NORTEL NETWORKS

Passport - MDM

Network Security: Secure Communications Configuration

NN10600-607

Passport - MDM

Network Security: Secure Communications Configuration

Publication: NN10600-607
Document status: Standard
Document version: 15.1 RSUP, PCR 6.1
Document date: August 2004

Printed in Canada

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

NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration* provides procedural information on implementing network security for engineers or anyone who provisions security measures in a network.

Secure communications configuration 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.
- NN10600-271 *Nortel Networks Multiservice Switch 7400/15000/20000 Network Management Connectivity* explains concepts and procedures directly related to network security and start-up.
- NN10600-605 *Passport - MDM Network Security: Operations* provides conceptual information on secure communications and other network security features.
- *Sun Microsystems, IPSec and IKE Administration Guide (816-7264-10)*.
- *Microsoft, Step-by-Step Guide to Internet Protocol Security (IPSec)* at www.microsoft.com.

What's new in secure communications?

This document was updated for:

- "CR Q00680390" (page 10)
- "Secure communications" (page 10)

CR Q00680390

The section "Configuring secure FTP authentication on a Passport" (page 46) was updated for the customer CR Q00680390.

Secure communications

The following sections were updated:

- "Secure communications configuration" (page 11)
- "IPSec configuration" (page 13)
- "IPSec in tunnel mode" (page 73)

Chapter 1
Secure communications configuration

Configure secure communication features to maintain network security when there are communications between devices in the network. You can configure IPSec or Secure FTP.

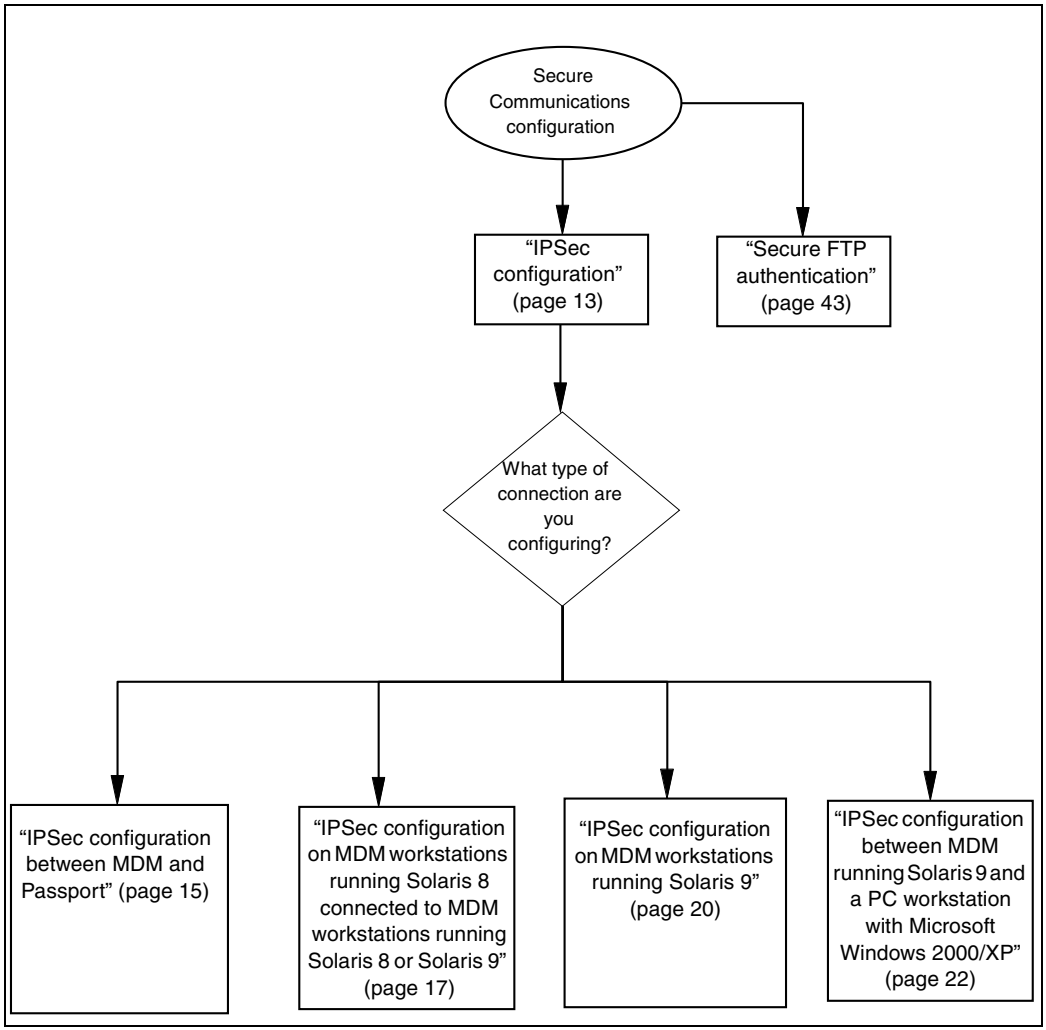
Navigation links

- "Secure communications configuration flow" (page 11)
- "Task navigation" (page 12)

Secure communications configuration flow

"Secure communications configuration task flow" (page 12) shows you the sequence of tasks you perform to configure local security policies on Preside Multiservice Data Manager and Passport nodes.To link to any procedure go to "Task navigation" (page 12).

Figure 1
Secure communications configuration task flow



Task navigation

- "IPSec configuration" (page 13)
- "Secure FTP authentication" (page 43)

Chapter 2
IPSec configuration

IPSec configuration tasks you must perform depend on the devices IPSec is configured between. There are four possible IPSec configuration methods.

- "IPSec configuration between MDM and Passport" (page 15)
- "IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9" (page 17)
- "IPSec configuration on MDM workstations running Solaris 9" (page 20)
- "IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP" (page 22)

In addition to IPSec configuration, there are a number of maintenance tasks described in "IPSec maintenance procedures" (page 34).

Refer to "Communication methods used between devices" (page 14) for a summary of the possible secure communication connections.

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

Prerequisites to IPsec configuration

- MDM is currently installed.
- IPSec services require a Sparc Ultra 10 workstation (minimum) and Solaris 8 and Solaris 9 operating environment.

Table 1
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

Legend:

PP: Passport, S8: MDM workstation running Solaris 8, S9: MDM workstation running Solaris 9, PC: PC workstation running Microsoft Windows 2000/XP.

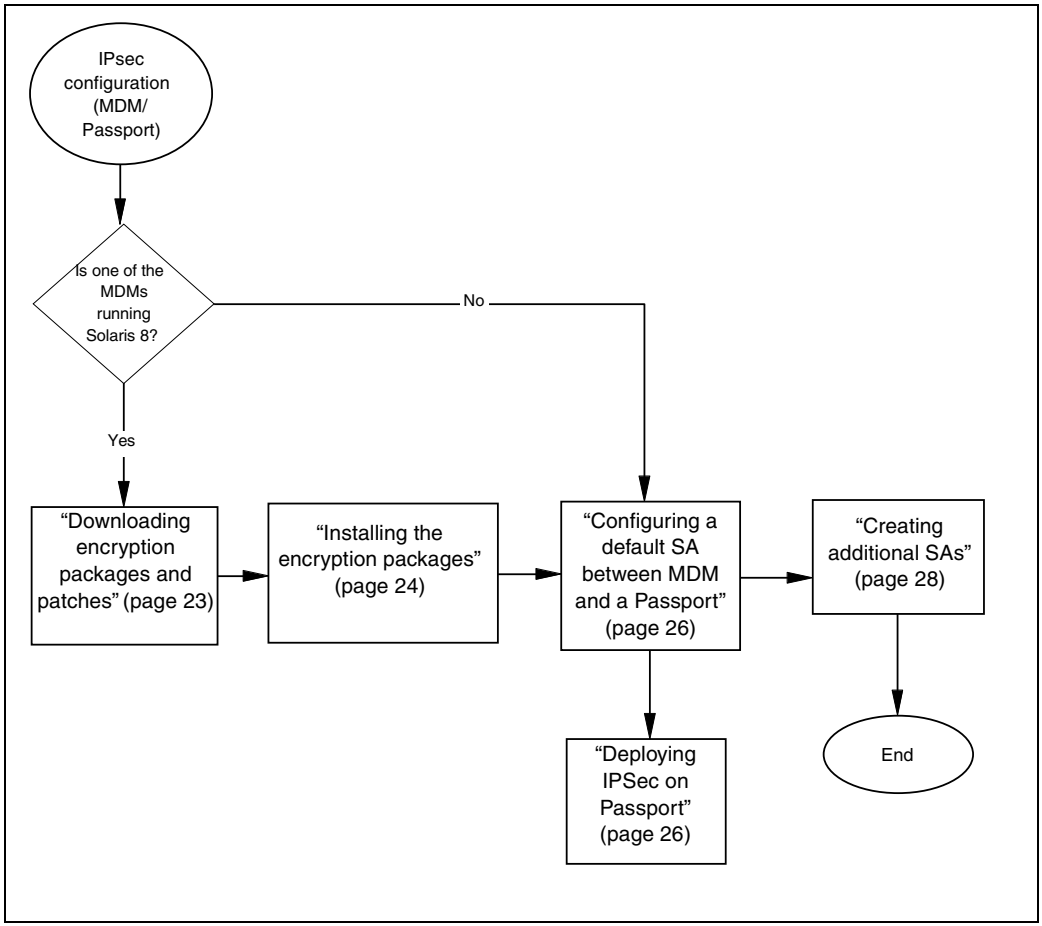
IPSec configuration between MDM and Passport

Configure IPSec between an MDM workstation and a Passport node to provide security for information flowing between the two devices. IPSec must be configured on both MDM and Passport.

IPSec configuration flow

"IPSec configuration between MDM and Passport task flow" (page 16) shows you the sequence of tasks you perform to configure IPSec between an MDM workstation and a Passport node. To link to any procedure go to "Task navigation" (page 16).

