Copyright © 2005, Nortel Networks

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. Internet Protocol security (IPSec) information is presented later in this document with procedures for establishing IPSec on OAMP communication between the MG 9000 and the MG 9000 Manager. Procedures also address securing call control communication between the MG 9000 and the Gateway Controller.

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 on page 20.

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

Authentication

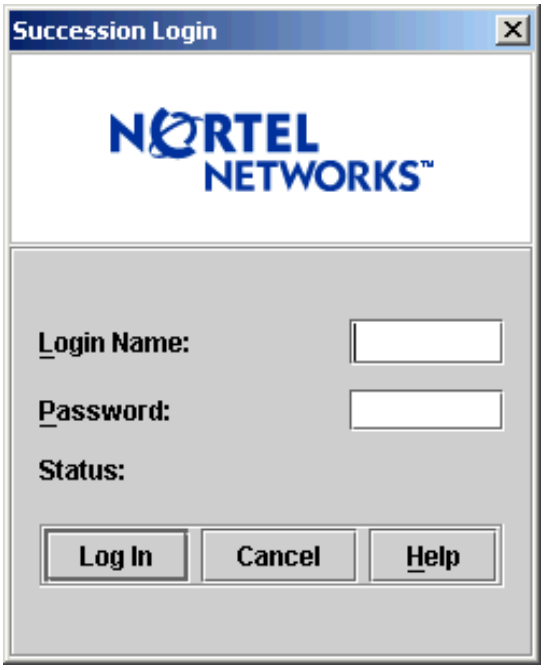
The MG 9000 Manager GUI client authentication is controlled by the MG 9000 Manager mid-tier process. In a T1400 configuration, the MG 9000 Manager mid-tier process runs on a stand-alone server; however, in an N240 configuration, both the MG 9000 Manager mid-tier and EM processes are co-resident. When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

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
Import NE	nortel.ems.iprov	X	X			
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 - 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 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	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		

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 / 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		
- 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		

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		
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.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
- 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		
- 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		

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	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	
- 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		

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
- 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		

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
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	
- create bundles	nortel.ems.mtc nortel.ems.sprov	X	X	X	X	
- delete bundles	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
- 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				
Create ESA Service Code Translation	nortel.ems.sprov	X	X		X	
Delete ESA Service Code Translation	nortel.ems.sprov	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
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 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_08
```

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_08
```

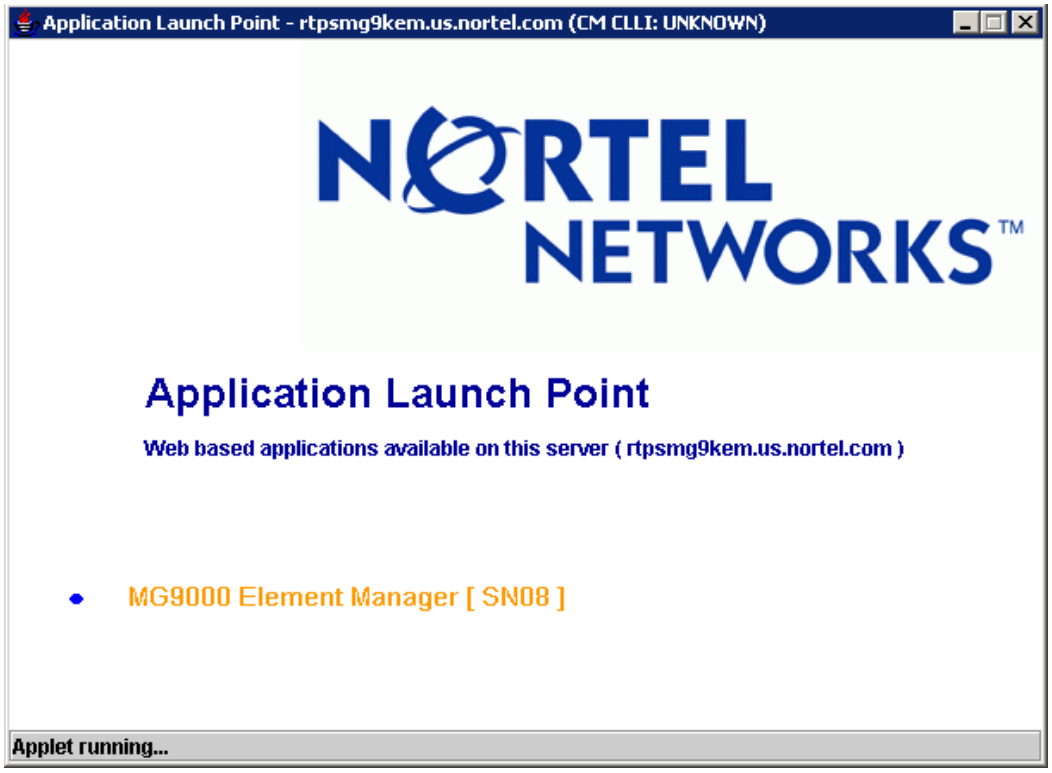
3 This procedure is complete.

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.

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.

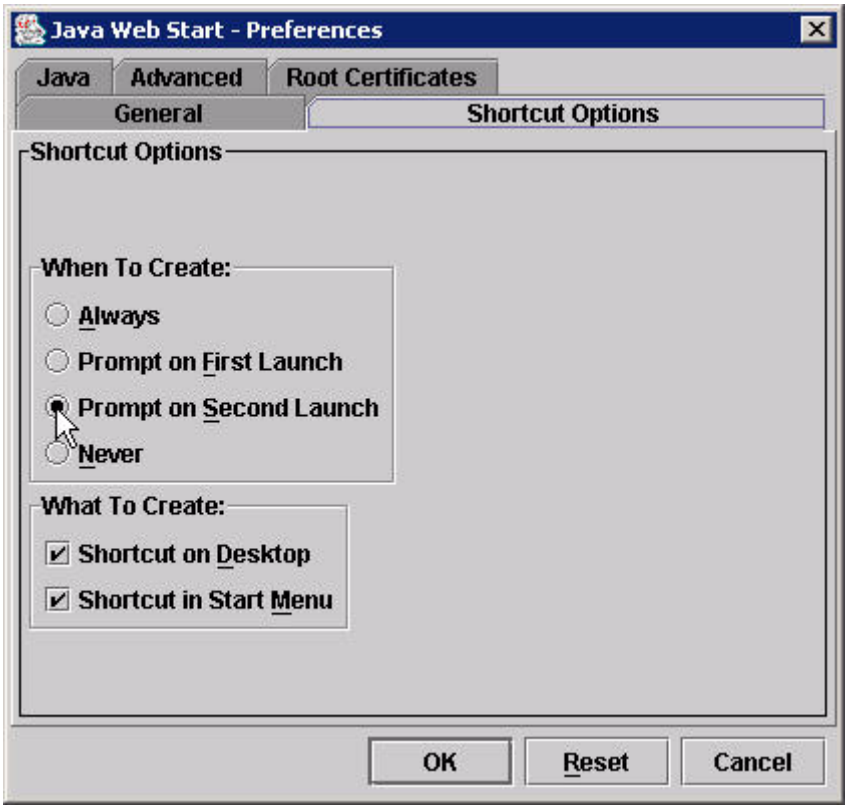
Users can choose whether to create a shortcut or not. There is no functional impact to the MG 9000 Manager client applications if a shortcut is used or not.

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.

