

PASSPORT® 4000 MESSAGE HANDLING SYSTEM

Configuration Manager Guide

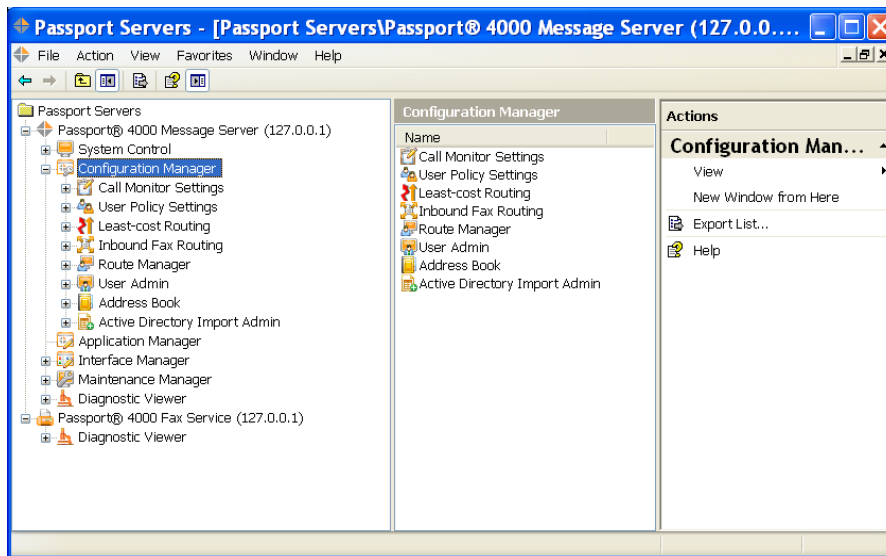




Table of Contents

Configuration Manager	1	LOCAL ROUTES	16
CALL MONITOR SETTINGS	2	ADD A NEW LOCAL ROUTE	18
DATABASE SETTINGS	3	GLOBAL ROUTES	19
DATABASE PROPERTIES	4	ADD A NEW GLOBAL ROUTE	20
DOCUMENT CONVERSION	5	ADDING A NEW ENTERPRISE MEMBER	22
DOCUMENT CONVERSION PROPERTIES	6	INBOUND FAX ROUTING	23
EVENT MAPPING	7	ADD A NEW DID ROUTE	24
ADD NEW EVENT	8	ROUTE MANAGER	25
LINE	8	ROUTE OBJECT PROPERTIES	26
TYPE	8	LABELS	27
COMMENT	8	OPTIONS	27
EVENT TYPE	8	USER ADMIN	31
CLUSTER CONFIGURATION	9	OPERATIONS	31
PROPERTIES	10	ADDING A NEW USER	32
CLUSTER MODE	10	NAME AND PASSWORD	32
NAME OF IP ADDRESS OF CLUSTER PARTNER	10	DELIVERY	33
FLOATING IP ADDRESS	10	REPORTS	34
USER POLICY	11	EMAIL INPUT	35
SETTINGS	11	FAX	36
PROPERTIES	11	FAX LIMITS	37
AUTHENTICATION AND SECURITY	11	PRIVILEGES	38
PASSWORD POLICIES	14	ADDRESS BOOK	39
AVAILABLE ROUTES	15	ADDING AN ADDRESS BOOK ENTRY	40
LEAST COST ROUTING	16	ACTIVE DIRECTORY IMPORT ADMIN	41

Configuration Manager

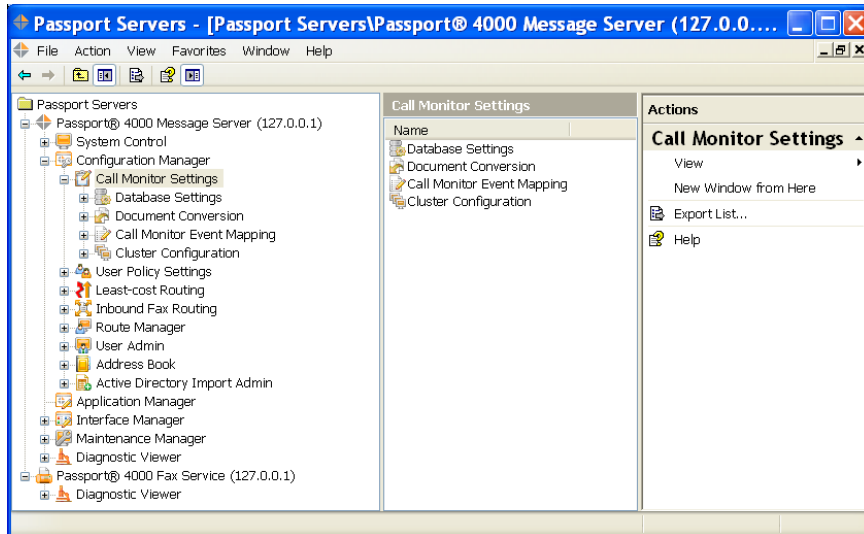


Use the Configuration Manager snap-in extensions for configuring the Passport 4000 System.

The following functions are available in the Configuration Manager

- **Call Monitor Settings**
Define the Call Monitor program settings
- **User Policy Settings**
Define the User Policy requirements.
- **Least Cost Routing**
Configure optimal local and global routing in your system, and in your enterprise.
- **Inbound Fax Routing**
Define the Inbound Fax Routes.
- **Route Manager**
Create all the system use routes.
- **User Admin**
Administer the Passport Users.
- **Address Book**
Create and Maintain the Address Book

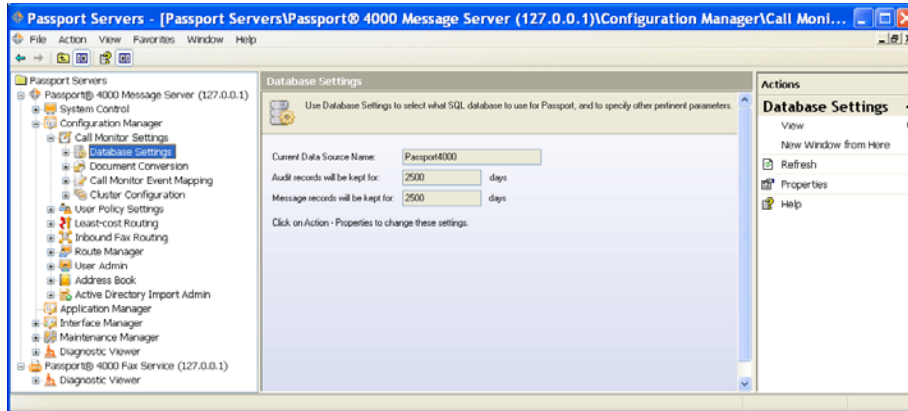
Call Monitor Settings




Use Call Monitor settings to configure various settings and parameters that control the processing of messages in your Passport.

- Database Settings
- Document Conversion
- Call Monitor Event Mapping
- Cluster Configuration

Database Settings




 Use Database Settings to select what SQL database to use for Passport, and to specify other pertinent parameters.




You should first configure your SQL server by adding a database for this Passport to use. Then, use the Windows Control Panel applet Data Sources (ODBC) on the Passport Message Server computer so that it can refer to your chosen database with a System DSN. Finally, come back here to specify to the Call Monitor what System DSN to use.

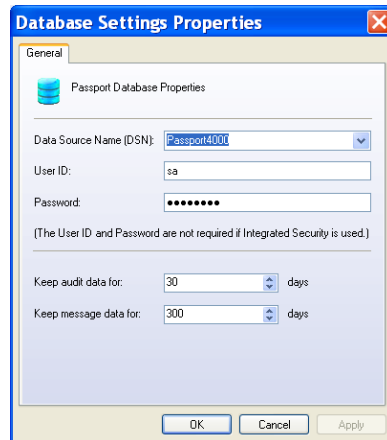
The summary display will show the current Data Source Name, and show how many days the audit and message records will be retained.

Operations

 **Refresh** Click **Refresh** in the Action Pane (or right-click on Database Settings in the console tree and select **Refresh**) to refresh the settings display.

 **Properties** Click **Properties** in the Action Pane (or right-click on Database Settings in the console tree and select **Properties**) to open Database Properties to change the settings.

Database Properties



Use Database Properties to display or change the properties of the Database settings.

Data Source Name (DSN)

Choose from this list the database that you have already configured to be used by Passport.



If your SQL Server uses SQL Server authentication using a log ID and password, then you must supply the ID and Password here. If your SQL Server uses Windows NT

authentication using the network login ID, then you do not need to supply an ID and Password.

With either authentication method, the Passport's SQL access must permit it to create tables and stored procedures, and to write and read table entries.

User ID

Enter the SQL Server Login ID (not required if SQL is using NT authentication).

Password

Enter the SQL Server Password (not required if SQL is using NT authentication).