Figure 2
IPSec configuration between MDM and Passport task flow



Task navigation

- "Downloading encryption packages and patches" (page 23)
- "Installing the encryption packages" (page 24)
- "Deploying IPSec on Passport" (page 26)
- "Configuring a default SA between MDM and a Passport" (page 26)
- "Creating additional SAs" (page 28)

IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9

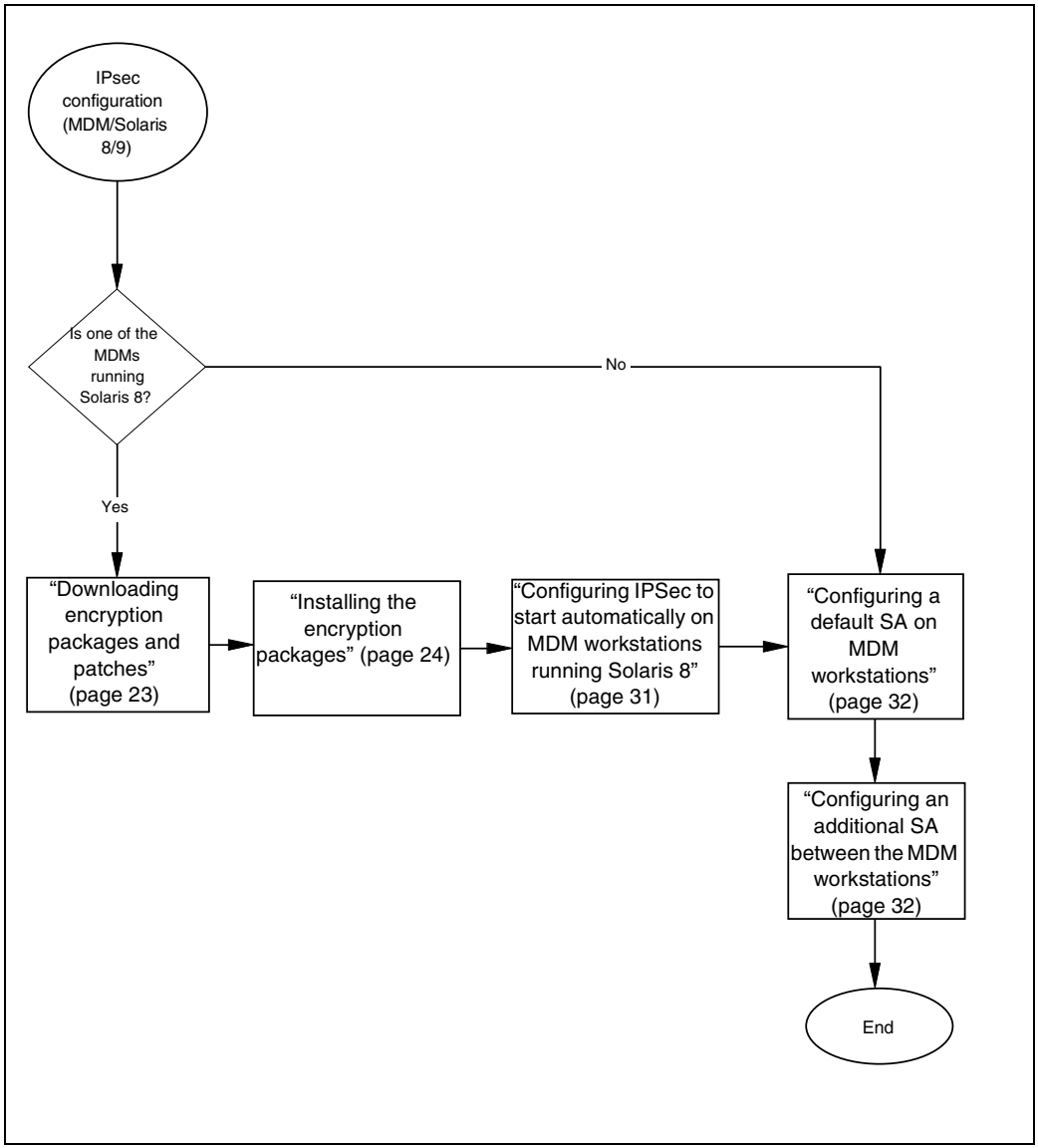
This section describes how to configure IPSec between the following:

- two MDM workstations both running Solaris 8
- an MDM workstation running Solaris 8 and an MDM workstation running Solaris 9

IPSec configuration flow

"IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9" (page 17) shows you the sequence of tasks you perform to configure IPSec between two MDM workstations running Solaris 8 or between an MDM workstation running Solaris 8 and an MDM workstation running Solaris 9. To link to any procedure go to "Task navigation" (page 19).

Figure 3
IPSec configuration between MDM running Solaris 8 or 9



Task navigation

- "Downloading encryption packages and patches" (page 23)
- "Installing the encryption packages" (page 24)
- "Configuring IPSec to start automatically on MDM workstations running Solaris 8" (page 31)
- "Configuring a default SA on MDM workstations" (page 32)
- "Configuring an additional SA between the MDM workstations" (page 32)

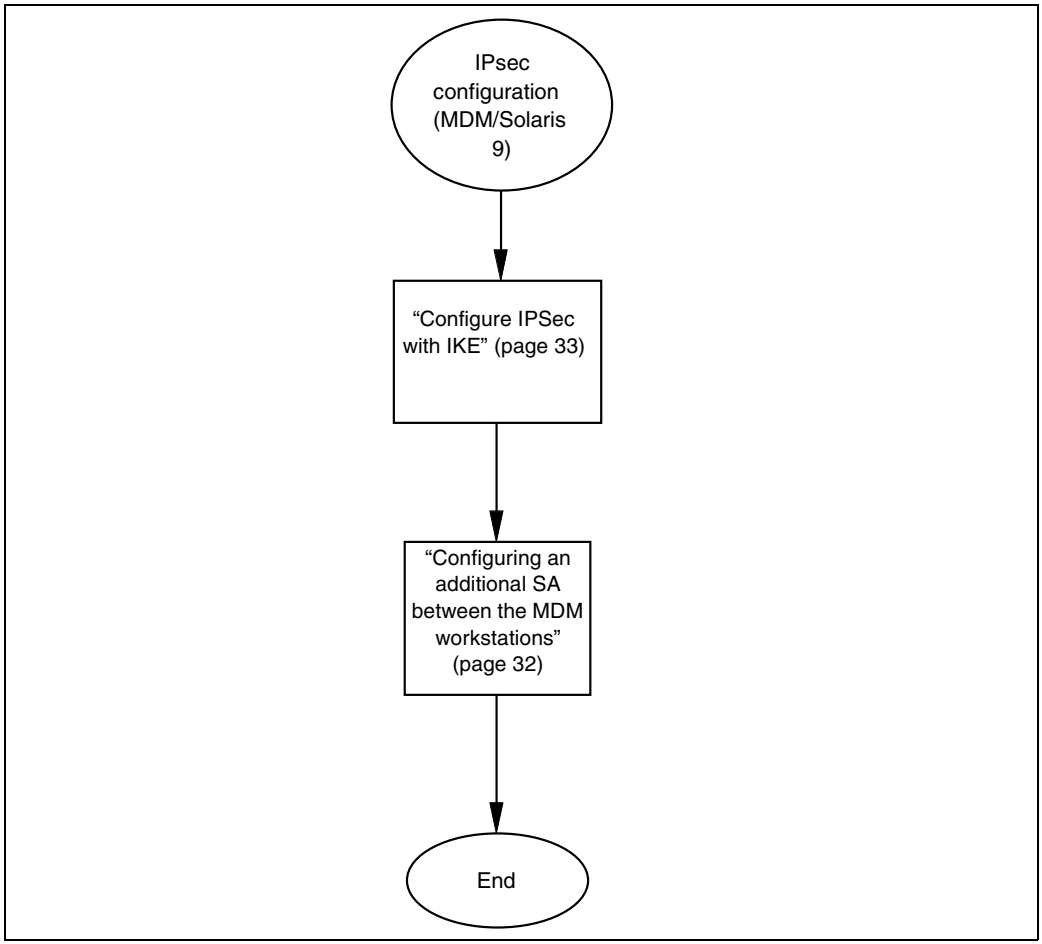
IPSec configuration on MDM workstations running Solaris 9

This section describes how to configure IPSec between two MDM workstations that are running Solaris 9.

IPSec configuration flow

"IPSec configuration between MDM workstations" (page 21) shows you the sequence of tasks you perform to configure IPSec between two MDM workstations running Solaris 9. To link to any procedure go to "Task navigation" (page 21).

Figure 4
IPSec configuration between MDM workstations



Task navigation

- "Configure IPSec with IKE" (page 33)
- "Configuring an additional SA between the MDM workstations" (page 32)

Note: If you use IPSec with IKE, it is not necessary to create SAs manually.

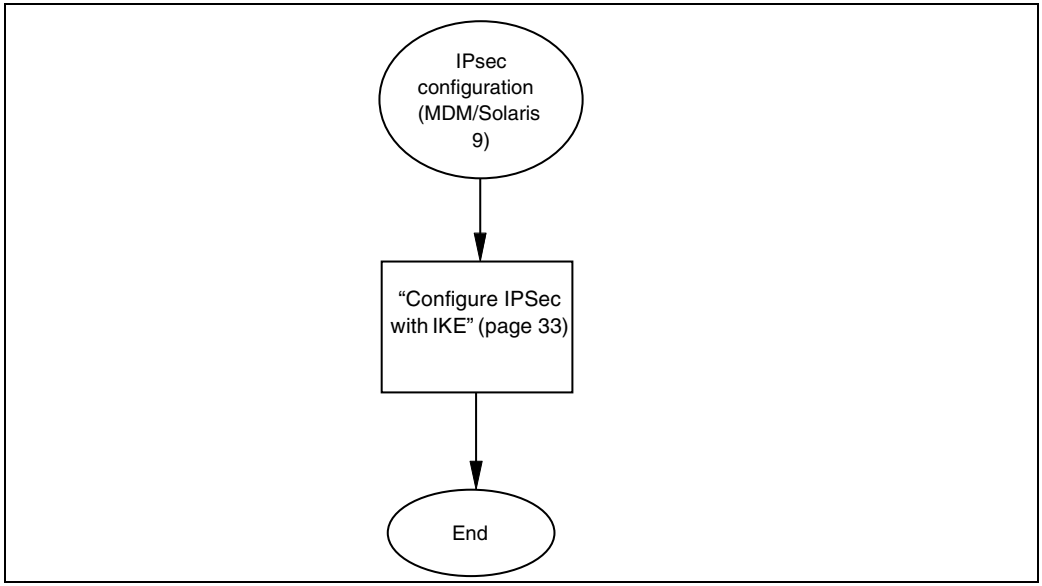
IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP

This section describes how to configure IPSec between an MDM workstation running Solaris 9 and a PC workstation with Microsoft Windows 2000 or Microsoft XP.

IPSec configuration flow

"IPSec configuration between an MDM workstation and a PC workstation with Microsoft Windows 2000/XP" (page 22) shows you the sequence of tasks you perform. To link to any procedure go to "Task navigation" (page 22).

Figure 5
IPSec configuration between an MDM workstation and a PC workstation with Microsoft Windows 2000/XP



Task navigation

- "Configure IPSec with IKE" (page 33)

  Note: If you use IPSec with IKE, it is not necessary to create SAs manually.

IPSec configuration procedures

All of the procedures contained in this section are referenced from one of the four IPSec connection types. Verify that you are using the correct procedure for your IPSec connection type.

Downloading encryption packages and patches

Download encryption packages and patches to obtain the appropriate encryption packages and patches in order to implement IPSec services on Preside Multiservice Data Manager.

Prerequisites

- To download software from the Solaris site you will require a Sun ID and the filename you require.

Procedure steps

1. Go to the appropriate Solaris download site.
   - http://wwws.sun.com/software/download/ (Solaris 9)
   - http://wwws.sun.com/software/solaris/encryption/download.html (Solaris 8)
2. Select and download the encryption package file.

