NORTEL NETWORKS

Passport - MDM

Network Security: User Access Configuration

NN10600-606

Passport - MDM

Network Security: User Access Configuration

Publication: NN10600-606
Document status: Standard
Document version: 15.1RSUP, 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 11
User access configuration prerequisites 11
What's new in network security operations? 12
Secure communications 12
User Administration system for centralized authentication 12

Chapter 1
User access configuration 13

Chapter 2
Local user configuration on Passport 17
Adding a new userId 20
Creating a new userId by copying an existing userId 23
Setting a password using a secure method 24
Configuring Passport telnet and local console timeout 27

Chapter 3
RADIUS Interface configuration 29
Configuring the internal MDM RADIUS interface for authentication requests 32
Configuring allowed and denied IP Addresses 32
Configuring shared secrets 34
Configuring network element properties 36
Loading configuration files while the server is running 37
Restarting the RADIUS server 38
Configuring the local directory server 39

Chapter 4
Centralized authentication configuration 41
Configuring the RADIUS component on the Passport 43
Configuring the RADIUS server with Passport VSAs 45
Passport RADIUS Vendor Specific Attribute Definitions 47

Chapter 5
Configuring the User Administration system 49
Configuring the MDM User Administrator server to use an External RADIUS server 53
Migration of user identities to an external repository 55
Migration of user identities from an external repository 56
Logging into the User Administration system 57
Configuring users 61
Viewing system account userids 61
Changing system account passwords 63
Changing Sun ONE Directory Manager password 66
Setting validation period for system account password 66
Setting validation period of user account password 67
Configuring the Mail server and port 67
Setting up a cron job to check for password expiry 68
Changing centrally authenticated passwords 68
Changing a user password in the Sun ONE IS console 69
Changing the Sun ONE IS Web Server admin account 69
Changing the password for amldapuser 70
Changing the password for dsameuser 71
Changing the password for puser 71
Changing the password for the amService-UrlAccessAgent account 71
Setting up redundant Directory Servers 73
Configuring the policy agent 76

Chapter 6
Basic security settings for User Administration system 77
Modifying password settings 80

Modifying user account settings 81
Modifying login warning definition 82
Customizing an email template for password expiry 83

Chapter 7
User Administration system user configuration 85

Creating users 89
Creating a centrally authenticated user using the User Administration system 89
Changing an existing Passport user to be centrally authenticated and locally authorized 90
Creating a role 91
Creating a policy 92
Adding a policy to subjects 95
Changing a Passport user ID to be centrally authenticated 96

Chapter 8
User access administration 97

Backing up User Administration information 99
Backing up Sun ONE Directory Server 99
Restoring a non replicated Sun ONE Directory Server 100
Restoring one Sun ONE Directory Server in a replicated pair 102
Restoring both Sun ONE IS servers in a replicated pair 105
Backing up desktop user interface data 107
Restoring desktop user interface data 107
Changing a centrally defined user ID attributes 108
Changing Passport user ID attributes 109
Changing a local Passport user password 110
Deleting a centrally defined user 111
Deleting a local Passport user 112
Deleting a role 113
Denying a centrally defined user access to a node 114
Displaying the number of user sessions on a Passport node 115
Displaying the user IDs on a Passport network management interface 117
Displaying the users on the User Management system 118

Managing policies 119
Restricting access through a Passport network element interface 120
Releasing a locked Passport network management interface 121
Resetting a centrally defined user password 122
Starting the Sun ONE DS console 123
Terminating a centrally defined user's session 124
Terminating a user session on a Passport network management interface 125
Terminate all user sessions on a Passport network management interface 126
Sun ONE Identity Server system recovery 127
Stopping the NDS processes 127
Recreating the DBVERSION files 128
Restarting the NDS processes 128

Chapter 9
Remote access using telnet 131
Connecting to a device using Telnet 133

About this document

NN10600-606 *Passport - MDM Network Security: User Access Configuration* provides procedural information on configuring user access and permissions for anyone who provisions security measures in a network.

User access 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.
- NN10600-030 *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.
- NN10600-605 *Passport - MDM Network Security: Operations* for an overview of security concepts related to user access and network security.

- Access to online help: The majority of the tasks in this guide are documented in the online help for User Administration. In each procedure, you may be directed to the online help for additional information.

What's new in network security operations?

The following features were added to this document:

- "Secure communications" (page 12)
- "User Administration system for centralized authentication" (page 12)

Secure communications

The following section was added:

- "Remote access using telnet" (page 131)

User Administration system for centralized authentication

The following section was added:

- "Configuring the User Administration system" (page 49)
- "Basic security settings for User Administration system" (page 77)

The following sections were updated:

- "RADIUS Interface configuration" (page 29)
- "Centralized authentication configuration" (page 41)
- "User Administration system user configuration" (page 85)
- "User access administration" (page 97)

The following section was removed:

- LDAP server configuration. This section was removed because the LDAP server on the Sun ONE IS cannot be used for centralized user authentication. You must use a separate server for this purpose.

Chapter 1
User access configuration

Configure user access to deploy authentication methods in which userIDs, passwords, and access permissions are stored locally or on a remote, centralized device using the RADIUS protocol.

Navigation links

- "Prerequisites to user access configuration" (page 13)
- "User access configuration flow" (page 13)
- "Task navigation" (page 16)

Prerequisites to user access configuration

- a user access plan for the network defining the types of users (roles) and policies you will have and how they will be authenticated.
- a Solaris 9 workstation or a Solaris 8 workstation with the 02-02 (February 2002) update and the latest Solaris 8 patch bundle installed. You can download the update and the patches from the Sun website.
- Access to online help: The majority of the tasks in this guide are documented in the online help for the User Administration system. In each procedure, you may be directed to the online help for additional information.
- *Management Technology Security Services Developer Guide.*

User access configuration flow

These taskflows show you the sequence of tasks you perform to configure user access to a node. To link to any task go to "Task navigation" (page 16).

Figure 1
User access configuration task flow (sheet 1 of 2)

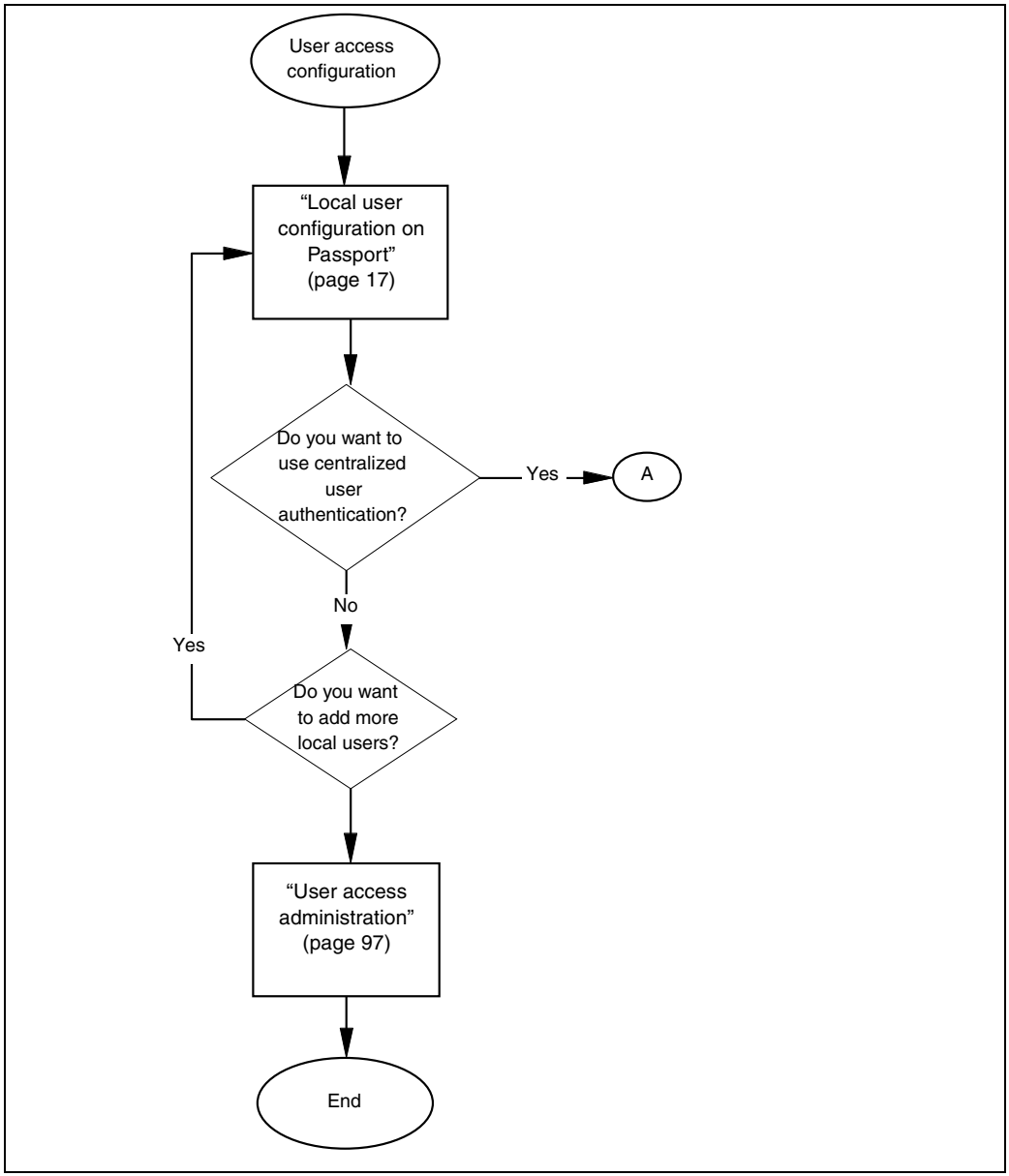
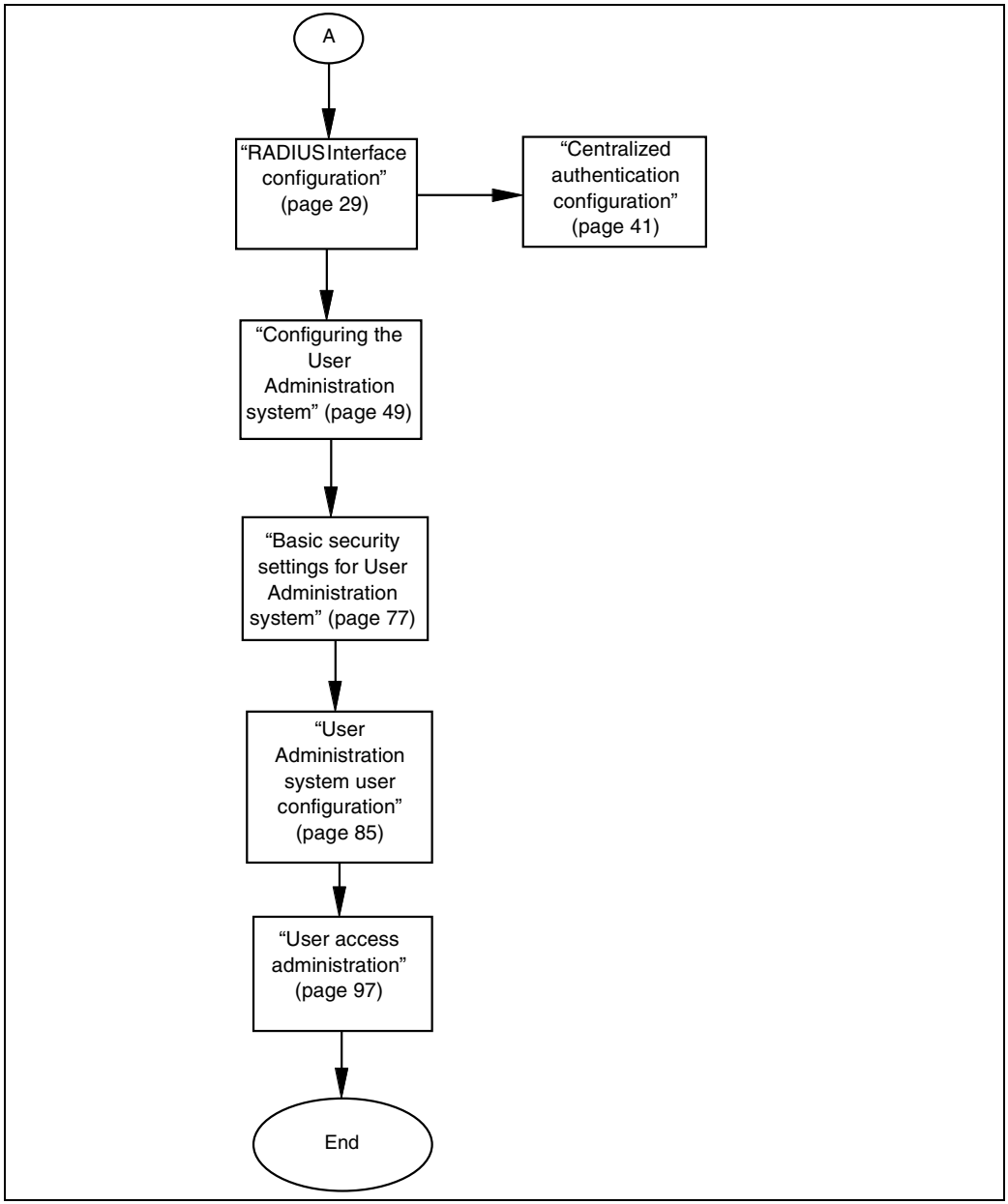


Figure 2
User access configuration task flow (sheet 2 of 2)



Task navigation

- “Local user configuration on Passport” (page 17)
- “RADIUS Interface configuration” (page 29)
- “Centralized authentication configuration” (page 41)
- “Configuring the User Administration system” (page 49)
- “Basic security settings for User Administration system” (page 77)
- “User Administration system user configuration” (page 85)
- “User access administration” (page 97)
- “Remote access using telnet” (page 131)

Chapter 2
Local user configuration on Passport

Configure local users to set session timeouts, enable command logging and add local users.

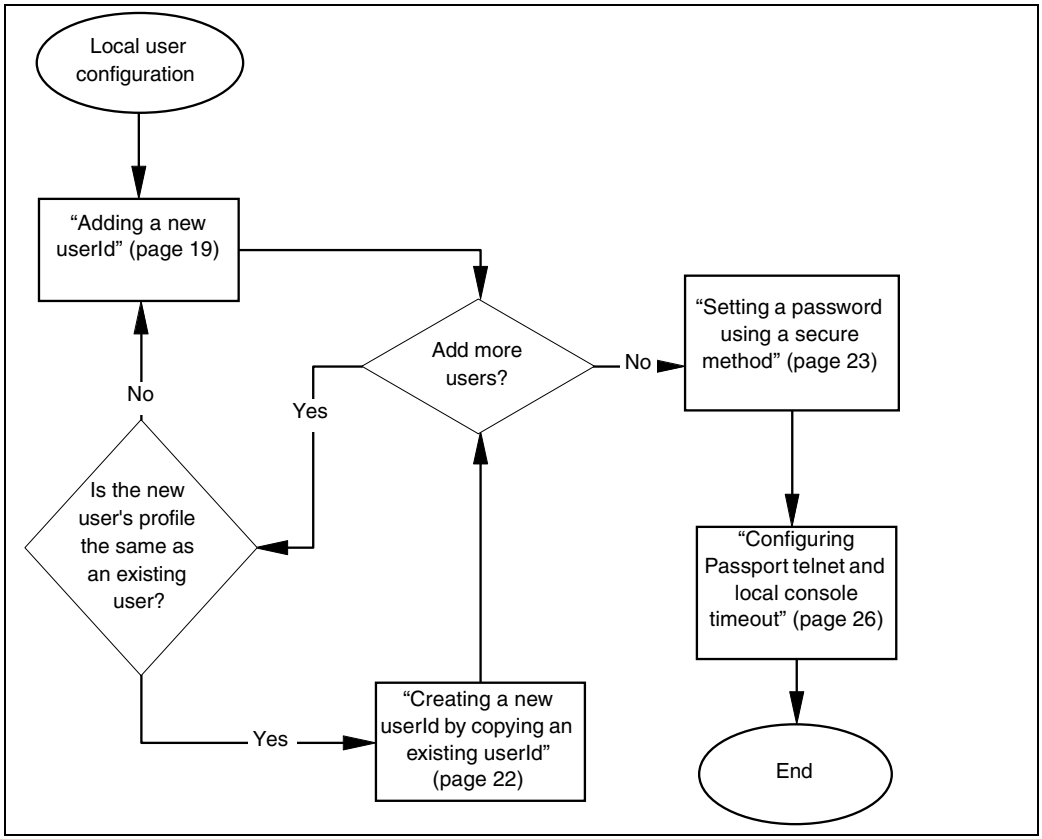
Navigation links

- "Local user configuration flow" (page 17)
- "Task navigation" (page 18)

Local user configuration flow

This taskflow shows you the sequence of procedures you perform to configure local users. To link to any procedure, go to "Task navigation" (page 18).