Keep audit data for

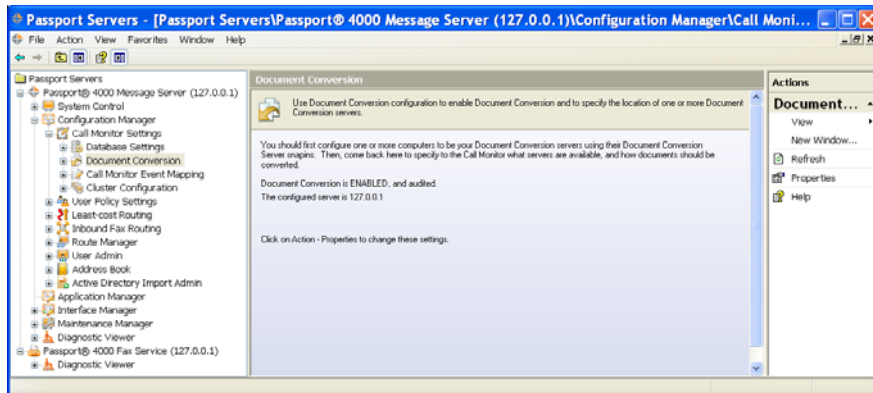
Enter the number of days (30-999) to keep audit data in the database.


Keep message data for

Enter the number of days (30-999) to keep message data in the database.

Make changes as desired, then click either **OK** to make the changes and close Database Properties, or **Apply** to make the changes and leave the properties open. Or, click **Cancel** to leave the properties without making any change.

Document Conversion



 Use Document Conversion configuration to enable Document Conversion and to specify the location of one or more Document Conversion servers.



You should first configure one or more computers to be your Document Conversion servers using their Document Conversion Server snapins. Then, come back here to specify to the Call Monitor what servers are available, and how documents should be converted.

The summary display will indicate whether or not Document Conversion has been enabled and is audited, and what servers have been assigned.

Operations

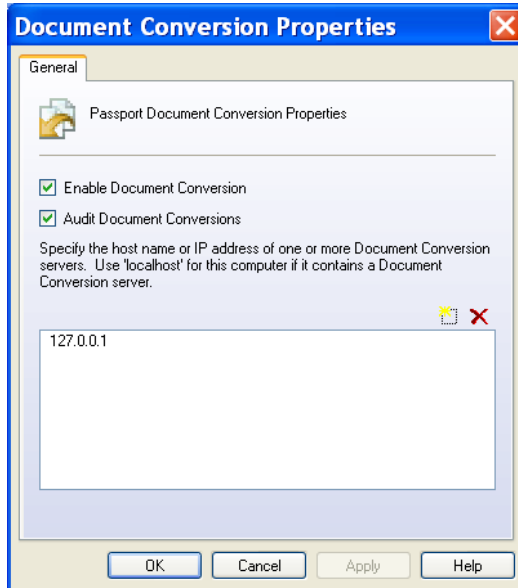
 **Refresh**

Click **Refresh** in the Action Pane (or right-click on Document Conversion in the console tree and select **Refresh**) to refresh the configuration display.

 **Properties**

Click **Properties** in the Action Pane (or right-click on Document Conversion in the console tree and select **Properties**) to open Document Conversion Properties to change the configuration.

Document Conversion Properties



Enable Document Conversion

Check or uncheck this box to enable Document Conversion on this system.

If disabled, no conversion or transmission of incompatible attachments will be attempted. For example, any kind of attachment can be sent to email, but only group 3 tiff attachments can be sent directly to fax.



If enabled, attachments will be converted to tiff to permit transmission to fax destinations.

Audit Document Conversion

Check or uncheck this box to audit Document Conversion functions on this system.

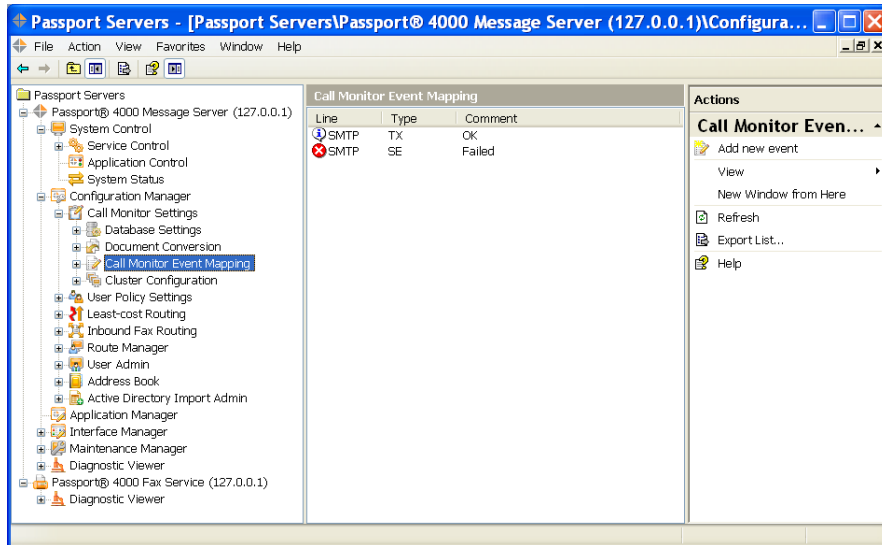
If enabled, all Document Conversions will be entered in the audit log.


Server List Operations

-  **Add new entry** Click on the Add new entry toolbar icon to initiate the entry of a new server. Type in the host name or IP address of the Document Conversion server, then hit the Enter key.
-  **Delete selected entry** Select an existing server entry and then click on the Delete selected entry toolbar icon to delete the selected server from the list.
- Change selected entry** Select an existing server entry, wait a couple of seconds, then click again on the selected entry. Make changes as desired, then hit the Enter key.

Make changes as desired, then click either **OK** to make the changes and close Document Conversion Properties, or **Apply** to make the changes and leave the properties open.

Event Mapping



 Use Call Monitor Event Mapping to add, delete, and show properties of Passport events that are mapped to Windows events.

Passport events are generally viewed with the Passport Audit viewer. You may map certain Passport events so that they will also appear in the Windows Event Log.

Operations

Refresh

Click **Refresh** in the Action Pane (or right-click on Call Monitor Event Mapping in the console tree and select **Refresh**) to refresh the list of mappings.

Add new event

Click **Add new event** in the Action Pane (or right-click on Call Monitor Event Mapping in the console tree and select **Add new event**) to open the New Event dialog to create new event mappings.

Once an entry has been selected, additional options will appear in the Action Pane (or when right-clicking an entry, in the context menu). Double-click an entry to show properties for that entry.

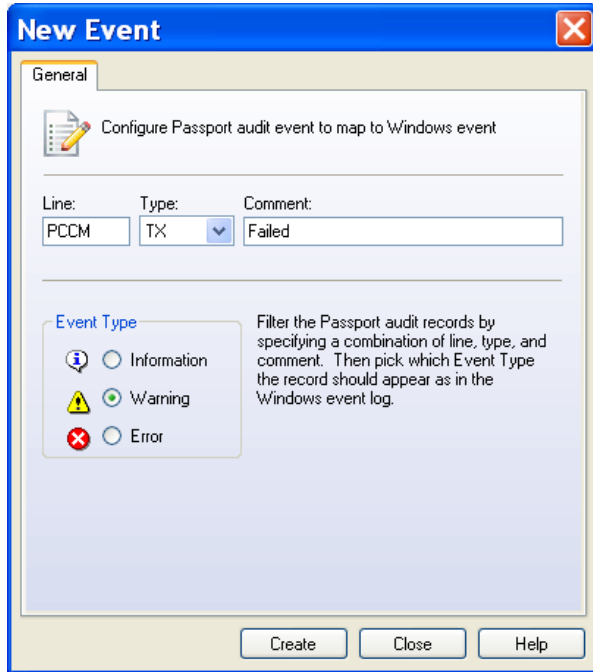
Properties

Click **Properties** to open the properties dialog allowing modification of the entry.

Delete

Click **Delete** to delete the selected entry.

Add New Event



Line

Enter all or the beginning part of the line name to which this mapping should apply. For example, enter FX to apply to all fax line names beginning with FX. Leave the line entry blank to apply to all line names.

Type

Choose a type from the list of audit record types to which this mapping should apply. Choose *(all)* to apply to all audit record types.

Comment

Enter all or part of the audit record comment to which this mapping should apply. Unlike the line filter, this comment filter may appear anywhere in the audit record comment, but the spelling and case must match exactly. For example, enter *Conversion failure* to apply to all audit records that contain that string anywhere within the comment. Leave the comment entry blank to disregard the comment contents.




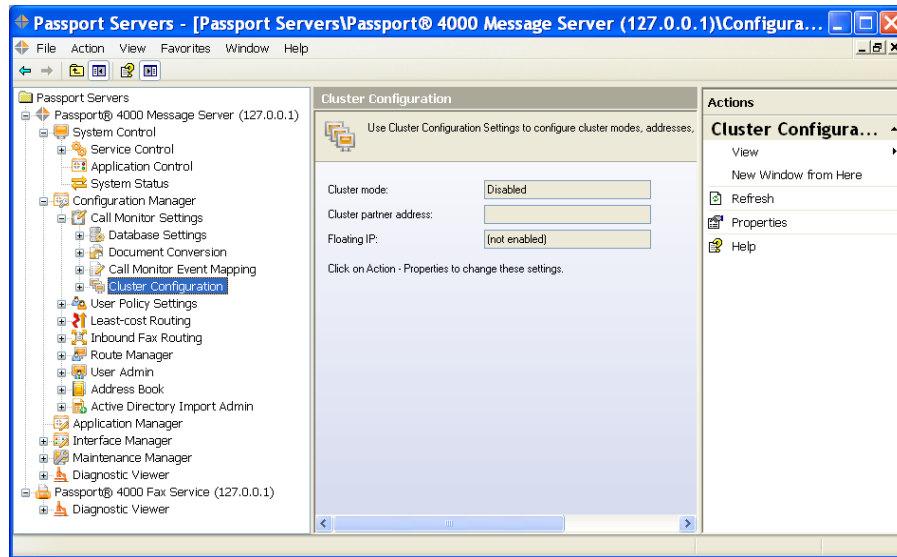
Event Type




Choose how you want this event to be shown in the Windows Event Log. You may choose **Information**, **Warning**, or **Error**. After making your entries, click **Create** to create the new event mapping. You may then create another event mapping. When you are finished, click **Close** to leave New Event.

