NORTEL NETWORKS

Passport - MDM

# Network Security: Operations

NN10600-605

Passport - MDM

# Network Security: Operations

Publication: NN10600-605
Document status: Standard
Document version: 15.1RSUP, PCR 6.1
Document date: August 2004

# Publication history

## August 2004

15.1 RSUP Standard
Commercial availability except for MPE support which will be available in a future release.

# Contents

# About this document

NN10600-605 *Passport - MDM Network Security: Operations* provides procedural and conceptual information on implementing network security for engineers or anyone who provisions security in a network.

## Network security operations prerequisites

- An understanding of the architecture and operation of Nortel Networks products and Preside Multiservice Data Manager.
- Basic UNIX knowledge.
- NN10600-002 *Nortel Networks Using Task-based Documentation Job Aid* explains using the task based structure and flows that are in this publication.
- See NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/ 20000 Overview* for more information on text conventions and where to get help with technical problems.
- NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview* explains concepts and procedures directly related to network security.
- NN10600-271 *Nortel Networks Multiservice Switch 7400/15000/20000 Network Management Connectivity* explains concepts and procedures directly related to network security.
- NN10600-606 *Passport - MDM Network Security: User Access Configuration* for configuring the user access features described in this NTP.

- NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration* for configuring the secure communication features described in this NTP.

# What's new in network security operations?

The following features were added to this document:

- "User Administration for centralized authentication" (page 12)
- "Security Audit Logging" (page 12)

## User Administration for centralized authentication

The following sections were updated:

- "Infrastructure security" (page 15)
- "User authentication" (page 59)
- "Securing the infrastructure" (page 83)

## Security Audit Logging

The following sections were added for this feature:

- "Security log fundamentals" (page 20)
- "Security log procedures" (page 47)

# Chapter 1
# Network security overview

"Infrastructure security" (page 13), "User access" (page 13) and "Secure communications" (page 14) are the areas of network security which allow you to answer these questions about your network:

- Who can access the network?
- What network impact permissions they have?
- How can the network be accessed?
- Where can the network be accessed from?
- How is data kept secure as it is communicated throughout the network?

## Infrastructure security

"Infrastructure security" (page 15) is maintained by implementing security tools that promote data integrity and confidentiality in your network infrastructure.

## User access

"User authentication" (page 59) controls who can access the network and the permissions they have while using the network. Users may access a network element by connecting locally or remotely, over telnet, ftp or fmip network management interfaces.

## Secure communications

All information exchanged with node is confidential and secure when using the Passport or MPE node's secure communications features. "Secure communications" (page 73) is protecting exchanged information in the form of software downloads by FTP or operational and provisioning commands.

# Chapter 2
# Infrastructure security

Infrastructure security features are used to maintain data integrity and confidentiality in your network infrastructure. Use the following features as part of "Securing the infrastructure" (page 83) of your network.



## Authorized IP access on Passport

Using the *IpAccess* component, you can specify the IP addresses of devices that you want to allow access to the node. You can also specify an entire IP subnetwork using an IP address and a subnetwork mask

The *IpAccess* component prevents users from logging into a Passport node from an unauthorized device. When one or more *IpAccess* components exist, the node checks each authentication attempt against the list of valid IP addresses. If the authentication attempt is from a device with an invalid IP address, the node rejects the attempt.

If you do not add an *IpAccess* component, all devices can access the node regardless of their IP address.

### Authorized IP access using the User Administration system

The packets are sent to the RADIUS server where the IP address of the device is compared against two lists in the nas.properties file to determine whether to accept or deny access. The accept list identifies all the IP addresses that are granted access to the RADIUS server. The deny list identifies all the IP addresses that are denied access to the RADIUS server.

If the IP address matches an address in the accept list, the device's IP address is then compared against a list of IP addresses contained in the ne.properties file. The ne.properties file contains a mapping of IP addresses to a specific network element (NE) ID. Depending on which NE the IP address belongs to, specific messages are returned to the device.

### Shared secret between client and RADIUS server

Transactions between the client and RADIUS server are authenticated through the use of a shared secret. The radius_secret.properties configuration file defines and contains the mapping between the shared secret text and each individual RADIUS client. When a client sends a request to the server, the corresponding secret is used for authentication. If the secret is not matched, the authentication fails.

## MDM Password encryption

This section describes how password encryption between Passport and Preside Multiservice Data Manager (MDM) works, depending on which equipment initiates the connection.

### Encryption on the FMIP interface

When you log in to a Passport node from a MDM workstation, the FMIP interface is used. The workstation automatically encrypts your password using a public key encryption algorithm before sending it to the node for validation. This encryption ensures that your password travels across the network securely.

### Secure FTP authentication

Secure FTP authentication uses encrypted passwords for FTP sessions between a Passport node and an Preside MDM workstation. For more information, refer to “Secure FTP authentication” (page 75).

## Solaris operating system hardening

OS hardening improves the resistance of commercial operating systems to attacks. The system may be hardened during the installation and configuration of the operating system and is a relatively quick task to perform. Along with OS hardening the following should be considered:



### Patching internet standard protocol (NTP)

To make xntpd free of any known vulnerabilities a Sun patch should be applied to the operating system. More information about xntpd vulnerability is available at http://www.kb.cert.org/vuls/id/JSHA-53ZUEY.

### File system lockdown

The Solaris file system partitions can be mounted with various options that enhance security. It is possible to mount a file system in read-only mode to prevent file modification. This configuration prevents an attacker from storing backdoor files or overwriting and replacing files on a file system. Whenever possible, file systems should be mounted in read-only mode, and should be mounted to ignore the set-user-ID bit on files. For more information, refer to the Solaris documentation on Network File Systems.

### Log file maintenance

BSM, which can be enabled as an option of OS hardening, may require large amounts of storage space depending on the audit policy. Timely processing of the log is recommended to avoid either its filling up the file system or losing audit records. Regular rotating/processing of the /var/log/authlog is also required since as a result of OS hardening, every failed login attempt will be logged.

### Flushing mails

Sendmail daemon is disabled as a result of OS hardening. Local mails should be flushed (e.g., allowing outgoing mails) regularly before the mails fill up the file system.

## Disabling SNMP

To improve security against attacks, SNMP agents should be disabled during installations when it is not required.

For more information on SNMP see NN10600-300 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: SNMP* and 241-6001-118 *Preside MDM SNMP Surveillance Adapter Guide*.

## Firewalls

For more information on using firewalls as an added security measure, see NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*.

## Passport Idle session timeout

Passport provides a configurable inactivity interval timer that automatically detects and terminates idle telnet and local console port sessions. When the idle session times out, system resources held by the session are freed and new sessions can be created.

A single session can be held on each of the active and standby CPs through the local operator. The local and telnet *timeoutPeriod* attribute is disabled by default, meaning sessions can remain idle indefinitely. This state of inactivity uses up system resources needlessly as well as offers a security risk since unauthorized access is a possibility. With a command impact of *systemAdministration*, you can provision the *timeoutPeriod*, meaning that

each session will be tracked for inactivity. If a session remains idle for a provisioned length of time (5-120 minutes), the user is logged out. If that user wants to reconnect, username and password have to be re-entered.

> ***Note:*** A warning message will be issued one minute prior to the session being terminated. For example, if the *timeoutPeriod* has been set to 10 minutes and a session has been idle for 9 minutes, the user will receive a warning that they will be logged out of that session in 1 minute.

The *timeoutPeriod* is applicable to all sessions that are created after this attribute is set. If the value of the *timeoutPeriod* is changed, only new sessions created after the activation will be affected.

Any user can display the *idleTime* of an operator session. This attribute is read-only and indicates how long a session has been inactive, even if the *timeoutPeriod* attribute is disabled.

> ***Note:*** A local or telnet session is only considered to be idle after the final response of a command has been printed on the interface and no subsequent commands have been entered.

All terminations due to inactivity are logged and an override capability is available. The override capability allows users with a command impact of *systemAdministration* to disable the *timeoutProtocol* for specific userIDs. Those userIDs for which the timeoutProtocol has been disabled are exempt from inactivity tracking. The timeoutProtocol is enabled by default, therefore, when a timeoutPeriod has been configured, it applies to all local sessions.

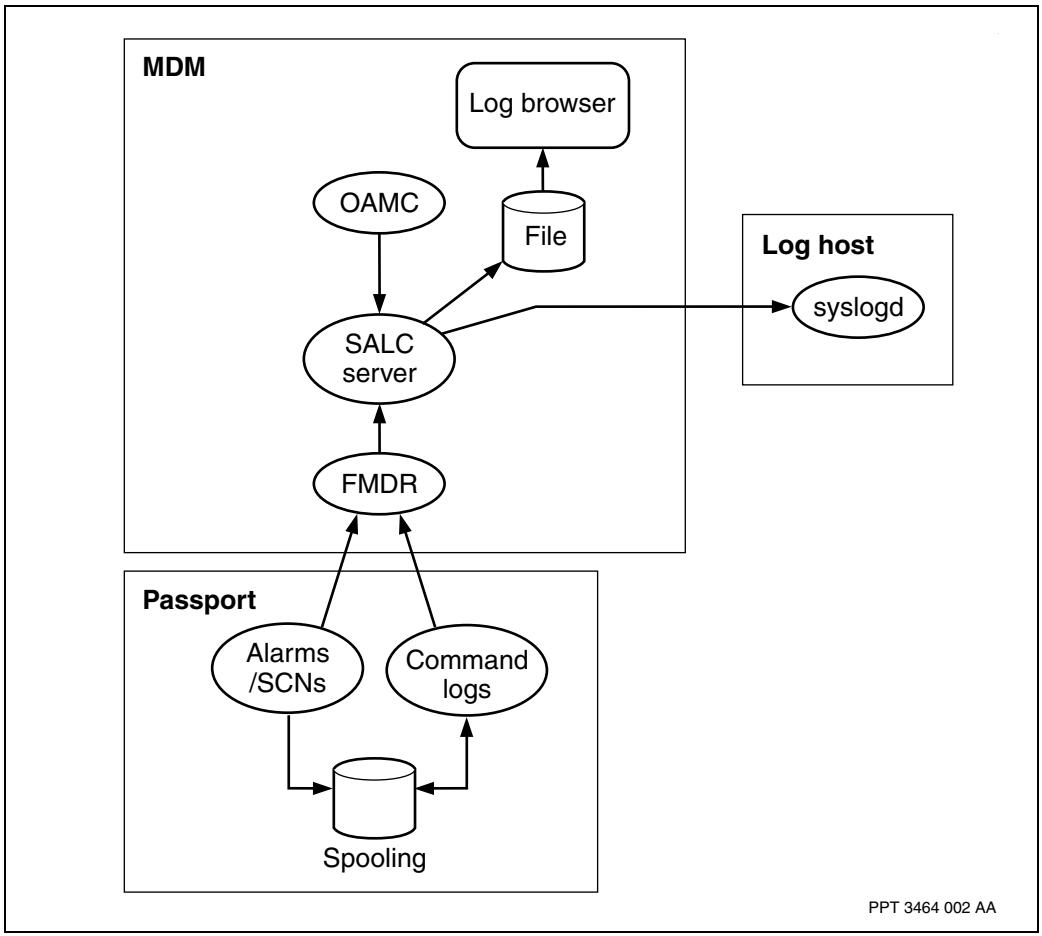
## Idle MDM operator sessions

Information about session timeouts for Preside Multiservice Data Manager is available in 241-6001-310 *Preside MDM Server Reference Guide* in the procedure for creating an FDTM user account.

# Security log fundamentals

The Security Audit Log Collector (SALC) server provides a central source of security audit information for both Passport nodes and the Preside Multiservice Data Manager (MDM). Information collected can be written to file or sent to syslogd in real-time for further analysis (see the diagram "Security log and command log data collection" (page 20)).

**Figure 1**
**Security log and command log data collection**



The SALC server receives command log and alarm streams from Passport, and security-related events from the OAMC server, and then normalizes and reformats the content prior to output. While all Passport command log information is used, the Passport alarms and the OAMC forwarded logs are filtered so that only security or operator-related events are captured. The security audit information can either be written to file in a Nortel Networks format based on the W3C Extended Log File Format, or sent to a syslogd process in real-time in a Nortel Networks recommended and RFC-3164 compliant format.