Figure 3
Local user configuration task flow



Task navigation

- "Adding a new userId" (page 19)
- "Creating a new userId by copying an existing userId" (page 22)
- "Setting a password using a secure method" (page 23)
- "Configuring Passport telnet and local console timeout" (page 26)

Adding a new userId

Add a new userID to a node to specify who is allowed access. You can add new userIDs when you are setting up a new node and any time after that.

Prerequisites

- Unless this is a new node, you must be logged in with a userID with a command impact of systemAdministration.
- If you are using only locally defined userIDs, it is recommended that you define at least the following userIDs:
  - Two userIDs with command impact of systemAdministration
  - A userID that lets you view node alarms on Preside Multiservice Data Manager. This userID must have a command scope of network, command impact of service, and allowed access of FMIP.
- Command logging can be used as a tool to monitor user access.
- If you are using RADIUS authentication, it is recommended that you define at least one locally defined userID with a command scope of network, command impact of systemAdministration, and allowed access of all network management interfaces. However, the userID defined locally needs to be different than those on the RADIUS server. Otherwise the authentication method defaults to local.

Procedure steps

1. Add a userID.

   ```
   add Ac Userid/<user_id>
   ```

2. Set the password.

   ```
   set Ac Userid/<user_id> password <pswd>
   ```

3. Set the customer identifier (CID).

   ```
   set Ac Userid/<user_id> cid <cust_id>
   ```

4. Set the command scope.

   ```
   set Ac Userid/<user_id> commandScope <scope>
   ```

5. Set the command impact.

   ```
   set Ac Userid/<user_id> commandImpact <impact>
   ```

6 Set the allowed network management interfaces.

```
set Ac Userid/<user_id> allowedAccess <nmifs>
```

Note: To disallow a network management interface, type the attribute value preceded by a tilde (~).

7 Set the allowed out access.

```
set Ac Userid/<user_id> allowedOutAccess <out_access>
```

8 Optionally, set the timeout protocol.

```
set Ac Userid/<user_id> timeoutProtocol
<timeoutProtocol>
```

9 Optionally, set the user login directory for file system commands or FTP commands.

```
set Ac Userid/<user_id> loginDirectory <directory>
```

Variable definitions

Variable	Value
<cust_id>	The customer identifier restricts a user's access to those components with the same CID. However, 0 (zero) can access any component. Only userIDs with a CID of 0 (zero) can provision. When you assign a CID to a component, every subcomponent that is to be seen by the same user must be manually provisioned with a CID value equal to that of the parent component.
<directory>	The login directory for the userID. This is similar to a home directory in UNIX. The default is /, which is the root directory.
<impact>	One of *passive*, *service*, *configuration*, or *systemAdministration*. The default is *passive*.
<nmifs>	One or more allowed network management interfaces for the userID: • *local* (for a directly connected VT100 terminal) • *fmip* (for Preside Multiservice Data Manager) • *telnet* (for a standard telnet connection) • *ftp* (for a standard FTP connection) The default is *local*.

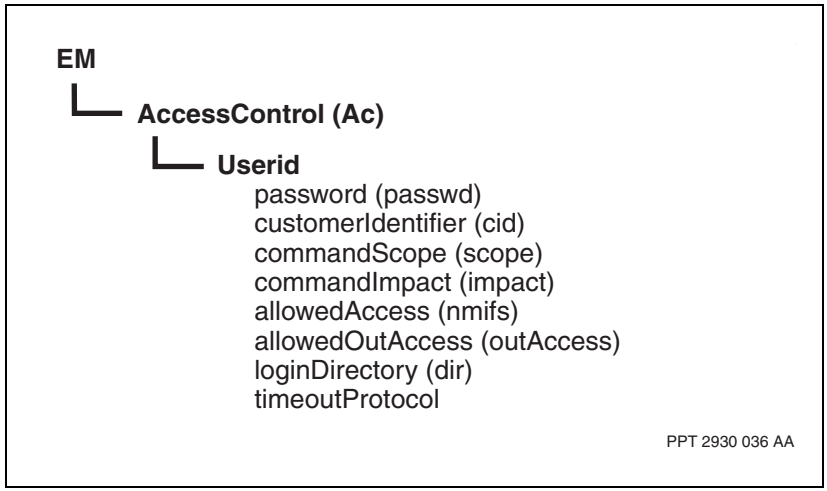
(Sheet 1 of 2)

Variable	Value
<out_access>	Either *telnet* or *~telnet* If you want the userID to be able to establish outgoing telnet connections, use *telnet*. If not, use *~telnet*.
<pswd>	The initial password for the new userID. It needs to be five to eight characters long. Passwords are case sensitive. When you are setting a password, it displays on the screen. Once set, the password cannot be displayed again. Locally defined passwords do not expire.
<scope>	One of *application*, *device*, or *network*. The default is *application*. For Preside Multiservice Data Manager configuration tools for Passport devices, set <scope> to *network*.
<timeoutProtocol>	A setting to exempt individual users from the configured timeoutPeriod, meaning specific sessions can remain idle without being tracked for inactivity. The timeoutProtocol is enabled by default, meaning the timeoutPeriod applies to all users.
<user_id>	A new user identifier. It needs to be one to eight characters long.

(Sheet 2 of 2)

Procedure job aid

Figure 4
New userID component hierarchy



Creating a new userId by copying an existing userId

Create a new userId by copying an existing userId to easily create a large number of userIDs that have the same attributes, except the password. Once you copy a *userID* component, you only need to change the password.

Prerequisites

- You must be logged in with a userID with command impact of systemAdministration.
- To change the password of the new userID, see "Changing a local Passport user password" (page 110).
- To change any other attribute of the new userID use the *set* command, as shown in "Changing Passport user ID attributes" (page 109).

Procedure steps

1. Copy the *Userid* component.

   ```
   copy -s(Ac Userid/<old_user_id>) -d(Ac Userid/
   <new_user_id>) Prov
   ```

2. Set the password for the new userID.

   ```
   set Ac Userid/<new_user_id> password <pswd>
   ```

Variable definitions

Variable	Value
<new_user_id>	The new user identifier. It needs to be from one to eight characters long.
<old_user_id>	The old user identifier.
<pswd>	The password for the new userID. It needs to be five to eight characters long. Passwords are case sensitive. When you set a password, it displays on the user interface. Once set, the password cannot be displayed again.

Setting a password using a secure method

Set a password using a secure method to minimize the security risk when setting or changing a password for a userID.

Prerequisites

- This procedure assumes that you have a physically secure node where you can make password changes, and that you need to change a password on different but insecure node.
- The userID that needs the changed password exists on both the secure and the insecure node.
- You must be logged in with a userID with command impact of systemAdministration.
- Be aware of the following security risks when setting or changing a password:
  - The actual characters of the password appear on the user interface.
  - When you are not using a local session, the password travels over the network in easy-to-read ASCII format.
  - Local and telnet sessions have a command recall queue, which stores the last ten commands. The command in which you set the password can be recalled from the queue using the Up-Arrow and Down-Arrow keys.

Procedure steps

1. Log in to a secure node.

   Access this node from a workstation in a physically secure area using a local VT100 session. You can also use a telnet session as long as you use a secure connection. Do not establish a telnet session across a public network.

2. Start provisioning mode.

   ```
   start Prov
   ```

3. Set the password.

   ```
   set Ac Userid/<user_id> password <pswd>
   ```

4. Save the userID with the changed password.

```
save -component(Ac Userid/<user_id>) -file(<name>)
Prov
```

5 End provisioning mode.

```
end Prov
```

6 Log out of the secure node to clear the command recall queue.

```
logout
```

7 Transfer the partial saved view containing the *userID* component from the secure node to an insecure node using FTP.

Since FTP may or may not have a secure login mechanism, do not use the same userID for FTP access as you have stored in the partial saved view.

8 Transfer the partial saved view from the secure node to a workstation using FTP. You can find the partial saved view you created in the /provisioning directory of the node.You must use the complete name of the view, which is in the form <name>.part.<num>.

9 Transfer the partial saved view from the workstation to the insecure node using FTP. Put it in the /provisioning directory.

10 Log in to the insecure node.

11 Start provisioning mode.

```
start Prov
```

12 Load the partial saved view.

```
load -file(<view_name>) Prov
```

13 Verify that the provisioning changes you have made are acceptable.

```
check Prov
```

Correct any errors, then verify the provisioning changes again.

14 If you want these changes as well as other changes made in the edit view to take effect immediately, activate and commit the provisioning changes.

```
activate Prov
confirm Prov
commit Prov
```

15 End provisioning mode.

```
end Prov
```

Variable definitions

Variable	Value
<name>	A descriptive name for the partial saved view. To save a partial view to the file system, use its complete name in the form <name>.part.<num>, where <num> is an automatically generated sequence number. The *save Prov* command responds with the complete name of the view, for example, UserRoot.part.001.
<pswd>	The new password for the userID. It must to be from five to eight characters long. When you set a password, it displays on the user interface. Once set, the password cannot be displayed again.
<user_id>	The userID whose password you are changing.
<view_name>	The complete name of the partial saved view, which is in the form <name>.part.<num>.

Configuring Passport telnet and local console timeout

Configure node telnet and local console timeout to set the amount of time a session can remain idle before it is terminated.

Prerequisites

- Your user ID must have a command impact of systemAdministration.
- The new timeoutPeriod that is set only applies to new sessions.

Procedure steps

1. Configure the timeoutPeriod to specify how long a session can remain idle before it is terminated:

   ```
   set Nmis <telnet or local> timeoutPeriod <newValue>
   ```

2. If you want to make a particular user exempt from this setting, override the timeoutPeriod for that userid.

   ```
   set Ac Userid/<userid> timeoutProtocol disabled
   ```

Variable definitions

Table 1

Variable	Value
<newValue>	A value between 5 and 120 minutes.
<telnet or local>	Specify the NMIS interface to be affected.
<userid>	The userid of the session to be exempt from being terminated due to inactivity

Chapter 3
RADIUS Interface configuration

If you are using centralized user authentication, you must configure a RADIUS server. You can use the internal MDM RADIUS interface or an existing external RADIUS server to provide both authentication and authorization. If you are using the internal MDM RADIUS interface, you must also configure the local directory server.

If you are using an external RADIUS server, refer to "Configuring the MDM User Administrator server to use an External RADIUS server" (page 53).

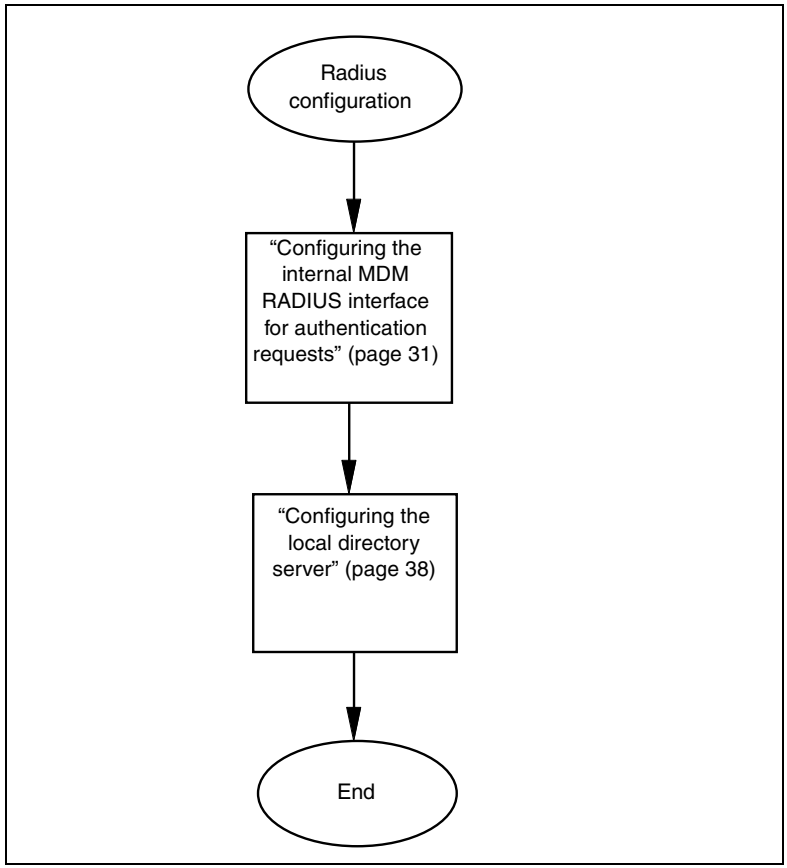
Navigation links

- "RADIUS interface configuration flow" (page 29)
- "Task navigation" (page 30)

RADIUS interface configuration flow

This taskflow shows you the sequence of procedures you perform to configure the internal MDM Radius Interface. To link to any procedure go to "Task navigation" (page 30).

Figure 6
RADIUS server configuration taskflow



Task navigation

- "Configuring the internal MDM RADIUS interface for authentication requests" (page 31)
- "Configuring the local directory server" (page 38)

Configuring the internal MDM RADIUS interface for authentication requests

There are three procedures you perform to configure the internal MDM RADIUS interface to accept authentication requests from NEs:

- "Configuring allowed and denied IP Addresses" (page 31)
- "Configuring shared secrets" (page 33)
- "Configuring network element properties" (page 35)

Prerequisites

- MDM must be installed with the Operator Client/Security option selected.
- Some local users should be configured on network elements.

Configuring allowed and denied IP Addresses

When a user attempts to login to a node, the IP address of the user is checked against two lists in the nas.properties configuration file to determine whether to allow or deny this user access.

The nas.properties configuration file contains two lists of specific IP addresses or subnets, separated by commas:

- The NAS-allowed list (radius.server.nas.allow) identifies IP addresses that are allowed access to the RADIUS server.
- The NAS-denied list (radius.server.nas.deny) identifies IP addresses that are denied access to the RADIUS server.

Procedure steps

1 Navigate to the following directory.

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

2 Backup the nas.properties file with another name (for example (nas.properties. orig) before making any changes to it.

3 If you are modifying an existing IP address, locate it in the file and change it as required.

If you are adding an allowed IP address, verify that it is not already in either the NAS-allowed or NAS-denied list, and then add the IP address to the line which reads “radius.server.nas.allow=”.

If you are adding a denied IP address, verify that it is not already in either the NAS-allowed or NAS-denied list, and then add the IP address to the line which reads “radius.server.nas.deny=”

4 Save the file in the same location with the same name.

5 Run the reloading script. For more information, refer to “Loading configuration files while the server is running” (page 36).