Cluster Configuration

 Use Cluster Configuration to designate the cluster partner, specify the clustering mode, and configure a floating IP address.



Clustering is an optional feature with Passport, and may not be available on your system. 

To configure clustering, first configure two Passport Message Servers both to use a common SQL server and common file server. Then, come back here to specify the cluster settings, thus interconnecting the two Message Servers into a single clustered system.

The summary display will show the current Cluster mode, the cluster partner address, and the Floating IP address (if set).

Operations

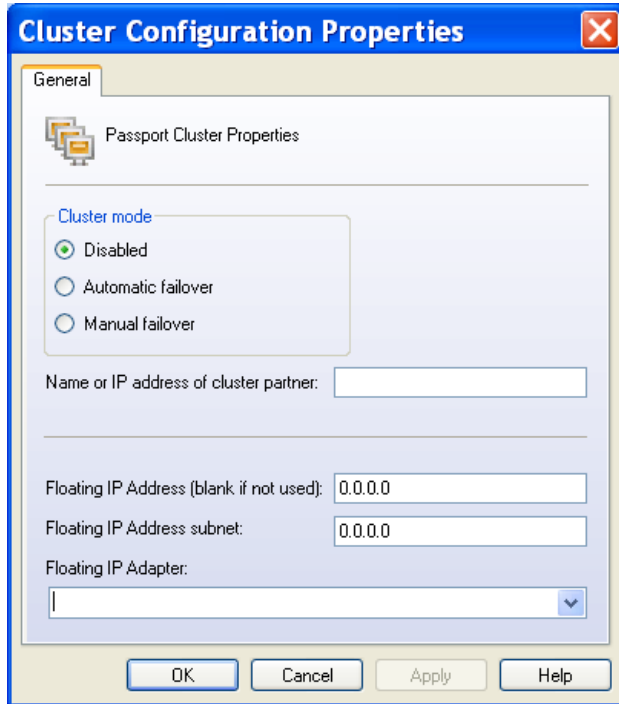
Refresh

Click **Refresh** in the Action Pane (or right-click on Cluster Configuration in the console tree and select **Refresh**) to refresh the configuration display.

Properties

Click **Properties** in the Action Pane (or right-click on Cluster Configuration in the console tree and select **Properties**) to open Cluster Configuration Properties to change the properties.

Properties



Cluster mode

Select the mode of operation for your clustered system. **Disabled** will disable the communications between the two cluster partners, and will cause the two systems to function

independently. Do not permit both systems to run with a common database and file server; data corruption will occur. **Automatic failover** will cause this system to monitor the partner system for responsiveness. If the partner fails, this system will takeover automatically. **Manual failover** will permit this system to start if the partner system is unresponsive, or to enter the standby mode if the partner system is responsive. However, if the partner system later becomes non-responsive, this system will not take over automatically.



Name of IP address of cluster partner

Enter the host name or the IP address of the cluster partner.

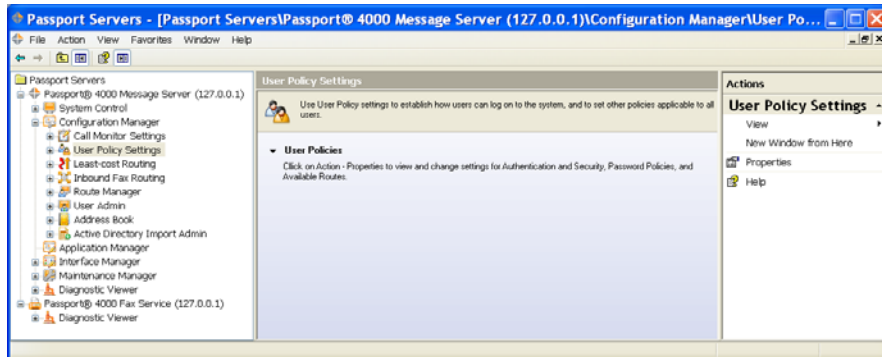
Floating IP Address


A clustered Passport system can share a single floating IP address. This can simplify connections from external client computers or other messaging systems. To do this, enter the floating IP address to be used, and its subnet. Note that these two entries must be identical on both cluster partners. Choose which network adapter is to be used for this floating IP address.

NOTE: In order for the Passport system to assign and release a floating IP address, the Passport service must be running under an account with administrator privileges.



User Policy Settings

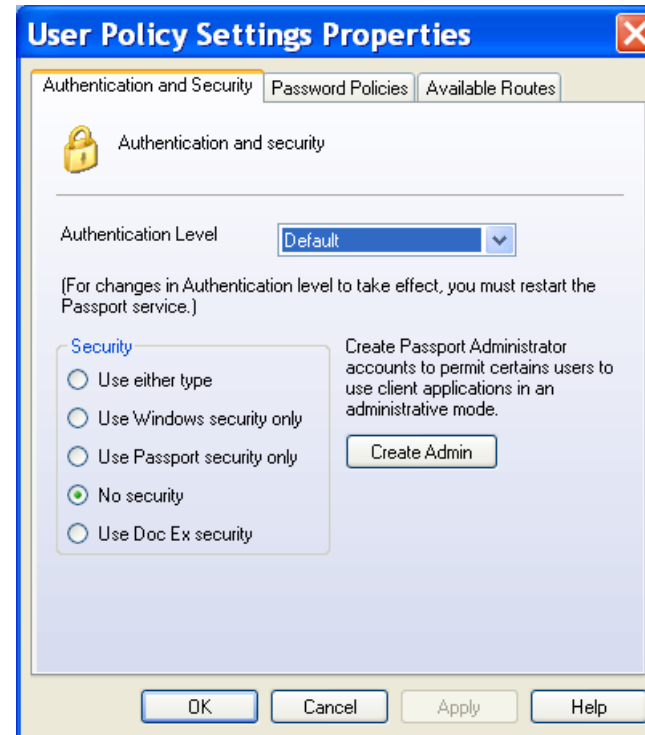


 Use User Policy settings to establish how users can log on to the system, and to set other policies applicable to all users.

Properties

Click **Properties** in the Action Pane (or right-click on User Policy Settings in the console tree and select **Properties**) to open User Policy Properties to change the settings. The User Policies are organized into three groups described further below.

Authentication and Security



Authentication level Description

Default	Uses authentication level that is configured for the computer
None	No authentication
Connect	Authenticate credentials only when the client initially connects to the server
Call	Authenticate credentials at the start of each remote call
Packet	Authenticate every packet received from the client
Packet Integrity	Authenticate every received packet and verify that received data has not been modified
Packet Privacy	Authenticate and encrypt all packets

You should understand that each increase in the level of authentication incurs greater network and computer overhead.



Also note that if you change the authentication level, you will need to restart the Passport service to implement the change.



Login Security

Security	Description
Use either type	Uses Windows security to identify the user. Failing that, uses Passport security.
Use Windows security only	Uses Windows security to identify the user
Use Passport security only	Always require user to log on with a Passport user ID and password
No security	No user identification attempted
Use Doc Ex security	Login users according to an associated Document Exchange system

If you use Windows security, you can eliminate the need for users to login every time they run a Passport application. Users are identified by their Windows login, which is passed as part of the Authentication described above. Thus the Passport user is always the same as the Windows user. Windows security can identify the user properly only if the Authentication level is something other than 'None', and also if the guest account is not enabled. Make changes as desired, then click either OK to make the changes and close properties, or Apply to make the changes and leave the properties open. Or, click Cancel to leave the properties without making any change.

Create Admin

Passport Administrator accounts enjoy special privileges in many Passport applications. They can view, and sometimes control, all functions of the Passport system without regard to user or departmental boundaries.

Password policies



Policy

Description

Passwords are optional

Makes the requirement of a password optional for each user

Passwords never expire

Disables the expiration of passwords that normally requires users to change passwords regularly

Password expiration is optional per user Disables password expiration for selected individual users

The Password policies apply only if you are using Passport security, or a mixture of Passport and Windows security. (see Security) For Windows security, use the Windows utilities to set policies.

Other policies

Policy

Description

Permit non-user department originator codes

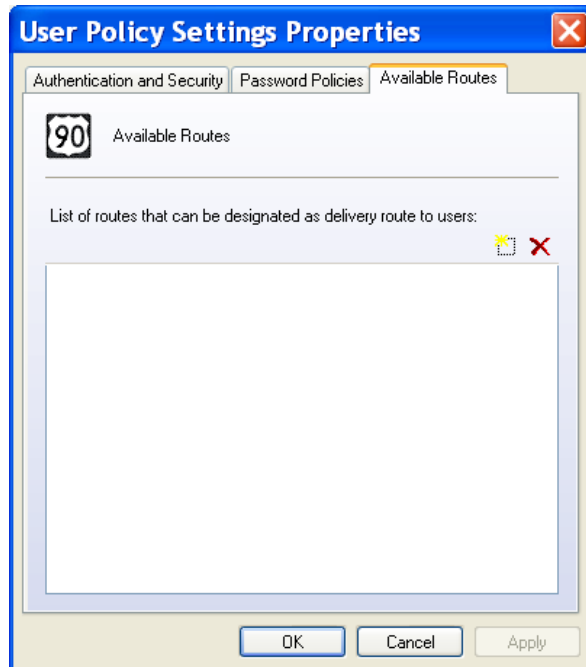
Permits the creation of originator codes that are not otherwise Passport users

Allow retrieval of received as well as sent messages

Allows users to retrieve messages they have received in addition to messages they have originated

Make changes as desired, then click either OK to make the changes and close properties, or Apply to make the changes and leave the properties open. Or, click Cancel to leave the properties without making any change.