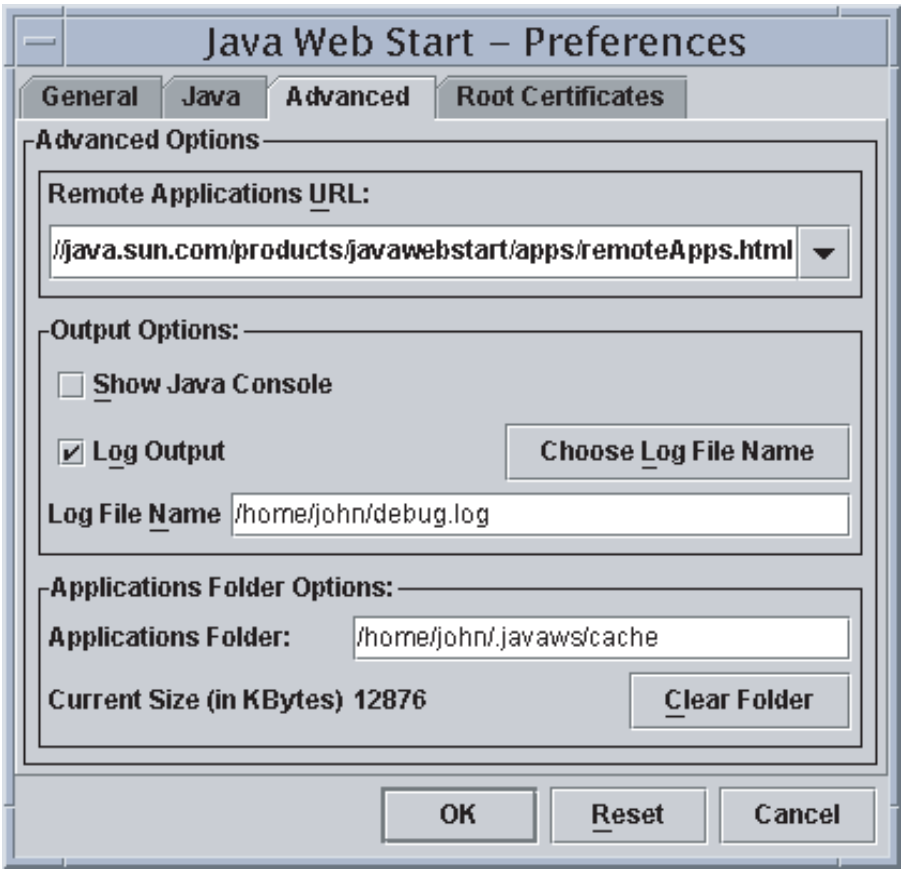
Note: The JWS logging system is not able to retrieve and save MG 9000 Manager client application logs that were generated before the Log Output option is enabled as presented in the following procedure.

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), 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

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.

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 on the other. The DB-9 connects to the laptop and the RJ-45 connects to port 1 which is an RS-232 port labeled as “Serial port to external test head” in the following figure. The pin-outs for the connectors on this cable are shown in the following figure.

MTA-to-laptop cable connector pinouts

RJ-45 to MTA

Pin	Description
1	Isolated ground
2	Receive data
3	Transmit data
4	No connection
5	No connection
6	No connection
7	Data set ready (not supported)
8	Data terminal ready (not supported)

DB-9 to laptop PC

Pin	Description
1	Data carrier detect
2	Receive data
3	Transmit data
4	Data terminal ready
5	Signal ground
6	Data set ready
7	Request to send
8	Clear to send
9	Ring indicator

Resetting the LCI password

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.
3. Once connected (the response may be slow), type

   `enter:`

   enter the root user password

4 Change directory to the MTA dshell by typing

```
cd dshell
```

5 After the MTA dshell prompt is received, type

```
/resetpasswd
```

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

6 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 is 10.0.0.1.

3 This procedure is complete.

Backup and restore

File systems and Oracle data on the MG 9000 Manager master server SSPFS-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 SSPFS-based server"
- "Performing a backup of file systems on an SSPFS-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 Integrated EMS 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 Integrated EMS 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 Integrated EMS 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

Internet Protocol security (IPSec) can be provisioned for the following:

- OAMP link between the MG 9000 Manager and the MG 9000
- signaling connection between each VMG and its associated Gateway Controller

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.

For more information on IPSec, its terms and overall security architecture, refer to *GWC Security and Administration*, NN10213-611 and to *ATM/IP Solution-level Security and Administration*, NN10402-600.

User level authorization

IPSec controls access to and from the MG 9000 Manager server as far as network connectivity is concerned. Therefore, only a high-level administrative or security user privilege will have access to the IPSec. Only the EMSADM user level will have access to make configuration changes.

Setting up IPSec in the MG 9000 between the MG 9000 and the MG 9000 Manager

The following steps provide an overview of the actions required to set up a secure OAMP connection between the MG 9000 and the MG 9000 Manager.

Note: Ensure the MG 9000 and MG 9000 Manager are at SN08.

1. Provision IPSec on the MG 9000 DCC through the LCI.
2. Add IPSec Entry on the MG 9000 Manager using the Server Security Manager.

   Note: There will be a loss of connectivity between the MG 9000 and the MG 9000 Manager between these two steps.

3. Add IKE Entry on the MG 9000 Manager using the Server Security Manager.
4. Enable IPSec on the MG 9000 DCC through the LCI.

The following procedure provides the steps for setting up IPSec on the OAMP connection.

Configuring IPSec between the MG 9000 and the MG 9000 Manager

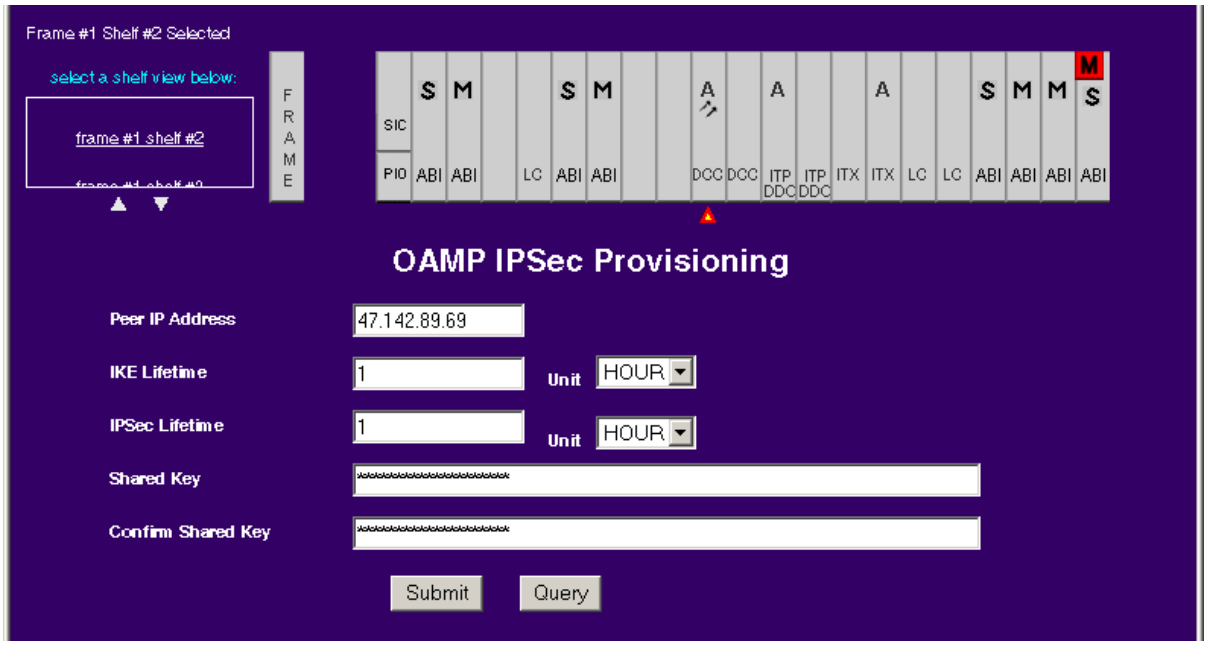
At the MG 9000 LCI

1 To configure security on the OAMP link, click on the Maintenance button, select the master shelf from the frame/shelf selector on the left.

2 Click on the active DCC card and select the IPSec Config->Provisioning menu and provision the following information:

- IKE Lifetime - set to 8 Hours
- IPSec Lifetime - set to 8 Hours
- Shared Key and Confirm Shared Key- this key must be between 20 and 120 alphanumeric characters. This is the same as the Preshared Key set up in the Connections->OAMP view of the LCI. (Refer to Changing NE Encryption Keys on page 59 for information on the Preshared Key.)