6 If the server **is not running**, start the server. The new properties will take effect after startup. For more information, refer to “Restarting the RADIUS server” (page 37).

7 Test the access modification by checking the log messages in the log file (/opt/nortel/logs/applications/security/radius), and sending requests to the server from the new IP addresses.

Procedure job aid

In addition to the rules listed in the nas.properties file, the following rules apply when you update the nas.properties file:

- Any line starting with a # or ! is ignored.
- Within each list, the first match is used.
- The same IP address must not appear in both lists, otherwise the IP address in the denied list has precedence.
- An empty file or a file containing only lines starting with semicolons are accepted. However, both lists are considered empty.
- To indicate a subnet, add a “/” and the number of significant bits for the subnet. For example 47.135.180.237/24. In this example, the first 24 bits of the address are relevant; the others are ignored. This means that addresses 47.135.180.0 through 47.135.180.255 match.
- There should be, at most, one line for “radius.server.nas.allow=”. If there is more than one line for the NAS-allowed list, the last allowed list line is used for the NAS-allowed list.
- There should be, at most, one line for “radius.server.nas.deny=”. If there is more than one line for the NAS-denied list, the last denied list line is used for the NAS-denied list.

Configuring shared secrets

For network security, transactions between the client and RADIUS server are authenticated through the use of a shared secret. The shared secret consists of text that both the server and client use and is equivalent to a password.

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 password is encrypted using shared secret as a part of the key. If the secret is not matched, the password will be incorrect and the authentication will fail.

Procedure steps

1. Using a new terminal display, navigate to the following directory.

   ```
   /opt/nortel/applications/security/current_radius/
   swmgmt/bin
   ```

2. Enter the following command.

   `./encrypt_secret.sh`

   You are prompted for the shared secret to be encrypted.

3. Enter the shared secret.

   The script outputs a generated string which is the encrypted and encoded shared secret.

   The system displays a message “Would you like to encrypt another secret?”.

4. If you require additional shared secrets, enter **Y(es)** each time you are prompted. If you do not require additional shared secrets, enter **N(o)**.

   The script outputs shared secrets until you enter **N(o)**.

5. Navigate to the following directory.

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

6. Backup the radius_secret.properties file with another name (for example radius_secret.properties.orig) before making any changes to it.

7. Open the file “radius_secret.properties” using a text editor.

8. On a new line, add the IP address of the client and it’s shared encrypted secret. For example 47.128.185.78 = QH3lkAjKJj0=.

Note: Perform the procedure "Configuring the RADIUS component on the Passport" (page 43) at the same time so that you can enter the shared secret in both locations and avoid errors.

9 Save the file in the same location with the same name.

10 Run the reloading script. For more information, refer to "Loading configuration files while the server is running" (page 36).

11 If the server **is not running**, start the server. the new properties will take effect after startup. For more information, refer to "Restarting the RADIUS server" (page 37).

12 Test the access modification by checking the log messages in the log file (/opt/nortel/logs/applications/security/radius), and sending requests to the server from the new IP addresses.

Procedure job aid

In addition to the rules listed in the radius_secret.properties file, the following rules apply when editing the radius_secret.properties file:

- the secret must not be empty
- the secret must be at least as large and unguessable as a well-chosen password. It is recommended that the secret is at least 16 characters.
- Any line starting with a # or ! will be ignored (comment line).
- It is recommended that you use a different shared secret for each RADIUS client.
- Shared secret must be one word.
- An IP address must appear only once in the file. If the same IP address appears more than once, the first match is used.

Configuring network element properties

The ne.properties configuration file is used to map a specific IP address or subnet to a network element identifier. The ne.properties file contains a mapping of IP addresses to a specific network element ID, which identifies a network element as a Passport or another type of network element.

Procedure steps

1. Navigate to the following directory.

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

2. Backup the ne.properties file with another name (for example ne.properties.orig) before making any changes to it.
3. Open the “ne.properties” file using a text editor.
4. On a new line, enter an IP address or subnet and the network element identifier (NEID). For example, 47.128.185.78 = Passport.
5. Save the file in the same location with the same name.
6. Run the reloading script. For more information, refer to “Loading configuration files while the server is running” (page 36).
7. If the server **is not running**, start the server. the new properties will take effect after startup. For more information, refer to “Restarting the RADIUS server” (page 37).

Procedure job aid

In addition to the rules listed in the ne.properties file, the following rules apply when modifying the ne.properties file:

- the NEID must be one word, containing no white spaces and no =, : characters. It is matched against the NEID list contained in the configuration file, ne_policy.properties.
- one NEID currently exists: Passport.
- The list can contain both individual IP addresses and subnets.
- The first match of the IP address in the configuration file is used. For example, if there is a previous record in the file matching the newly added IP address or subnet, and this record is not removed or modified, the old settings are used and the new addition does not take effect.

Loading configuration files while the server is running

If you make configuration changes without stopping the server, you can load the nas.properties and radius_secret.properties configuration files while the server is running.

Procedure steps

1. Navigate to the following directory:

   ```
   /opt/nortel/applications/security/current_radius/
   swmgmt/bin
   ```

2. Enter the following command to reload these two files.

   ```
   ./configure_radius.sh -reload
   ```

   If there is no server process running, a message "*The RADIUS Server is not running*" is displayed on the terminal. The new properties take effect after the server is started.

Restarting the RADIUS server

When you restart the server the changes you made are automatically loaded. You must restart the server to load changes to the ne.properties configuration file.

Procedure steps

1 Navigate to the following directory:

```
/opt/nortel/applications/security/current_radius/bin
```

2 Enter the following commands to reload these two files.

```
./configure_radius.sh stop

./configure_radius.sh -inittab
```

The server process will start in the background. If there is an existing RADIUS Server running, the message "*The RADIUS Server already started*" is displayed, and the server is not started.

Configuring the local directory server

If you do not plan to authenticate users via external RADIUS server(s), configure the local directory server so your local users can authenticate on the local directory server.

Procedure steps

1. Navigate to the following directory:

   ```
   /opt/nortel/applications/security/current_core/
   swmgmt/bin
   ```

2. Enter the following command:

   ```
   ./upgrade_seccore.sh -c scheme
   ```

   The system displays three Authentication Service Names.

3. Select **1** for **AuthConfigLDAP** to configure MDM to attempt user authentication only with the local directory server.

4. Restart the IS clients including MDM RADIUS server.

   To restart the Apache server, use the following command:

   ```
   /opt/nortel/3rd_party/apache/current_apache/bin/
   apachectl stop
   ```

   To restart the RADIUS interface, refer to “Restarting the RADIUS server” (page 37).

Chapter 4
Centralized authentication configuration

Configure Passport centralized authentication to enable the node to work with RADIUS for centralized user authentication. This configuration is necessary whether you have either an external RADIUS server or an internal RADIUS interface.

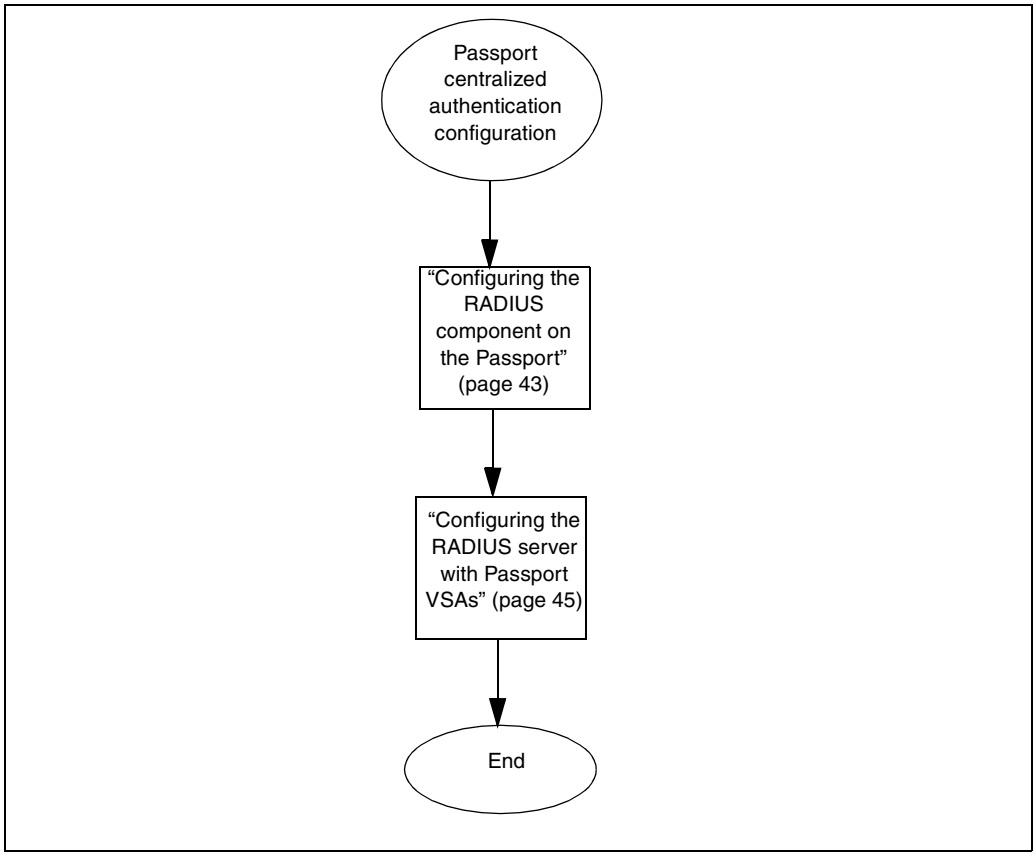
Navigation links

- "Centralized authentication configuration flow" (page 41)
- "Task navigation" (page 42)

Centralized authentication configuration flow

This taskflow shows you the sequence of procedures you perform to configure centralized authentication. To link to any procedure go to "Task navigation" (page 42).

Figure 8
Centralized authentication taskflow



Task navigation

- "Configuring the RADIUS component on the Passport" (page 43)
- "Configuring the RADIUS server with Passport VSAs" (page 45)

Configuring the RADIUS component on the Passport

Configure the Passport node for RADIUS as part of implementing RADIUS authentication between your network management system and the node.

Prerequisites

- If IP security (IPSec) is enabled, you must provision security policies to allow RADIUS traffic to be forwarded correctly. If component *Vr Ip Spd* exists, IPSec is enabled. See NN10600-607 *Passport - MDM Network Security: Secure Communications Configuration* for more information on IP Security.
- IP connectivity must configured on the node. To configure IP on the VR, see OAM Ethernet port configuration in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*. To configure ipiFr and ipiVc, see Connecting Passport to the network manually in NN10600-271 *Nortel Networks Multiservice Switch 7400/15000/20000 Network Management Connectivity*
- For security reasons, it is recommended that you use a local session, particularly when provisioning the shared secret. When you are not using a local session, the information you enter travels over the network in easy-to-read ASCII format.
- The oamRadius feature must be provisioned in the featurelist of the FP that is providing management access (for example `set sw lpt/cp fl oamradius`).

Procedure steps

1. Add a primary RADIUS server.

   ```
   add -s Ac Radius Server/0
   ```

2. Specify the IP address that the node uses to communicate with the RADIUS server.

   ```
   set Ac Radius nasIdentifier <nas_ip_addr>
   ```

3. Set the attributes for the primary RADIUS server.

   ```
   set Ac Radius Server/0 sharedSecret <prm_ss>

   set Ac Radius Server/0 serverPortNumber <port_nbr>

   set Ac Radius Server/0 serverIpAddress <prm_ip_addr>
   ```

```
set Ac Radius Server/0 ipStack <ip_stk>
```

Note: Perform the procedure “Configuring shared secrets” (page 33) at the same time so that you can enter the shared secret in both locations and avoid errors.

4 Activate this provisioning. For more information, refer to NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*.

5 If required, configure another RADIUS server as a backup.

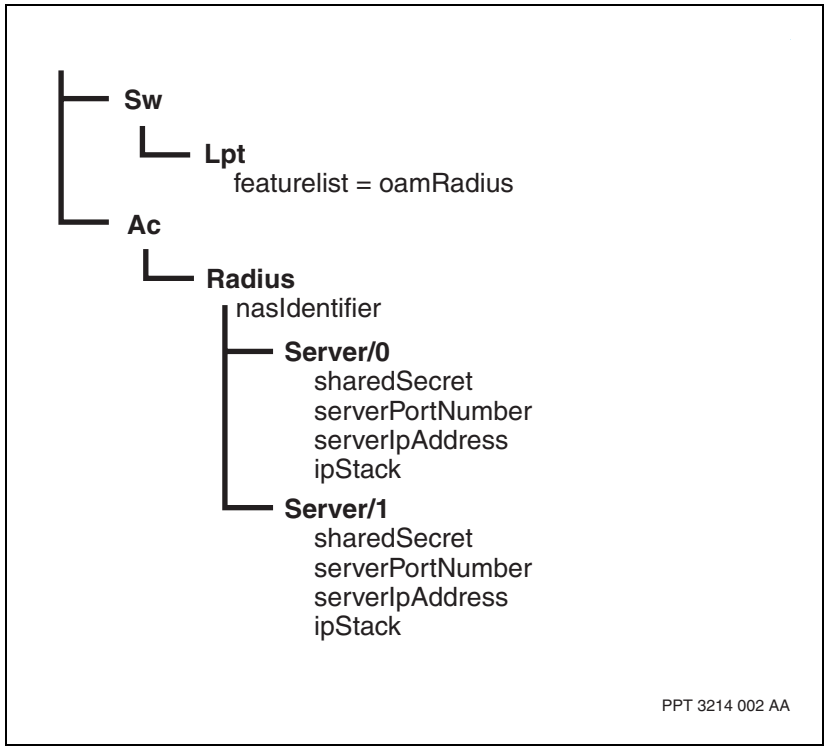
```
add -s Ac Radius Server/1 sharedSecret <bkup_ss>,
serverPortNumber <port_nbr>, serverIpAddress
<bkup_ip_addr>, ipStack <ip_stk>
```

Variable definitions

Variable	Value
<bkup_ip_addr>	The IP address of the backup RADIUS server.
<bkup_ss>	The shared secret of the backup RADIUS server.
<ip_stk>	The Vrip or ipiFripiVc depending on the connection between Passport and RADIUS. If a backup RADIUS server has been provisioned, the ip_stk value must be the same for both servers.
<nas_ip_addr>	If the connection for Passport to RADIUS uses oamEnet, this is the IP address of the management VR. If the connection from the node to RADIUS uses ipiFr or ipiVc, this is the ipiFr or ipiVc address respectively.
<port_nbr>	The UDP port the node is using to send requests to the RADIUS server.
<prm_ip_addr>	The IP address of the primary RADIUS server.
<prm_ss>	The shared secret of the primary RADIUS server.
<user_id>	The locally-defined userID.

Procedure job aid

Figure 9
Node for RADIUS component hierarchy



Configuring the RADIUS server with Passport VSAs

If your system uses an external RADIUS server, you must configure the RADIUS server to use the Passport vendor-specific attributes (VSAs) so that Passports can use the RADIUS server for authentication. The VSAs specify authorization data that must be returned from the RADIUS server to the Passport in a RADIUS Access-Accept PDU. The VSAs are stored in dictionary files.

There are a number of files that are shipped with Passport that identify the Network Element as a Passport to the RADIUS server you are using for authentication. These files are stored in the mgmt/radius directory. Specific

files must be modified so that the Network Element can be recognized by your specific RADIUS. Consult your RADIUS documentation for the modification procedures.