Available Routes



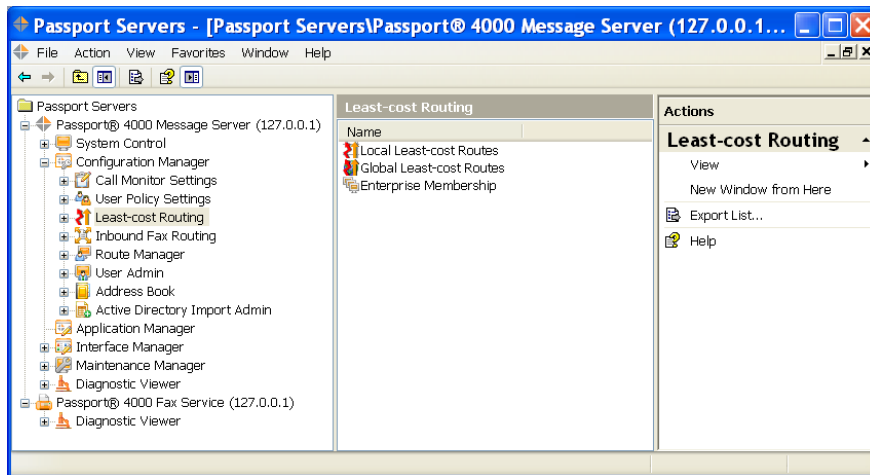
Route List Operations

- Add new entry** Click on the Add new entry toolbar icon to initiate the entry of a new route. Type in the name of the route to be added to the list, then hit the Enter key.
- Delete selected entry** Select an existing route in the list, then click on the Delete selected entry toolbar icon to delete the selected route from the list.
- Change selected entry** Select an existing route entry, wait a couple of seconds, then click again on the selected entry. Make changes as desired, then hit the Enter key.

The available routes are typically *wild* routes, which are combined with an address to define how messages, delivery notices, etc, are delivered to a user.

Make changes as desired, then click either **OK** to make the changes and close Available Routes, or **Apply** to make the changes and leave the properties open. Or, click **Cancel** to leave the properties without making any change.

Least Cost Routing



Use Least-cost Routing to configure optimal local and global routing in your system, and in your enterprise.

Note:



The **Global** and **Enterprise** facilities are optional items, and may not be available in your system.

Local Routes

You can use local routes to define how messages are routed in your Passport system based on a combination of both the message's route and address. For example, fax messages to a particular number can be handled differently than those to another number. Typically this is used to route a message according to the cheapest or most-reliable transport, possibly by way of another Passport system. But it can also be used to totally alter the method of transport, for example by sending faxes addressed to a particular number as emails.

Operations



Refresh


Click **Refresh** in the Action Pane (or right-click on Local Least-cost Routes in the console tree and select **Refresh**) to refresh the list of local routes.



Add new route

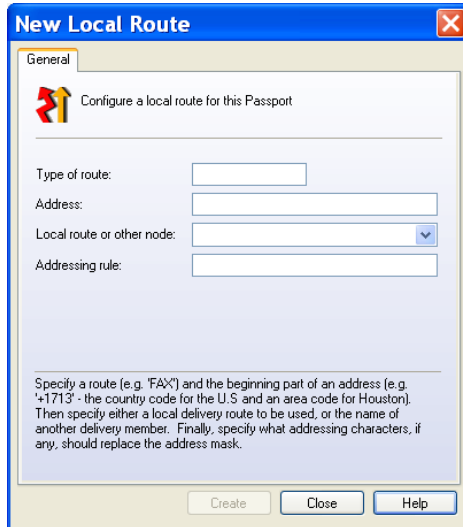
Click **Add new route** in the Action Pane (or right-click on Local Least-cost Routes in the console tree and select **Add new route**) to open the New Local Route dialog to create new local routes.

Once an entry has been selected, additional options will appear in the Action Pane (or when right-clicking an entry, in the context menu). Double-click an entry to show properties for that entry.

 **Properties** Click **Properties** to open the properties dialog allowing modification of the entry.
See *Add a New Local Route* for more details.

 **Delete** Click **Delete** to delete the selected entry.

Add a New Local Route



Type of route

Enter the type of route of address class to which this route will apply. For example, enter *FAX* to specify a local route for the given route of 'FAX' and the partial address given below.

Address

Enter all or the beginning part of the address(es) to which this route will apply. For example, enter *+1713* to specify the global country code ('+1' for the U.S.) and an area code ('713' for Houston).

Local route or other node

Enter the local delivery route that should be used, or enter the name of another enterprise member that will perform the delivery.

Addressing rule

Specify what addressing characters, if any, should replace the address mask given above.

Note that local routes take precedence over global routes. In general, if you define a global route, then you must also define that same route as a local route at the delivery member, using a local delivery route.

Local routes may also specify another enterprise member for the final delivery. This might be done if it is not appropriate for all the enterprise members to use a global route for those message addresses.

There is a special entry for the **Address** of *DEFAULT*. This designates that the corresponding local delivery route should be used for messages that do not have a matching explicit Address.

There is a special entry for the **Local route or other node** of *BARRED*. This designates message delivery to the corresponding address will not be attempted. This is useful for inhibiting accidental calls to 911 or other similar addresses. After making your entries, click **Create** to create the new route. You may then create another route. When you are finished, click **Close** to leave New Local Route.


Global Routes




You can use global routes to define how messages are routed in all members of your Passport enterprise based on a combination of both the message's route and address. For example, fax messages to a particular number can be handled differently than those to another number. Typically this is used to route a message according to the cheapest or

most-reliable transport, possibly by way of another Passport system. But it can also be used to totally alter the method of transport, for example by sending faxes addressed to a particular number as emails.


Operations

 **Refresh** Click **Refresh** in the Action Pane (or right-click on Global Least-cost Routes in the console tree and select **Refresh**) to refresh the list of global routes.

 **Add new route** Click **Add new route** in the Action Pane (or right-click on Global Least-cost Routes in the console tree and select **Add new route**) to open the New Global Route dialog to create new global routes.

Once an entry has been selected, additional options will appear in the Action Pane (or when right-clicking an entry, in the context menu). Double-click an entry to show properties for that entry.

 **Properties** Click **Properties** to open the properties dialog allowing modification of the entry.

 **Delete** Click **Delete** to delete the selected entry.

Add a New Global Route



New Global Route

General

Configure a global route for all Passports in the enterprise to use

Type of route:

Address:

Delivery member:

Specify a route (e.g. 'FAX'), and the beginning part of an address (e.g. '+44' - the country code for the U.K.), and then choose which Enterprise member should deliver these messages.

Create Close Help

Type of route

Enter the type of route of address class to which this route will apply. For example, enter *FAX* to specify a global route for the given route of 'FAX' and the partial address given below.

Address

Enter all or the beginning part of the address(es) to which this route will apply. For example, enter *+44* to specify the global country code ('+44' for the U.K.).

Delivery member

Enter or choose the name of the enterprise member that will perform the final delivery of these messages.


Note that in general, when you define a global route, then you must also define a corresponding local route at the specified delivery node.

After making your entries, click **Create** to create the new route. You may then create another route. When you are finished, click **Close** to leave New Global Route.

Enterprise Membership

The members of a Passport enterprise all share a common set of global least-cost route definitions. Messages in a Passport enterprise can be routed to any other member of the enterprise for final routing.

Operations

 **Refresh** Click **Refresh** in the Action Pane (or right-click on Enterprise Members in the console tree and select **Refresh**) to refresh the list of members.

Add new member Click **Add new member** in the Action Pane (or right-click on Enterprise Members in the console tree and select **Add new member**) to open the New Enterprise Member dialog to create new members of the enterprise.

Once an entry has been selected, additional options will appear in the Action Pane (or when right-clicking an entry, in the context menu). Double-click an entry to show properties for that entry.

 **Properties** Click **Properties** to open the properties dialog allowing modification of the entry.

 **Delete** Click **Delete** to delete the selected member.

Adding a New Enterprise Member



New Enterprise Member

General

Configure a member of the Passport Enterprise

Name:

Host name or IP address:

Specify a meaningful name, and the host name or IP address, of the member of the Passport Enterprise.

