoA Service Properties
	Refresh icon	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

		User group				
MG 9000 Manager GUI actions	**Permissions required**	**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
Configure Collection Interval	nortel.ems.iprov	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 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		
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		

		User group				
MG 9000 Manager GUI actions	**Permissions required**	**ems-adm**	**ems-rw**	**ems-mtc**	**ems-sprov**	**ems-ro**
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		
DCC - GigE						
- 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	nortel.ems.mtc	X	X	X		
- Reinitialize	nortel.ems.mtc	X	X	X		
- Restart - current, primary	nortel.ems.mtc	X	X	X		
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		

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	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		
- 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		
- online / offline / deprov	nortel.ems.mtc	X	X	X		
GLC -						
- Coefficient Table Manager	nortel.ems.mtc	X	X	X		

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- 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		
- 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.mtcn ortel.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						

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- 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		
- 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.mtcn ortel.ems.sprov	X	X	X	X	
- online / offline	nortel.ems.mtcn ortel.ems.sprov	X	X	X	X	
- Capture Rx Path Trace ID	nortel.ems.mtcn ortel.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	

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- 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		
GigE Port						
- Maintenance - Set Thresholds	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	
Tx RFI enable/disable Rx RTI enable/disable	nortel.ems.mtc nortel.ems.sprov	X	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		
- 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						

		User group				
MG 9000 Manager GUI actions	**Permissions required**	**ems-adm**	**ems-rw**	**ems-mtc**	**ems-sprov**	**ems-ro**
- 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	
- 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	

MG 9000 Manager GUI actions	Permissions required	User group				
		ems-adm	ems-rw	ems-mtc	ems-sprov	ems-ro
- 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				
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

Firewall configuration for RMI tunnelling

The following ports should be open on an installed firewall for the RMI tunnelling mechanism to work:

- Ports 11000 and 12000 incoming to the MG 9000 mid-tier from clients
- Ports 12001, 12002, and 12003 outgoing from the MG 9000 mid-tier to clients

Troubleshooting RMI tunnelling error

Use the information in the following table to resolve the RMI tunnelling error.

RMI tunnelling error

Error	Symptom	Solution
Client reports three GUIs are running	There are three GUIs running on the same client workstation already. Only three separate MG 9000 GUI client instances are supported per workstation.	Close an existing client GUI. Connect using another workstation. Also, check that no other applications are listening on ports 12001-12003.

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" (page 11) 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

Step Action

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.

—End—

Adding a new user to user group succssn

Step Action

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.

—End—

Registering an existing user to user group succssn

Step Action

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.

—End—

Verifying a user is added to user group succssn

Step Action

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.

—End—

Setting or modifying user password

Step Action

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.

—End—

Showing a list of users added to user group succssn

Step Action

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.

—End—

Unregistering a user from user group succssn

Step Action

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.

—End—

Removing a user from system

Step Action

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.

—End—

Removing user group succssn

Step Action

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'" (page 28) procedure.

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

```
groupdel succssn
```

5 This procedure is complete.

—End—

Logging into the MG 9000 Manager

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

Starting the MG 9000 Manager server

Step Action

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_08
```

3 This procedure is complete.

—End—

Starting the MG 9000 Manager mid-tier

Step Action

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_08
```