For details on the Passport VSA attributes, refer to “Passport RADIUS Vendor Specific Attribute Definitions” (page 47).

Passport RADIUS Vendor Specific Attribute Definitions

```
OPTION bundle-vendor-specific-attributes=yes

MACRO Nortel-VSA(t,s) 26 [vid=562 type1=%t% len1=+2 data=%s%]
ATTRIBUTEPassport-Command-Scope Nortel-VSA(200,integer)
VALUE Passport-Command-Scopenetwork              1
VALUE Passport-Command-Scopedevice               2
VALUE Passport-Command-Scopeapplication          3

ATTRIBUTEPassport-Command-ImpactNortel-VSA(201,integer)
VALUE Passport-Command-Impactdebug               3
VALUE Passport-Command-ImpactsystemAdministration4
VALUE Passport-Command-Impactconfiguration5
VALUE Passport-Command-Impactservice6
VALUE Passport-Command-Impactpassive7

ATTRIBUTE Passport-Customer-IdentifierNortel-VSA(202,integer)

ATTRIBUTEPassport-Allowed-AccessNortel-VSA(203,integer)**
VALUE Passport-Allowed-Accesslocal0
VALUE Passport-Allowed-Accesstelnet1
VALUE Passport-Allowed-Accessfmip2
VALUE Passport-Allowed-Accessftp3

ATTRIBUTEPassport-AllowedOut-AccessNortel-VSA(204,integer)
VALUE Passport-AllowedOut-Accesstelnet0
VALUE Passport-AllowedOut-Access none1

ATTRIBUTEPassport-Login-DirectoryNortel-VSA(205,stringnz)

ATTRIBUTEPassport-Timeout-ProtocolNortel-VSA(206,integer)
VALUE Passport-Timeout-Protocoldisabled0
VALUE Passport-Timeout-Protocolenabled 1

ATTRIBUTE Passport-RoleNortel-VSA(207,stringnz)
```

** all attributes are single-value return variables with the exception of Passport-Allowed-Access which can be a multi-valued return variable.

Chapter 5
Configuring the User Administration system

Configure the User Administration system for centralized authentication using the procedures in this section.

Navigation links

- "User Administration system configuration flow" (page 49)
- "Task navigation" (page 51)

User Administration system configuration flow

This taskflow shows you the sequence of procedures you perform to configure the system administrator security settings for the User Administration system. To link to any procedure go to "Task navigation" (page 51).

Figure 10
User Administration system configuration task flow (sheet 1 of 2)

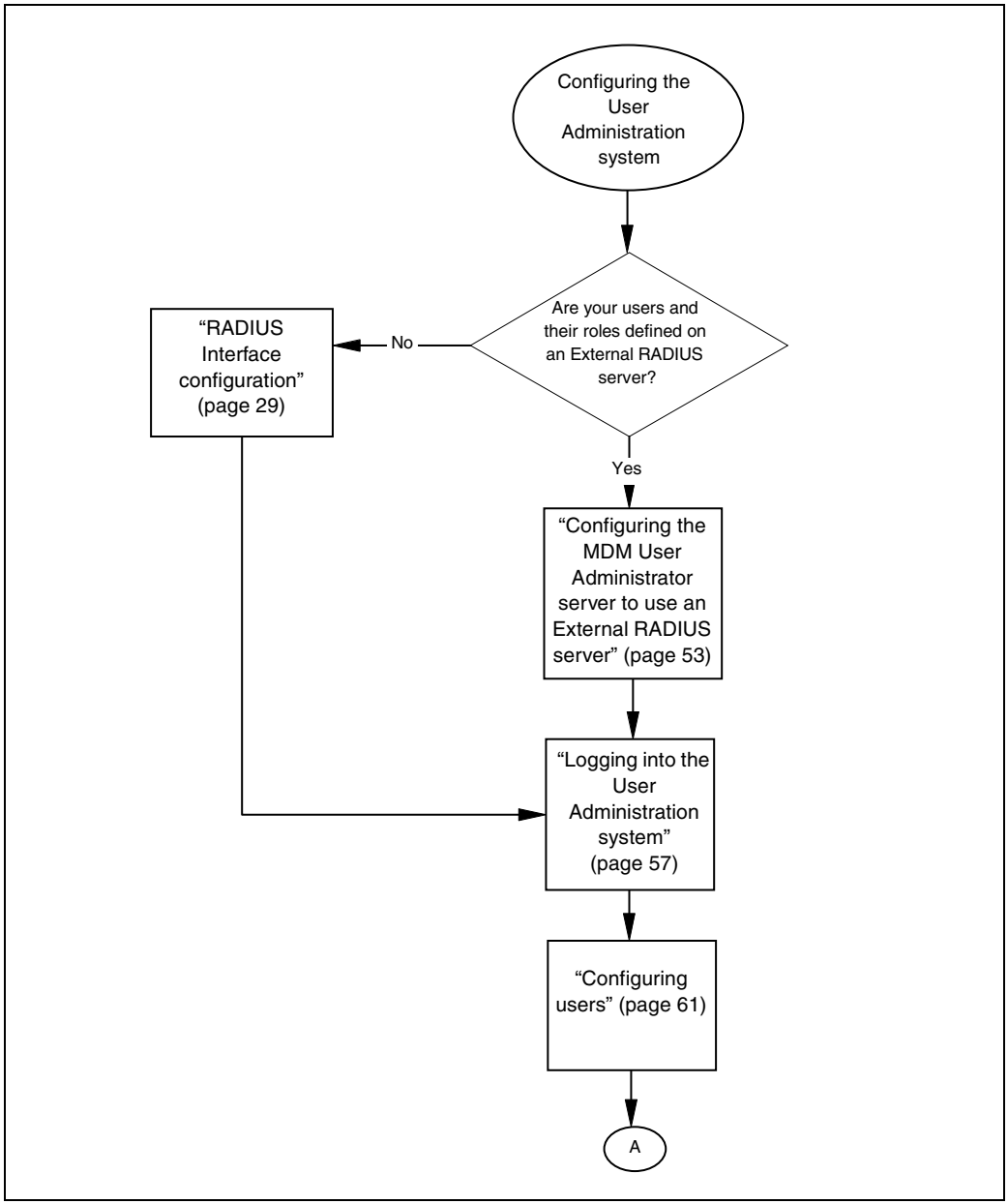
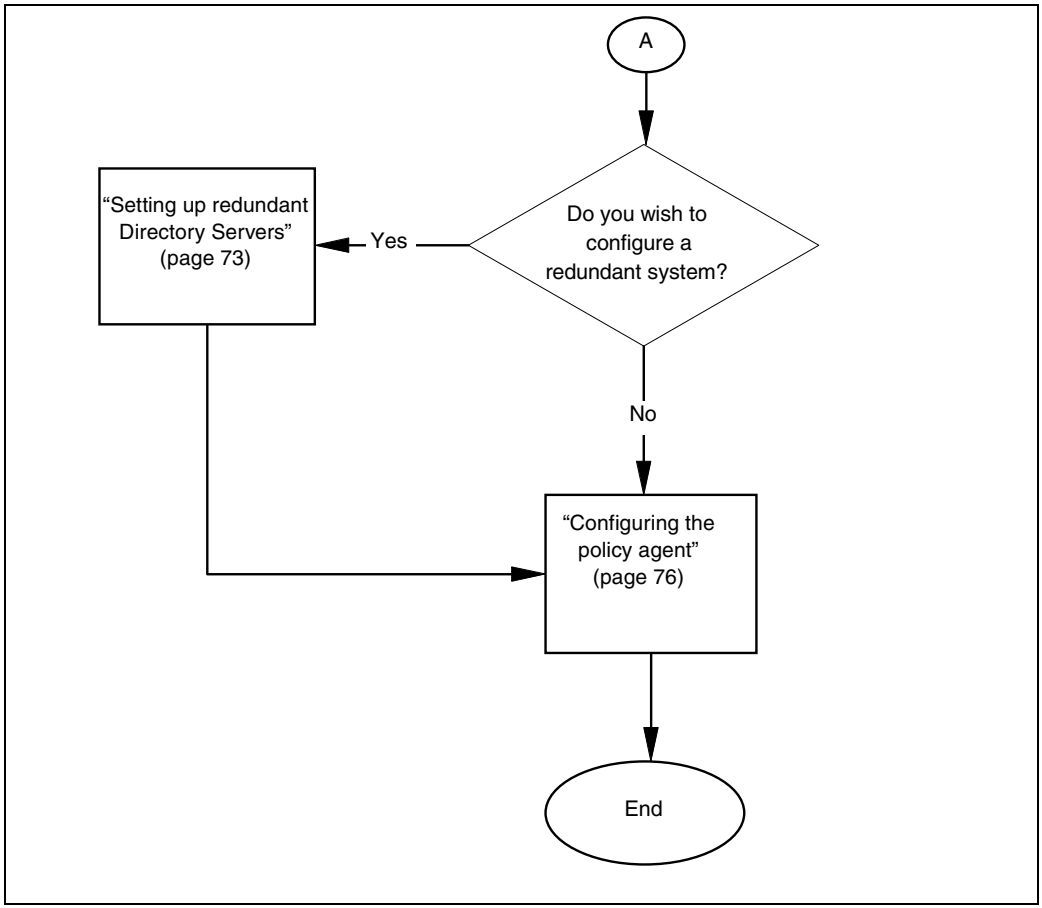


Figure 11
User Administration system configuration task flow (sheet 2of 2)



Task navigation

- "Configuring the MDM User Administrator server to use an External RADIUS server" (page 53)
- "Migration of user identities to an external repository" (page 55)
- "Migration of user identities from an external repository" (page 56)
- "Logging into the User Administration system" (page 57)
- "Configuring users" (page 61)

- “Setting up redundant Directory Servers” (page 73)
- “Configuring the policy agent” (page 76)

Configuring the MDM User Administrator server to use an External RADIUS server

A script must be run if you wish to use the external RADIUS server to authenticate user requests for Operator Client users via the Sun ONE IS and NE users (Passport, MPE) via the RADIUS interface.

Note: If you are using the internal MDM RADIUS interface to authenticate user requests, refer to "RADIUS Interface configuration" (page 29).

Procedure steps

1. Navigate to the following directory:

   `/opt/nortel/applications/security/current_core/swmgmt/bin`

2. Enter the following command:

   `./upgrade_seccore.sh -c radius`

   The system displays a series of prompts.

   Note: Refer to "Radius script prompts" (page 54) for a description of the available options in this script.

3. Enter the following command:

   `./upgrade_seccore.sh -c scheme`

4. Select **2** for **AuthConfigRadius** to configure MDM to attempt user authentication with the external RADIUS server

   OR

   Select **3** for **AuthConfigRadiusPlusLDAP** to configure MDM to attempt user authentication with the external RADIUS server first and then, if an access-reject RADIUS response is received, attempt user authentication with the local directory server

5. Restart **all** the IS clients.

   To restart the Apache server, use the following command:

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

To restart the RADIUS interface, refer to “Restarting the RADIUS server” (page 37).

Procedure job aid

Table 2
Radius script prompts

Option	Description
RADIUS server 1 (IP Address)	IP address of an external RADIUS server. Enter “0” if you are not using it. The default value is 127.0.0.1.
RADIUS Server 1 Shared Secret	Secret used by MDM and the external RADIUS server.
RADIUS Server 1 Port	The port the node is using to send requests to the RADIUS.
RADIUS server 2 (IP Address)	IP address of an external RADIUS server. Enter “0” if you are not using it. The default value is 127.0.0.1.
RADIUS Server 2 Shared Secret	Secret used by MDM and the external RADIUS server.
RADIUS Server 2 Port	The port the node is using to send requests to the RADIUS.
RADIUS server port	Port number used on the configured external RADIUS server(s).
Timeout (seconds)	Time to wait, in seconds, for a response from an external RADIUS server.
Number of Retries	Number of retries for an external RADIUS server if it does not respond.
Vendor ID for the Role Attribute	Vendor identifier that the external RADIUS server uses for the role VSA(s) returned in an access accept response message. The default value is 562 (the vendor ID for Nortel).
Vendor Specific Attribute ID for Role	Type identifier for the role VSA(s) returned by the external RADIUS server(s).
NAS Identifier	The Passport attribute that identifies the RADIUS server to use.
NAS IP Address (IP address)	Identifies the IP address of the NE that uses the RADIUS server.

Migration of user identities to an external repository

If you currently define user identities in the MDM LDAP directory and you migrate your system to use an external repository to define user identities, you must use the User Manager tool to delete the users currently stored in the MDM LDAP directory. For more information, contact your Nortel representative.

Note: You may also have to reconfigure your Passport NEs to point to the new RADIUS server(s).

Migration of user identities from an external repository

If your user identities are defined an external repository and you migrate your system to use the MDM LDAP directory, you must also migrate the user identities. For more information, contact your Nortel Networks representative.

Logging into the User Administration system

The User Administration system consists of four applications that are accessed from the Preside Multiservice Data Manager Toolset. Access to these applications is provided by a set of default administration user IDs.

Procedure steps

1. From the Toolset, select **System->Security->User Manager**.
2. Select the appropriate security application for the task you wish to perform.
3. Enter the appropriate userID and password. For more information, refer to “Default administrator userIDs for User Administration system” (page 58).
4. Select **Accept** to accept the conditions of use.

Procedure job aid

There are a number of administrator user accounts that are predefined for you. You must use the correct procedure to change these passwords. The only password that does not expire is the cn=directory manager userid password.

Table 3
Default administrator userIDs for User Administration system

system	UserID	Use	Password	Procedure to change password
User Administration	administrator	The default security administrator account for managing users and policies.	adminpass	"Changing centrally authenticated passwords" (page 68)
Sun ONE IS	amadmin	Superuser for the Sun ONE IS. Used to handle administration and configuration requests. For example policy registration, bulk operations, replication configuration and SSL configuration.	s1isamadmin	"Changing system account passwords" (page 63)
Sun ONE IS	admin	Account for the S1IS admin server. Allows administration of the server through a web GUI.	s1isadmin	"Changing the Sun ONE IS Web Server admin account" (page 69)

Table 3
Default administrator userIDs for User Administration system

system	UserID	Use	Password	Procedure to change password
Sun ONE IS	amldapuser	Used to bind and search the directory for LDAP and Membership authentication modules. Also used for policy configuration.	s1isadmin	"Changing the password for amldapuser" (page 70)
Sun ONE IS	dsameuser	Used for binding purposes when the IS server SDK performs operations on the DS that are not linked to a particular user (for example, retrieving service configuration information)	s1isamadmin	"Changing the password for dsameuser" (page 71)
Sun ONE IS	puser	Proxy user. Can take on any user's privileges. Used for all queries made to the DS by the IS.	s1isamadmin	"Changing the password for puser" (page 71)
Sun ONE IS	urlaccessagent	User for the Application Authentication module.	s1isadmin	"Changing the password for the amService-UrlAccessAgent account" (page 71)

Table 3
Default administrator userIDs for User Administration system

system	UserID	Use	Password	Procedure to change password
Sun ONE DS	ndsadmin	administration account (not all the privileges of the directory manager account). Used in the installation of trusted certificates for SSL.	s1ndsadmin	"Changing system account passwords" (page 63)
Sun ONE DS	cn=directory manager	privileged database administrator (comparable to the root user in UNIX)	directory	"Changing Sun ONE Directory Manager password" (page 66)
Replication Manager	cn=Replication Manager, cn=config	Used by replication mechanism to communicate between two LDAP servers	replicaman	"Changing system account passwords" (page 63)

Configuring users

Perform the following tasks to set up userids for your system:

- "Viewing system account userids" (page 61)
- "Changing system account passwords" (page 63)
- "Changing Sun ONE Directory Manager password" (page 66)
- "Setting validation period for system account password" (page 66)
- "Setting validation period of user account password" (page 67)
- "Setting up a cron job to check for password expiry" (page 68)
- "Changing centrally authenticated passwords" (page 68)
- "Changing a user password in the Sun ONE IS console" (page 69)

Viewing system account userids

User IDs are displayed in the User Manager application. The permissions associated with user IDs are displayed in the Policy Manager application.