OAMP IPSec Provisioning screen



3 Click Submit

At a PC or workstation with a web browser

4 Perform procedure IPSec provisioning at Server Security Manager on page 45 and return to this step.

5 Perform procedure IKE provisioning at Server Security Manager on page 48 and return to this step.

At the MG 9000 LCI

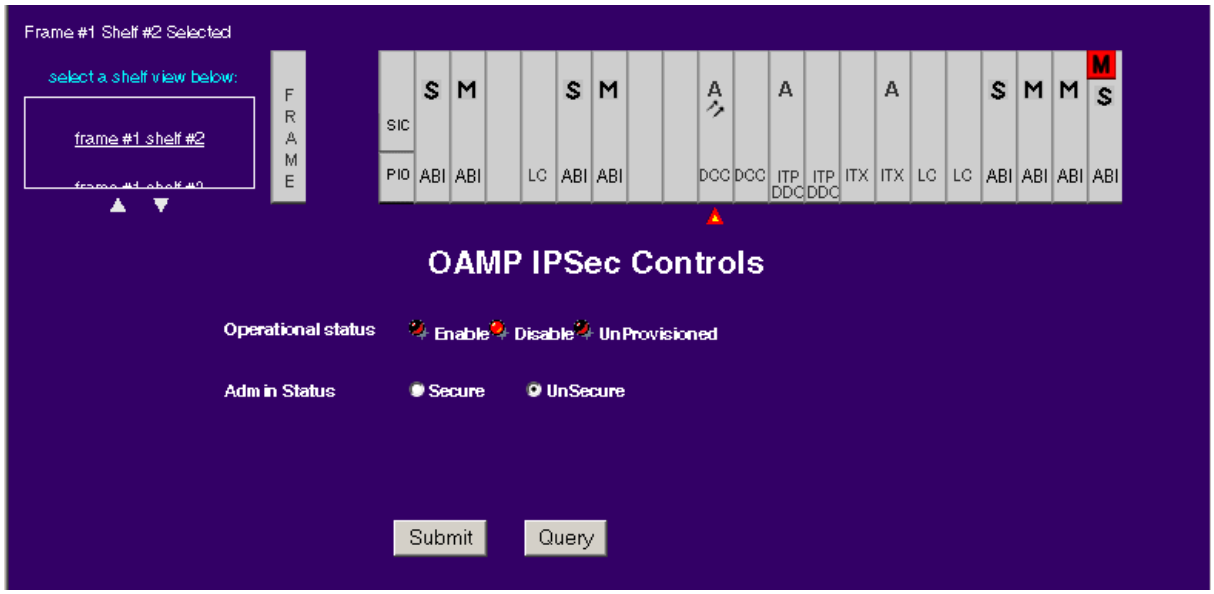
6 To Enable security on the OAMP link, click on the Maintenance button, select the master shelf from the frame/shelf selector on the left.

7 Click on the active DCC card and select the IPSec Config->Controls menu.

8 Click Secure then click Submit.

9 Click Query to verify that secure communication operational status changes to enabled.

OAMP IPSec Controls screen showing the status as Enabled

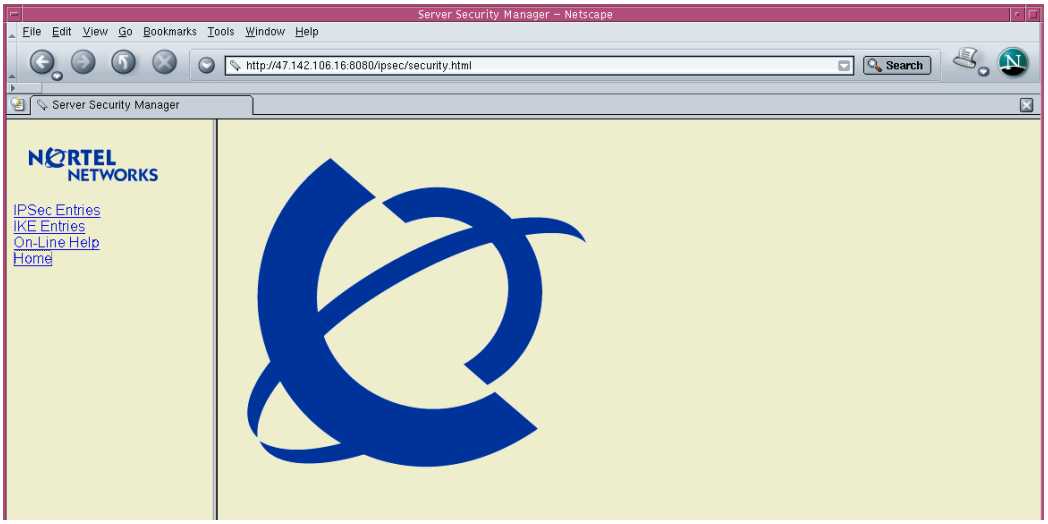


10 This procedure is complete.

Configuring Server Security Manager

The Server Security Manager is an HTML web page is used to define security parameters for securing MG 9000 Manager to MG9000 OAM&P communications. The following figure shows the Server Security Manager main page.

Server Security Manager main page



Two tables are available in the HTML page representing currently provisioned security parameters, one for IPSec parameters and one for IKE parameters. Options to add and delete entries are available. Adding entries is performed using HTML forms.

- The IPSec Entries page allows retrieval and manipulation of IPSec policies for a host server. Once the policies are configured, all outbound and inbound datagrams are subject to policy checks as they exit and enter the host server. If no entry is found, no policy checks will be completed, and all the traffic will pass through. Depending upon the match of the policy entry, a specific action will be taken.
- The IKE Entries page allows retrieval and manipulation of Internet Key Exchange policies for a host server. Once a policy is configured, the IKE daemon running on the host server, discovers a remote host's public encryption key. The local system can then encrypt messages destined for the remote host whose public key it has discovered.

Parameters in these files are used to setup security associations, keys, and protection mechanisms. Enforcement of IPsec policies will be system-wide and per-socket as provided by the Solaris IPSec implementation. The technician will not be limited to securing the

MG 9000 Manager to MG 9000 connection, but will be able to manage all network connectivity in and out of the MG9000 Manager Server.

IPSec data set up in the Server Security Manager is SSPFS data that must be saved using the procedure “Performing a data backup on an SSPFS-based server” in *ATM/IP Solution Level Security and Administration* NN10402-600. To restore backed up data, refer to procedure “Performing a data restore on a Sun server” in *ATM/IP Solution Level Security and Administration* NN10402-600.

On line help that describes the values in each form is available by clicking the On-Line Help on the left side of the page.