Create Close Help

Name

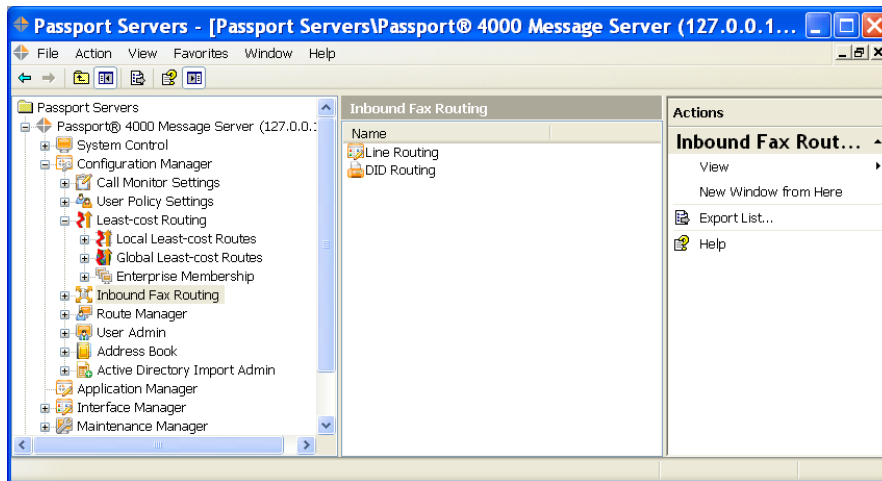
Enter some meaningful name for this enterprise member by which it will be referred to at all other members. For example, enter *UK* to specify a member located in the U.K. such that other Passport administrators will recognize that this member will deliver messages destined for U.K. destinations.




Host name or IP address


Enter Host name or IP address of the member. After making your entries, click **Create** to create the new member. You may then create another member. When you are finished, click **Close** to leave New Enterprise Member.


Inbound Fax Routing



 Use the Inbound Fax Routing snap-in to define the DID/DTMF departmental routing.

Operations


 **Refresh** Clicking Refresh in the Action Pane, or right-clicking on Inbound Fax Routing in the console tree and clicking Refresh, will refresh the lists.

 **Add new...(DID Route)**

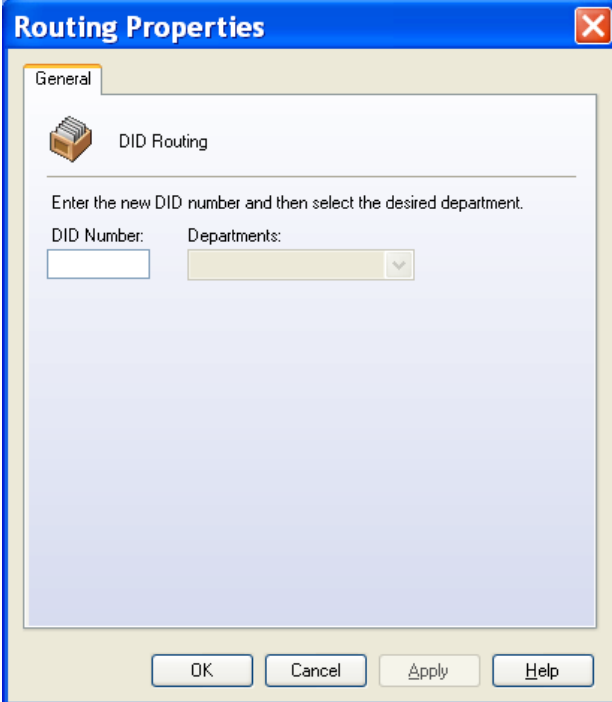
Clicking Add new...(DID Route) in the Action Pane, or right-clicking on Inbound Fax Routing in the console tree and clicking Add new...(DID Route), will open the properties dialog to create a new DID Route entry.

Select an entry and additional options will appear in the Action Pane, or right-click an entry and these options appear in the context menu. Double-clicking an entry will open the property dialog for that entry. The Line Routing list allows multi-selection.

 **Properties** Clicking Properties opens the properties dialog allowing modification of the entry.

 **Clear/Delete** When a Line Route is selected, the function Clear is available. This will remove the department entry for the selected line(s). When a DID Route is selected, the function Delete is available. This will delete the selected entry.

Add a New DID Route

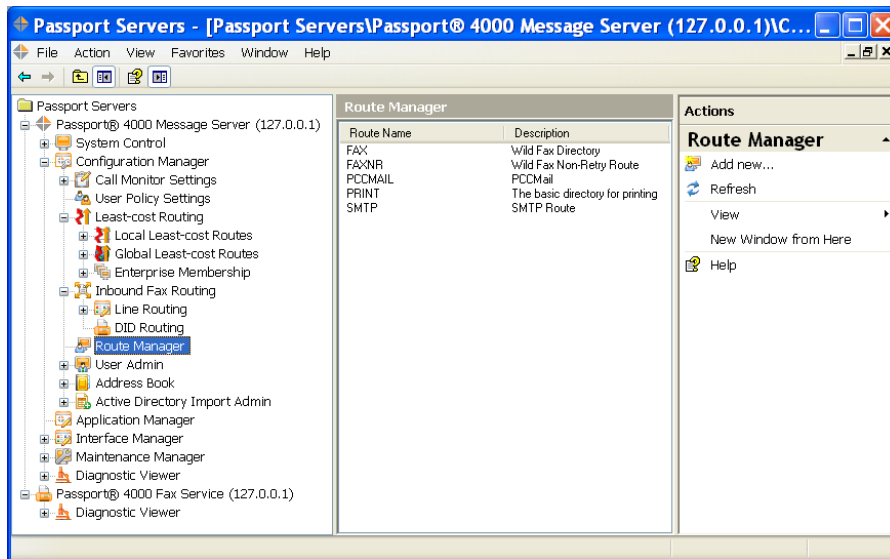



The image shows a dialog box titled "Routing Properties" with a close button (X) in the top right corner. The dialog has a "General" tab selected. Inside the dialog, there is a "DID Routing" section with a telephone icon. Below this, there is a text prompt: "Enter the new DID number and then select the desired department." There are two input fields: "DID Number:" followed by a text box, and "Departments:" followed by a drop-down menu. At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Help".

On the Line Routing properties page, first enter the number to be routed in the DDI number field. Then, select the department to be assigned to the line(s) from the drop-down list.


Then select either **OK** or **Apply** to set the changes.


Route Manager




 Use the Route Manager snapin to create and maintain routing objects. Routing objects are used by Passport® to route documents to destinations. A routing object defines a protocol and communication port to use, destination specific information, and options for reporting the status of the delivery attempt.


Operations

 **Refresh** Clicking **Refresh** in the Action Pane (or right-clicking on Route Manager in the console tree and selecting Refresh) will refresh the lists.

 **New Routing Object** Clicking **New Routing Object** in the Action Pane (or right-clicking on Route Manager in the console tree and selecting **New Routing Object**) will open the properties dialog to create a new route object.

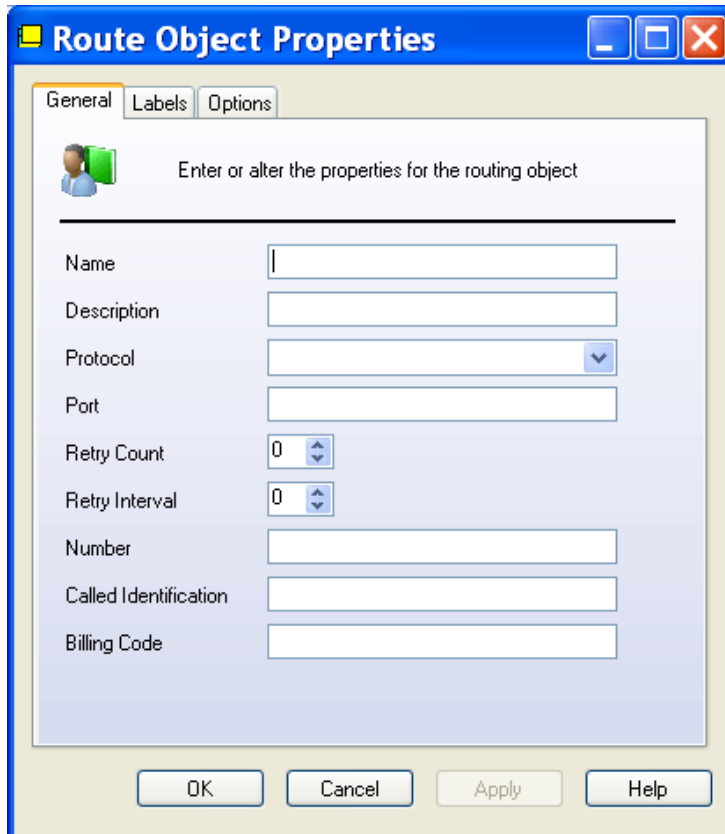
Once an entry has been selected, additional options will appear in the Action Pane (or when right-clicking an entry, in the context menu). Double-clicking an entry will open the property dialog for that entry.

 **Modify** Selecting **Modify** opens the properties dialog allowing modification of the entry.

 **Delete** When a routing object is selected, the function **Delete** is available. This will remove the routing object from the system.

Route Object Properties

General



The screenshot shows a Windows-style dialog box titled "Route Object Properties" with a blue title bar. It has three tabs: "General", "Labels", and "Options", with "General" selected. The main area contains a header with a person icon and the text "Enter or alter the properties for the routing object". Below this is a list of fields: "Name" (text box), "Description" (text box), "Protocol" (dropdown menu), "Port" (text box), "Retry Count" (spin box with value 0), "Retry Interval" (spin box with value 0), "Number" (text box), "Called Identification" (text box), and "Billing Code" (text box). At the bottom are four buttons: "OK", "Cancel", "Apply", and "Help".

Name - The name of the routing object. This is the name you will see in most lists. (Required)

Description - A more detailed description of the routing object.