Procedure steps

1. Login to the User Manager application.

   For more information, refer to "Logging into the User Administration system" (page 57).

2. Select the **Users** tab.
3. Select a user from the list.

   If this user is associated with a role, it is displayed in the Roles pane.

4. Click **Edit** to view the user's name, phone number and email address.
5. Open the Policy Manager application.
6. Select a policy.
7. Click the **Subjects** tab.
8. In the drop-down list, select **Users** and search for the username.
9. Continue to search through the policies until you find the user.
10. When you find the policy that the user or one of it's role is associated with, select the policy in the Policies pane.
11. Click the **Rules** tab.

12 Select the rule and click **Edit**.

The permissions are displayed in the right hand pane.

Changing system account passwords

Administrators are required to change the passwords on system accounts. A command line password change utility is provided for this purpose.

Procedure steps

1 Navigate to the following location:

```
/opt/nortel/applications/security/current_isclient/
bin
```

2 Enter the following command:

```
./is_passwd [-server] [-local] [-nds_passwd |
-is_passwd | -replica_passwd] [-exp days] [read |
write] [pass_file]
```

Note: You must run this script once on the machine where the Sun One IS is located and for each user account.

Refer to “System account password script options” (page 63) and “System account password script operands” (page 64) for a description of the available options and operands in this script.

3 Refer to “Exit codes for system account script” (page 64) to verify that the script was successful.

Procedure job aid

Table 4
System account password script options

Option	Description
-server	Changes the password only in the server repository and does not write a local password file. If this option is used, the password_file operand is ignored.
-local	Changes the password only in the local password file and not in the server repository. If this option is used, you cannot define a password expiry period; for example, the -exp will be ignored even if specified.
-nds_passwd	Creates a password file for the Directory Server administrator. Uses the environment variable to obtain the credentials of the Directory Server administrator or to change the password of the Directory Server administrator.

Table 4
System account password script options

Option	Description
-is_passwd	Creates a password file for the Identity Server administrator. Reads or changes the credentials of the IS administrator using the environment variable for the credentials file path.
-replica_passwd	Reads or changes the credentials of the Replication Manager, which counts what will be used by the replication process.
-exp days	Sets the number of days before the password will expire. A value of zero sets the expiration date as indefinite. If this option is specified, the user is prompted for the LDAP administrator user name and password.

Table 5
System account password script operands

Operand	Description
read	Reads the credentials from the local file.
write	Writes the credentials to the local file or/and sets the new user's password to the Directory server.
pass_file	The filename of the file to write the new credential information to. This operand is ignored if the -server option is specified.

Table 6
Exit codes for system account script

Option	Description
0	Command executed successfully
1	Invalid parameters passed in
2	Password change in IS repository failed.
3	Setting of the password expiration date failed
4	Failed to save the server credentials to a local file.

Table 6
Exit codes for system account script

Option	Description
5	Failed to read the credentials from the file
6	Unexpected exception.

Changing Sun ONE Directory Manager password

The Sun ONE Directory Manager password does not expire and should be changed regularly to maintain system security.

Procedure steps

1. Login as root.
2. Set DISPLAY environment variable.
3. Start the Sun ONE DS console.

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

4. Login using the directory manager account (cn=directorymanager).
5. In the left panel, expand <host_name>.<domain_name>.
6. Expand “Server Group”.
7. Click on “Directory Server”.
8. From the right panel, click on **Open**.
9. Click on **Configuration** tab.
10. From the right panel, click on **Manager** tab.
11. Enter the new password value in **New password** and **Confirm password** fields.
12. Click **Save**.

Setting validation period for system account password

Specify the number of days before the system account passwords expire. If no value is specified, the system account password will not expire.

Procedure steps

1. Navigate to the following location:

   ```
   /opt/nortel/applications/security/current_isclient/
   bin
   ```

2. Enter the following command:

   ```
   ./is_passwd -exp <number_of_days>
   ```

   The system prompts you for the administrator username and password.

3. Enter the Directory Server administrator name and password.

For more information, refer to "Logging into the User Administration system" (page 57).

4 Refer to "Exit codes for system account script" (page 64) to verify that the script was successful.

Any change that you make to the validation period, takes effect only for users created from this time forward. Existing settings do not change.

Setting validation period of user account password

The validation period for individual users is set using the Security Settings interface. For information on setting a system wide validation period, refer to "Setting validation period for system account password" (page 66).

Procedure steps

1 Log into the Security Settings application.

For more information, refer to "Logging into the User Administration system" (page 57).

2 Select the **User Password** tab.

3 In the **Validity Period** field, set the number of days after which the user password will expire.

4 Click **Save**.

Configuring the Mail server and port

Configure the Mail server and port for the system users.

Procedure steps

1 Navigate to the following directory:

```
/opt/nortel/applications/security/current_core/
swmgmt/bin
```

2 Type the following command:

```
upgrade_seccore.sh -c smtp
```

3 Enter the following information in the prompts that are displayed:

- Mail Server Hostname: [**wcars1hy.ca.nortel.com**]
- Mail Server Port Number: [**25**]

Setting up a cron job to check for password expiry

This script is run daily to check for expiring passwords and to send an email to notify users. If you have enforced password expiry in the Security Settings window, set up this cron job.

Procedure steps

1 Navigate to the following directory:

```
/opt/nortel/config/applications/security/core/auth
```

2 Open the following file:

```
AMConfig.auth.java.properties
```

3 Verify that the following properties are set:

- com.iplanet.am.smtphost=<mail_server_host>
- com.sun.identity.sm.smptpport=<mail_server_port>

4 Enter the following command:

```
crontab -e
```

5 Add the following entry:

```
0 * * * *
/opt/nortel/applications/security/current_core/bin/
passwdExpirationNotification.sh 1>tmp/PWD.log 2>&1>
```

Changing centrally authenticated passwords

Users can use the MDM Operator Client interface to change centrally authenticated passwords.

Prerequisites

- access to the Security-User category of applications

Procedure steps

1 Login to the MDM Operator Client.

If your password has expired, the **Password Expiration** dialog displays.

2 If your password has expired, click **Change Password** otherwise, from the menu, click **Utilities->Security->Change Password**.

3 Enter your new password and confirm it.

4 Click **OK**.

Changing a user password in the Sun ONE IS console

Users who do not have access to the User Administration system or to the Change Password dialog in Operator Client, can change their passwords and their profile information through the Sun ONE IS console.

Procedure steps

1 On the machine where the Sun ONE Identity Server is located, launch the Web IS Console, and login with your user ID.

2 If SSL is **not** enabled, enter the following command:

```
http://<node_name>.<domain>.com:58080/amconsole
```

If SSL is enabled, enter the following command:

```
https://<node_name>.<domain>.com:<ssl_port>/amconsole
```

3 At the login screen, enter the user name and password, and click **Login**.

4 If you are an administrative user, click on the Identity Management tab, and from the **View** pull down menu, select **Users** to display the User Management window showing user profile information.

If you are a non-administrative user, the User Management screen is automatically displayed for you.

5 Enter the new password in the Password and Password (confirm) fields and click **Save**.

Changing the Sun ONE IS Web Server admin account

This account is used to install trusted certificates for SSL.

1 Login to the Sun ONE IS Web Server admin application.

```
http://<host_name>.<domain>.com:58888/
```

2 Select the **Preferences** tab.

3 Click on **Superuser Access Control** in the panel on the left.

4 Enter the new password in the **Authentication Password** field and confirm it.

5 Click **OK**.

6 Click **OK** in the dialog that appears.

7 If prompted to re-authenticate, use the new password you just entered.

Changing the password for amldapuser

Procedure steps

1. Launch the web IS console and login as user admadmin.

   If SSL is not enabled use the url
   http://<node_name.<domain>.com:58080/amconsole

   If SSL is enabled use the url
   http://<node_name.<domain>.com:<ssl_port>/amconsole

2. From the **View** pulldown menu, select **Services**.
3. Under **Authentication**, select **LDAP**.
4. Enter the new password in the **Password for Root User Bind** field and confirm it.
5. Click on **Save**.
6. Change the LDAP password using the IS console:
   a. Login to the server as root.
   b. Set the DISPLAY environment variable.
   c. Start the Sun ONE IS console.

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

   d. Login to the console using the directory manager account (cn=directory manager).
   e. From the left panel, expand **<host_name>.<domain_name>**.
   f. Expand **Server Group**.
   g. Click on **Directory Server**.
   h. From the right panel, expand **<org_name>.com**.
   i. Click on **DSAME Users**.
   j. From the right panel, double click on **amService-UrlAccessAgent**.
   k. Enter the new password in the **Password** field and confirm it.
   l. Click **OK**.
7. Restart the IS server and all the client applications.

Changing the password for dsameuser

Procedure steps

1. Login as root.
2. Run the following command and when prompted enter existing and new password information.

   ```
   /opt/nortel/3rd_party/security/current_s1is/bin/
   adpassword -admin
   ```

3. Restart the IS server and all client applications.

Changing the password for puser

Procedure steps

1. Login as root.
2. Run the following command and when prompted enter existing and new password information.

   ```
   /opt/nortel/3rd_party/security/current_s1is/bin/
   ampassword -proxy
   ```

3. Restart the IS server and all client applications.

Changing the password for the amService-UrlAccessAgent account

Procedure steps

1. Change the com.sun.am.policy.am.password property in /opt/nortel/config/applications/security/core/policy/AMConfig.policy.cpp.properties to the new password value.
2. Encrypt the password and set the password for the IS Policy Agent and C/C++ applications:
   a. Run /opt/nortel/3rd_party/security/current_s1is/capi/bin/crypt_util<new_password>

b. Copy the output from this command and paste it to the following files:

com.sun.am.policy.am.password property in the file /opt/nortel/config/3rd_party/security/s1is/es6/config/https<hostname>/AMAgent.properties

com.sun.am.policy.am.password property in the file /opt/nortel/config/3rd_party/security/s1is/capi/config/AMAgent.properties

com.nortel.mft.policy.am.password property in the file /opt/nortel/config/applications/security/core/policy/AMConfig.policy.cpp.properties

3 Encrypt the password and set the password for the IS Server and Java applications:

a. Run /opt/nortel/3rd_party/security/current_s1is/bin/ampassword --encrypt <new password>.

b. Copy the output from this command and past it to the following files:

com.iplanet.am.service.secret property in the file /opt/nortel/config/3rd_party/security/s1is/lib/AMConfig.properties

com.iplanet.am.service.secret property in the file /opt/nortel/config/3rd_party/security/core/policy/AMConfig.policy.java.properties

4 Restart the IS server and all the client applications.

Setting up redundant Directory Servers

The Redundant server script allows you to configure a primary and a secondary Directory Server for redundancy. It adds additional attributes to the existing schemas and sets up a master-to-master replication between two Directory Servers.

Note: Any existing data on the secondary Directory Server is lost when you set up redundancy. If required, save the existing information prior to setting up redundancy.

Prerequisites

- all upgrades and schema changes are applied to the Directory Server

Procedure steps

1. Navigate to the following location on the primary server machine:

   `/opt/nortel/applications/security/current_core/bin`

2. Enter the following command:

   `./config_s1is_replica.sh [-h] [-is_passwd] [-nds_passwd]`

3. Navigate to the following location on the secondary server machine:

   `/opt/nortel/applications/security/current_core/bin`

4. Enter the following command:

   `./config_s1is_replica.sh [-h] [-is_passwd] [-nds_passwd] -r`

   If the script runs successfully, the exit code 0 is displayed.

5. Refer to “Exit codes for Redundant server script” (page 74) to verify that the script was successful.

Procedure job aids

Table 7
Redundant server script option

Operand	Description
-is_passwd	The filename of the file containing the IS administrator user name and password. This file is created using the `-local` option of the `is_passwd` utility described in "Changing system account passwords" (page 63).
-nds_passwd	Use the environment variable to get the credentials of Directory Server administrator from the file.
-r	Re-start the IS server and Directory Server on local machine. Use this option for the secondary server only. Do not use this option for the primary server.
-h	Specifies the help menu.

Table 8
Redundant server script environment variables

Variable	Description
IS_AUTH_CONFIG_URL	Space delimited list of URLs in authentication configuration properties file.
IS_AMADMIN_PASSWD_FILE	The IS Administrator password file.
DIRMGR_PWD_FILE	The Directory Server administrator password file.

Table 9
Exit codes for Redundant server script

Exit code	Description
0	Command executed successfully.
1	Servers have not been set and configured properly.
2	IS initialization failed.

Table 9
Exit codes for Redundant server script (Continued)

Exit code	Description
3	Communication with IS server failed.
4	IS Administrator password was invalid.
5	Directory Server Administrator password was invalid.
6	Configuration failed.

Configuring the policy agent

The Apache Policy agent authenticates users before they can launch any applications through Java Web Start. This prevents users from downloading files and applications that they may not have the correct privileges to use. Use this procedure to secure the Apache Web server that is used to launch client applications using Java Web Start.

Procedure steps

1 Navigate to the following directory:

```
/opt/nortel/applications/security/current_isclient/
bin
```

2 Enter the following command:

```
./is_config_apacheagent.sh
```

Chapter 6
Basic security settings for User Administration system

Configure the basic security settings for all the users in the User Administration system for centralized authentication. You cannot configure security settings for users that are authenticated via an external RADIUS server. This authorization is handled by the external RADIUS server.

Prerequisites

- access to online documentation.