IPSec provisioning at Server Security Manager

At a PC or workstation with a web browser

1 To access the Server Security Manager, point a web browser to http:///(ip address of server)/ipsec/security.html

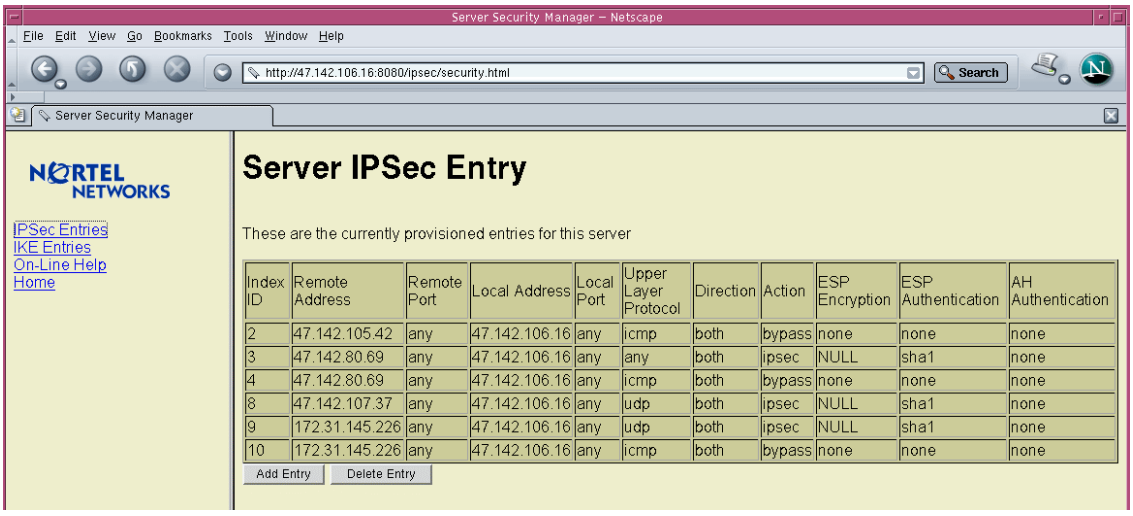
where

ip address is the address of the MG 9000 Manager master server

2 Login with the MG 9000 Manager user id and password having emsadm privileges.

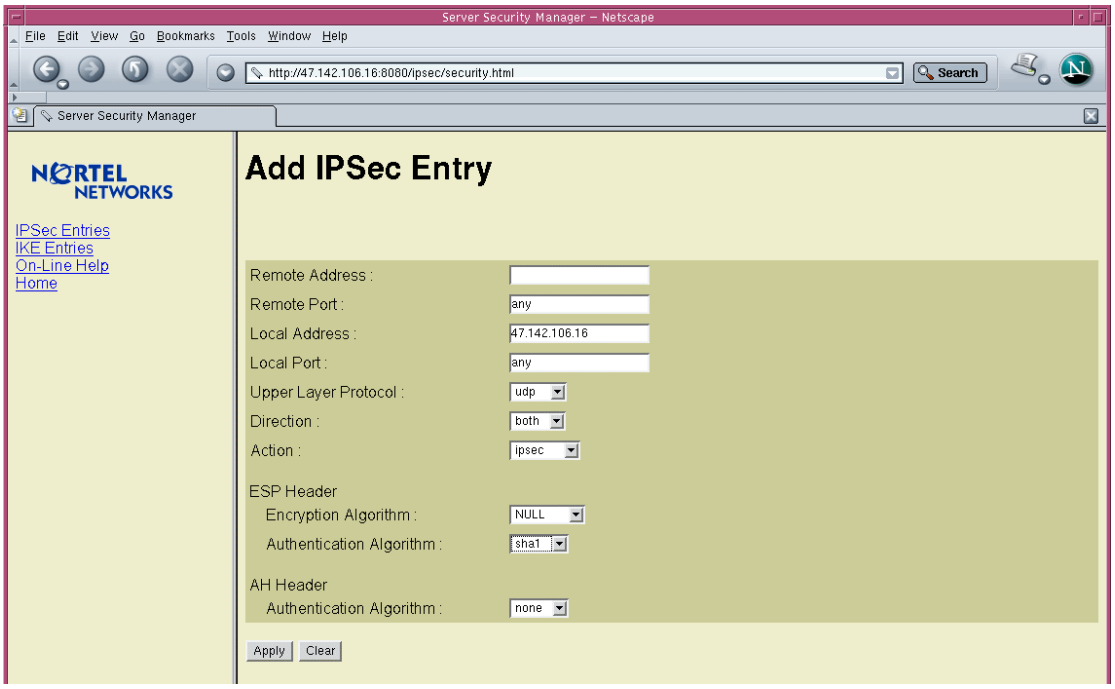
3 Click on the IPSec Entries link. The Server IPSec Entries page appears as shown in the following figure.

Server IPSec Entry page



4 Click the Add Entry button. The Add IPSec Entry page appears as shown in the following figure.

Add IPSec Entry page



5 Configure the IPSec Parameter settings, to enable secure communications between the MG 9000 and the MG 9000 Manager. The following table lists the security values for the IPSec entry and appropriate entries.

IPSec fields

Field	Description	Entry
Index ID	Internal index used by the server to track and reference IPSec entries.	Integer. No entry required.
Remote Address	Remote Address means the source address on incoming packets and destination address on outgoing packets.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the remote address of the MG 9000 as seen by the MG 9000 Manager.
Remote Port	IP port of the remote system communicating with this server.	1 - 65535. Enter any.

IPSec fields

Field	Description	Entry
Local Address	Local Address means the destination address on incoming packets and source address on outgoing packets.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the local address of the MG 9000 Manager as seen by the MG 9000.
Local Port	IP port of this server.	1 - 65535. Enter any.
Upper Layer Protocol	Determines which protocol traffic this entry is matched against.	any, icmp, tcp, and udp. Enter udp.
Direction	Determines whether this entry is for inbound or outbound traffic.	in, out, and both. Enter both.
Action	Determines the action to take when the traffic pattern is matched.	bypass, drop, and ipsec. Enter ipsec.
ESP Encryption	Describes the encryption algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to "ipsec".	none, any, NULL, des, and 3des. Enter NULL.

IPSec fields

Field	Description	Entry
ESP Authentication	Describes the authentication algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to "ipsec".	none, any, sha1, and md5. Enter sha1.
AH Authentication	Describes the encryption algorithm that will be used to apply the IPSec AH header on outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to "ipsec".	none, any, sha1, and md5. Enter none.

6 Click on the Apply button to add the entry.

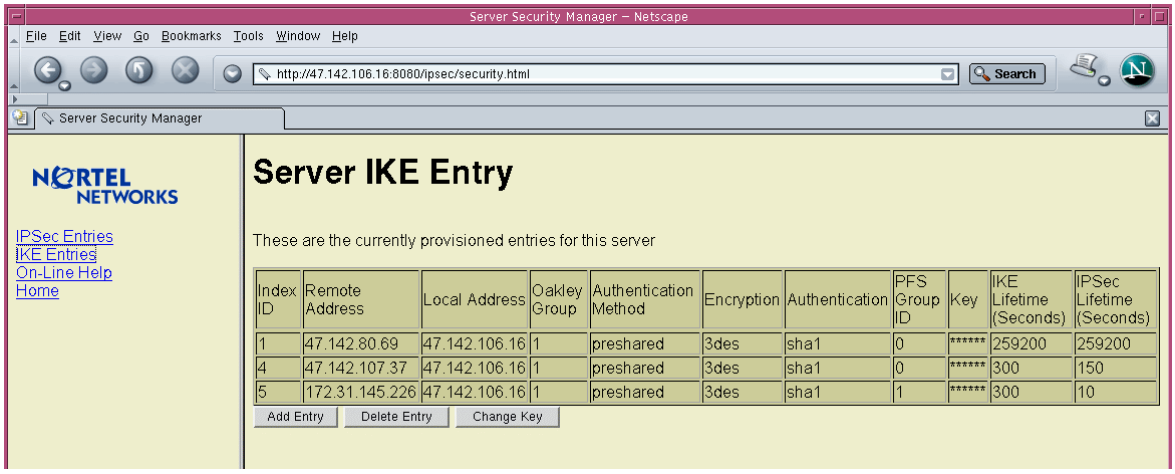
7 This procedure is complete.

IKE provisioning at Server Security Manager

At a PC or workstation with a web browser

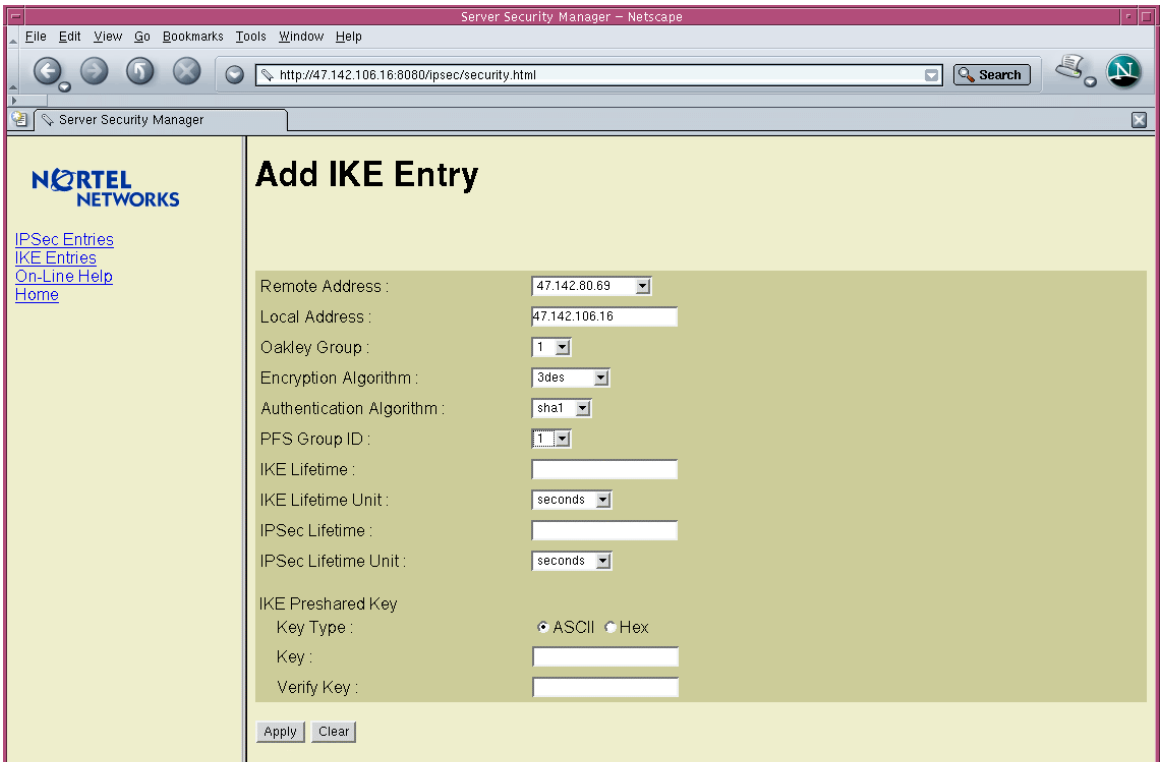
1 Click on the IPSec Entries link. The Server IPSec Entries page appears as shown in the following figure.