Protocol - The protocol that will be used by the routing object when sending documents. (Required)

Port - The port that will be used when sending the document. (Required)

Retry Count - The number of times a transmission will be attempted before a failure is declared.

Retry Interval - The number of minutes to wait between transmit attempts.

Number - The number to call or other delivery information to use when connecting to the destination.

Called Identification - Information received from the destination to verify a valid connection.

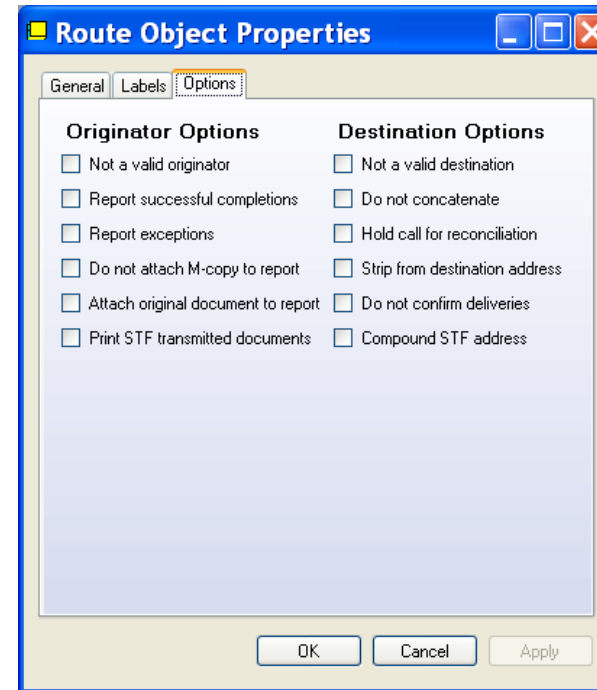
Billing Code - Accounting information that will be applied to a successful transmission

Labels



Label fields allow for the entry of information that is unique to the specific routing object. The type of information varies with the object type, the destination, the type of communication lines, etc. You will need to contact Lane Support for a definition of the fields required for your particular installation.

Options



Originator Options

Not a valid originator - This option designates a routing object that cannot be used as the originator of a message.

To insure that only authorized users are sending traffic through the message server, originator checking should be enabled. This is accomplished through a setting in the STF parameters. By default, any directory that exists is a valid originator. Selection of the invalid originator option will cause this directory to fail the originator check. Messages that fail this check are sent to the exception processor.

Such a code may still represent a valid destination.

Report successful completions - This option instructs Passport to send to the originator a report that his message was successfully transmitted. Normally a delivery notice is not generated for a successful completion. Because delivery problems are reported, the lack of a notice implies success. However, some system users like to be informed of all deliveries. Selection of this control word option will cause a report to be generated and sent to the originator for all successful transmissions.

Report Exceptions - Delivery problems, called exceptions, are normally reported through the exception process and handled by a message server operator. However, some system users like to be informed of problems so they can use their own recovery methods. Selection of this control word option will cause an exception report to be generated and sent to the originator for all delivery problems.

When this option is selected, exception processing on the message server is bypassed

Do not attach M-copy to report - Normally a copy of the transmitted message is attached to successful delivery reports. The wording of the delivery report shows the successful delivery date and time as well as the original text name. This may be sufficient for some users.

Attach original document to report - If this option is enabled, a copy of the original document will be attached to the delivery report.

Print STF transmitted documents - This option is used in an originator's directory entry to specify that transmissions from that originator are to be printed, thus possibly overriding global settings to the contrary. This might be used in an environment where the message switching center has the responsibility for maintaining a full hard-copy audit trail for certain originator's messages, but not others.

Destination Options

Not a valid destination - This option is used to designate an address code which cannot be used as a destination. Such a code may still represent a valid originator. Use of this directory in a message will force that message into exception processing.

Do not concatenate - This option will suppress the normal operation of the Store-and-forward system which combines all destination codes, that have a common routing into a single transmission. Normally, this combination, or concatenation as it is called here, would eliminate the sending of the same message multiple times to a single destination. However, in some cases it may be necessary for each addressee to have a complete transmission of the message. This could be the case, for example, if several destination codes were routed to a single common printer. You would suppress concatenation so that each recipient of a message would have an individual copy printed out.

Hold call for reconciliation - This option is used when the destination is accessed via another Store-and-forward switch or a communication service. In such situations, the successful transmission of a message to the other switch does not guarantee that the message will be successfully transmitted to its final destination. This option will hold the call until a delivery report is received from the distant switch indicating that the final transmission was completed. Note that this option is only effective when used with customized message reconciliation options, which are available on special order.

Strip from destination address - This option is used to suppress the inclusion of this destination's address code from the addressing portion of the transmitted message. This

option is effective only if the global STF parameters are set to enable address stripping. This option might be used when sending to certain types of destination systems that do not tolerate the inclusion of this type of addressing information.

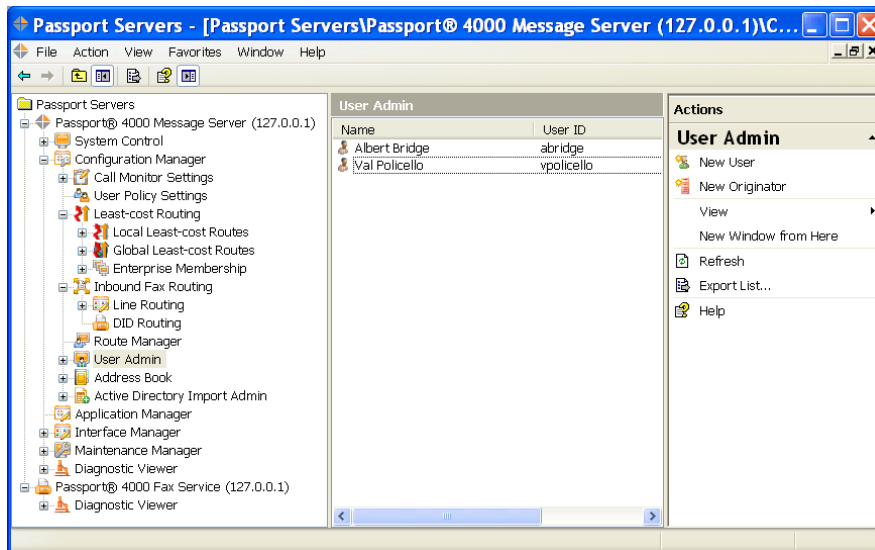
Do not confirm deliveries - This option is used to suppress any confirmation messages for messages sent to this destination. This might be used if the destination system will provide its own acceptance or delivery message back to the originator.

If this message server is directly connected to another message server or switch, care must be taken in how confirmation messages are handled. Typically, STF messages, which delivery notices are, are not sent out the communication port that they were received on, if that port is connected to another switch. This prevents the ping-pong effect that can occur when switches process messages that have destination codes that point to the other switch and those codes are not stripped or recognized as originating from another switch. If the other switch is capable of handling this type of situation, and confirmation notices are desired, then this option must be selected.

Compound STF address - This option is used to designate a special form of addressing, which is generally passed on to another message switching system. A compound address is a full text line of addressing information that will be handled by the other switch. The primary address code (i.e. the first




mnemonic in the line) is used merely to tell this system how to access the other system. The remainder of the line is used only by the other system. Such an address scheme could be used to pass addresses that are "wild" in the other system. If the Strip from destination address option is also selected, then the addressing line passed onward will consist of the remainder of the original compound address, less the primary address code, otherwise the onward address line will include the entire original address line.

User Admin





Use the User Admin snap-in to create and manage user profiles..

Operations

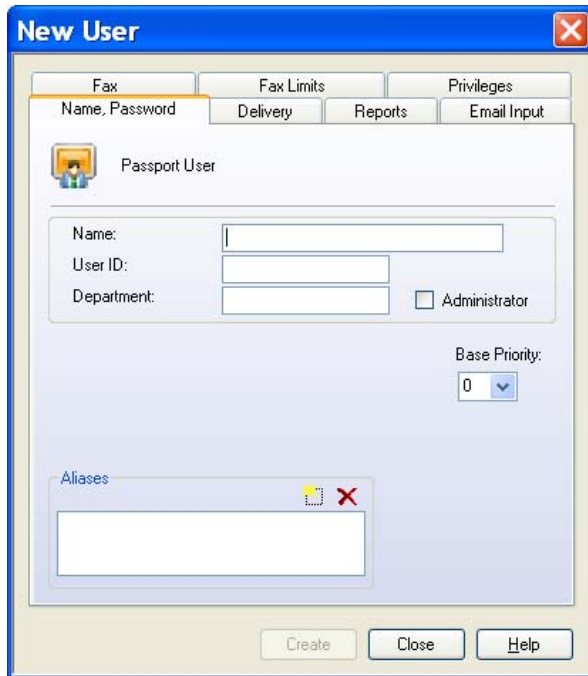
-  **Refresh** Clicking Refresh in the Action Pane, or right-clicking on User Admin in the console tree and clicking Refresh, will refresh the list of users.
-  **New User** Clicking New User in the Action Pane, or right-clicking on User Admin in the console tree and clicking New User, will open the properties dialog to create a new entry.
-  **New Originator** Clicking New Originator in the Action Pane, or right-clicking on User Admin in the console tree and clicking New Originator, will open the properties dialog to create a new entry.

Select an entry and additional options will appear in the Action Pane, or right-click an entry and these options appear in the context menu. Double-clicking an entry will open the property dialog for that entry.