   It is suggested that you download this file to a temporary directory.
3. Go to the following url:

   http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access
4. Select and download the latest version of patch 112438. This patch is required for IPSec.
5. Return to the appropriate task flow for your procedure:
   - “IPSec configuration between MDM and Passport” (page 15)
   - “IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9” (page 17)
   - “IPSec configuration on MDM workstations running Solaris 9” (page 20)
   - “IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP” (page 22)

Installing the encryption packages

Install the encryption packages to implement IPSec in your IP network.

Procedure steps

1. Log in as root.
2. Untar the encryption files using the following command:

   ```
   tar -xvf <encryption_file_filename>
   ```

3. Navigate to the directory where the encryption packages are located:

   ```
   /<temporary_directory>/sparc/Packages
   ```

4. Enter the following command:

   ```
   pkgadd -d .
   ```

5. Answer the questions and follow the instructions that are displayed on the screen.
6. Enter the following command:

   ```
   pkginfo | grep SUNWcry
   ```

7. Confirm that the minimum required packages for IPSec are installed.
8. Install the patch using standard Sun procedures.
9. Return to the appropriate task flow for your procedure:
   - “IPSec configuration between MDM and Passport” (page 15)
   - “IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9” (page 17)
   - “IPSec configuration on MDM workstations running Solaris 9” (page 20)
   - “IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP” (page 22)

Procedure job aid

Table 2
Minimum required packages for IPSec

Package name
system SUNWcrman Encryption Kit On-Line Manual Pages
system SUNCRY Crypt Utilities
system SUNWcry64 Prototype package for Crypt Library (64-bit)
system SUNWcryr Solaris Root Crypto
system SUNWcryrx Solaris Root Crypto (64-bit)

Deploying IPSec on Passport

At the same time, you must deploy IPSec on the Passport node. IPSec can be deployed on the Passport in two ways:

- manually on the Passport by activating the IPSec software
- using the StartUp utility on Passport to install and configure the IPSec SAs (security associations) between each Passport node and Preside Multiservice Data Manager (MDM) pair in the network

For more information on deploying IPSec on Passport, refer to "Modifying IPSec on nodes manually" (page 81).

Configuring a default SA between MDM and a Passport

Configure a default encrypted SA to apply DES encryption to all traffic that is exchanged between Preside Multiservice Data Manager (MDM) and a Passport node that does not have a specific SA. DES encryption is required in case the data contains sensitive material such as passwords. This data includes telnet sessions or ftp-control channel traffic.

Procedure steps

1. Log in to the MDM as root.
2. Use the new SA script to configure a default SA with DES encryption. Type:

   ```
   ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -enc_alg
   des generate <Passport IP address>
   ```

   Note: You must only include the **generate** option if you are configuring a default SA on MDM first. Omit this option if you are configuring a default SA on the Passport first.

   This script generates three IPSec configuration files (ipseckey.cfg, ipsecinit.cfg, ipsecpolicy.cfg). For more information, refer to the Sun documentation. Note that the location of ipseckey.cfg is etc/inet/secret (Solaris 9) or /etc/inet (Solaris 8).

   After you enter this command, the system displays all the parameters that can be run remotely. You must then configure these parameters on the Passport.
3. Set the algorithms and keys of both the inbound and outbound policy security associations on the node.

For more information on setting the algorithms and keys, refer to step 11 and step 12 in the procedure “Modifying IPSec on nodes manually” (page 81).

4 Log on to the node and configure a corresponding SA. For more information, refer to “Modifying IPSec on nodes manually” (page 81).

5 Return to the task flow for “IPSec configuration between MDM and Passport” (page 15):

Variable definitions

Table 3

Variable	Definition
<Passport IP address>	The IP address of the node with which you are establishing an SA.
<spi_1>, <spi_2>	The security index parameter.

Creating additional SAs

You use a script to create additional SAs to fine tune the secure communications for your system's specific traffic type. This script is used to set up IPSec between MDMs or between an MDM and a Passport. When it is executed and both an inbound and outbound SPI value are specified, this script deploys two SAs between the workstations that are indicated.

Procedure steps

1 Navigate to the following location:

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

2 Type the following command:

```
./opt/MagellanNMS/bin/ipsec_newsa \
<IP address of the Passport or workstation> \
[<IP address of the local workstation>] \
[-inSPI <inbound SPI number>] \
[-outSPI <outbound SPI number>] \
[-destPort <destination port number>] \
[-srcPort <source port number>] \
[-proto <tcp|udp|icmp>] \
[-enc_alg <des|3des> <HEX key|generate>] \
[-enc_auth <sha|md5> <HEX key|generate>] \
[-pp <remote MDM> <PP group> <userID> <password>] \
[-h]
```

For information on these command parameters, refer to "New SA script parameters" (page 30). The system displays a set of values.

3 Run the command that is printed, after you perform step 2 above, to configure the other MDM workstation. For example:

```
./opt/MagellanNMS/bin/ipsec_newsa \
```

This sets up an SA on the remote device.

4 You can set up specific SAs depending on the type of traffic your system requires. For more information on the commands for specific SAs, refer to "Sample command lines to configure SAs for some protocols" (page 29).

5 Return to the task flow for "IPSec configuration between MDM and Passport" (page 15).

Procedure job aids

Table 4
Sample command lines to configure SAs for some protocols

SA type	Command
NTP	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -srcPort ntp -enc_auth sha generate <Passport IP address>
FTP data channel on Passport	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -destPort ftp-data -enc_auth md5 generate <Passport IP address>
FTP data channel bypass on MDM	ipsec_newsa -srcPort ftp-data <Passport IP address>
SNMP	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -destPort SNMP -enc_auth sha generate -enc_alg 3des generate <Passport IP address>
FMIP	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -destPort FMIP -enc_auth sha generate -enc_alg 3des generate <Passport IP address>
Telnet	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -destPort telnet -enc_auth sha generate -enc_alg 3des generate <Passport IP address>
ICMP	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -proto icmp -enc_auth sha generate -enc_alg 3des generate <Passport IP address>
TCP	ipsec_newsa -inSPI <spi_1> -outSPI <spi_2> -proto tcp -enc_auth sha generate -enc_alg 3des generate <Passport IP address>

Table 5
New SA script parameters

Parameter	Definition
IP address of the Passport or workstation	Specifies the IP address, host name or node name of the device with which you want to set up an SA. If the optional parameter -pp is used, the value of this field must exist in the /opt/Magellan/cfg/HGDS.cfg file on both the local and remote workstations. This is so that the node name of the network element can be resolved.
IP address of the local workstation	This optional parameter is the IP address or host name of the local workstation. If this address is not specified, then the IP address associated with 'hostname' is used.
-inSPI <inbound SPI number>	A value in the range of 256-4095 used for incoming packets. You must enter this value manually. If you do not specify a value, a bypass policy is created. The inbound SPI value must be the same as the outbound SPI value on the remote device.
-outSPI <outbound SPI number>	A value in the range of 256-4095 used for outbound packets. You must enter this value manually. If you do not specify a value, a bypass policy is created. The outbound SPI value must be the same as the inbound SPI valued on the remote device.
-destPort <destination port number>	This value is either an integer number or a port name that represents the port that the incoming packets are destined for. If you do not specify a value, the default of any is used.
-srcPort <source port number>	This value is either an integer number or a port name that represents the port that the outgoing packets are coming from. If you do not specify a value, the default of any is used.
-proto <tcp|udp|icmp>	This is the value of the upper layer protocol that you want to secure. If you do not specify a value, the default of any is used.
-enc_alg <des|3des> <HEX key|generate>	Specifies that an encryption algorithm will be applied to the SA. When you apply an encryption algorithm, you must specify an algorithm type of DES or triple DES. You must also provide an encryption key. You can either provide a HEX key that you have previously generated, or you can type the word "generate" and the script will call the ipsec_keygen script to generate a key of the appropriate length. Keys for DES must be 16 HEX characters in length with odd parity and keys for triple DES must be 48 HEX characters with odd parity. If you do not specify this option, the default value of null is used.
(Sheet 1 of 2)	

Table 5
New SA script parameters (Continued)

Parameter	Definition
-enc_auth <md5|sha> <HEX key|generate>	Specifies that an authentication algorithm will be applied to the SA. When you apply an authentication algorithm, you must specify an algorithm type of MD5 or SHA. You must also provide an encryption key. You can either provide a HEX key that you have previously generated, or you can type the word "generate" and the script will call the ipsec_keygen script to generate a key of the appropriate length. Keys for SHA must be 40 HEX characters in length and keys for MD5 must be 32 HEX characters.
-pp <remote MDM> <PP group> <userID> <password>	The optional parameter has four variables. The variable "remote MDM" specifies the name or IP address of the remote workstation that the script will use to provision the node. The variable "PP group" specifies the node group that the script will attempt to authenticate to. The group name is only significant to the remote workstation. The variable "userID" specifies the user ID that the script will attempt to authenticate to and "password" is the password that corresponds to the user ID.
-h	This parameter returns a help message that describes the parameters of this script.
(Sheet 2 of 2)	

Configuring IPSec to start automatically on MDM workstations running Solaris 8

Configure IPSec to start automatically to create a startup script that starts IPSec after every reboot to maintain IPSec service and avoid completing the IPSec configuration tasks again.

Setting up an automatic start up for IPSec is recommended.

Note: This configuration should not be setup on a Solaris 9 workstation.

Procedure steps

1 Go to the directory where the example run control file is stored. Type:

```
cd /opt/MagellanNMS/system/init/
```

2 Copy the example file to the following locations:

```
cp ipsec_set /etc/rc0.d/K42ipsec_setup
cp ipsec_set /etc/rc2.d/S69ipsec_setup
```

3 Return to the task flow for "IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9" (page 17).

Configuring a default SA on MDM workstations

Configure a default SA between two MDM workstations running Solaris 8 or between an MDM workstation running Solaris 8 and an MDM workstation running Solaris 9

Procedure steps

1 Log in to Preside Multiservice Data Manager (MDM) as root.

2 Use the new SA script to configure a default SA with 3DES encryption. Type:

```
ipsec_newsa -inSPI <spi_1> outSPI <spi_2> -enc_alg
3des generate <remote workstation IP address>
```

This displays a ipsec_newsa command that you must run on the other Solaris workstation that is running MDM. For information on the script variables, refer to "New SA script parameters" (page 30)

3 Login to the other Solaris workstation, running MDM and run the ipsec_newsa command.

4 Return to the appropriate task flow for your procedure:

- "IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9" (page 17)
- "IPSec configuration on MDM workstations running Solaris 9" (page 20)
- "IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP" (page 22)

Configuring an additional SA between the MDM workstations

Create a TCP SA between the MDM workstations to provide some security for information transfer.

Procedure steps

1 Navigate to the following location:

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

2 Type the following command:

```
./ipsec_newsa \
[-inSPI <inbound SPI number>] \
[-outSPI <outbound SPI number>] \
[-proto_tcp\
[-enc_alg <des|3des> <HEX key|generate>] \
[-enc_auth <sha|md5> <HEX key|generate>] \
[-h]
```

For information on these command parameters, refer to “New SA script parameters” (page 30). The system displays a set of values.