Server IKE Entry page



2 Click the Add Entry button. The Add IPSec Entry page appears as shown in the following figure.

Add IKE Entry page



3 Configure an IKE entry for each IPSec entry that was provisioned in step 2. The following table lists the security values for the IKE entry and appropriate entries.

IKE fields

Field	Description	Entry
Index ID	Internal index used by the server to track and reference IKE entries.	Integer. No entry required.
Remote Address	IP address of the remote system communicating with this server.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the Remote Address which is the address of the MG 9000 as seen by the MG 9000 Manager.

IKE fields

Field	Description	Entry
Local Address	IP address of this server.	A numeric internet IP address of the form: www.xxx.yyy.zzz. Enter the local address which is the address of the MG 9000 Manager as seen by the MG 9000.
Oakley Group	The Oakley Diffie-Hellman group used for IKE Security Association key derivation.	1 (768-bit), 2 (1024-bit), or 5 (1536-bit). Enter 1.
Encryption Algorithm	Specifies the encryption algorithm for a Security Association.	des and 3des. Enter 3des.
Authentication Algorithm	Specifies the authentication algorithm for a Security Association.	sha1 and md5. Enter sha1.
PFS Group ID	The Oakley Diffie-Hellman group used for IPsec Security Association key derivation.	0 (do not use Perfect Forward Secrecy for IPsec SAs), 1 (768-bit), 2 (1024-bit), and 5 (1536-bit). Enter 1.
IKE Lifetime	Specifies the lifetime for a IKE phase 1 Security Association.	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days. Enter 8.
IKE Lifetime Unit	Specifies the units.	Maximum allowed units in seconds, minutes, hours, or days. Enter hours.
IPSec Lifetime	Specifies the lifetime for an IPSec Security Association.	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days. Enter 8.

IKE fields

Field	Description	Entry
IPSec Lifetime Unit	Specifies the units.	Maximum allowed units in seconds, minutes, hours, or days. Enter hours.
IKE Preshared Key	Specifies the preshared key for this Security Association.	Radio button to select ASCII or hexadecimal. Select ASCII. 20 - 120 character ASCII string. Enter the same key that is entered in the MG 9000 twice.

4 Click on the Apply button to add the entry.

5 This procedure is complete.

Setting up IPSec between the MG 9000 and the GWC

The following steps provide an overview of the actions to set up a secure signaling connection between each MG 9000 VMG and its associated GWC.

1. From the CS 2000 Management Tools, select GWC and set up a Flex IPSec policy for a particular VMG controlled by this GWC. Refer to “IPSec configuration procedures” *GWC Security and Administration*, NN10213-611.
2. From the MG 9000 Manager, set up IPSec for the same VMG using the Switched LInes Services GUI.
3. From the CS 2000 Management Tools, select the same GWC/VMG and change the Flex policy to secure. Refer to “IPSec configuration procedures” *GWC Security and Administration*, NN10213-611.
4. Repeat for all VMGs as needed.

The following procedure provides the steps for setting up IPSec on the signaling connection.

Configuring IPSec between the MG 9000 and GWC

At the CS 2000 GWC Manager client

1 Set up a Flex IPSec policy for a specific VMG controlled by this Gateway Controller. Refer to “IPSec configuration procedures” in *GWC Security and Administration*, NN10213-611.

At the MG 9000 Manager

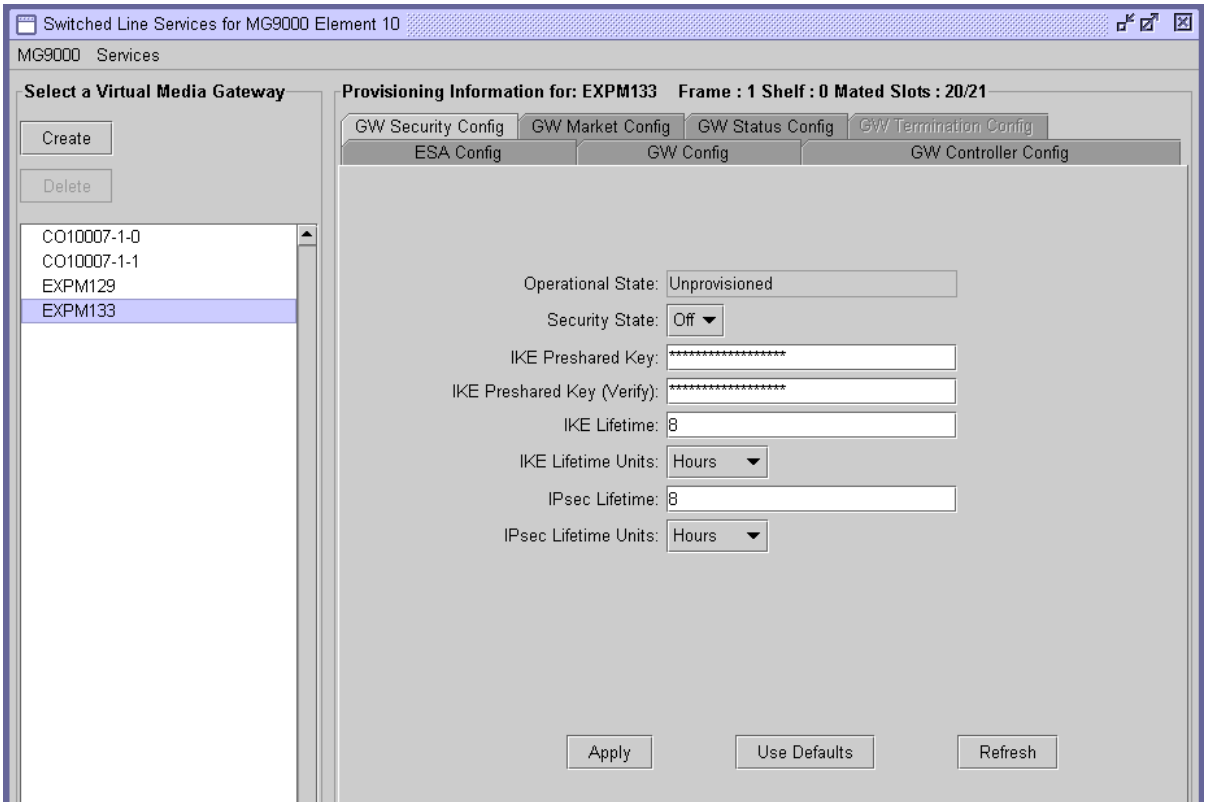
2 From the Subnet View, double click on the network element for which security on the call control link is to be provisioned. The NE desktop view appears.

3 Select Services->Switched Lines Services Manager from the menu bar. The Switched Lines Services Manager Appears.

4 Select the VMG for which security is to be provisioned.

5 Click on the GW Security Config screen. The GW Security Config screen is shown in the following figure.

GW Security Config screen



Use the information in the following table to complete the fields in the GW Security Config screen.

GW Security Config screen call control link security values

Field	Explanation	Entry
Operational State		Enabled, Disabled Click on Enabled.
Security State	Indicates if security is enabled.	Off, On Select On.
IKE Preshared Key	Preshared key used in the IKE establishment of a secure call control link.	20-120 digit hexadecimal string. Enter the same value at that entered at the CS 2000 Management Tools for the GWC.