The majority of the tasks in this section are documented in the online help for User Administration system. In each procedure, you may be directed to the online help for additional information. To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

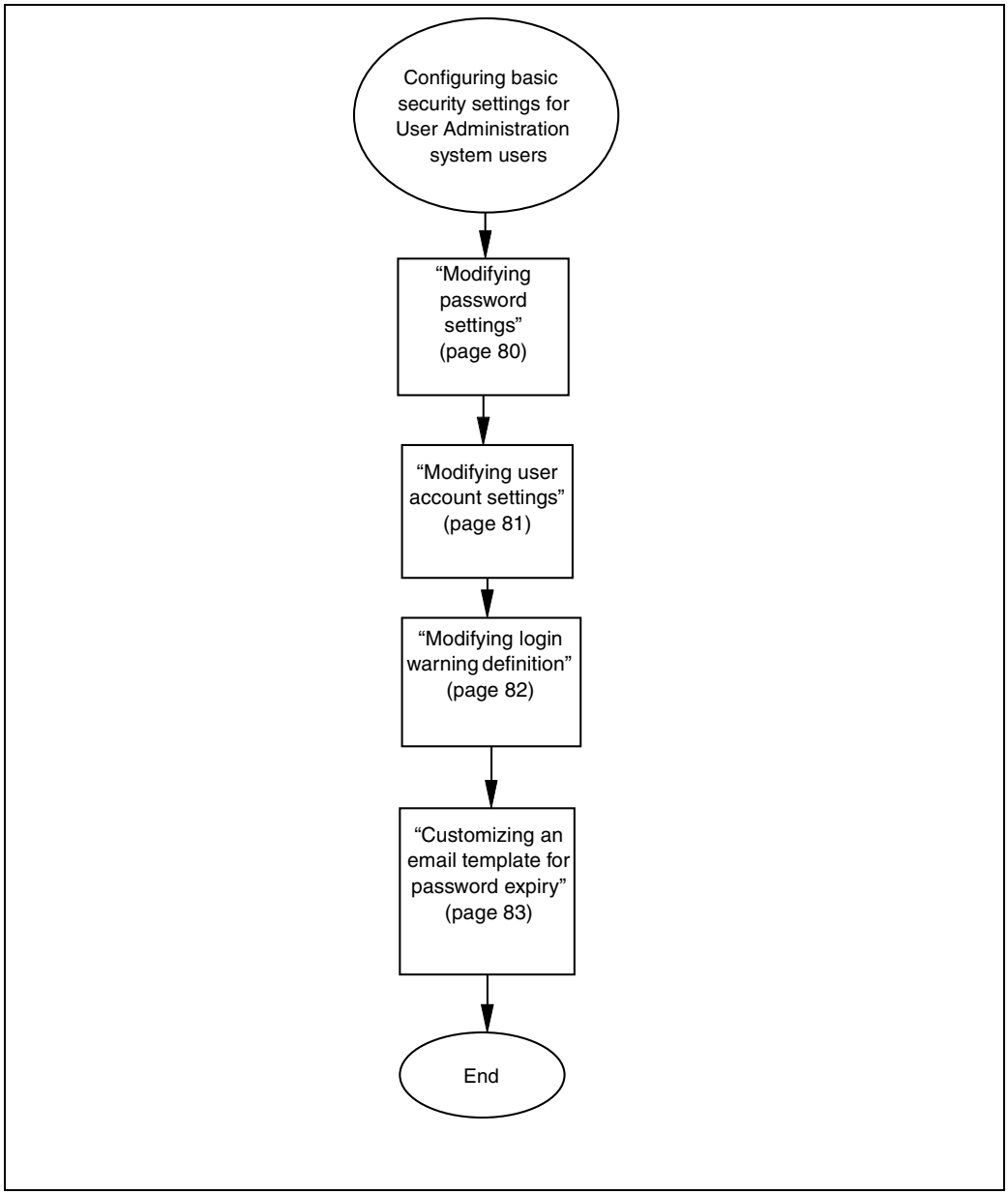
Navigation links

- "User Administration system authentication configuration flow" (page 77)
- "Configuring basic security settings taskflow" (page 78)

User Administration system authentication configuration flow

This taskflow shows you the sequence of tasks you perform to configure the basic security settings for all the users in the User Administration system. To link to any procedure go to "Task navigation" (page 79).

Figure 12
Configuring basic security settings taskflow



Task navigation

- "Modifying password settings" (page 80)
- "Modifying user account settings" (page 81)
- "Modifying login warning definition" (page 82)
- "Customizing an email template for password expiry" (page 83)

Modifying password settings

The basic password settings for all users, that are centrally defined, are configured with default values. Use the Security Settings application, in the User Administration system, to modify basic password settings.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. From the Toolset, select **System->Security->User Administration**.
2. Select the Security Settings application.

   For more information, refer to “Logging into the User Administration system” (page 57).
3. Modify the required password settings. For more information, refer to *Modifying password settings* in the online documentation.

   Note: At any time, you can revert to the default settings by clicking the **Reset to Defaults** button.

Modifying user account settings

The user account lockout settings for all centrally defined users are configured with default values. Use the Security Settings application, to modify the number of allowable invalid login attempts before a user is locked out and to modify the length of time the user is locked out.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the Security Settings application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Modify the user account lockout settings. For more information, refer to *Modifying user account settings* in the online documentation.

   Note: At any time, you can revert to the default settings by clicking the **Reset to Default** button.

Modifying login warning definition

The User Administration system is configured with a default login warning text that is displayed when users login. Use the Security Settings application, to modify this text to suit your requirements.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the Security Settings application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Modify the login warning text. For more information, refer to *Modifying login warning definition* in the online documentation.

   Note: At any time, you can revert to the default warning text by clicking the **Reset to Default** button.

Customizing an email template for password expiry

The User Administration system contains a default email template file (mail_template.dat). A script runs daily to scan this file and send email notifications to users whose passwords have expired. Use the Security Settings application, to customize the contents of this file and enable the password expiry notification.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Customize the email template for password expiry and enable the notification. For more information, refer to *Customizing an email template for password expiry* in the online documentation.

Chapter 7
User Administration system user configuration

Configure users for centralized authentication to set up user accounts and profiles on the User Administration system for centralized user authentication.

Prerequisites

- access to online documentation.

The majority of the tasks in this section are documented in the online help for User Administration system. In each procedure, you may be directed to the online help for additional information. To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Navigation links

- “User Administration system authentication configuration flow” (page 85)
- “Task navigation” (page 88)

User Administration system authentication configuration flow

This taskflow shows you the sequence of tasks you perform to configure users for centralized authentication. To link to any procedure go to “Task navigation” (page 88).

Figure 13
User Administration user configuration taskflow (sheet 1 of 2)

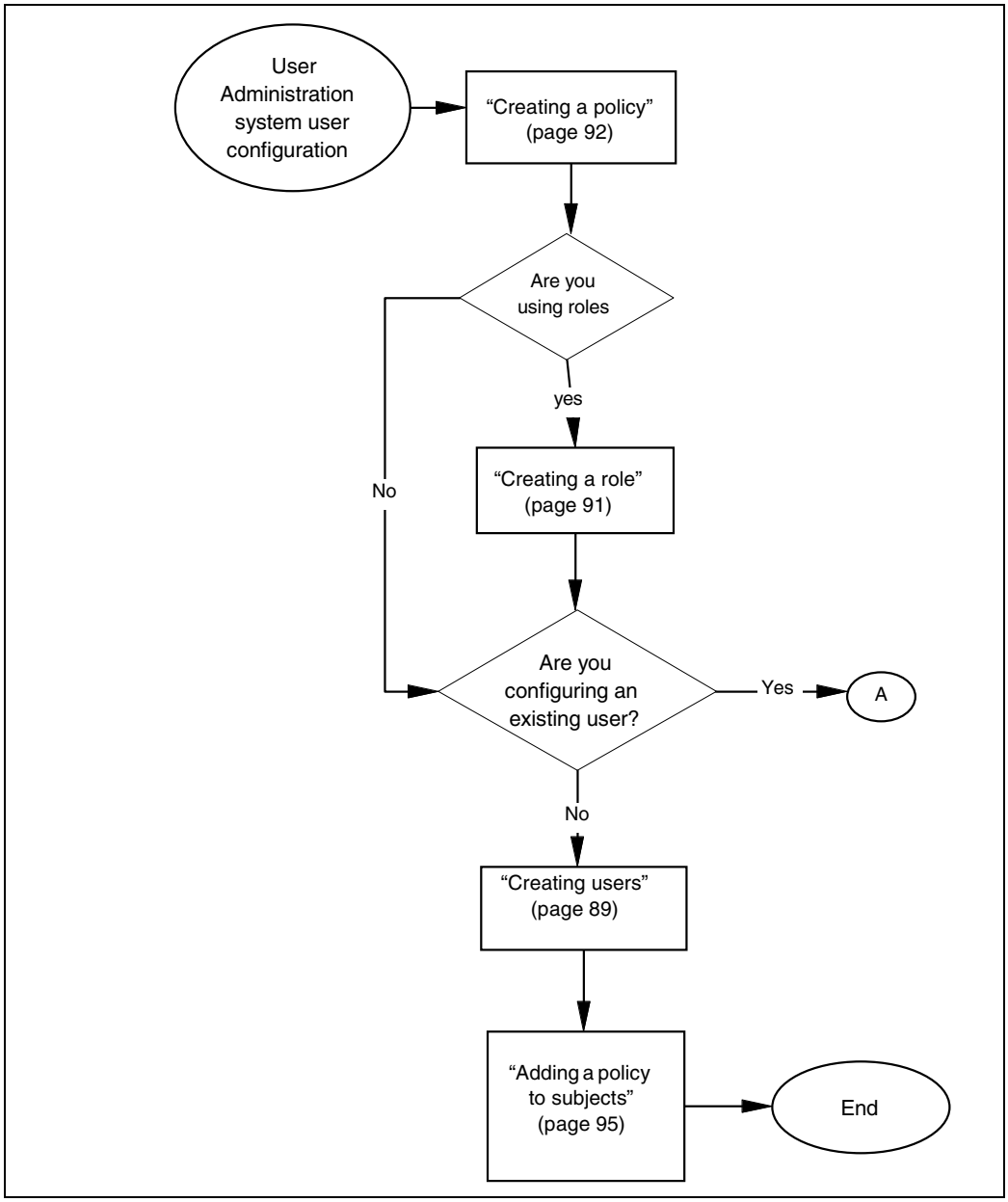
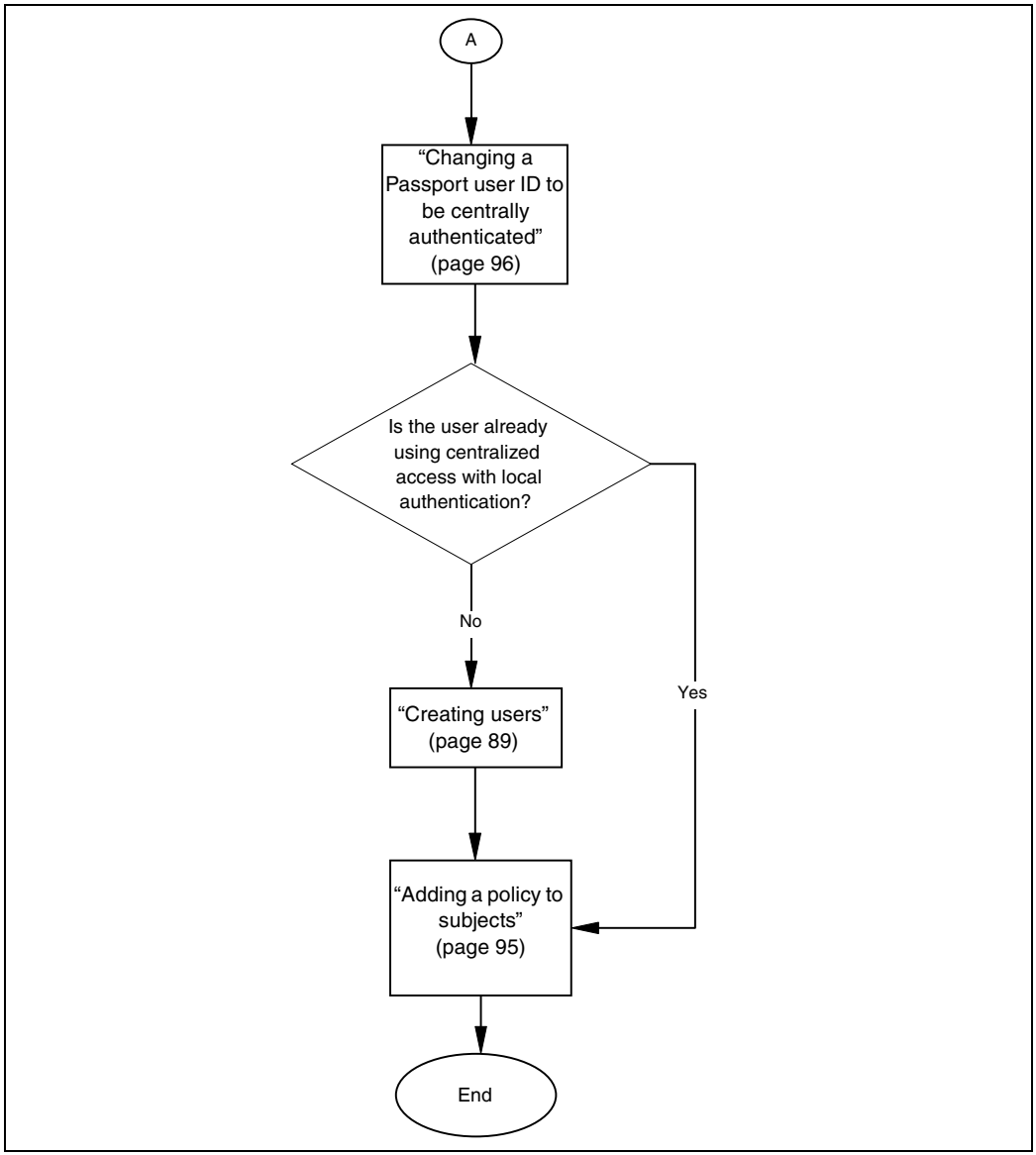


Figure 14
User Administration user configuration taskflow (sheet 2of 2)



Task navigation

- “Creating a policy” (page 92)
- “Creating a role” (page 91)
- “Creating users” (page 89)
- “Adding a policy to subjects” (page 95)
- “Changing a Passport user ID to be centrally authenticated” (page 96)

Creating users

You can create centrally authenticated users in two ways:

- "Creating a centrally authenticated user using the User Administration system" (page 89)
- "Changing an existing Passport user to be centrally authenticated and locally authorized" (page 90)

Creating a centrally authenticated user using the User Administration system

Use the User Manager application to create a user that is centrally authenticated.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.
- Users authenticated exclusively by the external RADIUS servers must not be associated with the Top-Level Admin role.

Procedure steps

1. Login to the User Manager application.

   For more information, refer to "Logging into the User Administration system" (page 57).

2. Create a user. For more information, refer to *Creating a User* in the online documentation.

3. Activate the user. For more information, refer to *Activating a User* in the online documentation.

   You can modify, deactivate or delete this user at any time. For more information, refer to *Modifying user information, Deactivating a user* and *Deleting a user* in the online documentation.

Changing an existing Passport user to be centrally authenticated and locally authorized

Use the Passport command line to create a user ID that has access defined by the RADIUS server.

Prerequisites

- You need to be logged in with a user ID with command impact of systemAdministration.
- For configuring additional user attributes refer to “Adding a new userId” (page 19).

Procedure steps

1 Enable remote authentication on the user ID.

```
set Ac userID/<user_id> remoteAuth enabled
```

Variable definitions

Variable	Value
<user_id>	A unique user ID.

Creating a role

Roles are used to group users that perform common tasks. Use the User Manager application to create roles in the User Administration system. For a more detailed description of roles, refer to NN10600-605 *Passport - MDM Network Security: Operations*.

Prerequisites

Before you can create a role, you require:

- role name: a name that is used for grouping users according to a function. For example, “Ottawa Fault”.
- role description: describes the function of the role. For example, “all users who perform fault management in Ottawa”.
- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the User Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Create a role. For more information, refer to *Creating a Role* in the online documentation.

   You can edit or delete this role at any time. For more information, refer to *Editing a role and Deleting a role* in the online documentation.

3. To simplify user administration, you can associate specific users with this role. For example, you can associate all the users who perform fault management in Ottawa, with the ”Ottawa Fault“ role. For more information, refer to *Associating one or more users with a role* in the online documentation.

   Note: If a user has been authenticated via an external RADIUS server, any locally assigned roles are lost.

Creating a policy

Create a policy by associating action permissions, and resources (Passport or Preside Multiservice Data Manager Operator Client).

Prerequisites

- verify which applications are launched from Operator Client
- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the Policy Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Create a policy. For more information, refer to *Creating a Policy* in the online documentation.

3. In the Policy Manager window, select the new policy.

4. Select the **Rules** tab and click **Add**.

5. In the Rule Name field, enter the name of the rule.

6. If you are using Operator Client, specify the applications to which the rule allows access from Operator Client:

   a. In Rule Definition for Resource type, use the drop-down arrow to select **Applications**.

   b. In the Resource Selection list, check one resource to include in the rule. This rule enables the launch of the applications that are included in this resource group.

      For a description of the applications included in each resource group, refer to “Application categories for authorization” (page 93).

   c. In the Action Selection list, select **Allow** or **Deny** from the drop-down menu opposite the Launch action.

   d. Click the **Save Rule** button.