3 Run the command that is printed, after you perform step 2 above, to configure the other MDM workstation. For example:

```
./opt/MagellanNMS/bin/ipsec_newsa \
```

This sets up an SA on the other MDM workstation.

4 Return to the appropriate task flow for your procedure:

- “IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9” (page 17)
- “IPSec configuration on MDM workstations running Solaris 9” (page 20)
- “IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP” (page 22)

Configure IPSec with IKE

It is recommended that IKE (Internet Key Exchange) be configured if you are configuring:

- a Windows-based PC running Windows 2000/XP communicating with Solaris 9 workstation
- two solaris 9 workstations communicating with each other

For detailed procedures on configuring IPSec with IKE, refer to the appropriate Microsoft Windows or Sun documentation.

To continue configuring IPSec, return to the appropriate task flow:

- "IPSec configuration on MDM workstations running Solaris 9" (page 20)
- "IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP" (page 22)

IPSec maintenance procedures

Perform the following IPSec maintenance tasks as required:

- "Deleting an SA between MDM and a node" (page 34)
- "Deleting an SA between two Solaris 8 workstations or between a Solaris 8 and a Solaris 9 workstation" (page 37)
- "Refreshing keys between MDM and a node" (page 38)
- "Refreshing keys between two Solaris 8 workstations or a Solaris 8 and Solaris 9 workstation" (page 40)
- "Generating encryption keys" (page 41)

Deleting an SA between MDM and a node

Delete an SA to remove an existing SA policy. The delete SA script deletes the policy and flushes it out of memory.

Procedure steps

1. Log onto Preside Multiservice Data Manager (MDM) as root.
2. Run the script to delete the SA locally and on the Passport node:

```
/opt/MagellanNMS/bin/ipsec_deletesa \
<IP address of the Passport or workstation> \
[IP address of the local workstation>] \
[-inSPI <inbound SPI number>] \
[-outSPI <outbound SPI number>] \
[-destPort <destination port number>] \
[-srcPort <source port number>] \
[-proto <tcp|udp|icmp>] \
[-pp <remote MDM> <PP group> <userID> <password>] \
[-h]
```

3. Test for connectivity using ping and telnet.

Procedure job aid

Table 6

Parameter	Definition
IP address of the Passport or workstation	Specifies the IP address, host name or node name of the device with which you want to delete an SA. If the optional parameter -pp is used, the value of this field must exist in the /opt/Magellan/cfg/HGDS.cfg file on both the local and remote workstations. This is so that the node name of the network element can be resolved.
IP address of the local workstation	This optional parameter is the IP address or host name of the local workstation. If this address is not specified, then the IP address associated with 'hostname' is used.
-inSPI <inbound SPI number>	A value in the range of 256-4095 used for incoming packets. You must enter this value manually. If you do not specify a value, a bypass policy is deleted. The inbound SPI value must be the same as the outbound SPI value on the remote device.
[-outSPI <outbound SPI number>]	A value in the range of 256-4095 used for outbound packets. You must enter this value manually. If you do not specify a value, a bypass policy is deleted. The outbound SPI value must be the same as the inbound SPI valued on the remote device.
-destPort <destination port number>	This value is either an integer number or a port name that represents the port that the incoming packets are destined for. If you do not specify a value, the default of any is used.
-srcPort <source port number>	This value is either an integer number or a port name that represents the port that the outgoing packets are coming from. If you do not specify a value, the default of any is used.
-proto <tcp|udp|icmp>	This is the value of the upper layer protocol that you want to secure. If you do not specify a value, the default of any is used.

(Sheet 1 of 2)

Table 6

Parameter	Definition
-pp <remote MDM> <PP group> <userID> <password>	The optional parameter has four variables. The variable “remote MDM” specifies the name or IP address of the remote workstation that the script will use to provision the node. The variable “PP group” specifies the node group that the script will attempt to authenticate to. The group name is only significant to the remote workstation and need not be configured on the local workstation. The variable “userID” specifies the user ID that the script will attempt to authenticate to and “password” is the password that corresponds to the user ID.
-h	This parameter returns a help message that describes the parameters of this script.

(Sheet 2 of 2)

Deleting an SA between two Solaris 8 workstations or between a Solaris 8 and a Solaris 9 workstation

Delete an SA to remove an existing SA policy. The delete SA script deletes the policy and flushes it out of memory.

Procedure steps

1. Log onto Preside Multiservice Data Manager (MDM) as root.
2. Run the script to delete the SA locally on the remote Solaris workstation:

   ```
   /opt/MagellanNMS/bin/ipsec_deletesa
   <remote workstation IP address>
   ```

3. Run the command that is printed, after you perform step 2 above, to configure the other MDM workstation.
4. Test for connectivity using ping and telnet.

Refreshing keys between MDM and a node

Refresh keys to periodically update and refresh the encryption keys between your network elements.

Procedure steps

1 Run the key refresh script to refresh the key between Preside Multiservice Data Manager (MDM) and the Passport node. Type:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh \
<IP address of the Passport or workstation> \
[<IP address of the local workstation>] \
[-inSPI <inbound SPI number>] \
[-outSPI <outbound SPI number>] \
[-enc_alg <des|3des> <HEX key|generate>] \
[-enc_auth <sha|md5> HEX key|generate>] \
[-pp <remote MDM> <PP group> <userID> <password>] \
[-h]
```

Procedure job aid

Table 7
Key refresh script variables

Parameter	Definition
IP address of the Passport or workstation	Specifies the IP address, host name or node name of the device with which you want to refresh an SA. If the optional parameter -pp is used, the value of this field must exist in the /opt/Magellan/cfg/HGDS.cfg file on both the local and remote workstations. This is so that the node name of the network element can be resolved.
IP address of the local workstation	This optional parameter is the IP address or host name of the local workstation. If this address is not specified, then the IP address associated with ‘hostname’ is used.
-inSPI <inbound SPI number>	A value in the range of 256-4095 used for incoming packets. You must enter this value manually. The inbound SPI value must be the same as the outbound SPI value on the remote device.
-outSPI <outbound SPI number>	A value in the range of 256-4095 used for outbound packets. You must enter this value manually. The outbound SPI value must be the same as the inbound SPI valued on the remote device.

(Sheet 1 of 2)

Table 7
Key refresh script variables

Parameter	Definition
-enc_alg <des|3des> <HEX key|generate>	Specifies that an encryption algorithm will be applied to the SA. When you apply an encryption algorithm, you must specify an algorithm type of DES or triple DES. You must also provide an encryption key. You can either provide a HEX key that you have previously generated, or you can type the word “generate” and the script will call the ipsec_keygen script to generate a key of the appropriate length. Keys for DES must be 16 HEX characters in length with odd parity and keys for triple DES must be 48 HEX characters with odd parity. If you do not specify this option, the default value of null is used. For more information on generating keys, refer to “Generating encryption keys” (page 41)
-enc_auth <md5|sha> <HEX key|generate>	Specifies that an authentication algorithm will be applied to the SA. When you apply an authentication algorithm, you must specify an algorithm type of MD5 or SHA. You must also provide an encryption key. You can either provide a HEX key that you have previously generated, or you can type the word “generate” and the script will call the ipsec_keygen script to generate a key of the appropriate length. Keys for SHA must be 40 HEX characters in length and keys for MD5 must be 32 HEX characters. For more information on generating keys, refer to “Generating encryption keys” (page 41)
-pp <remote MDM> <PP group> <userID> <password>	The optional parameter has four variables. The variable “remote MDM” specifies the name or IP address of the remote workstation that the script will use to provision the Passport. The variable “PP group” specifies the node group that the script will attempt to authenticate to. The group name is only significant to the remote workstation and need not be configured on the local workstation. The variable “userID” specifies the user ID that the script will attempt to authenticate to and “password” is the password that corresponds to the user ID.
-h	This parameter returns a help message that describes the parameters of this script.

(Sheet 2 of 2)

Refreshing keys between two Solaris 8 workstations or a Solaris 8 and Solaris 9 workstation

Refresh keys to periodically update and refresh the encryption keys between your network elements.

Procedure steps

1. Run the key refresh script to refresh the key between the Solaris workstations. Type:

```
/opt/MagellanNMS/bin/ipsec_keyrefresh \
<IP address of the Passport or workstation> \
[<IP address of the local workstation>] \
[-inSPI <inbound SPI number>] \
[-outSPI <outbound SPI number>] \
[-enc_alg <des|3des> <HEX key|generate>] \
[-enc_auth <sha|md5> HEX key|generate>] \
[-h]
```

2. Run the command that is printed, after you perform step 1 above, to configure the other MDM workstation.

Generating encryption keys

This script is used to generate encryption keys of the appropriate length based on the encryption or authentication algorithm. The syntax for the script is:

Procedure steps

1 Type the following command:

```
/opt/MagellanNMS/bin/ipsec_keygen \
[des|3des|sha|md5] \
[-parity <HEX key>] \
[-h]
```

Procedure job aid

Table 8
Encryption key parameters

Parameter	Definition
[des|3des|sha|md5]	These optional values represent the encryption algorithms DES and 3DES and the authentication algorithms SHA-1 and MD5. When you generate an encryption key, you must specify one of these values. You can only generate one key at a time and you must generate a separate key for each instance of each algorithm. When you configure an initial SA between a node and the Preside Multiservice Data Manager workstation, you can only use and encryption algorithm of DES. Therefore, you must generate a key using DES as the value.
[-parity <HEX key>]	This optional parameter tests whether the user supplied key is odd parity or not. Odd parity is used for DES and triple DES keys only. A return code of “0” means that the supplied key is odd parity. Any other return code means that it is not.
[-h]	This parameter returns a help message that describes the parameters of this script.

Chapter 3
Secure FTP authentication

Configure secure FTP authentication to ensure encrypted passwords are used for FTP sessions.

Navigation links

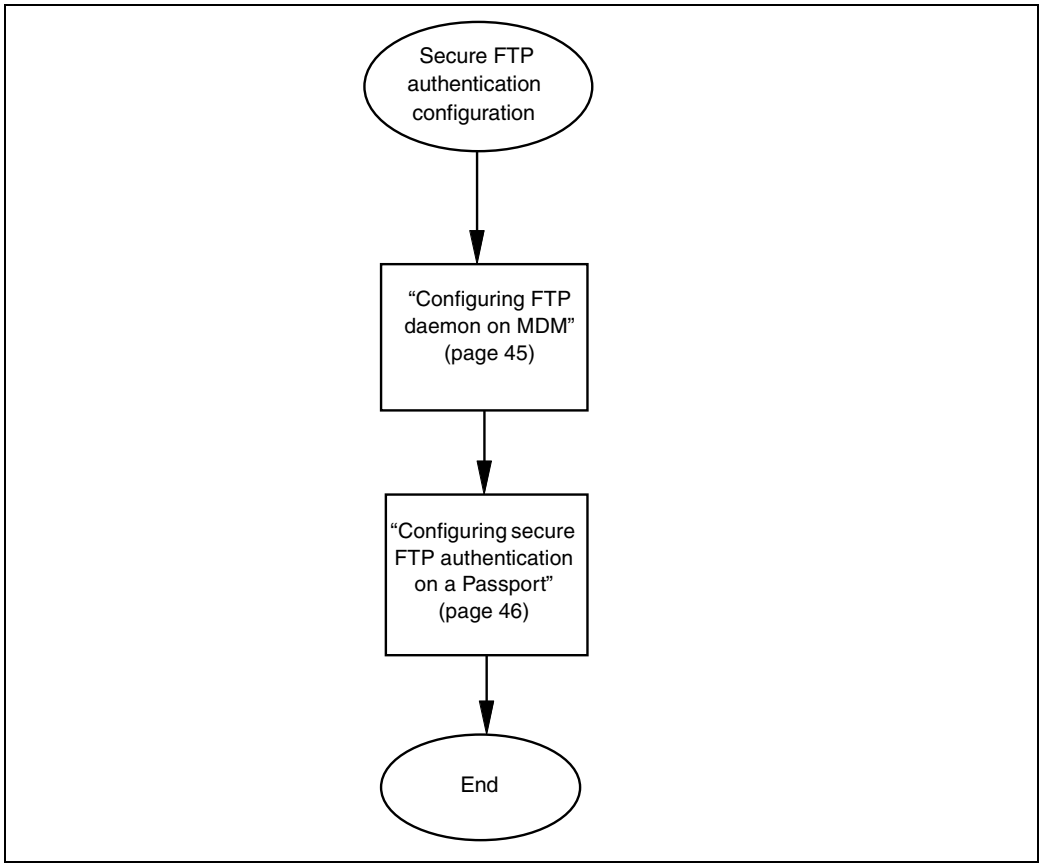
Prerequisites to secure FTP authentication

- When a Preside Multiservice Data Manager (MDM) or MDP workstation initiates an FTP session with a Passport node running software version PCR 4.2 or higher, secure FTP authentication is used automatically; no configuration is required.
- When a Passport node initiates an FTP session with an MDM workstation, for the purposes of downloading software, an FTP daemon must be configured in order to ensure that secure FTP authentication is used.

Secure FTP authentication flow

This task flow shows you the sequence of procedures you perform to configure secure FTP authentication. To link to any procedure, go to "Task navigation" (page 44).

Figure 6
Secure FTP authentication task flow



Task navigation

- "Configuring FTP daemon on MDM" (page 45)
- "Configuring secure FTP authentication on a Passport" (page 46)

Configuring FTP daemon on MDM

Configure FTP daemon on Preside Multiservice Data Manager (MDM) to ensure that FTP sessions initiated by Passport nodes are secure. The FTP server, supporting secure FTP authentication, must be set up on all MDM workstations that are acting as software distribution sites (SDSs).

Attention

Secure FTP authentication secures node-to-node encryption information only. Workstation-to-workstation communication should be secured using IPSec

Procedure steps

1. Log in as root.
2. Start the MDM Toolset.
3. Configure FTP daemon using the procedure *Adding a new server* in the 241-6001-303 *Preside MDM Administrator Guide*. For specific field entries, refer to "FTP daemon configuration field entries" (page 45)
4. Repeat this procedure on all target workstations.

Procedure job aid

Table 9
FTP daemon configuration field entries

Field	Value
Descriptive name	Secure FTPD
Startup command	/opt/MagellanNMS/bin/launchSecureFTPD
Automatic startup at reboot time	Select

Configuring secure FTP authentication on a Passport

Configure secure FTP authentication on a Passport node to force both the FTP Client and the FTP Server on the node to support secure FTP authentication communication only.

Attention

The secure FTP authentication feature is provisioned under the CP and removing it from the feature list causes a complete shelf reload which will disable all shelf services for 1 to 3 minutes.

Prerequisites

- You must also enable secure FTP authentication on the Preside Multiservice Data Manager (MDM) servers to ensure secure communications with the Passport node. See “Configuring FTP daemon on MDM” (page 45).

Procedure steps

1 Add the new security feature to the feature list of the CP:

```
set Software Lpt/CP0 featurelist secureFtpAuth1Only
```

Appendix A: Changing default port settings

The User Administration server is configured with a number of default port settings. If there is a conflict between some of these port settings and your existing port settings, the settings can be changed by the system administrator.

> ***Note:*** In addition, if you want to put Operator Client behind a firewall, there are a number of dynamic port settings that must be fixed. For more information, refer to “Operator Client ports” (page 70).

Table 10
Default port settings

Port	Protocol	Used by	Procedure to configure port
25	TCP	SMTP	“Change the sendmail server default port” (page 49)
389	TCP	Sun ONE DS server	“Changing the Sun ONE DS server default port” (page 54)
8443	TCP	Apache Server	“Changing the Apache server default SSL port” (page 50)
1812	UDP	Radius Server	“Changing the RADIUS server default port” (page 64)
8081	TCP	Tomcat server	“Changing the Tomcat server default port” (page 51)
8080	TCP	Apache Web Server	“Changing the Apache web server default port” (page 52)
24313	TCP	Sun ONE DS admin server	“Changing the Sun ONE DS admin default port” (page 62)

Table 10
Default port settings

Port	Protocol	Used by	Procedure to configure port
58080	TCP	Sun ONE IS Webserver	“Changing the Sun ONE identity server default port” (page 65)
58888	TCP	Sun ONE IS admin	“Changing the Sun ONE identity admin default port” (page 69)

Change the sendmail server default port

Change the sendmail server default port by changing the default port and then configuring the client process.

Procedure steps

1. Change the port number in the file /etc/services.
2. Stop the sendmail process.

   /etc/init.d/sendmail stop

3. Start the sendmail process.

   /etc/init.d/sendmail start

4. Configure the client process by changing the port number.

   /opt/nortel/applications/security/current_core/swmgmt/bin/upgrade_seccore.sh -c smtp

5. Restart the process.

   /opt/nortel/3rd_party/security/current_s1is/servers/https-<host_name>/restart

Changing the Apache server default SSL port

Procedure steps

1. Change the port number in the file

   `/opt/nortel/3rd_party/apache/current_apache/conf/ssl.conf`

2. Restart the Apache server by entering the following command:

   /opt/nortel/3rd_party/apache/current_apache/bin/apachectl -k stop

3. Start the client process by using the new port number in the URL. For example:

   https://<hostname>:<new_port>/UI

Changing the Tomcat server default port

Procedure steps

1. Change the default port:
   a. Change the port number in the file /opt/nortel/3rd_party/apache/current_tomcat/conf/server.xml
   b. Restart the logging server by entering the following two commands:

      /opt/nortel/3rd_party/apache/current_tomcat/bin/shutdown.sh

      /opt/nortel/3rd_party/apache/current_tomcat/bin/startup.sh

2. Configure the client process:
   a. Change the port number in the file /opt/nortel/3rd_party/apache/current_apache/conf/workers2.properties.
   b. Restart the Apache server.

      /opt/nortel/3rd_party/apache/current_apache/bin/apachectl -k stop

Changing the Apache web server default port

Changes made to this port are not persistent between MDM software upgrades. You must reset this port number after each MDM software upgrade.

Procedure steps

1. Change the port number.

   ```
   /opt/nortel/3rd_party/apache/current_apache/
   conf/httpd.conf
   ```

2. Restart the Apache server:.

   /opt/nortel/3rd_party/apache/current_apache/bin/apachectl -k stop

3. Change the port number in the following files:

   - /opt/nortel/config/applications/desktop/jws/resources/desktop/DesktopGUI.jnlp
   - /opt/nortel/config/applications/security/core/auth/AMConfig.auth.cpp.properties
   - /opt/nortel/3rd_party/security/current_s1is/capi/config/AMAgent.properties

4. If the WEB_FILE_MANAGER_LOCATION was configured, change the port number in the file /opt/nortel/config/applications/desktop/local/mft/resources/desktop/DesktopGUI.config.

5. Restart the Sun ONE IS using the following command:

   /opt/nortel/applications/security/current_s1is/servers/http s-<host_name>/restart

6. Restart the logging server using the following two commands:

   /opt/nortel/applications/security/current_core/bin/socketserver.sh stop

   /opt/nortel/applications/security/current_core/bin/socketserver.sh start

7. Start the client process by using the new port number in the URL. For example:

   https://<hostname>:<new_port>/UI

8 Restart any C++ applications that may have cached the IS client properties.

Changing the Sun ONE DS server default port

There are four procedures to perform when changing the Sun ONE Directory Server (DS) server default port:

- "Configuring the server port in the Sun ONE DS console" (page 54)
- "Configuring the client process" (page 55)
- "Configuring the client process in the Sun ONE DS console" (page 59)
- "Restarting the servers" (page 61)

Prerequisites

- Sun ONE DS console user ID and password

Configuring the server port in the Sun ONE DS console

Procedure steps

1. Open the Sun ONE DS console.

   ```
   /opt/nortel/3rd_party/netscape/current_nds/
   startconsole
   ```

2. In the login screen, enter the user ID and password.

   Note: If this is the first login, you must enter the administration URL http://<host_name>:24313.

3. In the Sun ONE DS console window, click the folder icon next to the host name.
4. Click the folder icon next to **Server Group**.
5. Click **Directory Server <host_name>**.
6. In the right frame, click **Open**.
7. Select the **Configuration** tab.
8. In the **Port** field, enter the new port number.
9. Click **Save**.
10. Click **Yes**.
11. Click **OK**.
12. Select the **Directory** tab.
13. Click the folder icon for **NetscapeRoot**.

14 Click the folder icon for <**organization**>.

15 Click **Global Preferences**.

16 In the right frame, double-click **User Directory**.

17 Change the port in the nsdirectoryurl.

18 Click **OK**.

19 Exit the Sun ONE DS console.

Configuring the client process

Procedure steps

1 Copy the following text and create a file called /tmp/389.1.sh

```
#!/bin/sh
org=$1
newport=$2
LD_LIBRARY_PATH=/opt/nortel/3rd_party/
security/current_s1is/ldaplib/solaris/sparc/
ldapsdk
export LD_LIBRARY_PATH

/opt/nortel/3rd_party/security/current_s1is/
bin/ldapsearch -o \
        -b
"ou=1.0,ou=iPlanetAMAuthCertService,ou=servic
es,$org" \
-D "cn=Directory Manager" -w directory -h
`hostname` -p $newport "(objectclass=*)"
sunserviceschema  > \
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amAuthCert.xml.tmp

cat  /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthCert.xml.tmp | sed -n '/
<ServicesConfiguration>/,/<\/
ServicesConfiguration>/p' \
| sed -e 's/sunserviceschema=//' > /opt/
nortel/config/3rd_party/security/s1is/config/
xml/amAuthCert.xml