GW Security Config screen call control link security values

Field	Explanation	Entry
IKE Preshared Key (Verify)	Re-enter the Preshared key in the previous field to verify value.	20-120 digit hexadecimal string. Re-enter the same Preshared key as entered in the previous field.
IKE Lifetime	Determines how long the currently established security session will last.	Non-negative integer. Enter 8
IKE Lifetime Units	Seconds, Minutes, Hours, Days	Enter hours.
IPSec Lifetime	Determines how long the currently established security session will last.	Non-negative integer. Enter 8
IPsec Lifetime Units	Seconds, Minutes, Hours, Days	Enter hours.
Use Defaults button	If Defaults is clicked, the values in Office Wide Defaults are used and the fields in the screen are grayed out.	Select Defaults if it is desired to use the values in Office Wide Defaults.

6 Click on Apply to complete securing the call control link on the VMG.

At the CS 2000 GWC Manager client

7 Select the same GWC/VMG and change the Flex policy to secure. Refer to “IPSec configuration procedures” in *GWC Security and Administration*, NN10213-611.

8 This procedure is complete. If additional VMG connections are to be secured, return to step 1 and repeat this procedure for each VMG.

Removing IPSec between the MG 9000 and the MG 9000 Manager

The following steps provide an overview of the actions required to remove a secure OAMP connection between the MG 9000 and the MG 9000 Manager.

1. From the SSM, delete the IKE Entry on the MG 9000 Manager.
2. From the SSM, delete the IPSec Entry on the MG 9000 Manager.
3. Set the IPSec connection to unsecure on the MG 9000 DCC through the LCI.

Removing IPSec from the OAMP connection between the MG 9000 and the MG 9000 Manager

At the PC or workstation with a web browser

1 To delete the IKE Entry, perform the following steps:

a To access the Server Security Manager, point a web browser to http://(ip address of server)/ipsec/security.html

where
ip address is the address of the MG 9000 Manager master server

b Login with the MG 9000 Manager user id and password having emsadm privileges.

c Click the IKE Entries link in the left frame of the HTML page. The Server IKE Entry page appears listing the entries.

d Click on the Delete Entry button.

e Click on the radio button next to the entry listing.

f Click on Apply.

2 To delete the IPSec Entry, perform the following steps:

a Click the IPSec Entries link in the left frame of the HTML page. The Server IPSec Entry page appears listing the entries.

b Click on the Delete Entry button.

c Click on the radio button next to the entry listing.

d Click on Apply.

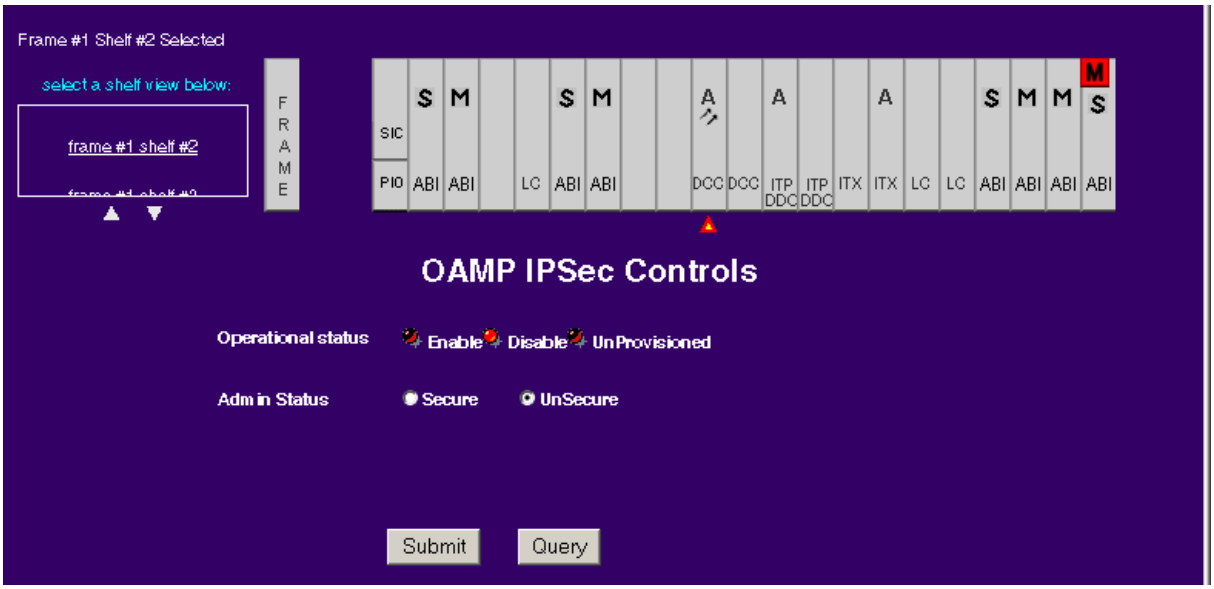
At the MG 9000 LCI

3 To disable security on the OAMP link, click on the Maintenance button, select the master shelf from the frame/shelf selector on the left.

4 Click on the active DCC card and select the IPSec Config->Controls menu.

5 Click Unsecure then click Submit.

OAMP IPSec Controls screen showing the status as disabled



6 This procedure is complete.

Removing IPSec between the MG 9000 and the GWC

The following steps provide an overview of the actions required to remove a secure signaling connection between each MG 9000 VMG and its associated GWC.

1. From the CS 2000 Management Tools, select GWC and change the IPSec policy to Flex for a particular VMG controlled by this GWC. Refer to *GWC Security and Administration*, NN10213-611.
2. From the MG 9000 Manager, set the security setting to Off for the same VMG using the Switched LInes Services GUI.
3. From the CS 2000 Management Tools, select the same GWC/VMG and delete the IPSec. Refer to *GWC Security and Administration*, NN10213-611.
4. Repeat for all VMGs as needed.

The following procedure provides the steps for removing IPSec from the signaling connection.

Removing IPSec between the MG 9000 and GWC

At the CS 2000 GWC Manager client

1 Change the IPSec policy to Flex for a specific VMG controlled by this Gateway Controller. Refer to *GWC Security and Administration*, NN10213-611.

At the MG 9000 Manager

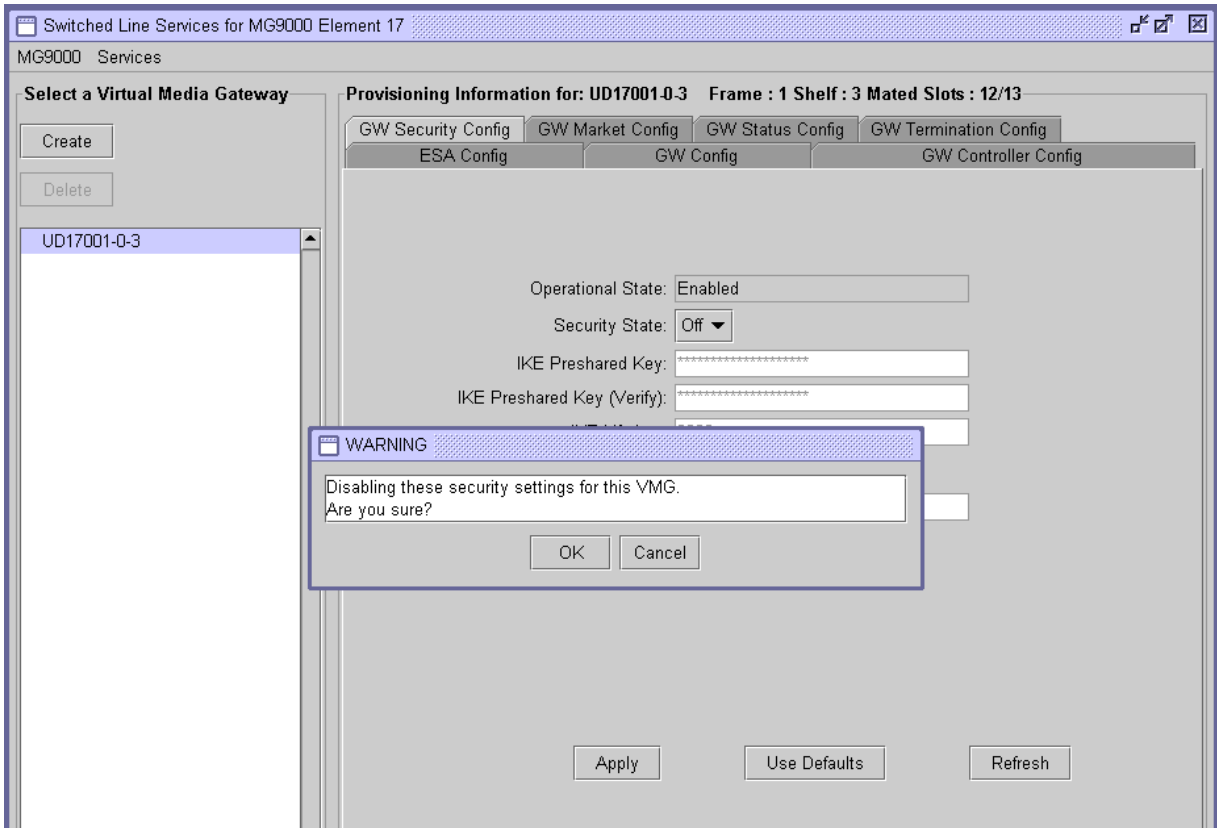
2 From the Subnet View, double click on the network element for which security on the call control link is to be provisioned. The NE desktop view appears.