7. If you are creating a rule to allow access to a Passport node, specify the actions permitted:

a. In Rule Definition for Resource type, select **Passport NE Access**.

b. In the Action Selection list, use the drop-down arrows to specify the permissions for each action. For a description of the permissions, refer to “Passport node Attributes” (page 94).

c. Click the **Save Rule** button.

8 Activate the policy to immediately apply it and its rules within the system. For more information, refer to *Saving (activating) a policy* in the online documentation.

You can modify or delete this policy and any of it’s rules at any time. For more information, refer to *Modifying a policy, Deleting a Policy, Modifying a policy rule* and *Deleting a policy rule* in the online documentation.

Procedure job aid

Table 10
Application categories for authorization

Categories	Applications
All resources	All of the applications listed
Security - User	Change Password
Performance	Data Viewer
Nodal Access - Passport	Passport Shelf View
Utilities	Service Selection, Log Viewer
Configuration - Admin	Passport Nodal Template Editor, MPE Nodal Template Editor
Configuration - MPE	MPE Nodal Provisioning
Configuration - Passport	Passport Nodal Provisioning
Utilities - CLI	Command Console, Telnet Access
Fault	Network Status, Alarm Display, Network Browser, Component Information Viewer

Table 11
Passport node Attributes

Attribute	Default value	Possible values
Customer Identifier	0	Range: 0 - 8191
Command Scope	application	network, device, application
Command Impact	passive	debug, systemAdministration, configuration, service, passive
Local Access	Allow	Allow, Deny
Telnet Access	Deny	Allow, Deny
FMIP Access	Deny	Allow, Deny
FTP Access	Deny	Allow, Deny
Telnet Out Access	Deny	Allow, Deny
Login Directory	/	1-128 ASCII printable characters
Timeout Protocol	enabled	disabled, enabled

Adding a policy to subjects

Once you have created a policy, you must associate it with subjects (users or roles) to specify the authorization permissions for these users or roles on specific nodes.

Prerequisites

- Users or roles created
- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the Policy Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Associate the policy with a user or role. For more information, refer to *Adding a Policy to Subjects: users or roles* in the online documentation.

   You can remove users or roles from a policy at any time. For more information, refer to *Removing users or roles from a policy* in the online documentation.

Changing a Passport user ID to be centrally authenticated

You can switch an existing user ID that has access defined locally on the Passport node to having access defined by the RADIUS server centrally authenticated.

Prerequisites

- the RADIUS server must be configured on the node where the existing user ID access is defined locally.
- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Create a centrally-defined user ID that is identical to the user ID that is defined locally on the node. For more information, refer to *Creating a User* in the online documentation.
2. Login to the appropriate application.

   For more information, refer to “Logging into the User Administration system” (page 57).
3. Associate the user with roles or policy such that the user ID’s current credentials on the node are duplicated. For more information, refer to *Associating a user with a role and Applying a policy to subjects: users or roles* in the online documentation.
4. Login to the User Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).
5. Activate the user. For more information, refer to *Activating a User* in the online documentation.
6. Delete the user ID from the node. For more information, refer to “Deleting a local Passport user” (page 112).

Chapter 8
User access administration

User access administration includes the procedures for managing remote and local user access.

Prerequisites

- access to online documentation.

The majority of the tasks in this section are documented in the online help for User Administration system. In each procedure, you may be directed to the online help for additional information. To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Navigation links

- "User access administration tasks" (page 97)

User access administration tasks

- "Backing up User Administration information" (page 99)
- "Changing a centrally defined user ID attributes" (page 108)
- "Changing Passport user ID attributes" (page 109)
- "Changing a local Passport user password" (page 110)
- "Deleting a centrally defined user" (page 111)
- "Deleting a local Passport user" (page 112)
- "Deleting a role" (page 113)

- "Denying a centrally defined user access to a node" (page 114)
- "Displaying the number of user sessions on a Passport node" (page 115)
- "Displaying the user IDs on a Passport network management interface" (page 117)
- "Displaying the users on the User Management system" (page 118)
- "Managing policies" (page 119)
- "Restricting access through a Passport network element interface" (page 120)
- "Releasing a locked Passport network management interface" (page 121)
- "Resetting a centrally defined user password" (page 122)
- "Starting the Sun ONE DS console" (page 123)
- "Terminating a centrally defined user's session" (page 124)
- "Terminating a user session on a Passport network management interface" (page 125)
- "Terminate all user sessions on a Passport network management interface" (page 126)
- "Sun ONE Identity Server system recovery" (page 127)

Backing up User Administration information

As part of your standard backup and restore process, perform the following backup procedures:

- "Backing up Sun ONE Directory Server" (page 99)
- "Restoring a non replicated Sun ONE Directory Server" (page 100)
- "Restoring one Sun ONE Directory Server in a replicated pair" (page 102)
- "Restoring both Sun ONE IS servers in a replicated pair" (page 105)
- "Backing up desktop user interface data" (page 107)
- "Restoring desktop user interface data" (page 107)

Backing up Sun ONE Directory Server

Backup up all the user, role, policy, identity server configuration, Sun ONE Directory Server configuration and security setting stored in the LDAP directory. In a replicated server deployment, you must backup both servers.

Procedure steps

1 Open the /etc/inittab file for editing

2 Stop the server processes:

a. In the /etc/inittab file, change the following process IDs from `respawn` to `off`.

- the NDS process IDs `nsdm` and `slpd`

- the identity server process IDs `sld1`, `sld2` and `sld3`

- the RADIUS server process ID `rad1`

b. Save and close the file.

c. Apply the changes by entering:

```
init q
```

3 Backup up all the security server configuration and data files by entering

```
tar cvf <backup_file_name>.tar \
/opt/nortel/config/applications/security \
/opt/nortel/config/3rd_party/netscape \
/opt/nortel/config/3rd_party/security \
```

```
/opt/nortel/data/applications/security \
/opt/nortel/data/3rd_party/netscape \
/opt/nortel/data/3rd_party/security \
/opt/nortel/logs/3rd_party/netscape \
/opt/nortel/logs/3rd_party/security \
/opt/nortel/logs/application/security \
```

4 Store the file in a safe location.

5 Start the managed processes:

   a. Open the /etc/inittab file for editing.

   b. In the /etc/inittab file, change the following process IDs from `off` to `respawn`.

   - the NDS process IDs `nsdm` and `slpd`

   - the identity server process IDs `sld1`, `sld2` and `sld3`

   - the RADIUS server process ID `rad1`

   c. Save and close the file.

   d. Apply the changes by entering:

   ```
   init q
   ```

Restoring a non replicated Sun ONE Directory Server

Restoring the Sun ONE Directory Server overwrites any existing database files. Any modifications you have made since the last backup are lost.

Procedure steps

1 Unistall and then reinstall the Sun ONE Directory server software. For more information, refer to 241-6001-100 *Preside MDM Installation*.

2 Stop the server processes:

   a. Open the /etc/inittab file for editing.

   b. In the /etc/inittab file, change the following process IDs from `respawn` to `off`.

   - the NDS process IDs `nsdm` and `slpd`

   - the identity server process IDs `sld1`, `sld2` and `sld3`

   - the RADIUS server process ID `rad1`

   c. Save and close the file.

d. Apply the changes by entering:

```
init q
```

3 Restore all configuration and data files to the directories by entering

```
tar xvf <backup_file_name>
```

4 Restart the server processes:

a. Open the /etc/inittab file for editing.

b. In the /etc/inittab file, change the following process IDs from `off` to `respawn`.

- the NDS process IDs `nsdm` and `slpd`

- the identity server process IDs `sld1`, `sld2` and `sld3`

- the RADIUS server process ID `rad1`

c. Save and close the file.

d. Apply the changes by entering:

```
init q
```

Restoring one Sun ONE Directory Server in a replicated pair

Restoring the Sun ONE Directory Server overwrites any existing database files. Any modifications you have made since the last backup are lost.

Procedure steps

1. Stop the server processes on the server that is not being restored:
   a. Open the /etc/inittab file for editing.
   b. In the /etc/inittab file, change the following process IDs from `respawn` to `off`.
      - the NDS process IDs `nsdm` and `slpd`
      - the identity server process IDs `sld1`, `sld2` and `sld3`
      - the RADIUS server process ID `rad1`
   c. Save and close the file.
   d. Apply the changes by entering:

      `init q`

2. Uninstall and reinstall the Sun ONE IS server software on the server that is to be restored. For more information, refer to 241-6001-100 *Preside MDM Installation*.
3. Restart the server processes on the server that is not being restored.
   a. Open the /etc/inittab file for editing.
   b. In the /etc/inittab file, change the following process IDs from `off` to `respawn`.
      - the NDS process IDs `nsdm` and `slpd`
      - the identity server process IDs `sld1`, `sld2` and `sld3`
      - the RADIUS server process ID `rad1`
   c. Save and close the file.
   d. Apply the changes by entering:

      `init q`

4. On the server being restored, stop the server processes.
   a. Open the /etc/inittab file for editing.

b. In the /etc/inittab file, change the following process IDs from `respawn` to `off`.

- the NDS process IDs `nsdm` and `slpd`

- the identity server process IDs `sld1`, `sld2` and `sld3`

- the RADIUS server process ID `rad1`

c. Save and close the file.

d. Apply the changes by entering:

```
init q
```

5 Restore all configuration and data files to the directories by entering

```
tar xvf <backup_file_name>
```

6 Restart the server processes on the restored server:

a. Open the /etc/inittab file for editing.

b. In the /etc/inittab file, change the following process IDs from `off` to `respawn`.

- the NDS process IDs `nsdm` and `slpd`

- the identity server process IDs `sld1`, `sld2` and `sld3`

- the RADIUS server process ID `rad1`

c. Save and close the file.

d. Apply the changes by entering:

```
init q
```

7 Synchronize the replicated servers:

a. Log in to the server with the data that you want to maintain. The data from this server will be propagated to the replicated server.

b. Open the Sun ONE IS console by entering

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

c. In the login dialog box enter the Sun ONE IS user ID (ndsadmin) and the password for the ndsadmin.

d. Expand the **<hostname>.<org>** entry. For example **<hostname>.nortelnetworks.com**.

e. Expand the **Server Group** entry.

f. Select the **Directory Server** entry.

g. Click **Open**.

h. In the Directory Server window, select the **Configuration** tab.

i. Select **Replication** and then **userRoot**.

j. Right-click on **<hostname>_agreement** and select **Initialize Consumer**.

k. In the dialog that informs you that the existing content will be removed from consumer, click **Yes**.

l. Click **OK**.

Restoring both Sun ONE IS servers in a replicated pair

Restoring the Sun ONE Directory Server overwrites any existing database files. Any modifications you have made since the last backup are lost.

Procedure steps

1 On both servers, uninstall and reinstall the Sun ONE IS server software. For more information, refer to 241-6001-100 *Preside MDM Installation*.

2 On both servers, stop the server processes:

   a. Open the /etc/inittab file for editing.

   b. In the /etc/inittab file, change the following process IDs from `respawn` to `off`.

   - the NDS process IDs `nsdm` and `slpd`

   - the identity server process IDs `sld1`, `sld2` and `sld3`

   - the RADIUS server process ID `rad1`

   c. Save and close the file.

   d. Apply the changes by entering:

   `init q`

3 Restore the configuration and data files on both servers. You must use the backup.tar file specific to the server. Do not use the same backup .tar file for both servers.

`tar xvf <backup_file_name>.tar`

4 On both servers restart the server processes by repeating the following steps:

   a. Open the /etc/inittab file for editing.

   b. In the /etc/inittab file, change the following process IDs from `off` to `respawn`.

   - the NDS process IDs `nsdm` and `slpd`

   - the identity server process IDs `sld1`, `sld2` and `sld3`

   - the RADIUS server process ID `rad1`

   c. Save and close the file.

   d. Apply the changes by entering:

   `init q`

5 Synchronize the replicated servers:

a. Log in to the server with the data that you want to maintain. The data from this server will be propagated to the replicated server.

b. Open the Sun ONE IS console by entering

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

c. In the login dialog box enter the Sun ONE IS user ID (ndsadmin) and the password for the ndsadmin.

d. Expand the **<hostname>.<org>** entry. For example **<hostname>.nortelnetworks.com**.

e. Expand the **Server Group** entry.

f. Select the **Directory Server** entry.

g. Click **Open**.

h. In the Directory Server window, select the **Configuration** tab.

i. Select **Replication** and then **userRoot**.

j. Right-click on **<hostname>_agreement** and select **Initialize Consumer**.

k. In the dialog that informs you that the existing content will be removed from consumer, click **Yes**.

l. Click **OK**.

Backing up desktop user interface data

Backup files that can be modified by a user and whose changes would be lost in the event of a system failure. For example, backup the following files:

- /opt/nortel/logs/applications/desktop
- /opt/nortel/data/applications/desktop
- /opt/nortel/config/applications/desktop

Note: To prevent having to recreate your customizations, prior to a software upgrade, backup the configuration files in /opt/nortel/config/applications/desktop.

Procedure steps

1 Type the following command:

```
tar cvf <backup file name or tape drive>.tar <path to files to backup>
```

For example:

```
tar cvf log_backup.tar /opt/nortel/logs/applications/desktop
```

Restoring desktop user interface data

Copy the backuped up files to their original locations.

Procedure steps

1 Type the following command:

```
tar xvf <backup file name or tape drive>.tar
```

For example:

```
tar cvf log_backup.tar
```

Changing a centrally defined user ID attributes

User ID attributes, of any centrally defined user, are modified in the User Manager application of the User Administration system.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the User Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Change userID attributes. For more information, refer to *Modifying user information* in the online documentation.

Changing Passport user ID attributes

Change Passport node user ID attributes to modify the profile of an existing user ID that is defined on the node.

Prerequisites

- You need to be logged in with a user ID with command impact of systemAdministration.

Procedure steps

1 Use the following command for each attribute of the userID component you need to change.

```
set Ac userID/<user_id> <attribute> <value>
```

Variable definitions

Variable	Value
<attribute>	The name of the attribute you want to change for this user ID.
<user_id>	An existing user ID.
<value>	The new value for the attribute you are changing.

Changing a local Passport user password

Change a Passport local user password to set or change an existing password for a user ID.

Prerequisites

- You must be logged in with a user ID with command impact of systemAdministration.
- When you set or change a password, the actual characters of the password appear on the user interface. To keep passwords private, make sure your workstation is in a secure area before changing a password. If you need a more secure way of setting a password refer to NN10600-605 *Passport - MDM Network Security: Operations* for ways of setting secure passwords.

Procedure steps

1 Set the password.

```
set Ac userid/<user_id> password <pswd>
```

Variable definitions

Variable	Value
<pswd>	The new password for the user ID. It needs to be from five to eight characters long. When you set a password, it displays on the user interface. After set, the password cannot be displayed again.
<user_id>	The user identifier whose password you are changing.

Deleting a centrally defined user

Delete a centrally defined user from the Sun ONE Identify server by deleting the user ID and associated privileges.

Note: Externally authenticated users are added automatically as users in the MDM LDAP directory and must be deleted periodically by the administrator.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the User Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Delete the user. For more information, refer to *Deleting a user* in the online documentation.

   If the user is still associated with your organization, you can also deactivate the user. For more information, refer to *Deactivating a user* in the online documentation.

Deleting a local Passport user

Delete a Passport node's local user to remove an existing user ID and its associated privileges.

Prerequisites

- You need to be logged in with a user ID with command impact of systemAdministration.

Procedure steps

1 Remove the user ID component.

```
delete Ac userID/<user_id>
```

Variable definitions

Variable	Value
<user_id>	The existing user ID that you want to delete.