In the event of a loss of connectivity between MDM and Passport, a non real-time capability is also provided that performs a similar filtering, normalization and reformatting function using BDF alarm and command log information. The following section provide more information on security logs, Passport command logs, the common logging format, and log attributes:

- "MDM security audit logs" (page 22)
- "Passport command logs" (page 26)
- "Common logging format" (page 27)
- "Log Browser" (page 28)
- "Security log attributes" (page 29)
- "Syslog format for security events" (page 33)
- "Log severity" (page 35)
- "Command log to security log attribute mapping" (page 37)
- "Node alarm events" (page 39)

In addition to the user information that is collected in MDM security logs, third-party logs also contain pertinent user information. See "Third-party security audit logs" (page 41).

See also the following section for information on security log procedures, "Security log procedures" (page 47).

## MDM security audit logs

MDM security events are collected by the SALC server (see “Security log and command log data collection” (page 20)). Security audit logs play an important role in the Preside Multiservice Data Manager network and are used to:

- record security critical events that hold users responsible for their security critical actions
- resolve possible disputes about events
- enable security breaches to be detected after they have occurred

Log messages can contain sufficient content to aid in real-time intrusion detection and after-the-fact analysis. Log messages can also deter malicious users if they know their actions are being recorded.

Security audit logs also provide evidence to help determine whether the system was in a non-secure state. Log files record the before and after state of objects changed; therefore, it is possible to recover the system to a safe state. See “MDM security audit events” (page 23) for a description of the MDM events collected.

### MDM security audit events

The OAMC server receives security audit events from individual Preside Multiservice Data Manager (MDM) servers. These events are filtered and then sent to the SALC server. The table "MDM security events logged" (page 23) lists the various security events that can be generated from the servers.

**Table 1**
**MDM security events logged**

| Area | Tool | Description |
|---|---|---|
| Fault | Network Viewer | Network Model Editing commands: Enable editing, create (NM model, node link), load, apply, save<br>Node Menu: Set ack. state, Set maint. state, ack/unack alarms. |
| Fault | Shelf View | Local clear, global clear, alarm ack/unack<br>Fault->alarm ack/unack on component<br>Fault->set maint. on. |
| Fault | Alarm Display | Start tool -> Fault -> Ack/unack alarms on component<br>Local clear, global clear |
| Fault | Network Status Bar | Troubled components -> FaultAck/unack component<br>Acknowledge |
| Fault | Component Information Viewer | Set Acknowledge state on<br>Set Maintenance state on<br>Start tool -> Fault -> Ack/unack alarms on component<br>Local clear, global clear<br>Ack/unack alarms |
| Fault | IP Discovery | Chg password<br>Pwd login success/fail |
| System > Administration | GMDR Admin | Admin mode - login success/fail, chg pwd reset db<br>Connect/disconnect<br>Edit, add, delete |

(Sheet 1 of 3)

**Table 1**
**MDM security events logged**

| Area | Tool | Description |
|---|---|---|
| System -> Security | Disruptive command safeguard | Enable/disable |
| System -> Security | Passport Encryption | Requires security log |
| Configuration ->Passport -> Devices ->Service Provisioning | Frame Relay Service | Template changes |
| Configuration ->Passport -> Devices -> Administration | ATM Traffic Management Profile Editor | Save/delete |
| System -> Administration | Nodal Provisioning Template Editor | Save |
| System -> Administration | Nodal Provisioning Administration | Save and change events |
| | DataSync configuration editor | Save/change events |
| System -> Administration | MDM Software Quickstart | QuickStart logs - configuration files |
| System -> Administration | Server Management | Admin mode - login success/fail, change password.<br>Server add, remove, start, stop, edit |
| System -> Administration | Service Selection | login success/fail<br>changing WS wide<br>pwd change |
| System -> Administration | HGDS admin | Security event for Save<br>Security event for kick Passport |

(Sheet 2 of 3)

**Table 1**
**MDM security events logged**

| Area | Tool | Description |
|---|---|---|
| MDP | mdpclean<br>mdpdiskmgr<br>gmdpcofig,<br>dpdmm,<br>mdpfmmgr,<br>mdpfpmgr,<br>mdpppmgr<br>mdpdpnmgr,<br>mdpsrs | non-administrator (mdpadmin) user trying to run some of the MDP applications |
| MDP | file prober, srs | adding, deleting, changing login user/password to connect to Passport<br>authentication failure when connecting to Passport |
| MDP | | turning alarms or traps on/off<br>changing log levels<br>turning collection of logs on/of |
| MDP | file mover | adding, deleting, and changing upstream ftp user/password |

(Sheet 3 of 3)

## Passport command logs

Passport command logs track operator activities while they are provisioning or accessing a switch. These logs contain enough information for analysis of security problems. Audit trail information also identifies the root cause of problems.

Operator command logging is a part of the Passport Data Collection System (DCS). These logs can be spooled to disk to be collected by MDP or streamed to the NMIS. Command logs include:

- all non-passive local and telnet session commands
- all non-passive FMIP session commands
- all login attempts (successful and unsuccessful)
- all logouts
- FTP server (internal) commands
- all non-passive SNMP SET commands

See “Passport command log to security log attribute mapping” (page 37) for details on how Passport command logs map to MDM security logs. Additionally, “Node alarm to log attribute mapping” (page 39) contains the translation of node alarms to MDM security logs.

For more information on the Passport command log format, see 241-6001-806 *Preside MDM MDP Data Formats for DPN Reference*. For more information on the Passport alarm format, refer to NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

## Common logging format

A common logging format defines common log attributes and log content that appear in MDM security logs. The destination of logs determines the format of the records. When security logs are sent to syslogd, the logs are written in the Nortel standard format in a flat file. A flat file format for logs allows MDM logs to be compatible with the Log Browser (see “Log Browser” (page 28)).

A flat file format is based on an Internet standard proposed by W3C body. The log format allows customized log files to be recorded in a format that is readable by a generic analysis tool. A header specifying the data types recorded precedes the start of each log. Fields within the record are delimited by a tab character. The logging format defines mandatory security log attributes that are a super set of mandatory application log attributes. These are used as the basis of a common log format. An example of a log file is given in “Example of security log file” (page 30).

## Log Browser

The Log Browser is a tool used for viewing logs that are generated in the Nortel Networks standard log file format. Several servers generate this type of log, which have the file extension of .nlog or .alog. The .nlog files contain information about security events while the .alog files contain application-specific logs.

Security log files are located in /opt/MagellanNMS/data/security and can be browsed by administrators using the Log Browser. The Log Browser can import multiple log files of the same type and filter and sort the resulting records based on field values.

The Log Browser tool is available from the Preside Multiservice Data Manager Toolset and from Operator Client. The Log Browser can be launched from the application main window by selecting **System -> Administration -> Log Browser** or from the **Operator Client** window by selecting **System -> Administration -> Log Browser**. For more information on the Log Browser, see the online documentation available from the **Help** menu of the Log Browser.

## Security log attributes

Security logs (.nlog) and application logs (.alog) contain pertinent information that describes an event. Application logs contain the common log attributes described in “Common log attributes” (page 29).

Security logs contain the common log attributes and additional recommended security attributes. The security log attributes are described in the table “Security log attributes” (page 31). The optional attributes (those listed as not recommended in the table) are not written to the Nortel Networks standard log file by default.

**Table 2**
**Common log attributes**

| Log attributes | Description |
|---|---|
| Date | The date and time attribute represents the time the event is recorded by the process which may not be represent the time the event actually occurred. The format of the date and time is <YYYYMMDD>T<HHMMSS.ss> in accordance with ISO standard 8601. |
| Src | The Src is the source of the event and can be of the form FQDN IpAddress:port. FQDN stands for fully qualified domain name. It represents the identity of the NE/EMS that issued the log. If the fully qualified domain name cannot be resolved then the hostname is sufficient. All other elements of the Src are optional, such as the ipaddress of the NE/EMS where the log was issued and the port from which the log was sent. |
| Process | This attribute is the name of the software process for which the log was generated. It can be of the form <process>:<pid>. The pid is the process id of the process running on the workstation. |
| Src_usr | This attribute is the name of the user for which the log is generated. This attribute may contain a userId or may contain the name of another software process. |
| Stat | The status of the event can be the following values:start, end, success, failure. |
| Message | An English message that describes the event. The message text should be self contained such that one does not need to rely on past log records to understand what is happening. |
| (Sheet 1 of 2) | |

**Table 2**
**Common log attributes (Continued)**

| Log attributes | Description |
|---|---|
| Level | The severity level of the event. |
| Logger | The logger instance that generated the log message within the process. |
| Log_type | The type of log being generated. Possible values are application, security, alarm. |
| (Sheet 2 of 2) | |

Security logs contain customized attributes. If a log generates an MDM alarm, certain log attributes are included for this event. Security-related log attributes are based on the Security IPT recommendations of mandatory logs attributes. Logs that raise MDM alarms contain log attributes specific to MDM that satisfy the minimum required content of an MDM alarm.

### Example of security log file

```
 #Fields: Date Level Logger Src_usr Src Process Message
Stat Log_type
Dst Doc Mid Src_offend Dst_usr Src_mail Rel
Vol Vol_sent Vol_rcvd Cnt Cnt_sent Cnt_rcvd
Host Host_type Prog_file Prog_line Tty Prot Cmd
Evnt_type Src_oid Log_date
#Start-Date: 2004-03-17 15:45:29UTC
#Type: W3C
20040317T104532EST INFO security.FMDR.salcserver PERF EM/
BARCELONA DCS empty success application - "NMIS FMIP
SESSION/9" "set Nmis Fmip Session/9 dataStreams ala ~deb
log scn ~rts " - - 20040317T104531EST

20040317T104532EST INFO security.FMDR.salcserver PERF EM/
SQUAW VALLEY DCS empty success application - "NMIS FMIP
SESSION/10" "LOGOFF PDU received fro
m 47.128.154.244" - - 20040317T104531EST

20040317T104532EST INFO security.FMDR.salcserver
```

**Table 3**
**Security log attributes**

| Log attribute | Recommended (Y/N) | Description |
|---|---|---|
| Dst | Y | <IP address or fully qualified host name><:port>Address of the device that triggered the security event. |
| Mid | Y | MDM.<program>.<msg code>. Message Identifier: allows the message text to change, for translation to other language or to fix a typo, without affecting analysis tools. (MDM fault/message code. Security events could be identified using this log attribute) |
| Doc | Y | Names of resources accessed. These may be a database, file, web site, or a switch component. |
| Event_type | N | User initiated Security Action - authentication attempts login, unauthorized access, and so forth.<br><br>1) User initiated Network Element provisioning actions<br>2) User Initiated EMS provisioning actions<br>3) User initiated Session monitoring actions<br>4) User initiated miscellaneous actions<br>5) System initiated Network Element event<br>6) System initiated EMS event<br>7) Scheduled NE action<br>8) Scheduled EMS action |
| Src_sl | N | Security level. This is the user privilege group of the user specified in Src_usr. |
| Src_offend | N | <IP address or fully qualified host name>:<port>. Address of the originating packet that triggered the security event. |
| Src_mail | N | Email address of the Src_usr. |
| Src_oid | N | OID of the Src. |
| Dst_usr | N | Destination userID. This could be the identifier of a human user, process, system, etc. |
| Cmd | N | Command that caused the log. This is filled in when available. |
| Vol | N | The total number of bytes. |

(Sheet 1 of 2)

**Table 3**
**Security log attributes (Continued)**

| Log attribute | Recommended (Y/N) | Description |
|---|---|---|
| Vol_rcvd | N | The number of bytes received. |
| Vol_sent | N | The number of bytes sent. |
| Cnt | N | The total count. |
| Cnt_rcvd | N | The quantity received. |
| Cnt_send | N | The quantity sent. |
| Host | N | The name of the host that issues the log. |
| Host_type | N | The device type from which the log was generated. |
| Prog_file | N | The name of the program source file from which the log was generated. |
| Prog_line | N | The line number of the Prog_file source file. |
| Tty | N | The terminal type. |
| Prot | N | The protocol used. |

(Sheet 2 of 2)

## Syslog format for security events

The SALC server sends security events to the local workstation syslog daemon, if it is added by the server management daemon in MDM. The format of the log message is not the common log format that is used to write logs to file.