-  **Properties** Clicking Properties opens the properties dialog allowing modification of the entry.
-  **Delete** Clicking Delete removes the entry. You are asked to confirm this operation.

Adding a New User

Name and Password



You get here by clicking **New User**, selecting an originator and clicking **Properties**, right-clicking a User and clicking **Properties**, or double clicking on a user.

- Name** You enter a descriptive name for the user in the Name field
- User ID** You enter the user ID in the User ID field, this should be the users network logon ID. If you are editing an existing user, you will not be allowed to change this field.
- Department** You enter the department (business unit) that this user is a member of.
- Administrator** You check this box to make this user an administrator for this department.
- Password** You enter the initial password for this user.
- Expiration Date** You enter the date the password will expire in the format given.
- Psw Failures** You initially set this box to zero. Later, this box may indicate the number of times this user has entered an incorrect password.
- User Is Suspended** You check this box to suspend a user, or uncheck it when the system has suspended a user and you wish to allow them access. Be sure to also set the Psw Failures back to zero.

Base Priority You set this to the default priority to be assigned to this users messages.

Aliases You enter alias names this user is known by in this field.

To enter an Alias, you click on (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click (delete)

Route

You select the route from the routes in the drop-down list.

Address

You enter the appropriate address for the route selected.

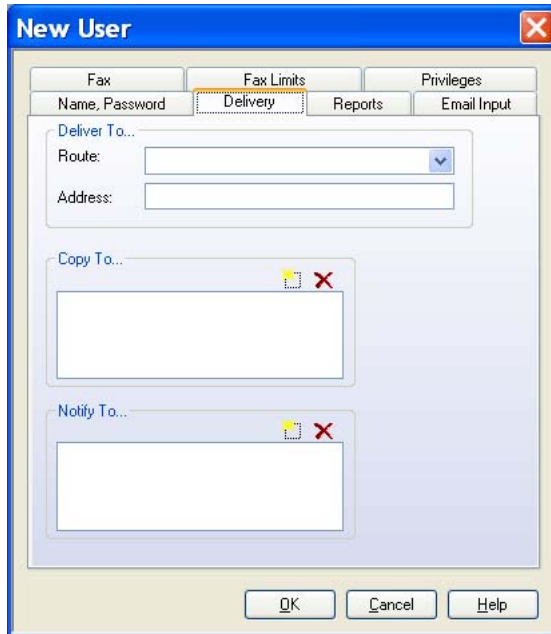
Copy To...

You enter additional destinations that will receive a copy of the messages. To enter a Copy To address, you click on (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click (delete).

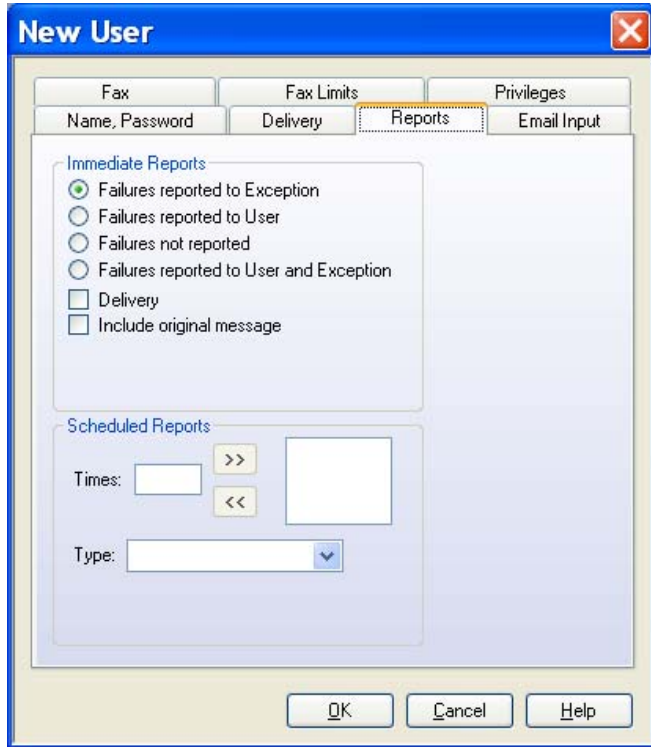
Delivery

Notify To...

You enter additional destinations that will receive a delivery notification. To enter a Notify To address, you click on (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click (delete).



Reports



Failures reported to Exception You check this option to force failures into the exception queue.

Failures reported to User You check this option to have failures returned to the user.

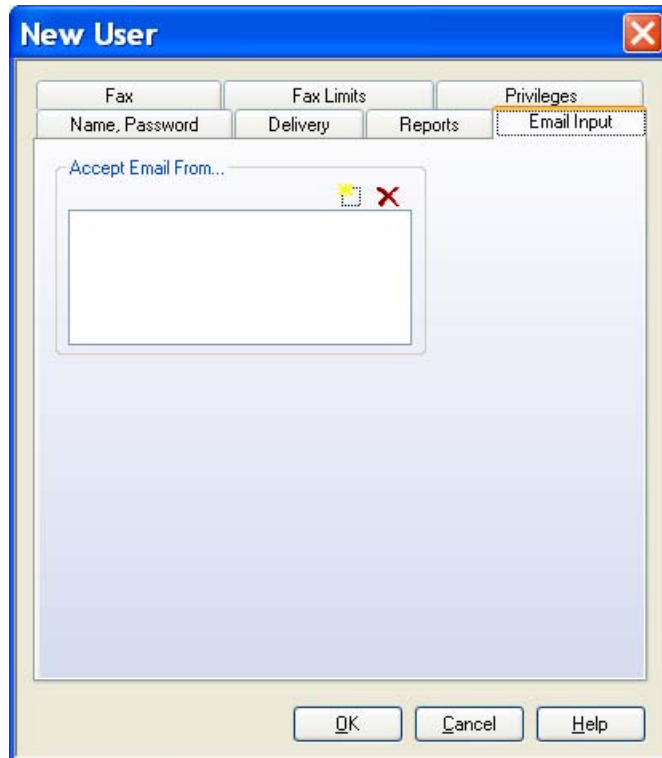
Failures not reported You check this option to not report any failures.

Failures reported to User and Exception You check this option to have the failures reported both to the user and put in the exception queue.

Delivery You check this option to receive delivery completion notices.



Include original message You check this option to include the original text, as opposed to the transmitted copy, in the delivery notices.

Email Input



Accept Email From...

If a user is sending messages to PASSPORT from their email account for onward delivery, then their email account may be verified against the user. One or more valid email addresses may be added for any user.

To enter an email address, you click on  (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click  (delete).



Fax



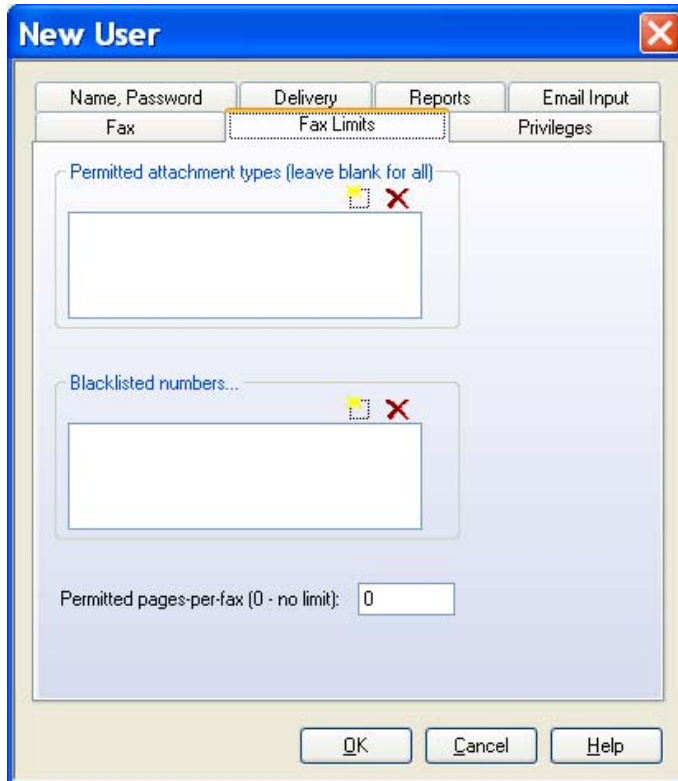
DTMF ID/Psw You define the Users ID and Password, which will be required when routing messages through the system from a fax machine in the fields provided.

Default Cover Sheet You select the default from the list of coversheets in the drop-down box.

DTMF/DID Routing Code(s) to send to this user Each user may be allocated multiple numbers on which to receive fax messages. When using this number the fax will automatically be delivered to the user without manual intervention.



To enter a routing code, you click on  (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click  (delete).

Fax Limits





Permitted attachment types

You enter here a list of attachments types (extensions) that this user is allowed to send. Unless there are special circumstances, this area should be left blank.

To enter an attachment type, you click on  (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click  (delete).

Blacklisted numbers...