/opt/nortel/3rd_party/security/current_s1is/
bin/ldapsearch -o \
```

```
-b
"ou=1.0,ou=iPlanetAMAuthLDAPService,ou=servic
es,$org" \
-D "cn=Directory Manager" -w directory -h
`hostname` -p $newport "(objectclass=*)"
sunserviceschema  > \
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amAuthLDAP.xml.tmp

cat  /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthLDAP.xml.tmp | sed -n '/
<ServicesConfiguration>/,/<\/
ServicesConfiguration>/p' \
| sed -e 's/sunserviceschema=//' > /opt/
nortel/config/3rd_party/security/s1is/config/
xml/amAuthLDAP.xml
/opt/nortel/3rd_party/security/current_s1is/
bin/ldapsearch -o \
-b
"ou=1.0,ou=iPlanetAMAuthMembershipService,ou=
services,$org" \
-D "cn=Directory Manager" -w directory -h
`hostname` -p $newport "(objectclass=*)"
sunserviceschema  > \
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amAuthMembership.xml.tmp

cat  /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthMembership.xml.tmp |
sed -n '/<ServicesConfiguration>/,/<\/
ServicesConfiguration>/p' \
| sed -e 's/sunserviceschema=//' > /opt/
nortel/config/3rd_party/security/s1is/config/
xml/amAuthMembership.xml

/opt/nortel/3rd_party/security/current_s1is/
bin/ldapsearch -o \
-b
"ou=1.0,ou=iPlanetAMPolicyConfigService,ou=se
rvices,$org" \
-D "cn=Directory Manager" -w directory -h
`hostname` -p $newport "(objectclass=*)"
sunserviceschema  > \
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amPolicyConfig.xml.tmp
```

```
cat  /opt/nortel/config/3rd_party/security/
s1is/config/xml/amPolicyConfig.xml.tmp | sed
-n '/<ServicesConfiguration>/,/<\/
ServicesConfiguration>/p' \
| sed -e 's/sunserviceschema=//' > /opt/
nortel/config/3rd_party/security/s1is/config/
xml/amPolicyConfig.xml
```

2 Execute the script.

/bin/sh /tmp/389.1.sh <org> <port>

For more information, refer to “Options for Client Process configuration” (page 59)

3 Change directory.

cd /opt/nortel

4 Change the port number in the following files:

- config/applications/security/core/auth/AMConfig.auth.cpp.properties
- config/applications/security/core/auth/ AMConfig.auth.java.properties
- 3rd_party/security/current_s1is/config/ums/serverconfig.xml
- 3rd_party/security/current_s1is/config/ldif/install.ldif
- 3rd_party/security/current_s1is/lib/AMConfig.properties
- 3rd_party/security/current_s1is/config/xml/amAuthCert.xml
- 3rd_party/security/current_s1is/config/xml/amAuthLDAP.xml
- 3rd_party/security/current_s1is/config/xml/amAuthMembership.xml
- 3rd_party/security/current_s1is/config/xml/amPolicyConfig.xml

5 Copy the following text and create a file called /tmp/389.2.sh.

```
#!/bin/sh

passwd=$1
host=$2
newport=$3

LD_LIBRARY_PATH=/opt/nortel/3rd_party/
security/s1is_6.0_SP1/ldaplib/solaris/sparc/
ldapsdk;
```

```
export LD_LIBRARY_PATH

( printf "dn: "; \
  cat /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthCert.xml.tmp | sed -n
1p; \
 echo "changetype: modify"; echo "replace:
sunserviceschema"; \
  /opt/nortel/3rd_party/netscape/current_nds/
bin/slapd/server/ldif -b sunserviceschema \
     < /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthCert.xml;  ) |  \
/opt/nortel/3rd_party/netscape/current_nds/
shared/bin/ldapmodify \
    -D "cn=Directory Manager" -w $passwd -h
$host -p $newport


( printf "dn: "; \
  cat /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthLDAP.xml.tmp | sed -n
1p; \
  echo "changetype: modify"; echo "replace:
sunserviceschema"; \
  /opt/nortel/3rd_party/netscape/current_nds/
bin/slapd/server/ldif -b sunserviceschema \
     < /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthLDAP.xml;  ) |  \
/opt/nortel/3rd_party/netscape/current_nds/
shared/bin/ldapmodify \
    -D "cn=Directory Manager" -w $passwd -h
$host -p $newport

( printf "dn: "; \
  cat /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthMembership.xml.tmp |
sed -n 1p; \
  echo "changetype: modify"; echo "replace:
sunserviceschema"; \
  /opt/nortel/3rd_party/netscape/current_nds/
bin/slapd/server/ldif -b sunserviceschema \
     < /opt/nortel/config/3rd_party/security/
s1is/config/xml/amAuthMembership.xml;  ) |  \
```

```
/opt/nortel/3rd_party/netscape/current_nds/
shared/bin/ldapmodify \
    -D "cn=Directory Manager" -w $passwd -h
$host -p $newport
( printf "dn: "; \
  cat /opt/nortel/config/3rd_party/security/
s1is/config/xml/amPolicyConfig.xml.tmp | sed
-n 1p; \
  echo "changetype: modify"; echo "replace:
sunserviceschema"; \
  /opt/nortel/3rd_party/netscape/current_nds/
bin/slapd/server/ldif -b sunserviceschema \
     < /opt/nortel/config/3rd_party/security/
s1is/config/xml/amPolicyConfig.xml;  ) |  \
/opt/nortel/3rd_party/netscape/current_nds/
shared/bin/ldapmodify \
    -D "cn=Directory Manager" -w $passwd -h
$host -p $newport
```

1 Execute the script.

/bin/sh /tmp/389.2.sh <directory_mng_pwd> <host> <port>

Procedure job aid

Table 11
Options for Client Process configuration

Option	Description
<org>	the top level organization in the Sun ONE DS database. For example o=ca.nortel.com.
<port>	new port number
<directory_mng_pwd>	the password for the cn=Directory Manager user in the NDS database.
<host>	the host name where the NDS database is running

Configuring the client process in the Sun ONE DS console

Procedure steps

1 Open the Sun ONE DS console.

/opt/nortel/3rd_party/netscape/current_nds/ startconsole

2. In the login screen, enter the user ID and password.
3. In the Sun ONE DS console window, click the folder icon next to the host name.
4. Click the folder icon next to **Server Group**.
5. Click **Directory Server <host_name>**.
6. In the right frame, click **Open**.
7. Change other client process references to the port:
   a. Select the **Directory** tab.
   b. Click the folder icon next to <**org**>.
   c. Click the folder icon next to **services**.
   d. Click the folder icon next to **iPlanetAMAuthLDAPService**.
   e. Click the folder icon next to **1.0**.
   f. Click **OrganizationConfig**.
   g. In the right frame, double-click **default**.
   h. Change the port value in the field **sunkeyvalue**.
   i. Click **OK**.
   j. Click the folder icon next to **iPlanetAMPolicyConfigService**.
   k. Click the folder icon next to **1.0**.
   l. Click **OrganizationConfig**.
   m. In the right frame, double-click **default**.
   n. Change the port value in the field **sunkeyvalue**.
   o. Click **OK**.

   If the replication between Sun ONE DS servers is not configured, restart the servers. For more information, refer to “Restarting the servers” (page 61).

   If the replication between Sun ONE DS servers is configured, continue with this procedure to change the replication client side.
8. Change the replication on the client side:
   a. Select the **Configuration** tab.
   b. Click the folder icon next to **Replication**.

c. Click **userRoot**.

d. In the **Current URLS for referrals**, click on the entry that contains the port.

e. Click **Delete**.

f. Enter a new URL for the new port.

g. Click **Add** then **Save**.

h. Click the folder icon next to **Data**.

i. Select <**organization**>.

j. Select the **Referrals** tab.

k. In **Current referrals for this suffix**, click on the entry that contains the port.

l. Click **Delete**.

m. Enter a new referral for the new port.

n. Click **Add** then **Save**.

Restarting the servers

Procedure steps

1 Exit the Sun ONE DS console.

2 Restart the directory server by entering the following two commands:

```
opt/nortel/3rd_party/netscape/current_nds/slapd-
<host_name>/stop-slapd
```

```
opt/nortel/3rd_party/netscape/current_nds/slapd-
<host_name>/start-slapd
```

3 Restart the admin server

```
opt/nortel/3rd_party/security/current_s1is/
servers/https-admserv/restart
```

4 Restart the server.

```
/opt/nortel/3rd_party/security/current_s1is/
servers/https-<host_name>/restart
```

Changing the Sun ONE DS admin default port

Changing the Sun ONE DS admin default port is a two part process:

- "Configuring the server port in the Sun ONE DS console" (page 62)
- "Configuring the client process" (page 62)

Configuring the server port in the Sun ONE DS console

Procedure steps

1. Open the Sun ONE DS console.

   ```
   /opt/nortel/3rd_party/netscape/current_nds/
   startconsole
   ```

2. In the login screen, enter the user ID and password.

   Note: If this is the first login, you must enter the administration URL http://<host_name>:24313.

3. In the Sun ONE DS console window, click the folder icon next to the host name.
4. Click the folder icon next to **Server Group**.
5. Select **Administration Server**.
6. Click **Open**.
7. Select the **Configuration** tab.
8. In the **Port** field, change the port number.
9. Click **Save** and then **OK**.
10. Restart the admin server by entering the following two commands

    ```
    /opt/nortel/3rd_party/netscape/current_nds/stop-
    admin
    ```

    ```
    /opt/nortel/3rd_party/netscape/current_nds/
    start-admin
    ```

Configuring the client process

Procedure steps

1. Open the Sun ONE DS console.

   ```
   /opt/nortel/3rd_party/netscape/current_nds/
   startconsole
   ```

2 In the login screen, enter the user ID and password.

3 Enter the new administration URL.

http://<host_name>:<new_port>

Changing the RADIUS server default port

Procedure steps

1. Change the port number in the file

   `/opt/nortel/config/applications/security/radius/radius.properties`

2. Stop the RADIUS server.

   `/opt/nortel/applications/security/current_radius/bin/configure_radius.sh -stop`

3. If you want to start the server as a managed process enter the following command:

   `/opt/nortel/applications/security/current_radius/swmgmt//bin/configure_radius.sh -inittab`

   If you want to start the server as an un-managed process enter the following command:

   `/opt/nortel/applications/security/current_radius/bin/configure_radius.sh -start`

Changing the Sun ONE identity server default port

Procedure steps

1 Change directories by entering:

```
cd /opt/nortel
```

2 Change the port number in the following files:

- /config/applications/security/core/auth/ AMConfig.auth.cpp.properties
- /config/applications/security/core/auth/ AMConfig.auth.java.properties
- /config/applications/security/core/is.env
- /3rd_party/security/current_s1is/capi/config/ AMAgent.properties
- /config/3rd_party/security/s1is/es6/config/ https-<host_name>/AMAgent.properties
- /config/3rd_party/security/s1is/es6/config/ https-<host_name>/response
- /3rd_party/security/current_s1is/lib/ AMConfig.properties
- /3rd_party/security/current_s1is/servers/ https-<host_name>/config/server.xml

3 Copy the text below and create a file called /tmp/58080.1.sh:

```
#!/bin/sh
org=$1
newport=$2
LD_LIBRARY_PATH=/opt/nortel/3rd_party/
security/current_s1is/ldaplib/solaris/sparc/
ldapsdk
export LD_LIBRARY_PATH