All fields that exist in the common log format are written in the syslog message in name value pairs: <Log attribute>=<value> or <Log attribute>="<value>". In the cases where a value does not exist for a particular attribute, a hyphen is inserted. An example syslog record is given below.

```
Feb 12 15:27:03 localhost DCS: class_security.ver01
CLIENT_DATE=20040212T153557 SRC.USR=FAULT SRC=EM/
SQUAWVALLEY MESSAGE=empty STAT=success
LOG.TYPE=application DST=- DOC="NMIS FMIP SESSION/35"
SRC.OFFEND=- DST.USR=- SRC.MAIL=- REL=- VOL=- VOL.SENT=-
VOL.RCVD=- CNT=- CNT.SEND=- CNT.RCVD=- HOST=- HOST.TYPE=-
PROG.FILE=- PROG.LINE=- TTY=- PROT=- CMD="LOGOFF PDU
received from 47.129.20.10" EVNT.TYPE=- SRC.OID=- MID=-
```

The PRI field is a key field for writing logs to syslogd since it determines how log records can be directed. It is equal to the sum of two quantities: an enumerated log severity value and an enumerated facility value (a facility value is a numerical categorization of an application or system). According to standards, only one facility value should be used for OAMC and another used for SALC server. A default facility value of local0 is chosen for the OAMC and local1 for the SALC; however, these facility values can be overridden through the command line for OAMC and SALC. The facility values that MDM may use are listed in the table “Facility values” (page 34).

**Table 4**
**Facility values**

| Numerical code | Value |
|---|---|
| 8 | user |
| 128 | local0 (default OAMC facility) |
| 136 | local1 (default Security log facility) |
| 144 | local2 (default for salcbdf) |
| 152 | local3 |
| 160 | local4 |
| 168 | local5 |
| 176 | local6 |
| 184 | local7 |
| | |

## Log severity

The Level field in the common log format can have the following tabulated Log severity values. Each log severity value corresponds to a syslog severity numerical code which represents the relative importance of a given log message. Security events can be written to syslog daemon instead of in the common log format. In this case, the syslog severity would be mapped as in the table "Log severity mapping" (page 35).

**Table 5**
**Log severity mapping**

| Log severity | MDM alarm severity |
|---|---|
| FATAL | CRITICAL |
| ALERT | |
| CRITICAL | MAJOR |
| ERROR | MINOR |
| WARNING | WARNING |
| CLEARED | CLEARED |
| NOTICE | INDETERMINATE |
| INFO | |
| DEBUG | |
| TRACE | |
| | |

If a critical alarm event is generated, a MAJOR alarm is sent and a CRITICAL log is generated in OAMC. Internally to MDM, these syslog severity do not provide the granularity required, so there is an internally-defined severity that maps to a severity for syslog. The table "Log severity values" (page 36) lists the log severity values.

**Table 6**
**Log severity values**

| Syslog numerical code | Log severity value | Description |
|---|---|---|
| 0 | Emergency: system unusable | A process is exiting due to a fatal error. |
| 1 | Alert: action must be taken immediately. | Immediate human intervention is needed. |
| 2 | Critical: critical conditions | Event needs human intervention, but no immediate action. Redundancy lost. |
| 3 | Error: error conditions | Restart, resource limit, fault, communications lost. |
| 4 | Warning: warning conditions | Event not yet requiring human intervention. Resource nearing limit, intrusion, account lockout. |
| 5 | Notice: normal but significant condition | Login denied, exception condition. |
| 6 | Informational: informational message | Login success, activity traces, security data change. |
| 7 | Debug: debug-level messages | Detailed information for software personnel and troubleshooting. |
| 7 | Trace: trace level messages | Trace logs describing entry and exit points of class methods. |
| | | |

## Command log to security log attribute mapping

The table "Passport command log to security log attribute mapping" (page 37) details the translation of the Passport log record into a Preside Multiservice Data Manager log record for security events.

**Table 7**
**Passport command log to security log attribute mapping**

| Log attribute | Values | Description |
|---|---|---|
| Date | "date time" in the security log | Time of the security event. |
| Client_date | "date time" in the security log | Actual time of security event on the node. |
| Src | componentName in the security lo | The first token value pair in the componentName is Src. |
| Process | "DCS" | Data Collection System on the node. |
| Mid | NA | Message Identifier: allows the message text to change for translation to other language or to fix a typo, without affecting analysis tools. |
| Src_offend | NA | Address of the originating packet that triggered the security event. |
| Dst | NA | Address of the device that triggered the security event. |
| Message | NA | Node command log does not contain an equivalent field for this attribute. |
| Doc | componentName field from Passport log | Name of resources accessed. These may be a database file, website, or a switch component. Remaining tokens in the ComponentName after the first two that is used for the Src. |
| Stat | response field from Passport log | The success/failure indicator of the command. Response field from the log. "OK" and return codes less than 400 for ftp are considered as a "success" and all others are considered as "failure." |

(Sheet 1 of 2)

**Table 7**
**Passport command log to security log attribute mapping (Continued)**

| Log attribute | Values | Description |
|---|---|---|
| Cmd | command field from Passport log | Command issued to switch. |
| Src_usr | userID field from the node log | UserID field from node log record. |
| (Sheet 2 of 2) | | |

## Node alarm events

Passport alarms are filtered to include only events that supplement command logs and include the following types of alarms:

- security - alarm indicates a problem related to security, for example, unauthorized access
- operator - alarm indicates that some event was caused by an operator action, for example, locking a component

The table "Node alarm to log attribute mapping" (page 39) details the translation of the node alarms into a Preside Multiservice Data Manager log record for security events.

**Table 8**
**Node alarm to log attribute mapping**

| Log attribute | Values | Description |
|---|---|---|
| Date | "date time" in the security log | Time of the security event. |
| Client date | "date time" in the security log | Actual time of the security event on Passport. |
| Src | componentName in the security log | The first token value pair in the componentName is Src. |
| Process | "DCS" | Data Collection System on the Passport. |
| Mid | MDM + originator-Class + faultCode | Message Identifier: allows the message text to change for translation to other language or to fix a typo, without affecting analysis tools. |
| Src_offend | NA | Address of the originating packet that triggered the security event. |
| Dst | NA | Address of the device that triggered the security event. |
| Message | probable cause + command | An message that describes the security event. |

(Sheet 1 of 2)

**Table 8**
**Node alarm to log attribute mapping (Continued)**

| Log attribute | Values | Description |
|---|---|---|
| Doc | componentName field from Passport log | Name of resources accessed. These may be a database file, website, or a switch component. Remaining tokens in the ComponentName after the first two that is used for the Src. |
| Stat | response field from Passport log | The success/failure indicator of the command. Event field is mapped as follows: set ->start, clear -> end, message->failure when “severity”=(major, minor, warning, critical); otherwise, message ->success for all other severity values. |
| Cmd | NA | Command issued to switch. |
| Src_usr | NA | UserID field from node log record. |
| (Sheet 2 of 2) | | |

## Third-party security audit logs

In addition to the user information collected in MDM and Passport security logs, third-party logs also collect user information. This section describes the third-party security audit logs that specifically contain references to users and user actions. Since this information can be correlated to individuals (through userid), it is documented here to address any information privacy requirements.

Third-party security audit events are logged in the following files:

- Access logs: list the clients that connect to the server and contain the following information: the uid_domain organization, and the IP address where the request originated. These events are stored in: /opt/nortel/logs/3rd_party/netscape/slapd<host name>/access.
- Authentication logs: contain user logins and user logouts. These events are stored in /opt/nortel/logs/3rd_party/security/s1is/logs/amauthentication.nlog.
- Amsso logs: contain single sign-on log records and list the following information: Login, Logout, Session Idle Timeout, Session Max Timeout, Failed to Login, Session Reactivation, and Session Destroy. These events are stored in /opt/nortel/logs/3rd_party/security/s1is/logs/amsso.nlog.

See the following sections for more information.


- "Configuring third-party security audit logs" (page 42)
- "Sending third-party security audit logs to file" (page 43)
- "Managing third-party security audit logs" (page 44)
- "Third-party security audit log events" (page 45)

### Configuring third-party security audit logs

The following user security logs are written to file by default:

- /opt/nortel/logs/3rd_party/security/s1is/logs/amauthentication.nlog
- /opt/nortel/logs/3rd_party/security/s1is/logs/amsso.nlog
- /opt/nortel/logs/3rd_party/netscape/slapd<host name>/access

The amsso.nolg and the amaauthentication.nlog files are rolled on a daily basis and then compressed. The logging threshold for these files is controlled by the following configuration file:

```
/opt/nortel/config/applications/security/core/logging/
log4j.xml
```

The access.log file is controlled by the Sun ONE directory server console. For detailed information on configuring and managing access logs, see the *Sun ONE Directory Server Reference Manaul*.

### Sending third-party security audit logs to file

The logs that are written to the amsso.nlog and amauathentication.nlog files can be re-directed to syslog. To do this, replace:

/opt/nortel/config/applications/security/core/logging/log4j.xml **with**

/opt/nortel/config/applications/security/core/logging/syslog-log4j.xml

The logs sent to the access.log file cannot be sent to syslog.

### Managing third-party security audit logs

The access.log file is managed through the Sun ONE directory server console. Logs are deleted based on size and based on disk free space and age.

For detailed information on the logging policy for access logs, see the *Sun ONE Directory Server Reference Manaul*.

The ammso.nlog and the amaauthentication.nlog files are not removed automatically and require that the system administrator remove them from the disk. MDM has a log cleanup script that can be configured to remove these files if the user chooses to do this. See "Removing log files using mdmlogclean" (page 57) for more information.

### Third-party security audit log events

The table below lists the user security audit events that are logged. The legend contains the list of files to which these events are logged.

**Table 9**
**Third-party security audit events logged to file**

| Events | A | B | C |
|---|---|---|---|
| **Successful authentication via JWS** | | | |
| Standard User | X | X | X |
| Admin User | X | X | X |
| **Successful authentication on Motif (authentication on demand)** | | | |
| Standard user | X | X | X |
| Admin user | X | X | X |
| **Successful authentication via Radius** | | | |
| Standard user | X | X | X |
| Admin user | X | X | X |
| **Authentication failure via JWS** | X | | X |
| **User lock-up based on authentication failure (JWS)** | X | | X |
| **Authentication failure on Motif** | | | |
| Standard user | X | | X |
| Admin user | X | | X |

**Legend**

A: /opt/nortel/logs/3rd_party/security/s1is/logs/amauthentication.nlog

B: /opt/nortel/logs/3rd_party/security/s1is/logs/amsso.nlog

C: /opt/nortel/logs/3rd_party/netscape/slapd<host name>/access

**Table 9**
**Third-party security audit events logged to file**

| Events | A | B | C |
|---|---|---|---|
| **Change password** | | | |
| Via JWS change password dialog (user) | | | X |
| Via the Web UI interface (NE user) | | | X |
| Via the Security UI management for admin | | | X |
| Via the Security UI management for user | | | X |
| **User Management via UI** | | | |
| Add new roles | | | X |
| Editing roles | | | |
| Activating user | | | X |
| Deactivating user | | | X |
| Security setting changes (any password setting) | | | X |
| **Policy UI** | | | |
| Adding new rules | | | X |
| Editing rules | | | X |
| Adding new policy | | | X |
| **Session UI** | | | |
| Kill session | | X | |
| Kill session and deactivate user | | X | X |

**Legend**

A: /opt/nortel/logs/3rd_party/security/s1is/logs/amauthentication.nlog

B: /opt/nortel/logs/3rd_party/security/s1is/logs/amsso.nlog

C: /opt/nortel/logs/3rd_party/netscape/slapd<host name>/access

# Security log procedures

See the procedures below for information on how to configure the SALC server, how to view logs, and clean up logs.

## Configuring the Security Audit Log Collector (SALC) server

Configure the SALC server to collect security logs and events from the Preside Multiservice Data Manager workstation and the network in order to monitor these logs for critical events that can lead to security breaches.

### Prerequisites

- The Security Audit Log Collector (SALC) server has been added to the list of servers in Server Administration. See Adding a new server in the 241-6001-303 *Preside MDM Administrator Guide*.
- FMDR groups must be defined for the node. See the 241-6001-303 *Preside MDM Administrator Guide*.
- The FMDR server needs to be started with a command line option specifying a user ID with command impact of systemAdministration and a scope of device or higher and a customer ID of 0.