3 Select Services->Switched Lines Services Manager from the menu bar. The Switched Lines Services Manager Appears.

4 Select the VMG for which security is to be provisioned.

5 Click on the GW Security Config screen. The GW Security Config screen is shown in the following figure.

GW Security Config screen with Security State Off message



6 Set the Security State to Off. A warning message will appear. Click on OK to continue.

7 Click on Apply to unsecure the call control link on the VMG.

At the CS 2000 GWC Manager client

8 Select the same GWC/VMG and delete the IPSec policy. Refer to *GWC Security and Administration*, NN10213-611.

9 This procedure is complete. If additional VMG connections are to be unsecured, return to step 1 and repeat this procedure for each VMG.

Changing NE Encryption Keys

NE Encryption Keys (Preshared Keys) must be configured in the MG 9000 and the MG 9000 Manager to encrypt certain values passed between the MG 9000 and the MG 9000 Manager and to support functions such as software upgrade and ESA data download because communication is secured for these activities. The NE Encryption Keys are configured when the MG 9000 and MG 9000 Manager are upgraded to SN08. After the upgrade is complete, no change is necessary unless the operating company wants to change the NE Encryption Keys. The password for the NE Encryption keys entered in the MG 9000 Manager and the LCI are identical to Preshared Key entered in SSM.

The Preshared key entered in the MG 9000 Manager and the LCI in the following procedure is the same value as the Shared Key entered in the OAMP IPSec Provisioning screen in the LCI.

The following procedure is provided for when the operating company want to change the NE Encryption Keys

Changing NE Encryption Keys

At the MG 9000 LCI

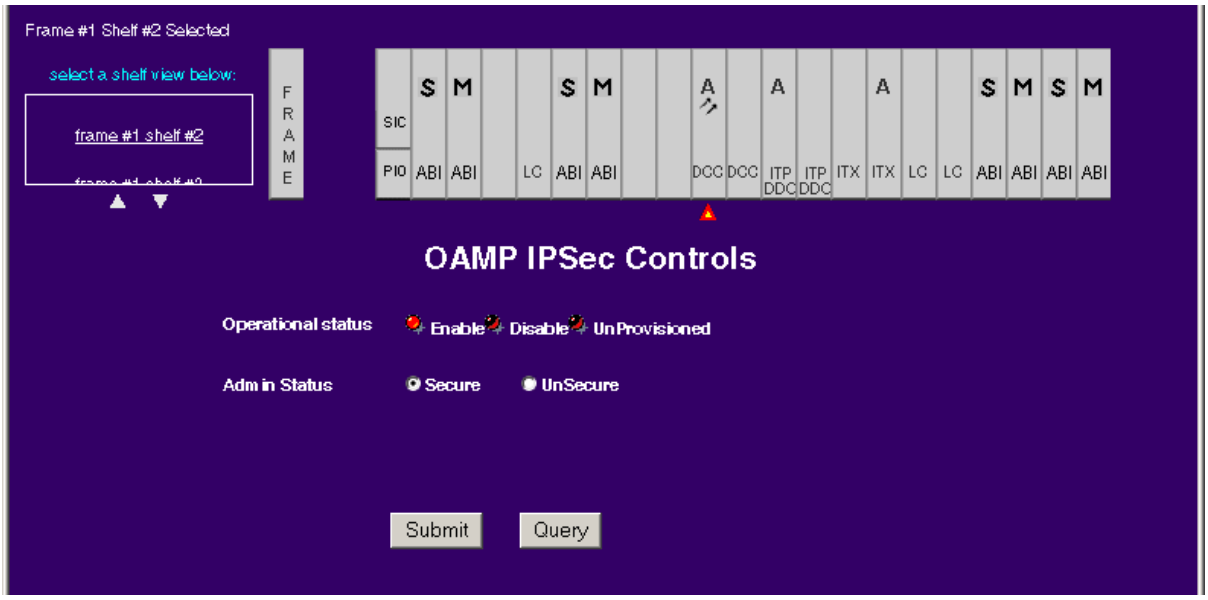
1 Use the information in the following table to determine the first step.

If IPSec is	Do
turned on	step 2
not turned on	step 5

2 From the LCI for the NE, select Maintenance.

3 Click on the active DCC card in the master shelf of the NE. From the menu bar at the left, select IPSec Config->Controls. The OAMP IPSec Controls screen appears.

OAMP IPSec Controls screen



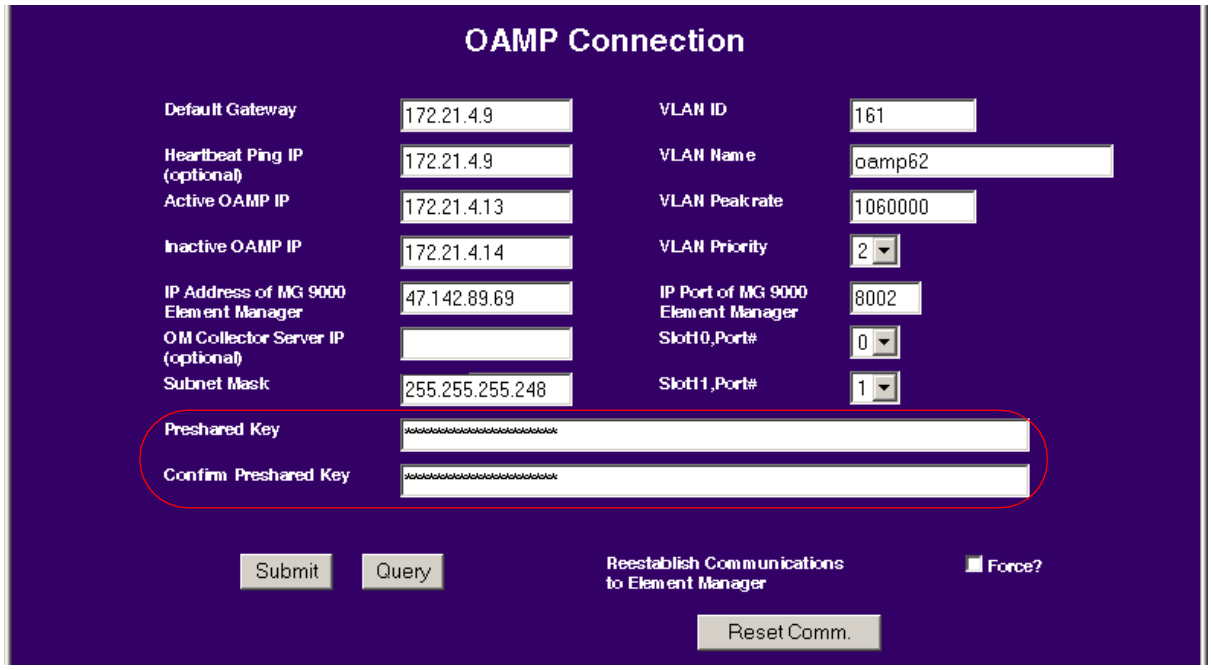
4 Set the Admin Status to UnSecure. Click Submit

At the MG 9000 LCI

5 From the LCI for the NE, select Connections.

6 Select OAMP Connection from the menu bar at the left. The OAMP Connection screen appears. The following figure shows the OAMP Connection screen.

OAMP Connection screen showing the Preshared Key field



7 In the Preshared Key field, enter 20-120 alphanumeric character key. Enter the same key in the Confirm Preshared Key field.