3 This procedure is complete.

—End—

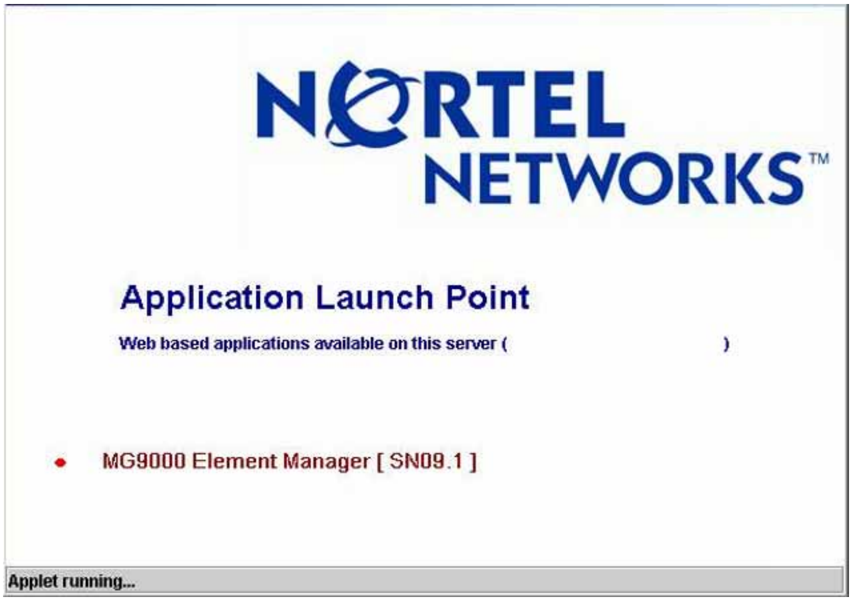
Starting the MG 9000 Manager client at a PC or Sun workstation

Step Action

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.



NORTEL NETWORKS™

Application Launch Point

Web based applications available on this server (   )

- MG9000 Element Manager [SN09.1]

Applet running...

3 Click 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.

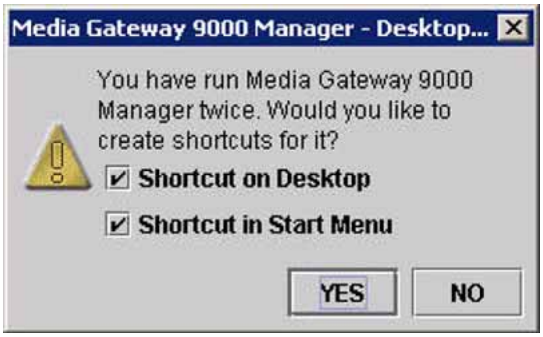
6 This procedure is complete.

—End—

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



Media Gateway 9000 Manager - Desktop...

You have run Media Gateway 9000 Manager twice. Would you like to create shortcuts for it?

☑ Shortcut on Desktop

☑ Shortcut in Start Menu

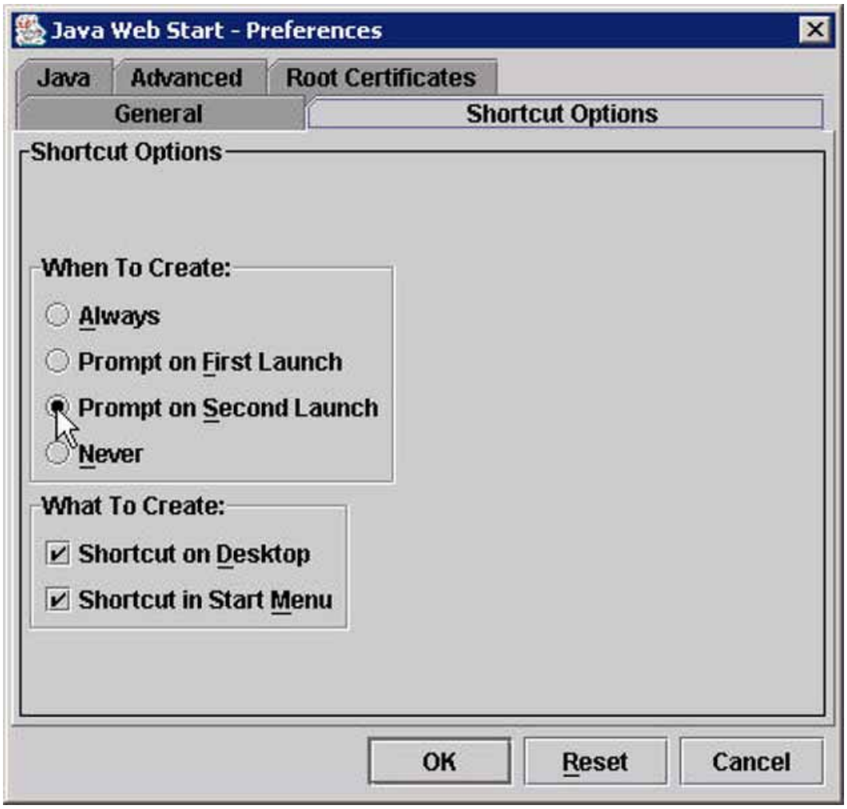
If Yes is selected, a shortcut to launch the MG 9000 Manager application will be created on the PC desktop and in the Start Menu under Start->Programs. Users can later use these shortcuts to launch the MG 9000 Manager applications without using any internet browser.