### Procedure steps

1 Create the SALC server configuration file:

```
vi /opt/MagellanNMS/cfg/SALCServer.cfg
```

2 Specify the list of workstation hostnames, OAMC and FMDR servers to connect with in the file /opt/Magellan/cfg/SALCserver.cfg using the following format:

```
Hostname: mdmhost

Servername: FMDR_GROUP1

UserID: mdmuser

Password: passwd1


Hostname: mdmhost

Servername: OAMC
```

***Note:*** Use blank lines to separate records.

**Variable definitions**

| Variable | Value |
|---|---|
| Hostname | is the Preside Multiservice Data Manager (MDM) workstation host name. |
| Servername | is the MDM server name. Possible values are OAMC and FMDR. |
| UserId | is the node user ID. At a minimum, the user ID must have systemAdministration impact and a scope of device or higher and a customer ID of 0. User ID and Password fields are not required for OAMC. |
| Password | is a clear-text password that corresponds to the user id. |
| EncryptedPassword | A Password line without an EncryptedPassword line is left unchanged by SALC. If the EncryptedPassword line is present, but empty, then SALC encrypts the value in the Password line and blanks it out. Then, it fills the EncryptedPassword value accordingly. If the customer wishes to change the Password value, the configuration file is edited by adding an un-encrypted password in place of the blank Password field value. When the configuration file is refreshed by SALC, the Password is encrypted, blanked out, and the Encrypted Password field value is replaced accordingly. |
| | |

### Example configuration

The following is an example of a configuration file prior to running the SALC server:

```
Hostname: MDM1
Servername: FMDR_G1
UserID: userid
Password: password1

Hostname: MDM2
Servername: FMDR_G2
UserID: userid2
Password: password2
EncryptedPassword:

Hostname: MDM1
Servername: OAMC

Hostname: MDM2
Servername: OAMC
```

This is the same configuration file after running the SALC server: the FMDR_G1 password remains unchanged as no ‘EncryptedPassword:’ line was specified. The FMDR_G2 password is now encrypted on the “EncryptedPassword:’ line and cleared from the ‘Password:’ line.

```
Hostname: MDM1

Servername: FMDR_G1

UserID: userid

Password: password1


Hostname: MDM2

Servername: FMDR_G2

UserID: userid2

Password:

EncryptedPassword: ncrptdpwd2


Hostname: MDM1

Servername: OAMC


Hostname: MDM2

Servername: OAMC
```

## Configuring the SALC server to send real-time security logs to Syslog daemon

Configure the SALC server to send logs to a Syslog daemon on a local or remote host for customers who use a centralized log collection system based on syslog.

### Prerequisites

- Be familiar with the SUN documentation or manpages for syslogd and syslog.conf.

### Procedure steps

1 Input the following command on the command line:

```
/opt/MagellanNMS/bin/salcserver -outputSyslog
<hostname>
```

### Variable definitions

| Variable | Value |
|---|---|
| hostname | is the host name of the workstation where the syslog daemon resides. |
| | |

## Configuring the SALC server to send real-time security logs to file

Configure the SALC server to send logs to file for customers who require that security events be logged to file.

### Procedure steps

1 Input the following command on the command line:

```
/opt/MagellanNMS/bin/salcserver -outputFile
```

Logs are sent to /opt/MagellanNMS/data/security/security.nlog.

## Configuring the salcbdf utility to send non-real time security logs to Syslog

Configure the salcbdf to send logs to Syslog to supplement the real-time data as a result of possible outages that prevent real-time data from being collected.

### Prerequisites

- The nodes must be provisioned to spool alarm and command log records.
- The MDP must be provisioned to collect and convert the spooled command log and alarm files.

### Procedure steps

1. Use the escape option to override escape characters on the command line for salcbdf. See the “Variable definitions” (page 57) below.
2. FTP or copy alarm and log bdf files that are to be converted into security log messages into

   **`/opt/MagellanNMS/data/salc`**
3. Run the salcbdf process from the command line:

   **`/opt/MagellanMDP/bin/salcbdf`**

### Variable definitions

| Variable | Value |
|---|---|
| - input <input directory> | is the directory where input alarm and log BDFs are stored. The default location is /opt/MagellanNMS/data/salc/. |
| - escape <escape character> | is the escape character used in the BDF file. By default, the escape character is set to %. |
| -start <start date> | is a mask to delimit the start time. If the hhmmss are not provided, the default hhmmss is 000000. If this argument is not present, then no masking occurs based on start time. |
| -end <end date> | is a mask to delimit the end time. If the hhmmss are not provided, the default hhmmss is 235959. If this argument is not present, then no masking occurs based on end time. |
| facility local [0..7] | is used to set the facility value for bdf security logs directed to syslog. The default is local2. |

(Sheet 1 of 2)

| Variable | Value |
|---|---|
| -outputSyslog <hostname> | is used to write bdf security logs to syslog daemon residing on <hostname>. If the hostname is not specified, then the local host is the default location. By default, the logs are sent to the local syslog when neither the -outputSyslog or -outputFile options are used. |
| -outputFile <filename> | is the output file destination for the node security log records. If this option is used, the default salcbdf syslog stream is disabled unless the -outputSyslog option is also specified on the command line. If the <filename> is not specified, the output is standard out. |
| -erase | is provided to allow BDF files that have been processed by salcbdf from the <input directory> to be removed. By default, the BDF file is not removed. |
| -help | provides usage information. |

(Sheet 2 of 2)

## Viewing security logs

View security logs to monitor for critical events that can lead to security breaches.

### Prerequisites

- The SALC server is writing security logs to file. See “Configuring the SALC server to send real-time security logs to file” (page 53).
- The Operator Client is launched.

### Procedure steps

| If running the Toolset, see... | If running Operator client, see... |
|---|---|
| step 1 | step 2 |

1 From the application main window, select System -> Administration -> Log Browser.

The Log Browser window opens and displays a dialog that prompts for the location of the security logs.

2 From the Operator Client window, select System -> Administration -> Log Browser.

The Log Browser window opens and displays a dialog that prompts for the location of the security logs.

3 Navigate to the file /opt/MagellanNMS/data/security/security.nlog.

For more information on the Log Browser, see the online documentation available from the Help menu of the Log Browser.

## Removing log files using mdmlogclean

Use this procedure to remove security log files after a given retention time. The mdmlogclean process is run from the command line; the actions are logged to file and to the OAMC server.

### Prerequisites

- You must be logged in as the root user.

### Procedure steps

1. Copy /opt/MagellanNMS/lib/cfg/MDMClean.cfg file to /opt/MagellanNMS/cfg if it does not already exist.
2. Edit the /opt/MagellanNMS/cfg/MDMClean.cfg file to add the security directory and the retention time using the following format:

```
Directory: /opt/MagellanNMS/data/security

RetentionDays: 30
```

3. Remove security log files by using the following command:

```
/opt/MagellanNMS/bin/mdmlogclean
```

### Variable definitions

| Variable | Value |
|---|---|
| Directory | is the directory that contains the log files. |
| RetentionDays | is the number of days the file remains in the directory before it is deleted. |
| | |

## Enabling mdmlogclean to write logs to file

Use this procedure to enable mdmlogclean to log its activities to file.

### Prerequisites

- You must be logged in as the root user.

### Procedure steps

1 Enable the mdmlogclean file by using the following command:

```
mdmlogclean -logFile <log level set>
```

### Variable definitions

| Variable | Value |
|---|---|
| -logFile <logLevels> | optionally, writes logs of a given level to a log file /opt/MagellanNMS/data/log/mdmlogclean/mdmlogclean.alog. Levels are one or more of the following, separated by commas: FATAL, ALERT, CRIT, ERROR, WARN, INFO, NOTICE, DEBUG, TRACE. If the log level is not specified, it defaults to “FATAL, ALERT, CRIT, CLEARED, NOTICE.” |
| | |

# Chapter 3
# User authentication

User authentication determines who has access to the network and the privileges they have for the elements in the network they are accessing.



## Passport user requirements

To access a Passport, privileges must be defined for the user that determine how the user can manipulate the node.

To manage the node, permissions must be defined regardless if a user is using "Local authentication on Passport" (page 62) or "Centralized authentication" (page 63).

The permissions the user has for managing the node are defined using the following:

- "Allowed out access" (page 62)
- "Login directory" (page 62)
- "Timeout protocol" (page 62)

## Command scope

The command scope determines on which components the user is allowed execute commands. Each user and each component has a command scope. To execute a command on a component, you must have a command scope equal to or greater than the scope of that component. The table shows the possible scopes, from highest to lowest.

**Table 10**
**Component scope values**

| Impact | Components that |
|---|---|
| Network | Affect the operation of the entire network |
| Device | Affect the operation of a node |
| Application | Affect the operation of a single service application or access port |
| | |

## Command impact

Command impact defines the importance of the commands a user can execute. Each user has a command impact. As well, each command includes a verb with an associated impact. To execute a command, you must have a command impact equal to or greater than the verb impact. The table shows the possible impacts, from highest to lowest.

**Table 11**
**Command and verb impacts**

| Impact | Verbs that |
|---|---|
| debug | Issue all commands including debugging commands.<br>WARNING: The debug level is not recommended for customer use and is typically limited for use by Nortel support personnel if required. |
| systemAdministration | Change the security of the node |
| configuration | Change the configuration of the node |
| service | Maintain services |
| passive | Display information about the node and services, but do not affect the operation or configuration of the node |
| | |

## Customer identifier

The customer identifier (CID) tells the system which customers have operational authority over each component. The CID is in the command messages that you send. You can perform operational commands only on those components that belong to the same CID as you. When you assign a CID to a component, any subcomponents that are to be accessed by that user must have the CID manually provisioned to the same value as that of the CID assigned to the parent component. Those subcomponents that already have a CID provisioned retain that value, regardless of the CID assigned to the parent component.

The network owner, known as the network manager, has a special CID of 0 (zero). Only users with a CID of 0 (zero) can do provisioning procedures.

## Allowed access

Allowed access specifies which network management interfaces (local, telnet, FMIP or FTP) the user can use to access the node.

For more information on network management interfaces, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

### Allowed out access

Allowed out access indicates if the user is allowed outgoing telnet access from the node. If it is set to *telnet*, you can telnet out of a node.

For more information on the *telnet Vr* command, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.

### Login directory

When you log into a node through FTP, the system places you into a default directory. Login directory specifies this default login directory, which is similar to the home directory in UNIX for a UserId.

### Timeout protocol

Timeout protocol specifies whether the user can override the specified time period that a telnet session and a local session can be idle before being terminated.

## Local authentication on Passport

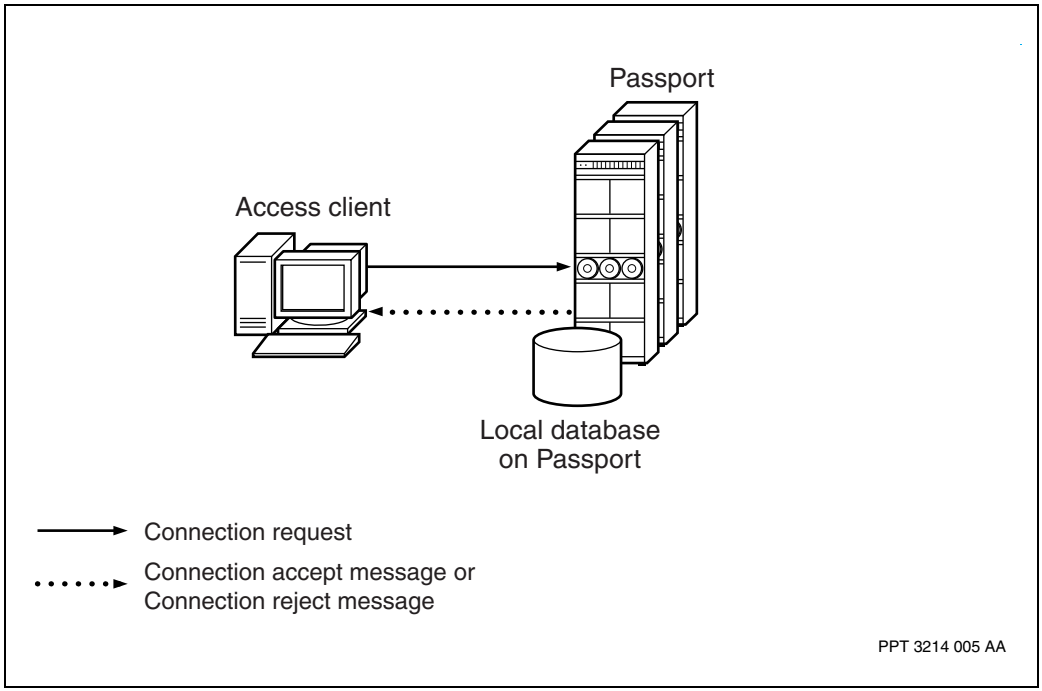
The userId component provides the ability to configure permissions to individual users specific to the node. If a userId is configured on a node then that user is considered to be a local user.