8 Click Submit.

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

If IPSec is	Do
turned on	step 10
not turned on	step 18

At a PC or workstation with a web browser

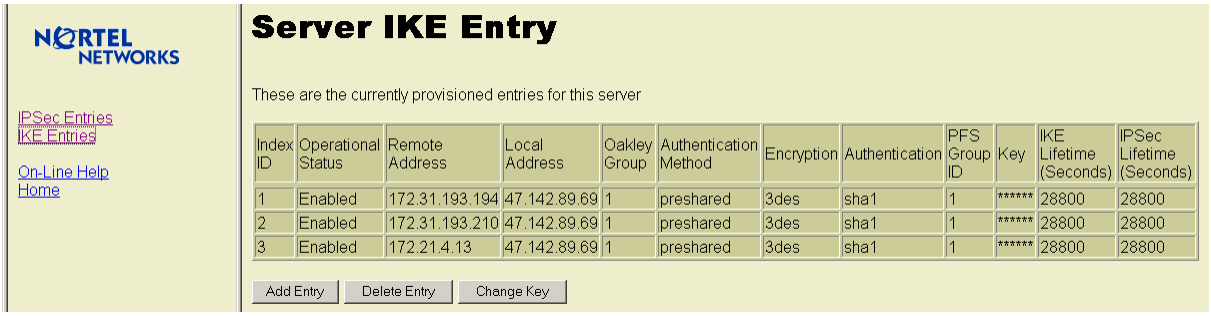
10 To access the Server Security Manager, point a web browser to http://(ip address of server)/ipsec/security.html

where
ip address is the address of the MG 9000 Manager master server

11 Login with the MG 9000 Manager user id and password having emsadm privileges.

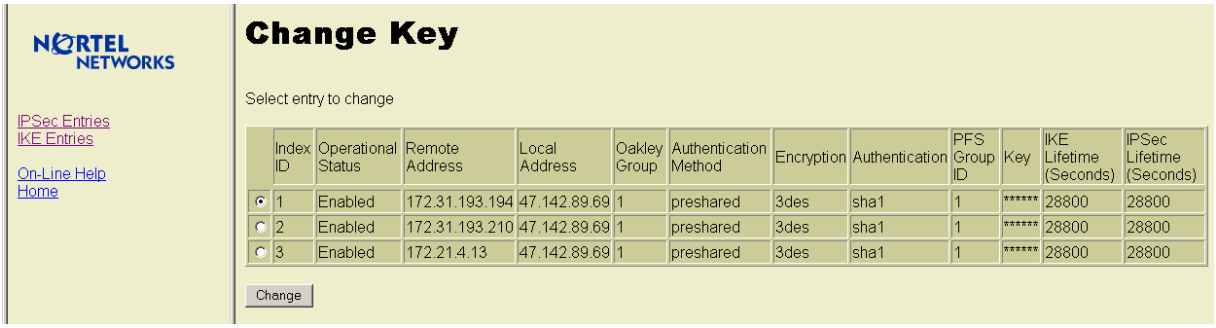
12 Click on the IKE Entries link. The Server IKE Entries page appears as shown in the following figure.

Server IKE Entry page



13 Click the Change Key button. The Change Key page appears as shown in the following figure.

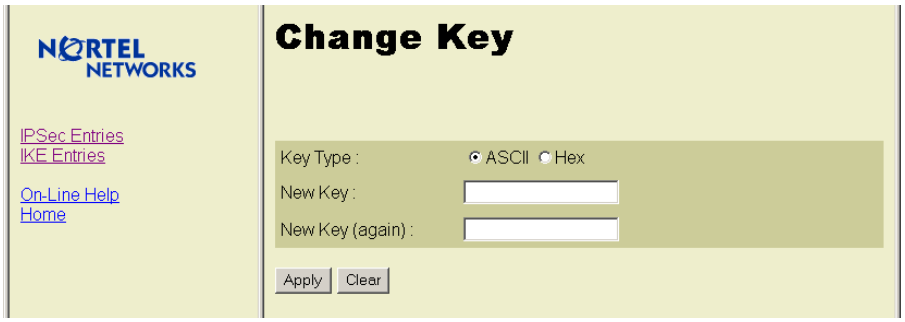
Change Key page



14 Click on the radio button next to the entry to be changed.

15 Click on the Change button. The Change Key page showing the New Key fields appears as shown in the following figure.

Change Key page with New Key fields



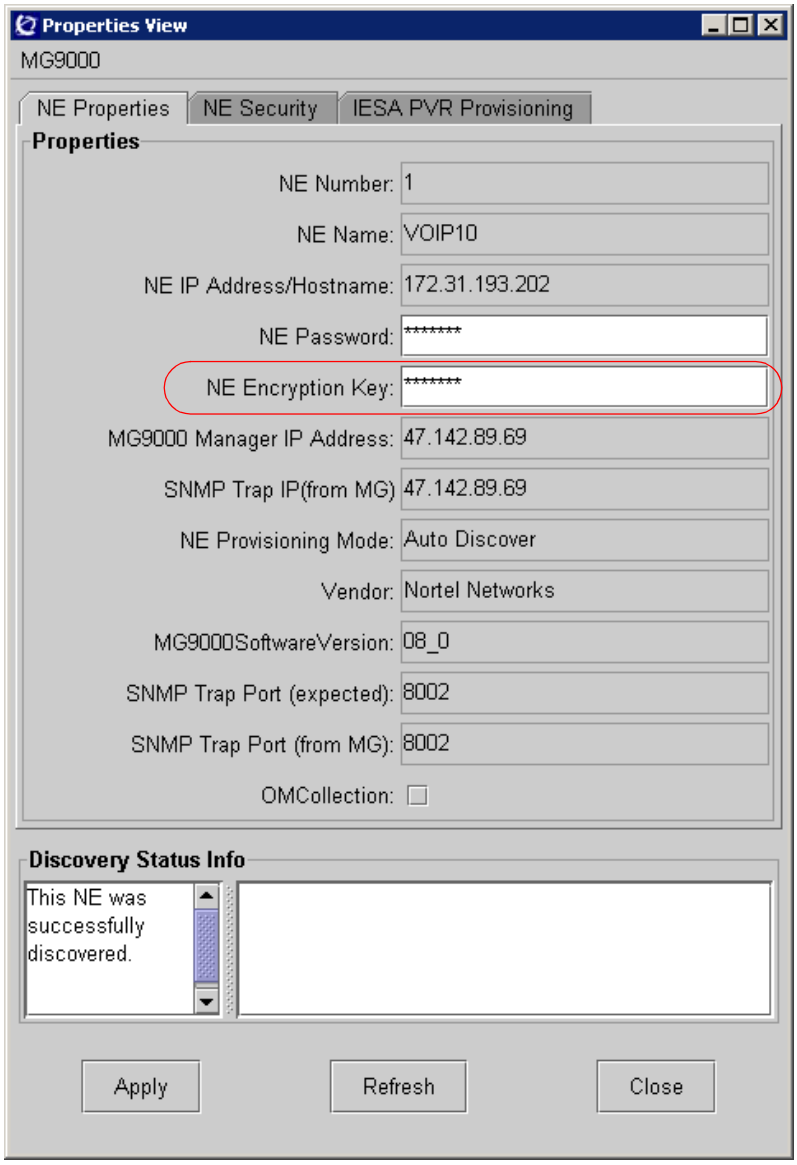
16 Enter the new key in the New Key field. Confirm the same entry in the New Key (again) field. The key must be a value between 20 and 120 alphanumeric characters and must be the same value as that entered in step 7.

17 Click on the Apply button to change the key.

At the MG 9000 Manager

18 From the MG 9000 Manager Subnet View, select the NE for which the NE Encryption Key is to be changed and select Configuration->View/Modify NE Properties. The Properties View appears. The following figure shows the Properties View.

Properties View showing the NE Encryption Key field



19 In the NE Encryption Key field, enter the same 20 to 120 alphanumeric character key that was entered in step 16.

20 Click Apply.

21 Use the information in the following table to determine the first step.

If IPSec is	Do
turned on	step 22
not turned on	step 25

At the MG 9000 LCI

22 From the LCI for the NE, select Maintenance.

23 Click on the active DCC card in the master shelf of the NE. From the menu bar at the left, select IPSec Config->Controls. The OAMP IPSec Controls screen appears.

24 Set the Admin Status to Secure. Click Submit

25 This procedure is complete.