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

Step	Action
	At the Windows PC desktop
1	Double-click 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



Java Web Start - Preferences

Java | Advanced | Root Certificates | General | Shortcut Options

Shortcut Options

When To Create:

○ Always

○ Prompt on First Launch

● Prompt on Second Launch

○ Never

What To Create:

☑ Shortcut on Desktop

☑ Shortcut in Start Menu

4 Click **OK** to apply the changes.

5 This procedure is complete.

—End—

Launching the MG 9000 Manager client from the 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

Step Action

At the Windows PC desktop

1 Double-click 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 a 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.

—End—

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

Step Action

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.

—End—

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

Step Action

At the MG 9000 Manager client Windows PC or Sun workstation

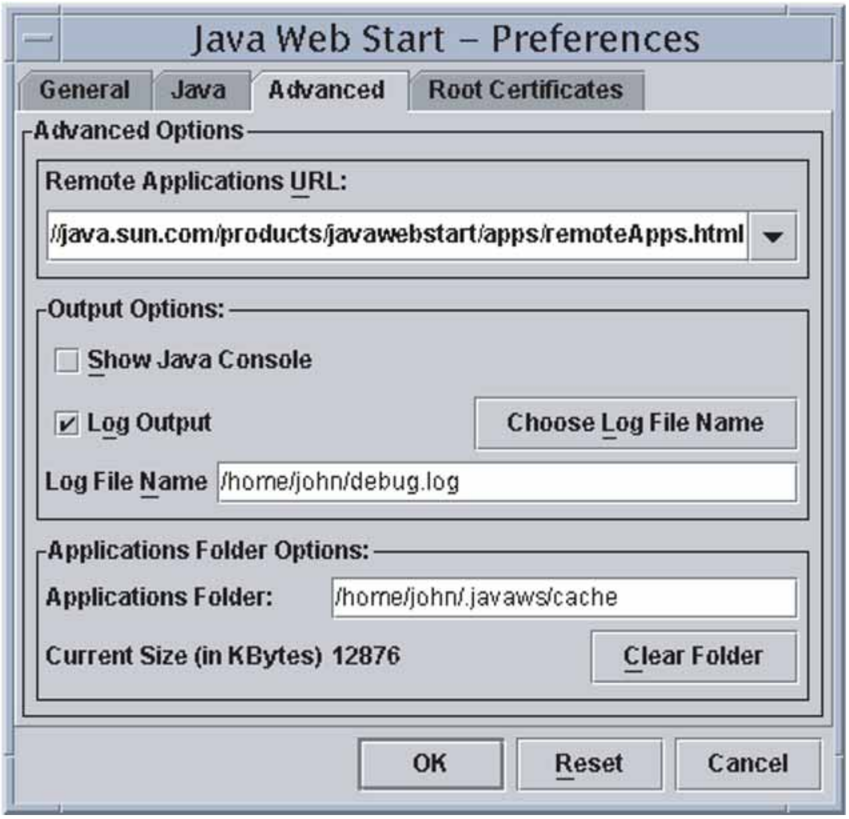
1 Access the Java Web Start Application Manager.

2 Select **File->Preferences** from the menu bar.

3 Click 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



Advanced Options

Remote Applications URL: //java.sun.com/products/javawebstart/apps/remoteApps.html

Output Options:

□ Show Java Console

☑ Log Output

Log File Name /home/john/debug.log

Applications Folder Options:

Applications Folder: /home/john/.javaws/cache

Current Size (in KBytes) 12876

5 Click **OK**. The changes will take effect the next time the application is launched.

6 This procedure is complete.

—End—

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

Step Action

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 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.