> ***Note:*** Local does not imply a physical proximity to the node, only that the userId is defined "locally" in the local database on Passport. (see "Local authentication" (page 63)).

A userId may be defined on numerous nodes and with completely different permissions. Any permissions change to the userId is independent of how the userId is configured on the other nodes.

With just "Local authentication" (page 63), you maintain the userIDs and associated passwords and access permissions on each node. If a user is not defined on the node they will not have access.

**Figure 2**
**Local authentication**




## Centralized authentication

There are five parts to centralized user authentication using RADIUS:

- Access client, which is a user session that is requesting access to the network. For example, a telnet session, FTP session, or a Preside Multiservice Data Manager (MDM) are access clients.
- Network access server (NAS), which can be the Nortel NE (Network Element such as Passport or MPE). It receives connection requests from the access client and passes on the request and associated data, such as the userID and password, to the RADIUS server.
- RADIUS server, which authenticates the connection request. For successful connection requests, the RADIUS server returns an access authorization (Access-Accept PDU) and a list of access permissions for in the form of vendor specific attributes (VSAs).

- Central database (Sun ONE directory server), where each userID and its associated password are stored and maintained. This LDAP server is used as a central authentication database for the Operator Client and the NEs. The User Administration system manages the information stored on this server.
- Optionally, the use of local authentication, by defining on the node at least one userID with system administration permissions. This userID serves as a backup authentication method in case the RADIUS server is unavailable.

## RADIUS authentication

Preside MDM provides centralized RADIUS-based authentication for users of NEs (Passport, MPE). You can use either the MDM RADIUS interface, that is installed with the security package, or your existing external RADIUS server. If you use RADIUS authentication, you can still make use of local authentication as a backup method if the RADIUS server is unavailable.

There are three options for RADIUS configuration:

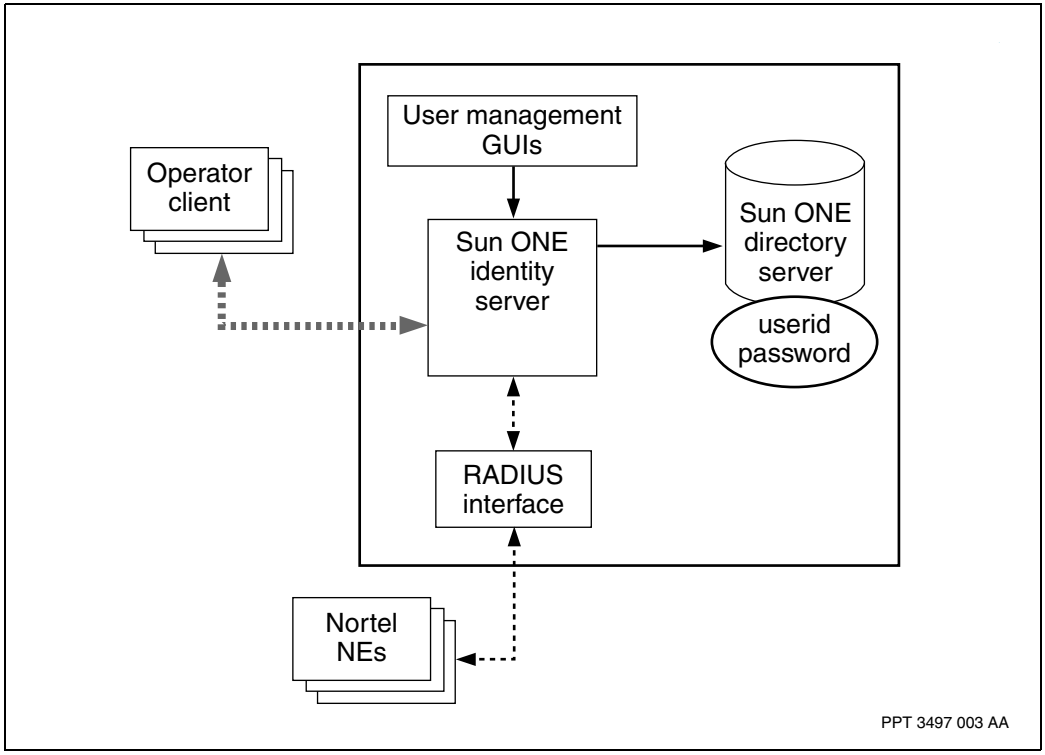
- MDM RADIUS interface only
- External RADIUS server where MDM RADIUS interface authenticates Nortel NEs
- External RADIUS server where external RADIUS server authenticates Nortel NEs

For procedures on RADIUS configuration, refer to NN10600-606 *Passport - MDM Network Security: User Access Configuration*.

### MDM RADIUS interface

The Nortel NEs are authenticated through the MDM RADIUS interface.

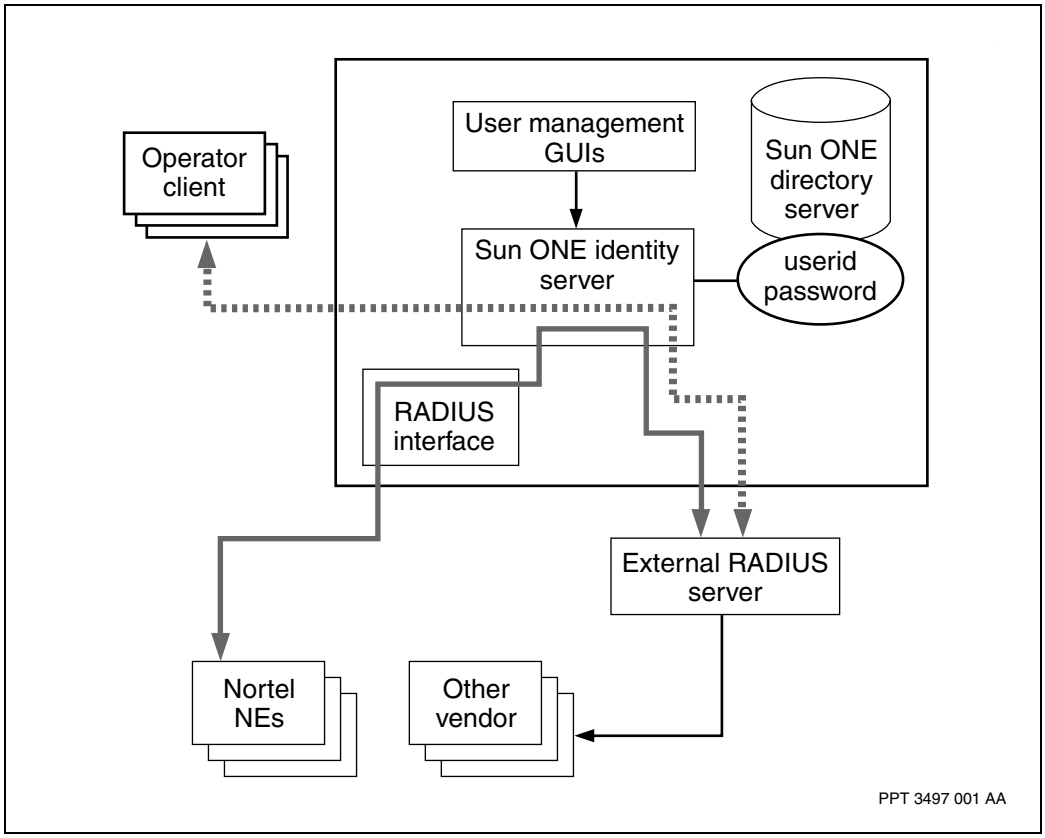
**Figure 3**
**User Management via MDM internal RADIUS interface**



### External RADIUS server where the Nortel RADIUS interface authenticates Nortel NEs

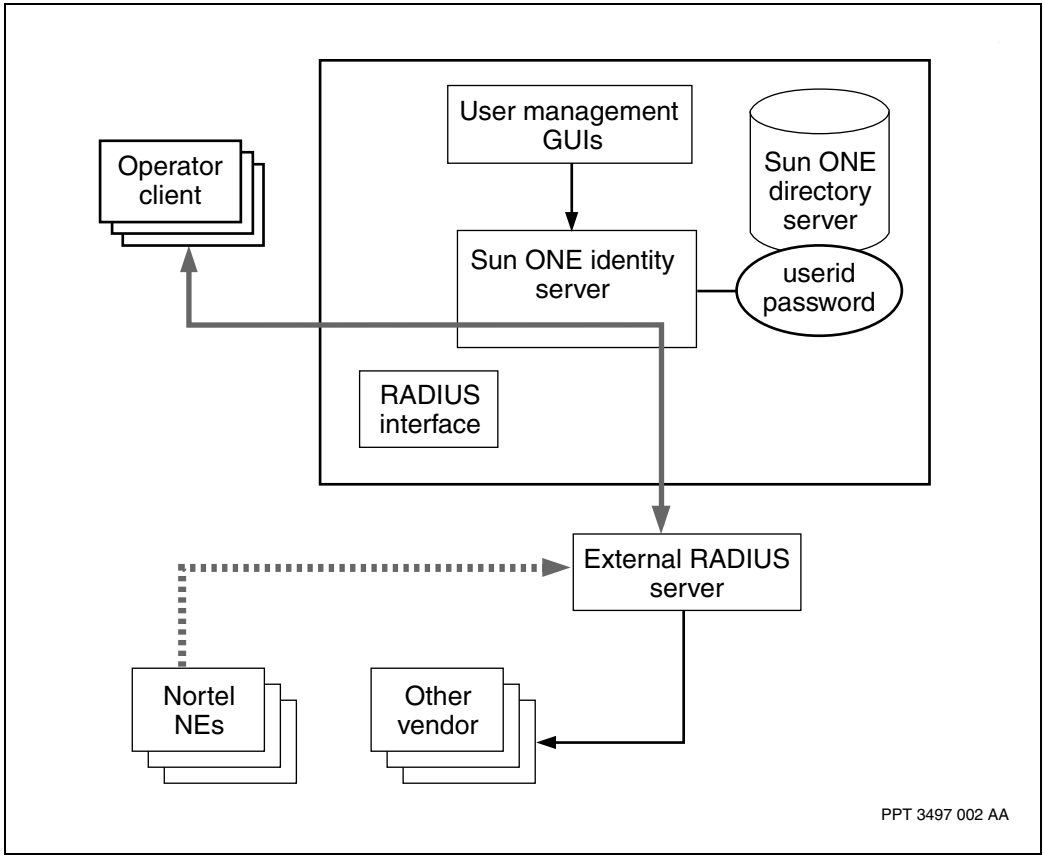
The following figure illustrates the Nortel recommended configuration which provides centralized Passport authorization for either PCR 5.1 and PCR 5.2 software releases.

**Figure 4**
**User Management where Nortel NEs authenticate users through MDM RADIUS interface but users are defined on an External RADIUS server**



**External RADIUS server where the external RADIUS server authenticates Nortel NEs**

**Figure 5**
**User Management via External RADIUS server**




In this configuration, the administrator must perform the following:

- in PCR5.1 release, the external RADIUS server must be configured to return the seven VSAs to the Nortel Passports. For more information, refer to “Radius VSAs for Passport” (page 68).
- In PCR5.2 release, you can configure the external RADIUS server to return a role name to the Passport but the role name must be defined on Passport with respect to the seven user attributes.

## RADIUS authentication recommendations

- It is highly recommended that you define at least one userID locally on the node in order to have a backup authentication method if the RADIUS server is unavailable. The local userID should have a command scope of network, command impact of systemAdministration, and allowed access to all network management interfaces.

**CAUTION**

**Local userIDs for backup authentication method**

If the RADIUS server is unavailable and you do not have any userIDs defined locally, access to the node is not possible.

- It is recommended that for redundancy purposes, each node is configured with a primary and a backup RADIUS server, each with its own database.
- It is recommended that each RADIUS server is cross-connected to each database.
- A third-party database is required. Using Sun ONE IS server as the database is recommended because Operator Client uses Sun ONE IS to authenticate users. This characteristic lets you use the same userIDs and passwords to access either nodes or MDM Operator Client.

## Radius VSAs for Passport

Each Vendor Specific Attribute (VSA) required for “Centralized authentication” (page 63) is identical to a particular Passport node attribute associated with a user that you must provision. The allowed values for each VSA and the corresponding attribute are the same.

When using remote authentication without locally defined permissions, the userIDs defined locally need to be different than those on the RADIUS server, otherwise the authentication method defaults to local for those userIDs defined both locally and remotely on the RADIUS server.