/opt/nortel/3rd_party/security/current_s1is/
bin/ldapsearch -o \
        -b "ou=1.0,ou=
iPlanetAMPlatformService,ou=services,$org" \
-D "cn=Directory Manager" -w directory -h
`hostname` -p $newport "(objectclass=*)"
sunserviceschema  > \
```

```
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amPlatform.xml.tmp

cat  /opt/nortel/config/3rd_party/security/
s1is/config/xml/amPlatform.xml.tmp | sed -n '/
<ServicesConfiguration>/,/<\/
ServicesConfiguration>/p' \
| sed -e 's/sunserviceschema=//' > /opt/
nortel/config/3rd_party/security/s1is/config/
xml/amPlatform.xml

/opt/nortel/3rd_party/security/current_s1is/
bin/ldapsearch -o \
-b "ou=1.0,ou=
iPlanetAMSAMLService,ou=services,$org" \
-D "cn=Directory Manager" -w directory -h
`hostname` -p $newport "(objectclass=*)"
sunserviceschema  > \
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amSAML.xml.tmp

cat  /opt/nortel/config/3rd_party/security/
s1is/config/xml/amSAML.xml.tmp | sed -n '/
<ServicesConfiguration>/,/<\/
ServicesConfiguration>/p' \
| sed -e 's/sunserviceschema=//' > /opt/
nortel/config/3rd_party/security/s1is/config/
xml/amSAML.xml
```

4 Execute the script by entering the following command:

/bin/sh /tmp/58080.1.sh <org> <port>

5 Change the port number in the following files:

- /opt/nortel/3rd_party/security/current_s1is/config/xml/amSAML.xml
- /opt/nortel/3rd_party/security/current_s1is/config/xml/amPlatform.xml

6 Copy the text below and create a file called /tmp/58080.2.sh :

```
#!/bin/sh

passwd=$1
host=$2
```

```
newport=$3

LD_LIBRARY_PATH=/opt/nortel/3rd_party/
security/s1is_6.0_SP1/ldaplib/solaris/sparc/
ldapsdk;
export LD_LIBRARY_PATH

( printf "dn: "; \
  cat /opt/nortel/config/3rd_party/security/
s1is/config/xml/amSAML.xml.tmp | sed -n 1p; \
  echo "changetype: modify"; echo "replace:
sunserviceschema"; \
  /opt/nortel/3rd_party/netscape/current_nds/
bin/slapd/server/ldif -b sunserviceschema \ <
/opt/nortel/config/3rd_party/security/s1is/
config/xml/amSAML.xml;  ) |  \
/opt/nortel/3rd_party/netscape/current_nds/
shared/bin/ldapmodify \
    -D "cn=Directory Manager" -w $passwd -h
$host -p $newport



( printf "dn: "; \
  cat /opt/nortel/config/3rd_party/security/
s1is/config/xml/amPlatform.xml.tmp | sed -n
1p; \
  echo "changetype: modify"; echo "replace:
sunserviceschema"; \
  /opt/nortel/3rd_party/netscape/current_nds/
bin/slapd/server/ldif -b sunserviceschema \
     < /opt/nortel/config/3rd_party/security/
s1is/config/xml/amPlatform.xml;  ) |  \
/opt/nortel/3rd_party/netscape/current_nds/
shared/bin/ldapmodify \
    -D "cn=Directory Manager" -w $passwd -h
$host -p $newport
```

7 Execute the script by entering the following command:

/bin/sh /tmp/58080.2.sh <directory_mng_pwd> <host> <port>

8 Restart the admin server by entering the following command:

/opt/nortel/3rd_party/security/current_s1is/servers/https-admserv/restart

9 Restart the server by entering the following command:

/opt/nortel/3rd_party/security/current_s1is,servers/https-<host_name>/restart

10 Change the port number in the file:

`/opt/nortel/config/applications/security/isclient/is_client.env`

11 If IS_AUTH_CONFIG_URL is configured, change the port number in the following files:

- `/opt/nortel/config/applications/desktop/jws/mft/resources/desktop/DesktopGUI.jnlp`
- `/opt/nortel/config/applications/desktop/local/mft/resources/desktop/DesktopGUI.config`

12 Restart the logging server by entering the following two commands:

/opt/nortel/applications/security/current_core/bin/socketserver.sh stop

/opt/nortel/applications/security/current_core/bin/socketserver.sh start

13 Restart the Apache server by entering the following command:

/opt/nortel/3rd_party/apache/current_apache/bin/apachectl -k stop

Procedure job aid

Table 12
Server default port options

Option	Description
<org>	the top level organization in the NDS database. For example o=ca.nortel.com
<port>	the NDS directory server port number

Table 12
Server default port options

Option	Description
<directory_mng_pwd>	the password for the cn=Directory Manager user in the NDS database
<host>	the host name where the NDS database is running

Changing the Sun ONE identity admin default port

Procedure steps

1. Change the port number in the following file:

   ```
   /opt/nortel/3rd_party/security/current_s1is/
   servers/https-admserv/config/server.xml
   ```

2. Restart the admin server by entering the following command:

   `/opt/nortel/3rd_party/security/current_s1is/servers/https-admserv/restart`

3. Start the NDS admin console by entering the following command:

   `/opt/nortel/3rd_party/netscape/current_nds/startconsole`

4. In the login window, use the URL http://<host_name>.<org>:<port>.

Procedure job aid

Table 13
Server default port options

Option	Description
<org>	the top level organization in the NDS database. For example o=ca.nortel.com
<port>	the NDS directory server port number

Operator Client ports

The dynamic ports listed inTable 14 “MDM server ports” (page 70) must be allowed through the firewall in order for Operator Client to communicate with MDM and the User Administrator server.

If your system uses any of the services listed below, change the port numbers in the /opt/MagellanNMS/cfg/private/IPCNameMap.cfg file. For information on how to change these ports, refer to the procedure to configure named TCP/UDP ports in the 241-6001-310 *Preside MDM Server Reference Guide*.

In addition, there are a number of fixed ports that may require changing if there is a conflict with your existing port settings. For more information, refer to Table 15 “Services on fixed ports” (page 71).

Table 14
MDM server ports

Server Name	Service	Protocol	Description
Network Model	NMAGENT	TCP	network model agent used to supply state information to fault applications
RTAC Agent	RTACAGENT	TCP	service used to access the RTAC agent
GMDR Agent	GMDRAGENT	TCP	service is used to receive fault information for fault applications
Fault Dev Access Agent	CCAGENT PSVAGENT NSVAGENT	TCP TCP TCP	services used by the fault tools. These services are created when /opt/MagellanNMS/bin/psvagent is started by svmdmn.
Data Viewer Agent	PMAGENT	TCP	service used to access the dataviewer agent

Table 14
MDM server ports

Server Name	Service	Protocol	Description
Nodal Provisioning Configuration Manager	CONFIGMAN	TCP	provides configuration services for the nodal provisioning interface. Note: this port is fixed through a command line.
Multinodal Name Service Agent	MNSDAGENT	UDP	two types of servers that allow inter-process communication to be established. Note: these two ports are fixed as default.

Table 15
Services on fixed ports

Server Name	Description
Apache Web Server	used to download the desktop jar files. Any change you make to this port number is not persistent between MDM software upgrades. You must reset this port number after every upgrade.
Sun ONE DS	used for password changes
Sun ONE IS Webserver	used for user authentication
Tomcat server	used for the online help system

Appendix B
IPSec in tunnel mode

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. Passport supports transport mode only.

The scripts and procedures that are described in "IPSec configuration" (page 13) are for setting up transport mode only. Tunnel mode SAs must be configured using manual procedures.

For more information, refer to *Sun Microsystems, IPSec and IKE Administration Guide (816-7264-10).*

Appendix C
Passport Procedures

The following procedures related to Secure Communications must be performed on the Passport node.

- “Configuring the initial SA on a node” (page 75)
- “Modifying IPSec on nodes manually” (page 81)
- “Configuring secure FTP authentication on a Passport” (page 46)

Configuring the initial SA on a node

Configure the initial SA on Passport nodes by configuring IPSec manually to set up IP security (IPSec) using a command line interface.

Prerequisites

- IPSec is supported for the OAM Ethernet, Ethernet, and ATM MPE media types. Before configuring IPSec, you must first configure the required media type.
- The ipsec feature must be configured in the software AVL. For more information on adding features to the AVL, see NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.
- To ensure absolute protection, the node IPSec policy must be set by connecting directly to the serial port with a Vt100, so that the encryption key can not be stolen. The key used on the node is the same key that must be used on the Preside Multiservice Data Manager (MDM) workstation, otherwise you will need to delete the policy and create it again

Procedure steps

1. Add an IPSec policy database.

   ```
   add Vr/0 Ip Spd/<spd_name>
   ```

2. Add a policy for inbound traffic.

   ```
   add Vr/0 Ip Spd/<spd_name> Policy/<pol_in>
   ```

3. Add a policy for outbound traffic.

   ```
   add Vr/0 Ip Spd/<spd_name> Policy/<pol_out>
   ```

4. Specify the action and direction for the inbound traffic policy.

   ```
   set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> action
   <action>, direction in
   ```

5. Specify the action and direction for the outbound traffic policy.

   ```
   set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> action
   <action>, direction out
   ```

6. Specify the selector attributes for the inbound traffic policy.

   ```
   set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> srcIpAddr
   <src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
   srcPort <src_port>, dstPort <dst_port>
   ```

7. Specify the selector attributes for the outbound traffic policy.

   ```
   set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> srcIpAddr
   <src_addr>, dspIpAddr <dst_addr>, protocol <protocol>,
   srcPort <src_port>, dstPort <dst_port>
   ```

8. Add the security association for the inbound policies that have *Vr Ip Spd Policy action* set to apply.

   ```
   add Vr/0 Ip Spd/<spd_name> Policy/<pol_in> Sa/
   <sa_addr_1>,<esp>,<spi_1>
   ```

   Adding the *Sa* component automatically creates a *ManEspSa* subcomponent.

9. Add the security association for the outbound policies that have *Vr Ip Spd Policy action* set to apply.

   ```
   add Vr/0 Ip Spd/<spd_name> Policy/<pol_out> Sa/
   <sa_addr_2>,<esp>,<spi_2>
   ```

   Adding the *Sa* component automatically creates a *ManEspSa* subcomponent.

10 Set the algorithms and keys for the inbound policy security association.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> Sa/
<sa_addr_1>,<esp>,<spi_1> ManEspSa encAlgorithm
<enc_alg>, encKey <enc_key_1>, authAlgorithm
<auth_alg>, authKey <auth_key_1>
```