—End—

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

Removing an MG 9000 Manager JWS application from cache

Step Action

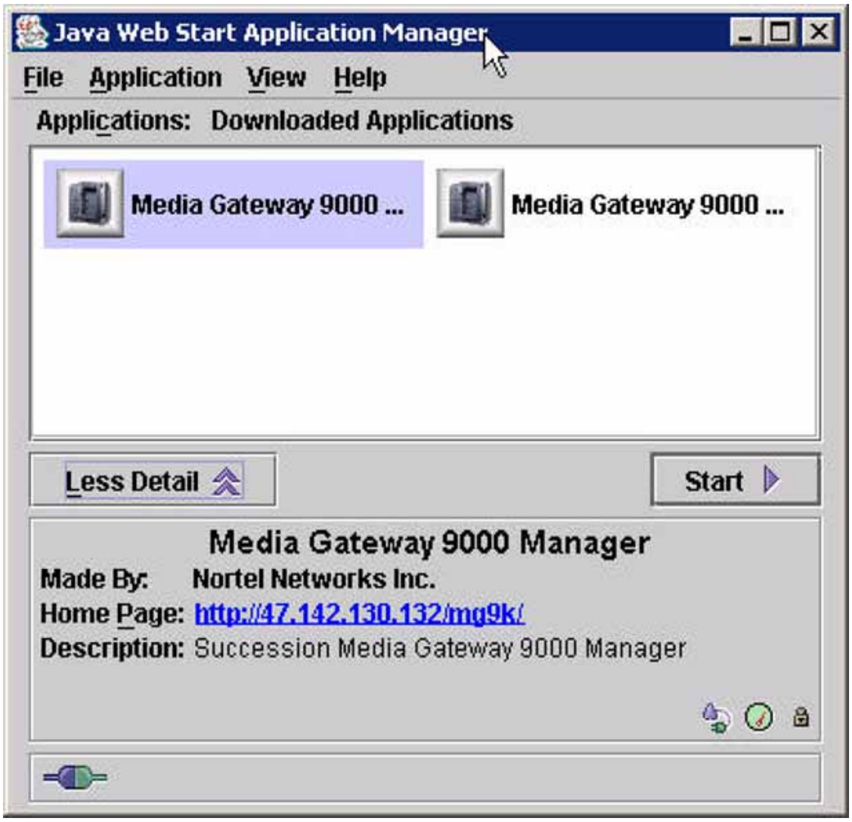
At the MG 9000 Manager client PC

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



Java Web Start Application Manager
File Application View Help
Applications: Downloaded Applications
Media Gateway 9000 ...
Media Gateway 9000 ...
Less Detail
Start

Media Gateway 9000 Manager

Made By: Nortel Networks Inc.

Home Page: http://47.142.130.132/mg9k/

Description: Succession Media Gateway 9000 Manager

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

5 This procedure is complete.

—End—

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

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* (NN10111-511).
Perform the local craft interface setup and access procedures
Bring the second GWC into service. Refer to *SAM21 Shelf Controller Configuration Management* (NN10111-511).
Perform the local craft interface setup and access procedures

The Data Control Card (DCC), NTNY45AA/CA (OC-3), NTNY45BA (DS1-IMA), or NTNY45FA (GigE), 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

Step Action

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 **Properties**.

7 Select the **IP Address** tab.

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 **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)

Menu path	Setting
[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.