If the RADIUS server and a node are using “Roles” (page 70) then only the role VSA needs to be returned from the RADIUS server. The other VSAs do not need to be returned to Passport when using roles.

Each VSA and the matching userId or role attribute is identified in the table "RADIUS VSA's and matching userId and role attributes" (page 69).

For more information on configuring the RADIUS server with Passport VSAs, refer to NN10600-606 *Passport - MDM Network Security: User Access Configuration*.

For more information on the Passport components and attributes used with VSAs, see NN10600-060 *Nortel Networks Multiservice Switch 7400/15000/ 20000 Component Reference*.

**Table 12**
**RADIUS VSA's and matching userId and role attributes**

| VSA | userId attribute<br>Ac Userid <attribute> | Role attribute<br>Ac Role <attribute> |
|---|---|---|
| Passport-Command-Scope | *Ac Userid commandScope* | *Ac Role commandScope* |
| Passport-Customer-Identifier | *Ac Userid cid* | *Ac Role cid* |
| Passport-Command-Impact | *Ac Userid commandImpact* | *Ac Role commandImpact* |
| Passport-Allowed-Access | *Ac Userid allowedAccess* | *Ac Role allowedAccess* |
| Passport-AllowedOut-Access | *Ac Userid allowedOutAccess* | *Ac Role allowedOutAccess* |
| Passport-Login-Directory | *Ac Userid loginDirectory* | *Ac Role loginDirectory* |
| Passport-Timeout-Protocol | *Ac Userid timeoutProtocol* | *Ac Role timeoutProtocol* |
| Passport - Role | *Ac Userid role* | *Ac Role* |

## User Administration system

Centralized authentication is administered via a set of four GUI-based applications in the User Administration system.

- User Manager: used to create centralized user accounts as well as roles, which group the users into common functions.
- Policy Manager: used to create policies which define the allowable actions that the user can perform on a network element and/or allowable applications of Operator Client.

- Security Settings: used to configure basic security settings for all centrally-defined users.
- Session Management: used to view or terminate current user sessions.

Window descriptions and basic procedures for these applications are described in the online documentation. To access the online documentation from the applications, select **Help->Help on Windows**.

# Roles

The role component provides the ability to configure permissions to groups of users with the same job function. Roles can be configured on the Passport and on the Sun ONE IS.

## Roles on Sun ONE IS

The Sun ONE IS role contains one attribute only, the role name, which is usually the name of a job function. A role can be associated with any number of users or policies. For example, an administrator can create the role of Fault Management and associate it with a number of users who have permission to perform Fault Management procedures. MDM is delivered with one default role, Top-Level Admin which has the highest level of permissions.

Roles can be added, deleted or edited using the *User Manager* application.

***Note:*** The first time a user is successfully authenticated via an external RADIUS server an entry for that user is automatically created in the MDM user repository. This is a “shadow” as opposed to a real user because it is a copy of a real identity stored elsewhere. This shadow user can be associated with a shadow role. However, it is recommended that roles are created using the *User Manager* application

## Roles on Passport

The Passport role component uses the same attributes for defining “Passport user requirements” (page 59).

An operator’s permissions can change depending on how the role is defined on each node in the network. Although the role is defined on each node the permissions associated with the role can differ, depending on the settings for that specific role.

A centrally authenticated user will get the permissions provisioned for a role whose name matches the value of the role VSA returned from the RADIUS server.

If the role is defined differently on the remote server than on the node the *remoteOverride* attribute determines which definition is used for defining the role permissions.

See NN10600-060 *Nortel Networks Multiservice Switch 7400/15000/20000 Component Reference* for more information on role components and attributes.

## Policies

The User Administration system allows administrators the ability to create policies. A policy contains a set of policy rules which define the allowable actions that can be performed on a specific resource type. Policies are created by associating action permissions and resource types.

The User Administration system defines two resource types: *Passport* and a generic resource type labelled *Application,* used to launch Operator Client. Each resource type contains a set of attributes that are used to define a policy rule for logging on to the resource type.

Using the *Policy Manager* application, the administrator creates a policy rule for a resource type by entering unique values in its attribute set. These values define the user permissions for that particular resource. For ease of administration, a number of policy rules can be created and then associated with one policy.

Once the administrator defines policy rules, they can be associated with any number of users or roles.

## Remotely authenticated local user

A userId may be set up so that its permissions are defined locally, but the user is authenticated by a remote server. In this scenario, user accounts and associated attributes are still stored on-switch for authorization purposes but the actual authentication takes place using RADIUS. Users of this type are

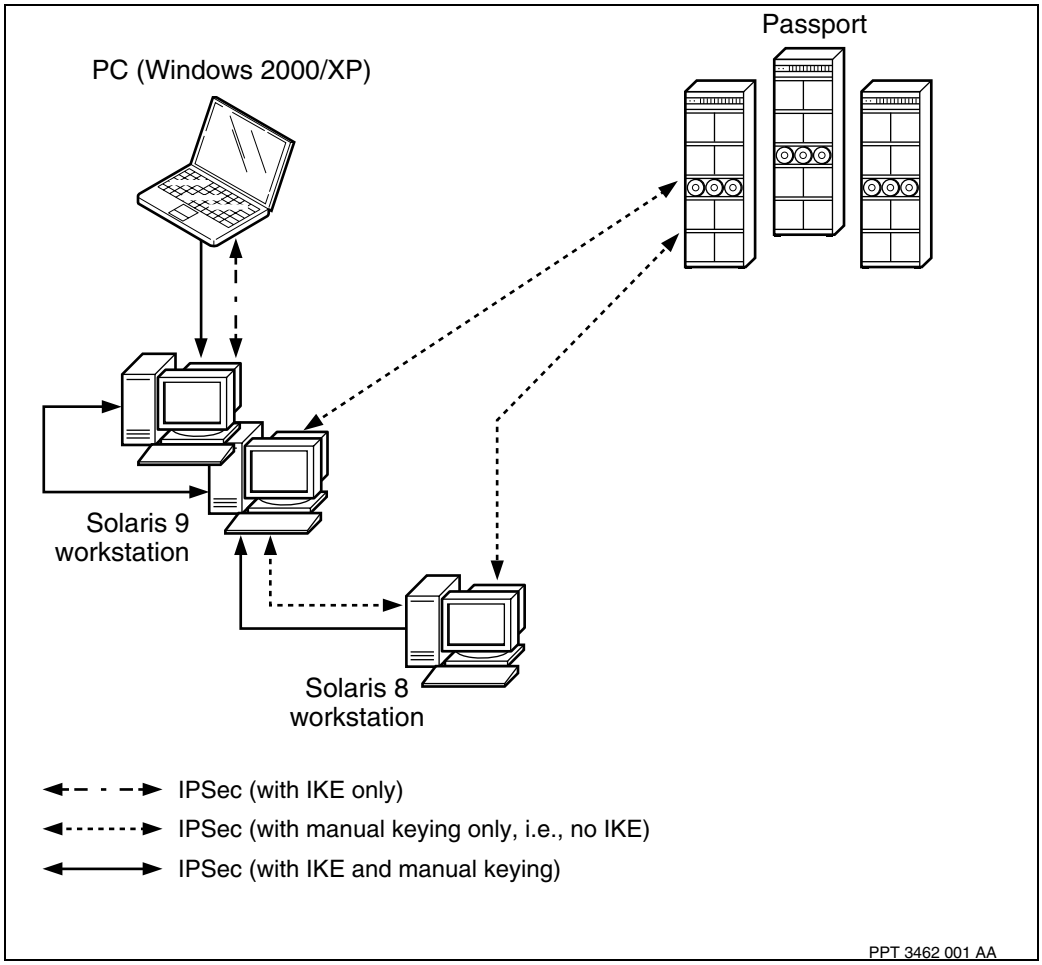
created locally on the Passport but a new user attribute called *remoteAuth* is set to *enabled* to indicate that the user is authenticated remotely on the RADIUS server.

# Chapter 4
# Secure communications

Secure communications between Preside Multiservice Data Manager (MDM) workstations, and between MDM workstations and network devices is provided via IP Security. In addition, secure FTP is used to provide encryption for passwords during FTP sessions between Passport and MDM. The methods used by each workstation and device is illustrated in "MDM Secure Communications" (page 74). For a comparison of these methods refer to "Secure communication usage" (page 74).

Use the secure communication features "Secure FTP authentication" (page 75) and "IP Security" (page 76) to ensure the data integrity and confidentiality of OAM information exchanged in the network.

**Figure 6**
**MDM Secure Communications**




## Secure communication usage

For details on the methods of secure communication used by each type of device, refer to “Communication methods used between devices” (page 75).

**Table 13**
**Communication methods used between devices**

| Method | MDM-PP | S8-S8 | S8-S9 | S9-S9 | S9-PC |
|---|---|---|---|---|---|
| IPSec | Manual key | Manual key | Manual key | IKE | IKE |
| Secure FTP Authentication | Yes | No | No | No | No |
| PP: Passport, S8: Solaris, S9: Solaris 9, PC: PC workstation | | | | | |

# Secure FTP authentication

Secure FTP authentication means that encrypted passwords are used for FTP sessions between a Passport node and a Preside Multiservice Data Manager (MDM) workstation.

When an MDM or MDP workstation initiates an FTP session with a node using PCR 4.2 software or higher, secure FTP authentication is used automatically. However, when a node initiates an FTP session with an MDM workstation, you need to configure an FTP daemon on the workstation to ensure that secure FTP authentication is used.

## Client/server communication scenarios

The client and the server use a best effort approach to FTP communications. In other words, either the client or the server attempts secure FTP authentication. If either end does not support the secure feature the transaction drops back to non-secure FTP communication. This applies to both the Preside Multiservice Data Manager and Passport node sides of the communications link.

- **secure client with non-secure server:** the client first attempts secure FTP but the server fails the communications and causes the client to drop back to non-secure FTP.
- **non-secure client with secure server:** the client initiates non-secure FTP with the server. The Passport server determines if the secure-only FTP feature is provisioned. If yes, the communication fails and the connection is closed. If it is not provisioned, the non-secure FTP proceeds over this connection.
- **secure client with secure server:** both client and server proceed with the secure FTP communications and its authentication mechanism.

In addition to the ability to ensure secure FTP authentication for sessions between MDM/MDP workstations and nodes, there is a provisionable feature that forces FTP communications on the node to be restricted to the secure type only.

# IP Security

IP Security (IPSec) is a standard for implementing security measures at the IP layer. IPSec helps to ensure a more secure overall network by protecting applications and securing communications across LANs, private WANs, public WANs, and the Internet.

Configuring IP security (IPSec) provides security for OAM traffic flowing between Passport nodes (if connected by the same management virtual router) or between Passport and Preside Multiservice Data Manager. Security protocols such as encapsulating security payload (ESP), along with key management, help to secure communication across an insecure network. Security policies (SP) define the security services to be applied to specific IP traffic flows. It is the user or system administrator who selects the SPs.

Secure communication between two peers is established in a two stage process: authentication and key establishment. Mutual authentication is required to ensure the authenticity of both parties. It is during this mutual authentication that a private session key is established to provide data authenticity and confidentiality. Keep in mind that this key must be symmetric, meaning both peers use the same key.

The following sections provide detailed conceptual information about IPSec:


- “Security associations” (page 77)
- “Security policies” (page 77)
- “Authentication and encryption algorithms” (page 78)
- “Manual Key management” (page 79)
- “Encapsulating security payload” (page 80)
- “IP flow filtering versus IPSec” (page 81)

## Security policies

Security policies (SPs) determine what security services are applied to specific OAM traffic. All security policies are contained within the security policy database (SPD).

IPSec can be applied to all IP traffic flows either terminating on or locally generated from the device (Passport, Preside Multiservice Data Manager workstation or Windows-based PC), depending on the selector associated with the packet and how it relates to the SPD. Selectors define what criteria are used in determining how IP security protocols are applied to a given packet. On Passport, one of three actions can be provisioned under the *policy* component: bypass, discard, or apply.

## Security associations

IPSec services are defined and executed through security associations (SAs). An SA is a one-way relationship that is defined between a sending and receiving host. IPSec services are applied to the traffic that is carried on SAs.

To create a peer relationship for two-way secure exchange, you need to create two SAs. An SA is uniquely identified by three parameters: a security protocol identifier, an IP destination address, and a security parameter index (SPI). Passport nodes and Preside Multiservice Data Manager (MDM) workstations establish an SA by negotiating that are defined in the security policy database.