11 Set the algorithms and keys for the outbound policy security association.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> Sa/
<sa_addr_2>,<esp>,<spi_2> ManEspSa encAlgorithm
<enc_alg>, encKey <enc_key_2>, authAlgorithm
<auth_alg>, authKey <auth_key_2>
```

12 Return to the appropriate task flow for your procedure:

- "IPSec configuration between MDM and Passport" (page 15)
- "IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9" (page 17)
- "IPSec configuration on MDM workstations running Solaris 9" (page 20)
- "IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP" (page 22)

Variable definitions

Variable	Value
<action>	The action to be taken when a packet is received that matches the policy.
<auth_alg>	The authentication algorithm for the security association. Specify at least one of *encAlgorithm* and *authAlgorithm*; they cannot both be set to none.
<auth_key_1> <auth_key_2>	The symmetric key for the keyed-hash function for the security association.
<dst_addr>	The destination IP address for traffic flows to which the policy applies.
<dst_port>	The destination TCP or UDP port number for traffic flows to which the policy applies.

(Sheet 1 of 2)

Variable	Value
<enc_alg>	The encryption algorithm for the security association. Specify at least one of *encAlgorithm* and *authAlgorithm*; they cannot both be set to none.
<enc_key_1> <enc_key_2>	The symmetric encryption key for the security association.
<esp>	The IPSec protocol type for the security association.
<pol_in>	The instance value of the policy for inbound traffic. The instance value specifies the policy's precedence. Policy lookup occurs in order of increasing precedence value.
<pol_out>	The instance value of the policy for outbound traffic. The instance value specifies the policy's precedence. Policy lookup occurs in order of increasing precedence value.
<protocol>	The layer 4 protocol to which the policy applies.
<sa_addr_1>	The IP address of the local node (for inbound SAs).
<sa_addr_2>	The IP address of the MDM workstation (for outbound SAs).
<spd_name>	The name of the security policy database.
<spi_1> <spi_2>	The security parameter index for the security association.
<src_addr>	The source IP address for traffic flows to which the policy applies.
<src_port>	The source TCP or UDP port number for traffic flows to which the policy applies.

(Sheet 2 of 2)

Example 1 of configuring the initial SA on a node

This example shows IPSec provisioning for FTP traffic where

- IPSec processing is applied
- The FTP connection is from the workstation to the node

Since the security policies are unidirectional and there are two separate traffic flows (FTP control channel and FTP data channel), four security policies are provisioned.

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/10
add Vr/0 Ip Spd/1 Policy/20
add Vr/0 Ip Spd/1 Policy/30
add Vr/0 Ip Spd/1 Policy/40
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/10 action apply, direction out
set Vr/0 Ip Spd/1 Policy/20 action apply, direction in
set Vr/0 Ip Spd/1 Policy/30 action apply, direction out
set Vr/0 Ip Spd/1 Policy/40 action apply, direction in
```

3 Set the traffic flow policy selectors for the FTP control channel.

```
set Vr/0 Ip Spd/1 Policy/10 srcIpAddr 20.10.2.1,
dstIpAddr 30.5.1.1, protocol tcp, srcPort ftp

set Vr/0 Ip Spd/1 Policy/20 srcIpAddr 30.5.1.1,
dstIpAddr 20.10.2.1, protocol tcp, dstPort ftp
```

4 Set the traffic flow policy selectors for the FTP data channel.

```
set Vr/0 Ip Spd/1 Policy/30 srcIpAddr 20.10.2.1,
dstIpAddr 30.5.1.1, protocol tcp, scrPort ftpdata

set Vr/0 Ip Spd/1 Policy/40 srcIpAddr 30.5.1.1,
dstIpAddr 20.10.2.1, protocol tcp, dstPort ftpdata
```

5 Add security associations (SAs) for the FTP control channel. A security association is required when attribute *Vr Ip Spd Policy action* is set to apply.

```
add Vr/0 Ip Spd/1 Policy/10 Sa/30.5.1.1,esp,300
add Vr/0 Ip Spd/1 Policy/20 Sa/20.10.2.1,esp,301
```

6 Set the algorithms and keys for the FTP control channel.

```
set Vr/0 Ip Spd/1 Policy/10 Sa/30.5.1.1,esp,300
ManEspSa encAlgorithm des, enckey d0efbc8a79462513,
authAlgorithm md5, authKey
fedcba98765432100123456789abcdef

set Vr/0 Ip Spd/1 Policy/20 Sa/20.10.2.1,esp,301
ManEspSa encAlgorithm des, enckey 132546798abcefd0,
authAlgorithm md5, authKey
0123456789abcdeffedcba9876543210
```

7 Add security associations (SAs) for the FTP data channel. The security parameter indexes (SPIs) can be the same for both SAs, as in this example.

```
add Vr/0 Ip Spd/1 Policy/30 Sa/30.5.1.1,esp,400
add Vr/0 Ip Spd/1 Policy/40 Sa/20.10.2.1,esp,401
```

8 Set the algorithms and keys for the FTP data channel.

```
set Vr/0 Ip Spd/1 Policy/30 Sa/30.5.1.1,esp,400
ManEspSa authAlgorithm sha1, authKey
fedcba98765432100123456789abcdeffedcba9876543210

set Vr/0 Ip Spd/1 Policy/30 Sa/20.10.2.1,esp,401
ManEspSa authAlgorithm sha1, authKey
0123456789abcdeffedcba98765432100123456789abcdef
```

Example 2 of configuring the initial SA on a node

This example shows IPSec provisioning for ICMP traffic, where all ICMP packets are discarded. This example applies to all ICMP traffic originating from either the Passport node or Preside Multiservice Data Manager workstation and destined for either the workstation or node, respectively.

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/50
add Vr/0 Ip Spd/1 Policy/60
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/50 action discard, direction
out
set Vr/0 Ip Spd/1 Policy/60 action discard, direction
in
```

3 Set the traffic flow policy selectors for all ICMP traffic.

```
set Vr/0 Ip Spd/1 Policy/50 protocol icmp

set Vr/0 Ip Spd/1 Policy/60 protocol icmp
```

Example 3 of configuring the initial SA on a node

This example shows IPSec provisioning for UDP traffic, where IPSec processing is bypassed. This example applies to all UDP traffic originating from either the Passport node or Preside Multiservice Data Manager workstation and destined for either the workstation or node, respectively.

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/70
add Vr/0 Ip Spd/1 Policy/80
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/70 action bypass, direction
out
set Vr/0 Ip Spd/1 Policy/80 action bypass, direction in
```

3 Set the traffic flow policy selectors for the UDP traffic.

```
set Vr/0 Ip Spd/1 Policy/70 srcIpAddr 20.10.2.1,
dstIpAddr 30.5.1.1, protocol udp
```

```
set Vr/0 Ip Spd/1 Policy/80 srcIpAddr 30.5.1.1,
dstIpAddr 20.10.2.1, protocol udp
```

Modifying IPSec on nodes manually

Modify IPSec on Passport nodes manually to change the IP Security (IPSec) configuration using command line interface without using Preside Multiservice Data Manager (MDM).

Prerequisites

- IPSec is supported for the OAM Ethernet, Ethernet, and ATM MPE media types. Before configuring IPSec, you must first configure the required media type.
- The ipsec feature must be configured in the software AVL. For more information on adding features to the AVL, see NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

Procedure steps

1 If necessary, add a policy for inbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_in>
```

2 If necessary, delete a policy for inbound traffic.

```
del Vr/0 Ip Spd/<spd_name> Policy/<pol_in>
```

3 If necessary, add a policy for outbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_out>
```

4 If necessary, delete a policy for outbound traffic.

```
del Vr/0 Ip Spd/<spd_name> Policy/<pol_out>
```

5 Specify the action and direction for an existing inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> action
<action>, direction in
```

6 Specify the action and direction for an existing outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> action
<action>, direction out
```

7 Specify the selector attributes for an existing inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
srcPort <src_port>, dstPort <dst_port>
```

8 Specify the selector attributes for an existing outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
srcPort <src_port>, dstPort <dst_port>
```

9 Add the security association for any inbound policies that have *Vr Ip Spd Policy action* set to apply.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_in> Sa/
<sa_addr_1>,<esp>,<spi_1>
```

Adding the *Sa* component automatically creates a *ManEspSa* subcomponent.

10 Add the security association for the outbound policies that have *Vr Ip Spd Policy action* set to apply.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_out> Sa/
<sa_addr_2>,<esp>,<spi_2>
```

Adding the *Sa* component automatically creates a *ManEspSa* subcomponent.

11 Set the algorithms and keys for the inbound policy security association.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> Sa/
<sa_addr_1>,<esp>,<spi_1> ManEspSa encAlgorithm
<enc_alg_1>, encKey <enc_key_1>, authAlgorithm
<auth_alg_1>, authKey <auth_key_1>
```

12 Set the algorithms and keys for the outbound policy security association.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> Sa/
<sa_addr_2>,<esp>,<spi_2> ManEspSa encAlgorithm
<enc_alg_2>, encKey <enc_key_2>, authAlgorithm
<auth_alg_2>, authKey <auth_key_2>
```

13 Return to the appropriate task flow for your procedure:

- "IPSec configuration between MDM and Passport" (page 15)
- "IPSec configuration on MDM workstations running Solaris 8 connected to MDM workstations running Solaris 8 or Solaris 9" (page 17)
- "IPSec configuration on MDM workstations running Solaris 9" (page 20)
- "IPSec configuration between MDM running Solaris 9 and a PC workstation with Microsoft Windows 2000/XP" (page 22)

Variable definitions

Variable	Value
<action>	The action to be taken when a packet is received that matches the policy.
<auth_alg_1> <auth_alg_2>	The authentication algorithm for the security association. Specify at least one of *encAlgorithm* and *authAlgorithm*; they cannot both be set to none.
<auth_key_1> <auth_key_2>	The symmetric key for the keyed-hash function for the security association.
<dst_addr>	The destination IP address for traffic flows to which the policy applies.
<dst_port>	The destination TCP or UDP port number for traffic flows to which the policy applies.
<enc_alg_1> <eng_alg_2>	The encryption algorithm for the security association. Specify at least one of *encAlgorithm* and *authAlgorithm*; they cannot both be set to none.
<enc_key_1> <enc_key_2>	The symmetric encryption key for the security association.
<esp>	The IPSec protocol type for the security association.
<pol_in>	The instance value of the policy for inbound traffic. The instance value specifies the policy's precedence. Policy lookup occurs in order of increasing precedence value.

(Sheet 1 of 2)

Variable	Value
<pol_out>	The instance value of the policy for outbound traffic. The instance value specifies the policy's precedence. Policy lookup occurs in order of increasing precedence value.
<protocol>	The layer 4 protocol to which the policy applies.
<sa_addr_1>	The IP address of the local node (for inbound SAs).
<sa_addr_2>	The IP address of the MDM workstation (for outbound SAs).
<spd_name>	The name of the security policy database.
<spi_1> <spi_2>	The security parameter index for the security association.
<src_addr>	The source IP address for traffic flows to which the policy applies.
<src_port>	The source TCP or UDP port number for traffic flows to which the policy applies.
(Sheet 2 of 2)	

Passport - MDM

Network Security: Secure Communications Configuration

Release 15.1RSUP

Publication: NN10600-607
Document status: Standard
Document version: 15.1 RSUP, PCR 6.1
Document date: August 2004
Printed in Canada

NORTEL NETWORKS