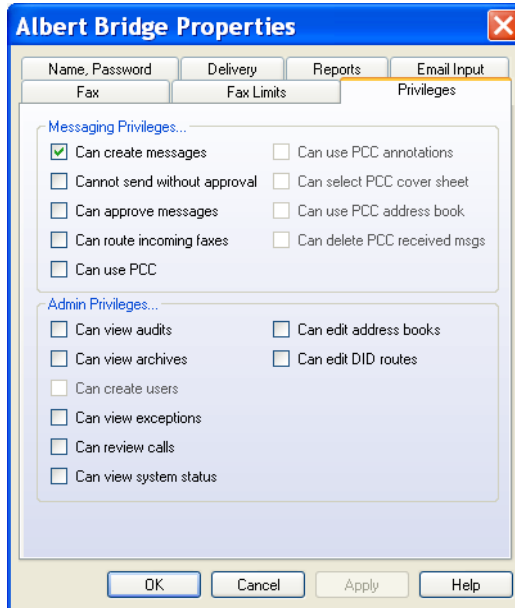
You enter here any fax numbers that this user is not allowed to send to.

To enter a blacklisted number, you click on  (new entry) and enter the information in the box indicated by the cursor. To delete an entry, select that entry and click  (delete).

Permitted pages-per-fax

You can use this field to limit the number of pages per message a user is allowed to send.

Privileges



Can create messages

You check this box if the user is allowed to create messages.

Cannot send without approval

You check this box if the user is not allowed to send messages without another user having authorized it.

Can approve messages

You check this box if the user is a message approver.

Can route incoming messages

You check this box if the user is allowed to route inbound fax messages.

Can use PCC

You check this box if the user is allowed to use the Personal Communications Center application.

Admin Privileges...

Can view audits

You check this box if the user is allowed to view the message audit files.

Can view archives

You check this box if the user is allowed to view the message archives.

Can create users

You check this box if the user is allowed to create other users.

Can view exceptions

You check this box if the user is allowed to view the exception queue.

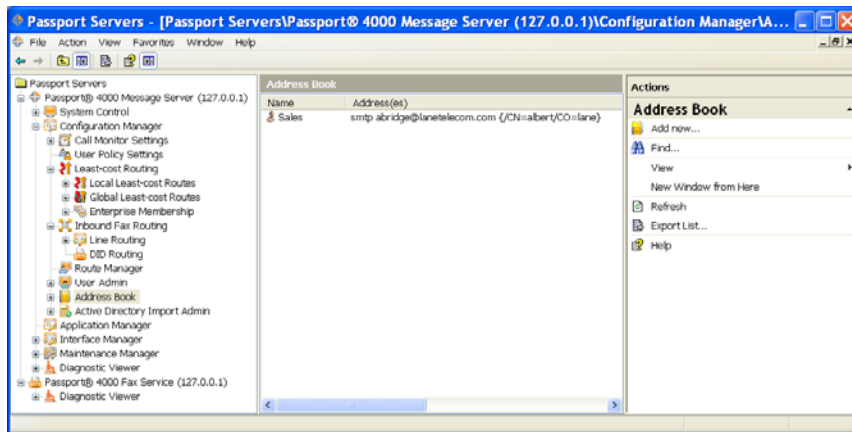
Can review calls


You check this box if the user is allowed to view the review queue.

Can view system status

You check this box if the user is allowed to use the Status application.

Address Book



 Use the Address Book snap-in to create and maintain the Address Book.

Refresh

Clicking **Refresh** in the Action Pane, or right-clicking on Address Book in the console tree and clicking **Refresh**, will refresh the list.

Add new...

Clicking **New Entry...** in the Action Pane, or right-clicking on Address Book in the console tree and clicking **New Entry...**, will open the properties dialog to create a new entry.
See [Address Book Properties](#) for more details.

Select an entry and additional options will appear in the Action Pane, or right-click an entry and these options appear in the context menu. Double-clicking an entry will open the property dialog for that entry.

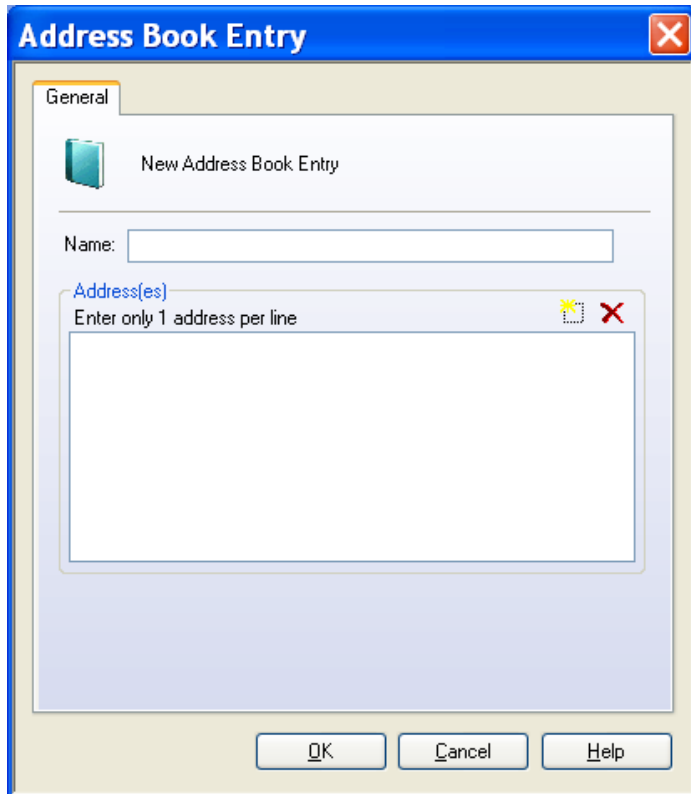
Properties

Clicking **Properties** opens the properties dialog allowing modification of the entry.
See [Address Book Properties](#) for more details.

Delete


Clicking **Delete** removes the entry. You are asked to confirm this operation.

Adding an Address Book Entry




General Name

You enter the name of the Address Book Entry in this field. This is only visible for new address book entries. This field may only contain letters, numbers, and hyphen.

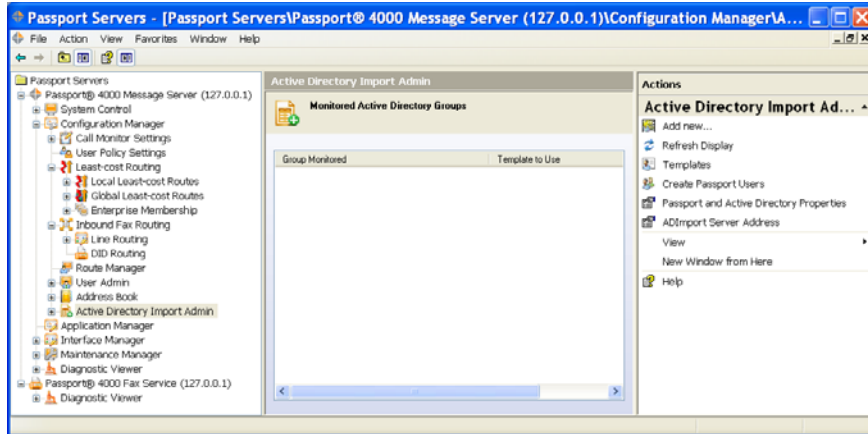
Address(es) To enter an address, you click on  (new entry) and enter the information in the box indicated by the cursor.


The addresses entry may consist of one to 4096 lines, with each line designating an individual destination. Each destination member may be entered as a 'wild' route and address pair, a 'non-wild' route, or another address-book name. For addresses entered as a 'wild' route and address pair, the route is verified to exist, but not verified to actually be a 'wild' route. The addresses may only contain letters, numbers, and certain punctuation characters known to be allowed in Passport addressing.

There must be at least one address entry to be able to save the address book.







To delete an address, select that address and click  (delete).


Active Directory Import Admin




 Active Directory Import creates Passport users from Active Directory users. Templates of Passport properties are created and assigned to Active Directory groups. Periodically, the groups will be scanned for users and those users will be imported as Passport users with properties as defined by the associated template.

The primary display of the ADImport process shows a list of Active Directory groups that have been selected for monitoring and the templates that have been assigned to each group. On the right side of the display is a list of functions available for ADImport.

-  **Add New** Add a new Active Directory group to monitor and assign a template to the group
-  **Refresh Display** Refresh the primary display
-  **Templates** Create, modify, or delete templates
-  **Create Passport Users** Force an immediate scan of all monitored Active Directory groups and create Passport users from all users found within the Active Directory groups. If the user already exists within Passport, the “create” will be skipped.
-  **Passport and Active Directory Properties** Define to ADImport the location and logon parameters of Active Directory and Passport. The scan frequency is also specified in this function
-  **ADImport Server Address** Define the location of the ADImport server. Typically it would be co-resident with Passport, but that is not necessary.

 **Properties** This function is only available when a group is selected from the list. Used **Properties** to change the template assigned to the group.

 **Delete** This function is only available when a group is selected from the list. It will delete the group from the monitor process.

The importation of Active Directory users is a one time process. Once a user is defined within Passport, the properties of that user will not be altered by ADImport. Changes to template properties and assignment of templates will not cause a change to a Passport user. However, if a Passport user is deleted and that user is still a member of a monitored Active Directory group, the user will be re-created within Passport upon the next scan.

When a user is found to be a member of two or more groups being monitored, the create process will merge the properties of the different groups and assign them to the new user.

North and South America
LANE Telecommunications, Inc.
Tel: +1 973 526 2979
Fax: +1 973 526 2988

United Kingdom and Europe
LANE Telecommunications Ltd.
Tel: +44 (0) 1256 301550
Fax: +44 (0) 1256 301555

Singapore and Asia
LANE Telecommunications, PTE.
Tel: +65 6353 0555
Fax: +65 6353 7448