All active SAs within a Passport node are contained within the security association database (SAD). For outbound processing, meaning packets that are generated locally and flow out to the workstation, each SA is associated with a security policy within the security policy database (SPD). If an SA can not be matched to a policy within the SPD, the OAM packet is discarded. For inbound traffic, meaning traffic that flows in from the workstation and is terminated locally, the SA entry applied to that packet is found within the SAD using fields in the IPSec packet. Both peers must be in agreement with the SA parameters specified.

Currently, SAs are limited to point-to point type connections only: you cannot configure a point-to-multipoint SA. Therefore, if you do not plan your SAs in advance, you could end up with a potentially unmanageable number of connections as your network grows.

## Security protocol identifier

The security protocol identifier specifies the type of security protocol you apply to an SA. You can choose to use authentication header (AH), encapsulating security payload (ESP), or AH plus ESP.

AH is used for data origin authentication and ESP is used for data integrity protection.

Both AH and ESP support two modes of use: transport mode and tunnel mode.

***Note:*** Passport nodes support ESP and transport mode only. AH is not supported.

## SPI

The SPI is a hex string that is automatically assigned to an SA. The SPI is carried in the AH or ESP headers.

## Destination IP address

On Passport, currently you can only specify unicast addresses as the destination IP address.

## Authentication and encryption algorithms

When you define an SA you must also specify authentication and encryption algorithms. If you are using AH alone, you only need to specify an authentication algorithm. If you are using ESP or AH plus ESP, you need to specify both an authentication and an encryption algorithm. The current specification states that you must choose an encryption algorithm that complies with the Data Encryption Standard (DES). Triple DES encryption is recommended over DES encryption.

## Transport mode

Transport mode extends protection to the payload of an IP packet. When a host runs AH or ESP, the payload is the data that normally follows the IP header. Transport mode is typically used for end-to-end communications between two hosts and should be sufficient for securing a corporate network.

## Tunnel mode

Tunnel mode encapsulates the entire IP packet within an IP packet to ensure that no part of the original packet can be changed as it moves through the network. The entire original or inner packet travels through a tunnel from one point in an IP network to another and no routers along the way need to examine the inner packet.

Tunnel mode is used when one or both ends of an SA is a security gateway, such as a firewall. Tunnel mode is also useful for dial-up access when a firewall or security gateway is used to protect an internal network. You should use tunnel mode if you are going to transport data across the Internet or through a firewall.

***Note:*** Tunnel mode cannot be implemented on a Passport node, because it supports transport mode only.

## Manual Key management

Key distribution can be configured manually on Passport nodes and Solaris 8 workstations. An encryption key (for example, DES), an authentication key, or both may be required to protect an IPSec session. These keys should be both unique and random. They must also be symmetrical, meaning that for a given Security Association (SA), those configured on a node must be the same as those configured on the workstation.

In order to ensure secure distribution of these keys, an SA must be established prior to sending provisioning data from the workstation to the node. The first SA must be added through a console port directly connected to the node and should be configured using StartUp. Distribution of the key to the console administrator of the node can be done by telephone, registered mail, or secure e-mail. After the first SA is established and traffic is protected, keys can be refreshed using this SA.

If the encryption and authentication keys are not saved in the committed provisioning file and the Passport node reboots, the Preside Multiservice Data Manager (MDM) workstation will have to provision the node with the new keying information prior to refreshing its own corresponding keys. While refreshing keys, there will be a temporary loss of connectivity because MDM

must first activate the node provisioning, then install the new keys on the workstation. After installing the new keys, connectivity will resume and confirmation of the provisioning can be completed.

> ***Note:*** If the keys are unknown, the console port on the node control processor will have to be used to restore the keys.

Scripts are provided with MDM software to configure SAs and apply encryption algorithms, as well as to generate and delete encryption keys. For a detailed description of the syntax of each script, see NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*.

> ***Note:*** If you are configuring IPSec on a Sun workstation using Operator Client only (not MDM), refer to the Sun documentation for standard procedures.

The scripts are for setting up transport mode only. Tunnel mode SAs must be configured using manual procedures.

For more information about the manual procedures that are required to set up IPSec in tunnel mode, see NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*.

## Automatic Key Management

IKE is the standard way for two IPSec clients to establish SAs or refresh keys automatically.The Solaris 9 operating system and Windows uses IKE (Internet Key Exchange) which provides a secure and automated IPSec SA negotiation.

Passport only supports manual key management.

## Encapsulating security payload

Encapsulating security payload (ESP) can provide a mix of the following security services: confidentiality, data origin authentication, connectionless integrity, and traffic flow confidentiality. The set of security services provided depends on the options selected at the time the SA is established. Encryption and authentication are optional services, however at least one of them must be selected.

The IPSec protocol used is determined by the protocol set in the IP header.

## IP flow filtering versus IPSec

When IPSec is enabled on OAM access cards (function processors) that support hardware IP flow filtering, the deny functionality of IP flow filtering should be used instead of the IPSec discard security policy. Packets will be discarded faster and there is less congestion on the CP. However, IP flow filtering is not as granular as IPSec so if any filtering must be performed on the protocol or at the TCP/UDP port level, IPSec must be used. For more information about IP flow filtering, see NN10600-800 *Nortel Networks Multiservice Switch 7400/15000/20000 IP Technology Fundamentals*.

# Chapter 5
# Securing the infrastructure

Use the procedures in this section as tools for securing the infrastructure.

## Infrastructure security tasks



## Hardening the Solaris operating system

OS hardening, during the installation and configuration of the operating system, improves the resistance of commercial operating systems to attacks.

If you upgrade Preside Multiservice Data Manager (MDM) on a Solaris operating system that was hardened prior to release 15.1, you must perform the following tasks:

- unharden the operating system using the existing MDM release and the scripts provided
- upgrade MDM to release 15.1

- harden the Solaris operating system using 15.1 operating system hardening and the scripts provided

## Prerequisites

- The operating system hardening procedures are for Solaris 8 and Solaris 9 operating systems only.
- If you are running software other than Preside Multiservice Data Manager (MDM) on the workstation, these activities could affect them.
- The OS hardening scripts are installed on the target workstation
- When you run the Solaris hardening script, unused services will be disabled and the files /var/adm/emerlog and /var/adm/loginlog will increase in size. You will need to clean up and check the partitions that contain these files routinely.

## Procedure steps

1. Log in as root from the local console.
2. Sync the file system and boot to single user mode.

   ```
   # sync;sync;sync;init s
   ```

3. Enter the root password to regain access to the workstation.
4. Run the OS hardening script.

   ```
   # /opt/MagellanNMS/bin/Solaris_OsHarden
   ```

5. Begin the OS hardening procedure. Select menu option 1:

   ```
   1) Default Hardening Configuration
   ```

   The hardening scripts are executed. Any attempt to interrupt the execution of the hardening scripts is ignored until the hardening is complete.
6. Select yes when the script asks you if you want to enable the Base Security Module (BSM).
7. Select yes when the script asks you if you want to update existing BSM configuration files with the ones that are delivered with MDM.
8. Select yes when the script asks you if you want to reboot the workstation.

# Customizing OS hardening

Customize OS hardening to control which services are disabled when you run the OS hardening script. To change the behavior of the OS hardening script, you must move the configuration files that control the script and alter their contents.

## Procedure steps

1. Copy the configuration files that you want to modify from /opt/MagellanNMS/lib/cfg/osh to /opt/MagellanNMS/cfg/osh.
2. Modify the configuration files to customize the behavior the OS hardening script to suit your specific needs.

   When you run the scripts, they will search the directory /opt/MagellanNMS/cfg/osh for customized configuration files and use those instead of the ones in the default directory.

## Procedure job aid

**Table 14**
**OS hardening scripts configuration files**

| File | Description |
|---|---|
| account_removal_list | Lists well known accounts that will be removed by the OS hardening scripts. |
| cron_disable_list | Lists users that are restricted from using cron. |
| ftp_disable_list | Lists users that are restricted from using ftp. |
| inetd_disable_list | Lists services or ports that will be disabled by the inet daemon. |
| kernel_modification_list | Describes two kernel modifications that can be made to /etc/systems. |
| netrc_lock_list | Lists accounts whose .netrc file will be touched and locked in each respective home directory |
| nfs_disable_list | Lists the tokens that can be used to disable parts of the Solaris NFS. |

(Sheet 1 of 2)

**Table 14 (Continued)**
**OS hardening scripts configuration files**

| File | Description |
|---|---|
| rauth_disable_list | Lists the tokens that disable r-services and locks the /etc/hosts.equiv file. |
| service_removal_list | Lists the run control files that will be removed from /etc/rc2.d and rc3.d. |
| (Sheet 2 of 2) | |

**Table 15**
**Replacement configuration files for OS configuration files**

| File | Description |
|---|---|
| new_audit_class, new_audit_event, new_audit_control, new_audit_user | Replaces audit_class, audit_event, audit_control, and audit_user in /etc/security to control BSM logging. |
| new_default_ftpd | Replaces /etc/default/ftpd and installs a new ftp banner. |
| new_default_telnetd | Replaces /etc/default/telnetd and installs a new telnet banner. |
| new_issue | Replaces /etc/issue and installs an identification to be printed as a log in prompt. |
| new_inetinit | Replaces /etc/default/inetinit and improves the TCP initial sequence number generation. |
| new_inetsvc | Replaces /etc/rc2.d/S72inetsvc and /etc/init.d/inetsvc and disables the NIS, DHCP and multicast network services. |
| new_kbd | Replaces /etc/default/kbd and disable keyboard or serial device abort sequences (e.g., Stop A). |
| new_login | Replaces /etc/default/login and restricts the remote login of the root user. |
| new_nddconfig | Installs /etc/rc2.d/S70nddconfig and /etc/init.d/nddconfig and makes changes to the default system and network drivers. |
| (Sheet 1 of 2) | |

**Table 15 (Continued)**
**Replacement configuration files for OS configuration files**

| File | Description |
|---|---|
| new_nscd.conf | Replaces /etc/nscd.conf and changes the Name Service Cache daemon to hold only the host information. Password, group and RBAC are not cached. |
| new_passwd | Replaces /etc/default/passwd and increases password strength. |
| new_syslog.conf | Replaces /etc/syslog.conf and increases the logging done by the syslog daemon. |
| (Sheet 2 of 2) | |

# Unhardening the Solaris operating system

Unharden the Solaris operating system to upgrade to a new version of Preside Multiservice Data Manager (MDM) to ensure that you are using the most current version of the hardening script that is included with the latest version of MDM.

## Procedure steps

1. Log in as root.
2. Sync the file system and boot to single user mode.

   ```
   # sync;init s
   ```

3. Enter the root password to regain access to the workstation.
4. Run the OS hardening script.

   ```
   # /opt/MagellanNMS/bin/Solaris_OsUnHarden
   ```

   The OS Security UnHardening Menu opens.
5. Begin the OS unhardening procedure. Select menu option 1:

   ```
   1) Default UnHardening Configuration
   ```

   The unhardening scripts are executed. Any attempt to interrupt the execution of the unhardening scripts is ignored until the unhardening is complete.
6. Select yes when the script asks you if you want to disable the Base Security Module (BSM).
7. Select yes when the script asks you want to restore your previous BSM configuration files.
8. Select yes when the script asks you if you wish to reboot the workstation.

# Viewing the status of the Solaris operating system

View the status of the operating system before you the OS hardening script to determine whether it is in a hardened or unhardened state.

## Procedure steps

1. Log in as root.
2. Run the OS show status script.

```
# /opt/MagellanNMS/bin/Solaris_OsHardenStatus
```

# Generating secure passwords for MDM servers

Generate secure passwords for Preside Multiservice Data Manager (MDM) servers to use encrypted passwords with MDM servers and ensure increased security.

## Procedure steps

1. Log in as root.
2. Start the MDM Toolset.
3. From the **System** menu, click **Security->Password Encryption**.

   The **Password Encryption Tool** opens.
4. Type a password in the **Enter Password** text field.
5. Type the same password again in the **Confirm Password** text field.
6. Type a name for the file in which you want the encrypted password to be stored.

   The new file, containing the encrypted password will be stored in the directory `/opt/MagellanNMS/cfg/private`.
7. Click **Save**.
8. Click **Close**.

# Setting encrypted passwords on MDM servers

Set encrypted passwords on Preside Multiservice Data Manager (MDM) servers to increase security by preventing access by unauthorized users. You can set an encrypted password for accessing the edit mode in the FMDR, DMDR, PMSP, and Edit (edserver) servers.

## Procedure steps

1. Log in as root.
2. Start the MDM Toolset.
3. From the **System** menu, click **Administration->Server Administration**.