—End—

Resetting the password in the LCI

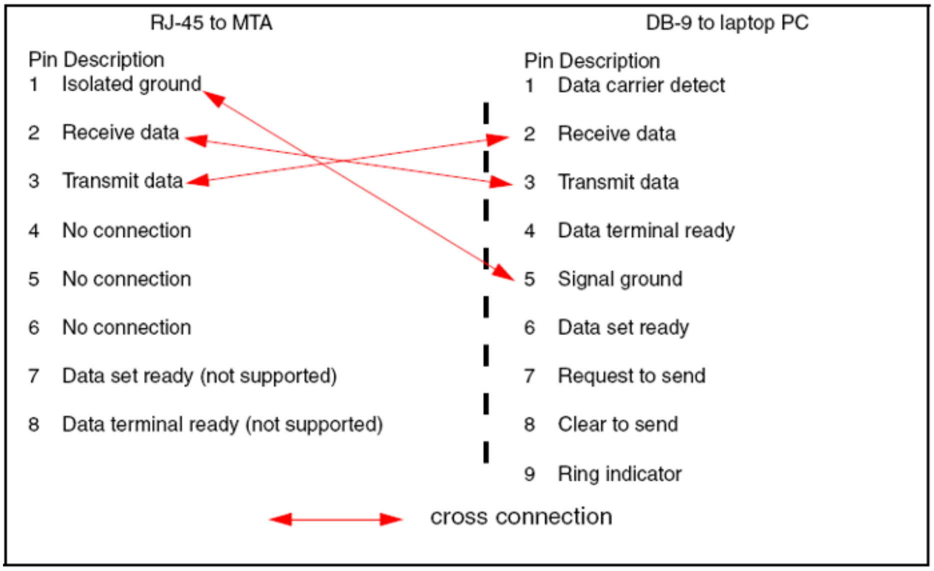
If it becomes necessary to reset the LCI password, make a cable with a DB-9 connector on one end and an RJ-45 connector on the other according to the instructions noted below. The DB-9 end of the cable connects to a laptop PC and the RJ-45 end connects to port 1 which is an RS-232 port labeled as "Serial port to external test head" on the MTA-TRC card.

When you prepare the cable, cross connect

- RJ-45 pin 1 to DB-9 pin 5
- RJ-45 pin 2 to DB-9 pin 3
- RJ-45 pin 3 to DB-9 pin 2

The pin-outs for the connectors on this cable appear in the following figure:

MTA-to-laptop cable connector pin-outs



Resetting the LCI password

Step Action

At the MG 9000 frame

1 Connect the laptop to the RS-232 port on the faceplate of the MTA-TRC card using the cable prepared in accordance with the previous figure.

2 Use HyperTerm to communicate with the MTA card. Connect to COM1.

The configuration of the Hyperterm must be as follows:

- Bits per second: 9600
- Data bits: 8
- Parity: none
- Stops bits: 1
- Flow control: none
- Under the Advanced tab of COM1 properties, ensure that "Use FIFO buffer/UART" is NOT checked.

The system responds with a prompt such as:

```
MTA [n n n] dSH>
```

where

`[n n n]` represents the number of the frame, shelf, and card slot for your MTA card.

3 At the dSH prompt, change your user permissions to "root" by typing:

```
su root <MG9K password of the day>
```

4 Press the **Enter** key.

```
The system acknowledges that your user name and
permissions have changed to "root".
```

5 Change directory to the MTA dshell by typing

```
cd dshell
```

6 Press the **Enter** key

7 After the system receives the MTA dshell prompt again, type

```
/resetpasswd
```

8 Press the **Enter** key.

A message is sent to reset the LCI password. The LCI password is reset to n0rtel.

9 This procedure is complete.

—End—

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

Step Action

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 is 10.0.0.1.

3 This procedure is complete.

—End—

Backup and restore

File systems and Oracle data on the MG 9000 Manager master server SPFS-based platform can be backed up and restored using Digital Audio Tape (DAT) for Sun t1400 servers or DVD for Sun Netra 240 servers. Refer to *ATM/IP Security and Administration* (NN10402-600) for information and procedures for performing the following:

- "Performing a backup of Oracle data on an SPFS-based server"
- "Performing a backup of file systems on an SPFS-based server"

The Backup Restore Manager provides centralized control of backup capabilities for the MG 9000 Manager data. The Backup Restore Manager consists of the

- Synchronous Backup Restore Manager (SBRM) software on the IEMS server
- Device Backup Restore Manager (DBRM) software on the MG 9000 Manager server

The SBRM software controls and synchronized backup-related activities on the MG 9000 Manager through the DBRM software.

The SBRM is launched through the IEMS GUI, and enables backups of database tables, configuration files, and property files on the MG 9000 Manager. Backup of program store and associated patches is not included in the functionality.

On the MG 9000 Manager server, the backup file is placed in directory "/data/bkresmgr/backup".

Prior to using the SBRM, the secure shell (SSH) must be configured between the IEMS server where the SBRM software is installed, and the MG 9000 Manager where the DBRM software is installed. To configure SSH, refer to procedure "Configuring SSH between the backup restore manager servers" in *ATM/IP Security and Administration* (NN10402-600).