Deleting a role

Delete a role to remove an existing role and its associated privileges. Role definitions that are exclusively referenced via an external RADIUS server are not automatically deleted when they are no longer referenced by the external RADIUS server; you must delete them manually.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the User Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. Delete the role. For more information, refer to *Deleting a role* in the online documentation.

Denying a centrally defined user access to a node

In the User Administration system, deny a centrally defined user access to a node by removing a user from a role or a role from a policy.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. If the user's access is defined by the policy they are associated with, login to the Policy Manager application.

   If the user's access is defined by the role they are associated with, login to the User Manager application.

   For more information, refer to "Logging into the User Administration system" (page 57).

2. If the user's access is defined by the policy they are associated with, remove the user from the policy. For more information, refer to *Removing users or roles from a policy* in the online documentation.

3. If the user's access is defined by the role they are associated with, remove the user from the role. For more information, refer to *Disassociating a user from one or more roles* in the online documentation.

Displaying the number of user sessions on a Passport node

Display the number of user sessions to determine how many users are logged in to the Passport node and which network management interfaces they are using.

Prerequisites

- You must be in operational mode.

Procedure steps

1. Display the number of simultaneous sessions currently active on a particular network management interface.

   ```
   display Nmis <interface> activeSessions
   ```

2. List the sessions logged in to a particular network management interface.

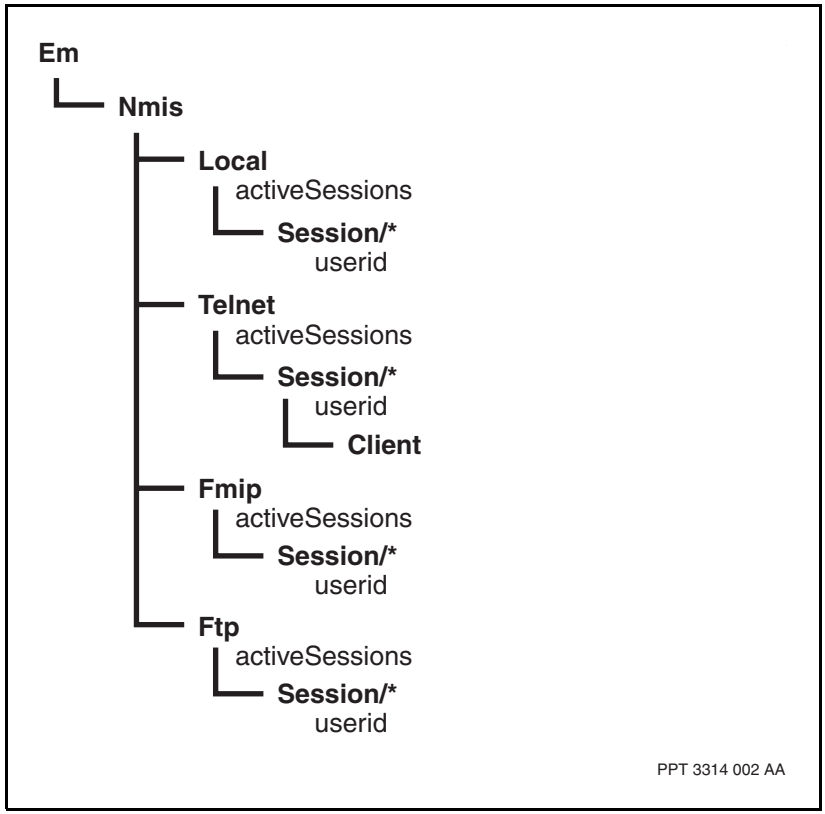
   ```
   list Nmis <interface> Session/*
   ```

Variable definitions

Variable	Value
<interface>	One of the network management interfaces: *Local*, *Fmip*, *Ftp*, or *Telnet*.

Procedure job aid

Figure 15
Displaying the number of user sessions component hierarchy



Displaying the user IDs on a Passport network management interface

Display the user IDs on an interface to determine which users are logged in to a particular network management interface.

Prerequisites

- You must be in operational mode.

Procedure steps

1 Display all the users logged in to a network management interface.

```
display Nmis <interface> Session/* userid
```

Variable definitions

Variable	Value
<interface>	One of the network management interfaces, *Local*, *Fmip*, *Ftp*, or *Telnet*.

Displaying the users on the User Management system

Use the Session Management application to display the users that are currently active on the Sun ONE IS.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1 Login to the User Session Manager application.

For more information, refer to “Logging into the User Administration system” (page 57).

2 View all the users currently active on the server. For more information, refer to *Viewing user sessions associated with a server* in the online documentation.

3 If you wish to search for a particular user, refer to *Finding (filtering) user sessions* in the online documentation.

Managing policies

The Policy Manager application allows you to manage policies and policy rules that specify the action permissions, and resources associated with a user.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1. Login to the Policy Manager application.

   For more information, refer to “Logging into the User Administration system” (page 57).

2. If a policy contains a rule that no longer applies to your system, change or delete the policy rule. For more information, refer to *Modifying a policy rule* and *Deleting a policy rule* in the online documentation.

3. If a policy, including all it’s policy rules and subjects, no longer applies to your system, change or delete the entire policy. For more information, refer to *Modifying a policy* and *Deleting a Policy* in the online documentation.

Restricting access through a Passport network element interface

Restrict access through a specified interface by placing the interface out of service. To place an interface out of service, lock the appropriate interface component. All current sessions continue until they are complete and no further sessions start until you unlock the interface.

Prerequisites

- You must be logged in with a user ID with a command impact of systemAdministration.
- You must be in operational mode.

Procedure steps

1 Lock the interface component.

```
lock Nmis <interface>
```

The interface moves to a shutting-down state and does not allow setup of further sessions. All current sessions continue until they are complete.

If you lock the telnet interface while you have a current telnet session, you can still set up outgoing telnet client connections (using the *telnet Vr* command), but you cannot set up new incoming telnet sessions.

Variable definitions

Variable	Value
<interface>	One of the allowed network management interfaces, *Fmip*, *Ftp*, or *Telnet*. You cannot restrict access through the local interface. You can lock any other interface component except the interface you are currently using to access the node.

Releasing a locked Passport network management interface

Use this procedure to release, or unlock, a locked network management interface. When you unlock an interface, it is once again available for users to set up new connections (sessions) on it.

Prerequisites

- You need to be in operational mode.

Procedure steps

1 Unlock the interface component.

```
unlock Nmis <interface>
```

Variable definitions

Variable	Value
<interface>	One of the allowed network management interfaces, *Fmip*, *Ftp*, or *Telnet*.

Resetting a centrally defined user password

Reset a centrally defined user password to change a password of a user without knowing the user's current password.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.
- After resetting a user password, notify that user that their password has been reset and that they have to change their password before logging on to the Passport node or workstation.

Procedure steps

1 Login to the User Manager application.

For more information, refer to "Logging into the User Administration system" (page 57).

2 Reset the user's password. For more information, refer to *Resetting a user's password* in the online documentation.

Starting the Sun ONE DS console

Start the Sun ONE DS console so you can use it to perform administration procedures on the LDAP server.

Procedure steps

1. Log on to the workstation where the LDAP server is installed.
2. Go to the server directory (the default is `/opt/nortel/3rd_party/netscape/current_nds`) and type:

   `./startconsole`

   The console login dialog box opens.
3. Enter the Directory Server administration userid (the default is admin) and the password (default is cn=directory manager).

   The console window opens.

Terminating a centrally defined user's session

You can terminate a user session in the User Administration system if you wish to perform maintenance. Note that if the user has been authenticated via an external RADIUS server, this procedure terminates their current session but it does not deactivate the user. Externally authenticated users must be deactivated on the external RADIUS server.

Prerequisites

- access to online documentation: To access the online documentation, from the application, select **Help->Help on Window**. Select the magnifying glass icon and enter the search text, displayed in italics, in the procedure step.

Procedure steps

1 Login to the User Session Manager.

For more information, refer to "Logging into the User Administration system" (page 57).

2 Search for a particular user. For more information, refer to *Finding (filtering) user sessions* in the online documentation.

3 Terminate the user session. For more information, refer to *Terminating a session* in the online documentation.

If you wish to terminate the user session and deactivate the user's access to the server, refer to *Deactivating a user* in the online documentation.

Terminating a user session on a Passport network management interface

Terminate an individual user session on a specific interface.

Prerequisites

- You must be logged in with a user ID with a command impact of systemAdministration.
- You must be in operational mode.

Procedure steps

1. Display all current sessions.

   ```
   list Nmis <interface> Session/*
   ```

   This command lists all sessions on the interface. Each session has a unique instance number.

2. Find the session number belonging to the user session you want to terminate.

3. Clear the *Session* component.

   ```
   clear Nmis <interface> Session/<n>
   ```

   The user session terminates. If a telnet session has a client connection (as represented by the *Client* subcomponent), the command terminates the client connection too.

Variable definitions

Variable	Value
<interface>	One of the allowed network management interfaces, *Fmip*, *Ftp*, or *Telnet*. You cannot terminate a user session on the local interface.
<n>	The session number you want to terminate.

Terminate all user sessions on a Passport network management interface

Use this procedure to terminate immediately all the user sessions on a particular interface and prevent the setup of new sessions on that interface.

Prerequisites

- You must be logged in with a user ID with a command impact of systemAdministration.
- You must be in operational mode.

Procedure steps

1 Force the lock on the interface component.

```
lock -force Nmis <interface>
```

The interface immediately terminates all its sessions, moves to a locked state, and does not set up further sessions.

Variable definitions

Variable	Value
<interface>	One of the allowed network management interfaces, *Fmip*, *Ftp*, or *Telnet*. You cannot terminate user sessions on the local interface. You can lock any other interface component except the interface you are currently using to access the node.

Sun ONE Identity Server system recovery

If the Sun ONE Indentity server (IS) experiences an uncontrolledshutdown, the DBVERSION files may become corrupted. Use these procedures to recover the system:

> ***Note:*** An abnormal system shutdown is strictly unsupported and it is strongly recommended that you use either the“init 0” (which will halt the system), “init 6” (which will halt and reboot the system) or “shutdown” commands before powering down the system.

- “Stopping the NDS processes” (page 127)
- “Recreating the DBVERSION files” (page 128)
- “Restarting the NDS processes” (page 128)

Stopping the NDS processes

You must stop all NDS processes before recreating the DBVERSION files.

Procedure steps

1. Open the /etc/inittab file for editing
2. In the /etc/inittab file, change the NDS process IDs `nsdm` and `slpd` from `respawn` to `off`.
3. Save and close the file.
4. Apply the change by entering:

   `init q`

5. Verify that the processes have stopped by entering:

   `ps -eaf | grep current_nds`

6. If NDS processes are still running, enter their stop commands directly:

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

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

   where:
   <hostname is the host name of the IS.

7 Due to the corrupt DBVERSION files, some NDS processes may remain. Repeat step 5 and kill any remaining NDS processes.

Recreating the DBVERSION files

Recreate the corrupted DBVERSION files.

Procedure steps

1 Copy the test below and create a file called `/tmp/dbversion.sh`

Note: You must replace <hostname> with the actual IS host name.

```
#! /bin/sh

cd
/opt/nortel/data/3rd_party/netscape/slapd-<hostname>/
db

for file in DBVERSION NetscapeRoot/DBVERSION userRoot/
DBVERSION

do

echo "iPlanet-ldbm/5.1" > $file
chmod 600 $file
chown adm:adm $file

done
```

2 Change permission on the file just created by entering

```
chmod +x dbversion.sh
```

3 Execute the script by entering

```
/bin.sh /tmp/dbversion.sh
```

Restarting the NDS processes

Once the DBVERSION files have been recreated, restart the NDS processes

Procedure steps

1 Open the /etc/inittab file for editing.

2 In the /etc/inittab file, change the NDS process IDs `nsdm` and `slpd` from `off` to `respawn`.

3 Save and close the file.

4 Apply the changes by entering:

```
init q
```

Chapter 9
Remote access using telnet

The tasks contained in this section allow users to authenticate themselves and connect to the appropriate devices.

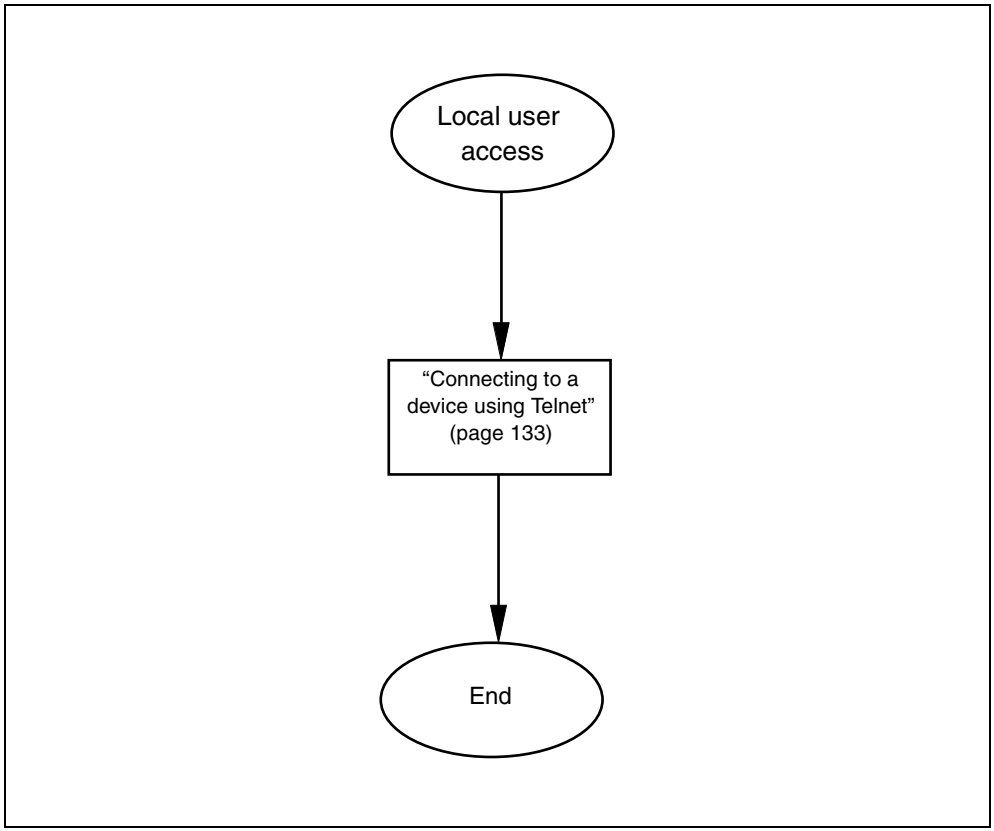
Navigation links

- "Remote access using telnet taskflow" (page 131)
- "Task navigation" (page 132)

Remote access using telnet taskflow

This taskflow shows you the sequence of procedures you perform to configure remote access using telnet. To link to any procedure go to "Task navigation" (page 132).

Figure 16
Remote access using telnet taskflow



Task navigation

- "Connecting to a device using Telnet" (page 133)

Connecting to a device using Telnet

You can use Preside Multiservice Data Manager Operator Client to launch a local telnet application which can be used to connect to a remote host (Solaris) or network element.

Prerequisites

- The user must have a valid user ID and password on the remote machine that is being accessed

Procedure steps

1. Start Operator Client.
2. From the **System** menu, select **Utilities>Remote Telnet Access**.
3. In the local telnet window, connect to the remote host.
   a. Enter **Open**.
   b. Enter your user ID and password.

Passport - MDM

Network Security: User Access Configuration

Release 15.1RSUP

Publication: NN10600-606
Document status: Standard
Document version: 15.1RSUP, PCR 6.1
Document date: August 2004
Printed in Canada

NORTEL NETWORKS