   The **Server Administration** tool opens.
4. From the **Security** menu, click **Authorize Editing**.

   The **SVM Enter Authorization Password** dialog box opens.
5. Enter the edit password.
6. From the **Server name** list area, right-click on the name of the server for which you want to set secure password.

   The server name is highlighted and the **Server Functions** pop-up menu opens.
7. From the **Server Functions** pop-up menu, click **Edit**.

   The **Server Administration** edit server dialog box opens.
8. In the **Startup command** text field, replace the current password text with the full path name of the file that contains the secure password.

   If we used the example password file from the previous procedure, the new command line would look as follows:

   ```
   /opt/MagellanNMS/bin/fmdr -g GROUP1 -u mdmfault -p /
   opt/MagellanNMS/cfg/private/FMDR_GROUP1.passwd -l AL
   ```
9. Click **Save and Restart** to save your changes.
10. Click **Cancel** to return to the **Server Administration** tool main window.

# Changing encrypted passwords for MDM servers

Change encrypted passwords for Preside Multiservice Data Manager (MDM) servers when you need to replace a password that has changed.

## Prerequisites

- If a password that is used to access a Passport node is changed, the existing secure password file is no longer valid.

## Procedure steps

1. Log in as root.
2. Start the MDM Toolset.
3. From the **System** menu, click **Security->Password Encryption**.

   The **Password Encryption Tool** opens.
4. Type a new password in the **Enter Password** text field.
5. Type the same password again in the **Confirm Password** text field.
6. Type the name of the file that contained the old secure password.
7. Click **Save**.
8. At the prompt, enter the old secure password.
9. Click **Close**.

# Disabling SNMP agents

Disable all native SNMP agents to increase security against attacks when performing an installation.

## Procedure steps

1. Log in as root.
2. Change to directory `/etc/rc2.d`.
3. Locate the file that starts with the letter “S” and contains the series of letters “dmi”.
4. Change the name of the file by adding “.No” to the beginning of the name.

   For example, a file named `S77dmi` would become `.NoS77dmi`.
5. Locate the file that starts with the letter “S” and contains the series of letters “snmpdx”.
6. Change the name of the file by adding “.No” to the beginning of the name.

   For example, a file named `S78snmpdx` would become `.NoS78snmpdx`.
7. Change to directory `/etc/rc3.d`.
8. Repeat steps 3 and 4.

# Chapter 6
# Network security troubleshooting

Check for alarms and log entries when you are troubleshooting security problems. Use the following sections to troubleshoot security issues:

- “Troubleshooting centralized authentication” (page 96)
- “Troubleshooting IPSec services” (page 101)

More information on user authentication is available in NN10600-606 *Passport - MDM Network Security: User Access Configuration*.

More information on IP security is available in NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration*

# Troubleshooting centralized authentication

Most of the troubleshooting for centralized authentication can be done by logging on to the RADIUS server or User Administration system and identifying errors.

See the following tables for detailed information for troubleshooting centralized authentication.

- “Unsuccessful authentication attempt on Passport” (page 97)
- “Probable cause and solutions for common centralized authentication problems” (page 98)
- “Unsuccessful authentication attempt on Passport due to time-out” (page 100)

**Table 16**
**Unsuccessful authentication attempt on Passport**

| Troubleshooting Tips |
| --- |
| Check for the following:<br>• Invalid userID or password.<br>(When this happens, attributes *Ac Radius Server accessRequest* and *Ac Radius Server accessRejects* will be incremented.)<br><br>Confirm that the userID and password exist and have valid values.<br>• RADIUS server sends an unrecognized PDU to the node. The only PDUs that the Passport node recognizes are Access-Accept and Access-Reject.<br>(When this happens, attribute *Ac Radius Server unknownTypes* will be incremented.)<br><br>Verify the RADIUS server is configured correctly.<br>• RADIUS server does not send all required VSAs to the node.<br>(When this happens, attributes *Ac Radius Server accessRequest*, *Ac Radius Server accessAccepts*, and *Ac Radius Server malformedAccessResponses* will be incremented.)<br><br>Confirm that the set of access permissions assigned to the userID has all of the required VSAs.<br>• Your method of system access (local, FMIP, FTP, or telnet) is not the same as the session type listed in the Passport-Allowed-Access VSA.<br>(When this happens, attributes *Ac Radius Server accessRequest* and *Ac Radius Server accessAccepts* will be incremented and your session ends.)<br>• Shared secret has not been correctly configured.<br>(When this happens, attribute *Ac Radius Server badAuthenticators* will be incremented.)<br><br>Verify the shared secret values on the Radius server and the node.<br>• Session time-out. Verify session time-out settings are correct. |
| |

**Table 17**
**Probable cause and solutions for common centralized authentication problems**

| Problem | Probable Cause | Recommended action |
|---|---|---|
| You are unable to log into a Passport node using a user ID or password that exists in the central LDAP database. | The password entered was incorrect. | Verify by examining the RADIUS server log file and confirming an LDAP Bind error with return code 49: Invalid credentials. Reset the password. |
| | There is a shared secret mismatch between the node and the RADIUS server. | Verify by examining the RADIUS server log file and confirming and LDAP Bind error with return code 49: Invalid credentials. Reset the shared secret on the node and the RADIUS server. |
| | The user does not exist on the LDAP server. | Verify by examining the RADIUS server log file and confirming an LDAP BIND error with return code 32- no such object. Add the user to the database. |
| | The RADIUS server does not bind to the IP address that is specified as the serverIpAddress of the RADIUS server component on the node. That is, the RADIUS server binds to another IP address on the workstation. This often happens when the RADIUS server is running on a Solaris 8 workstation that has more than one IP address. | Run a command such as netstat to verify that the RADIUS server binds to the specified port of the expected IP address. The default port is 1812. After running the netstat command, change the serverIpAddress for the RADIUS component to the IP address to which the RAIUS is binding. The command line for running the netstat command would look as follows:<br>`netstat -na -P udp \| grep 1812` |

(Sheet 1 of 2)

**Table 17 (Continued)**
**Probable cause and solutions for common centralized authentication problems**

| Problem | Probable Cause | Recommended action |
|---|---|---|
| | The password has expired or the account is locked out. | Verify by examining the RADIUS server log file. Change the password or account lock out policy settings. |
| | The RADIUS server did not send all the required VSAs to the node. | Verify by confirming that an MSG alarm for component Ac Radius Server/<n> has been generated and the operational attribute Access Radius Server/<n> malformedAccessResponses has been incremented on the node.<br>Using User Administration tools, ensure the policies have been configured for this user to allow this user to login to Passport. |
| The LDAP server is unavailable. | The administrator password has expired. | Check the status of the administrator password and reset the password, if necessary. You must change the administrator password before it expires. |
| | The LDAP server is down. | Restart the LDAP server. |
| | There is a networking problem. | Use the ldapsearch command to verify that you can open a connection to an LDAP server, bind, and perform a search using a user's DN and its password from the RADIUS server. Resolve the networking problems if necessary. |

(Sheet 2 of 2)

**Table 18**
**Unsuccessful authentication attempt on Passport due to time-out**

| **Troubleshooting Tips** |
| --- |
| Check for the following:<br>• Configuration on RADIUS server does not match attribute *Ac Radius nasIdentifier*, *serverPortNumber*, or *serverIpAddress.*<br>• Database connected to the RADIUS server is not operational.<br>• IP connectivity between the node and RADIUS server has been lost.<br>• Network congestion. |
| |

# Troubleshooting IPSec services

Many problems with IPSec services are caused by errors in the configured settings. Refer to the following:

- "Troubleshooting actions to fix common IPSec problems" (page 101)
- "Useful commands for troubleshooting IPSec" (page 101) to identify and fix IPSec configuration errors.
- "Useful commands for troubleshooting IKE" (page 102)

**Table 19**
**Troubleshooting actions to fix common IPSec problems**

| Problem | Probable cause | Recommended action |
|---|---|---|
| You can ping a node, but you cannot telnet or FTP to it. | Your policy file does not specify the matching source and destination addresses. Your policy file should contain reciprocal definitions for both peer hosts. | Use the ipsecconf -l command to view the details of your policy file and confirm the host addresses. |
| You cannot ping the peer host at the other end. | You have defined a different encryption key or security policy on the other host. | Use the "ipsecconf -l" and "ipseckey dump" commands to view the details of the policies files on both hosts and make sure that they match up. |
| | | |

**Table 20**
**Useful commands for troubleshooting IPSec**

| Command | Action |
|---|---|
| `ipsecconf -l` | lists the details of the security policy that is currently set |
| `ipseckey dump` | lists the currently defined encryption keys |
| `ifconfig -a` | lists the network interfaces |
| `netstat -rn` | displays the routing table |
| `ipsecconf -f` | flushes the configuration file so that you can start over |
| `pkgrm` | can be used to remove the IPSec encryption packages. See your UNIX man pages for more information about the `pkgrm` command. |
| | |

**Table 21**
**Useful commands for troubleshooting IKE**

| Command | Action |
|---|---|
| ikeadm | manipulates IKE parameters and states |
| /usr/lib/inet/in.iked -c | checks the syntax of the IKE configuration file |
| | |

# Chapter 7
# Roll back procedures

Use the procedures in this section Consult the following sections to roll back from secure passwords and IPSec.

## Navigation links

- “Roll back tasks” (page 103)

## Roll back tasks

# Rolling back IPSec on Solaris 8

Roll back IPSec on Solaris 8 by removing and disabling IPSec files.

*Note:* For information on rolling back IPSec on Solaris 9, refer to the Sun documentation.

## Procedure steps

1. Log in as root.
2. Remove the scripts that automatically start IPSec.

   **rm </etc/rc0.d/K42ipsec_setup>**

   **rm </etc/rc2.d/S69ipsect_setup>**
3. Go to `/etc/inet`.
4. Remove the IPSec initialization file.

   **rm ipsecinit.conf**
5. Remove the security policy.

   **/usr/sbin/ipsecconf -f**
6. Remove these packages.

   **pkgrm SUNWcrman SUNWcry SUNWcry64 SUNWcryr SUNWcryx**

   The system will prompt you for confirmation before removing each package.

# Rolling back GMDR servers

Roll back GMDR servers from using encrypted passwords to using unencrypted passwords by replacing the filename with a clear password.

## Procedure

1. Go to the directory `/opt/Magellan/cfg` and open the file `GMDR.cfg` using a text editor.
2. Remove the encrypted password from the sixth token, which is between the fifth and sixth colons (:).
3. Type a clear password in the fourth token, which is between the third and fourth colons (:).
4. Save and close the file.
5. Restart the server.

# Rolling back FMDR and PMSP servers

Roll back FMDR and PMSP servers from using encrypted password to using unencrypted passwords by replacing the file name with a clear password.

## Procedure

1. Go to the directory `/opt/Magellan/cfg` and open the file `SVMList.cfg` using a text editor.
2. Remove the name of the file that contains the encrypted password.
3. Type a clear password in the password option field.
4. Save and close the file.
5. Restart the server.

# Rolling back IP Discovery

Roll back IP Discovery by editing the network setting file.

## Procedure

1. Go to the directory `/opt/MagellanNMS/cfg/ipm` and a open the `nsdb` file using a text editor.
2. This is a tab delimited file. For each line, put the community string in the third token, and the write community string in the fourth token.
3. For each entry address, remove the encrypted communities from the last two tokens.

   For example, after completing steps 2 and 3, a line that looked like this:
   `*.*.*.*<tab><tab><tab>161<tab><tab>encrypted Community`
   would now look like this:
   `*.*.*.*<tab>public<tab>private<tab>161<tab>`

# Rolling back the DCD

Roll back the DCD by editing the seed file for each device type.

## Procedure

1. Stop the DCD.
2. Go to the directory `/opt/MagellanNMS/cfg` and a open all the `*.sed` files using a text editor.
3. For each IP address, replace the community string in the third token.
4. For each IP address, remove the encrypted password from the last token.

   For example, after completing steps 3 and 4, a line that looked like this:
   `GEN ROUTER-1:47.1.2.205::161:100:encryptedCommunity`
   would now look like this:
   `GEN ROUTER-1:47.1.2.205:public:161:100`
5. Restart the DCD.

Passport - MDM

# Network Security: Operations

Release 15.1RSUP, PCR 6.1



Publication: NN10600-605
Document status: Standard
Document version: 15.1RSUP, PCR 6.1
Document date: August 2004
Printed in Canada

NORTEL NETWORKS