To configure the SBRM service on the MG 9000 Manager server where the SBRM software is installed, for automated execution of backups, refer to procedure "Configuring the automated synchronous backup restore manager service" in *ATM/IP Security and Administration*, (NN10402-600).

IPSec configuration

The Nortel Carrier Voice over IP (CVoIP) network uses IP Security (IPSec) to protect the traffic flow between endpoints on a network. IPSec is a standard protocol that protects network traffic by authenticating the endpoints involved (verify endpoint identity) in data transmission, and also by encrypting the transmitted data.

The Nortel CVoIP security service solution involves the interaction of several network elements. For information regarding the provisioning of the MG 9000 and the MG 9000 Manager within the CVoIP solution, you must refer to *Nortel CVoIP IPSec Security Service Implementation Guide* (NN10453-100).

IPSec can be provisioned on the following network links:

- OAMP link between the MG 9000 Manager and the MG 9000 network element (NE)
- signaling connection between each Virtual Media Gateway (VMG) and its associated Gateway Controller (GWC)

These connections can be set up independently of each other. However, it is recommended that the OAMP link be set up first so that any VMG security-related information is sent from the MG 9000 Manager over a secure connection.

> ***Note:*** Beginning in SN09FF, you must configure the gateway security when provisioning a new VMG.

For more information on IPSec, its terms, and overall security architecture, refer to *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

IPSec authentication modes

The MG 9000 IPSec feature supports two authentication modes pre-shared key (PSK) and digital certificate (Public Key Infrastructure, PKI).

Node managers, the MG 9000 Manager and the GWC can be configured simultaneously to support either mode. The MG 9000 can only be configured in one mode or the other.

Pre-shared key authentication

PSK (Pre-shared Key, or Shared Secret) is a standard for authentication in which endpoints or gateways on the network communicate using a pre-configured and encrypted password. The password is known only to the endpoints. Before a connection can be established, a manual exchange of the password occurs between the peers. When a gateway receives a password from a peer, it decrypts it and compares it to its own. If the passwords match, authentication occurs and a secure communication channel is established.

Digital signature authentication

Digital signature authentication is based on Public Key Infrastructure (PKI), a standard that allows entities to establish trust relationships between endpoints on a network. The MG 9000 IPSec interfaces use digital certificates to authenticate the peers with which it establishes IPSec sessions.

The MG 9000 uses digital signature authentication to authenticate IPSec sessions to the MG 9000 Manger and to the Gateway Controller (GWC).

Transitions between IPSec authentication modes

The MG 9000 IPSec feature supports two authentication modes pre-shared key and digital certificate. When required, you can change the authentication mode from one to the other. To do so, you must use the detailed transition procedures in *Nortel CVoIP IPSec Security Service Implementation Guide* (NN10453-100).

Hardware and software requirements

Digital signature authentication requires SN09FF (or later) software for the MG 9000, the MG 9000 Manager and for the SPFS.

User level authorization

Only users with high-level administrative or security privileges have access to the IPSec functions. The EMSADM user level privileges are required to make IPSec configuration changes.

Date and time settings

Changes to time and date values can impact call processing when IPSec with Digital Signatures has been deployed within your network. Specifically, if the changes fall outside of the validity period of the associated certificates, dependent IPSec secure associations that support call processing and OAM will fail to renew. For further details, consult the *Nortel CVoIP IPSec Security Service Implementation Guide* (NN10453-100), or contact your next level of support.

CAUTION
Risk of communication disruption, loss of service, or outage
Changing the system time and date can result in a call processing outage if your network IP Security (IPSec) configuration is enabled to use digital signature authentication. Consult *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100 for additional details, or contact your next level of support.

IPSec configuration procedures

A description of the user interfaces and all procedures to configure IPSec on your network are treated in *Nortel CVoIP IPSec Security Service Implementation Guide* (NN10453-100).

Carrier VoIP

MG 9000 Security and Administration

Publication: NN10162-611
Document status: Standard
Document version: 09.02
Document date: 20 October 2006

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

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