Sterling Integrator®

Mailbox

Version 5.1

Sterling Commerce
An IBM Company

Contents

Getting Started with Mailbox

Overview of Mailbox Feature

Often, it is necessary to stage data passing between internal systems and external trading partners. Sometimes data is produced by internal systems when trading partner systems are unavailable. Other times requests are received from trading partners outside of processing windows. Processing windows (time frames) are created to accommodate system constraints, such as scheduled maintenance, or business constraints. For example, it may be preferable to delay transmission of payments to the latest date possible. Regardless of the business-to-business protocols, or the application or technology adapters involved, a need exists to store messages and documents for processing at a later time.

While this sort of staging and scheduling of data transmission is present to varying degrees in numerous applications and infrastructure components, businesses have found it beneficial to centralize the definition, operation, management, and control of this staging and scheduling. In this application, these capabilities are centralized in the Mailbox.

Quick Tour

The Mailbox feature is a secure business document repository with a store-and-forward communication infrastructure. It adds the facilities necessary to conveniently build B2B electronic commerce communities. In addition, it provides a trading partner browser interface called the Mailbox Browser Interface (MBI). No special software is required when the Mailbox feature is deployed to an electronic trading community. The MBI is secure and simple to use, requiring no special user training.

Although Mailbox can be used with any communication or B2B protocol service available in this application (such as EDIINT AS1, SMTP or HTTP), for convenience, it has been tightly integrated with AS2, the EDIINT service, and the HTTP/S communications adapter. You can configure the application to use Mailbox to stage documents for internal processing, while using the AS2 protocol for secure Internet-based document transport. This feature provides a scalable and functional alternative to the File System adapter with AS2. The existing AS2 Setup wizard has been enhanced to support use of mailbox in addition to the existing file system.

Mailbox also supports automated, scheduled, and manual processing of business documents using routing rules. Routing rules provide a powerful and easy-to-use mechanism for controlling document routing. Additionally, Mailbox is easily combined with native applicaton capabilities such as business processes, document translation, B2B protocols, and back end system integration.

Business documents stored in Mailbox are called *messages* and can contain business content in any format such as binary, EDI, or XML. Each message is assigned an extraction policy that specifies the rules for extracting messages from a mailbox. For example, you add a message to a mailbox and process it immediately, or process it at any scheduled time in the future.

Mailbox provides a hierarchical, OS platform-independent business document repository. It therefore offers storage, organization, and management advantages over the use of a file system. The repository provides many capabilities including support for relative mailbox paths (virtual roots) and a dead letter mailbox. The repository also provides efficient document storage. For example, multiple mailboxes containing the same message share a single copy of the message.

A management user interface provides easy management of existing mailboxes and routing rules.

Finally, the Mailbox uses the application's logging, state management, monitoring, and archiving capabilities, providing a truly integrated mailbox solution.

Mailbox System Components

The system components and features of the Mailbox feature are:

Component	Description
Mailbox	A storage area for business documents and provides an administrative hierarchy that is easy to manage and understand. System users have access to their documents, while administrators can organize and manage documents across all mailboxes. Mailboxes form a hierarchy. The top of the hierarchy is called the root mailbox and is denoted by a slash (/). Mailboxes can support sub-mailboxes. This organizational concept is referred to as a mailbox hierarchy.
Dead Letter Mailbox	Stores messages that cannot be added to a particular mailbox. The primary role of this mailbox is to provide temporary data storage until the administrator can correct the problem.
Message	A document existing in a mailbox. A message is assigned to a mailbox with a name and timestamp. Mailboxes are acted upon by business processes using services, which provide the ability to add, extract, query, and delete messages.
Mailbox Access Controls	Enables the system administrator to assign mailbox privileges to groups and users. Users who have the appropriate permissions in a mailbox can view, add, delete, and extract messages from the mailbox (using the Mailbox Browser Interface) and can run business processes acting upon the mailbox.
Global Permission Settings	Mailbox Administrators, by default, have global privileges that enable the execution of operations across all mailboxes. The Mailbox Global Delete and Mailbox Global Query permissions are two such global privileges. For example, a Mailbox Administrator can delete a mailbox because they have the permission Global Mailbox Delete. When necessary, Global permissions can be granted to other users and groups.

Component	Description
Mailbox Virtual Roots	A mailbox associated with a trading partner. Every mailbox referenced by that user is evaluated relative to that user's virtual root. For example, if the user's virtual root is **/Customers/Central/Dallas Hardware** and the user runs an action to add a message to mailbox **/Inbound**, the actual mailbox designated by the action will be **/Customers/Central/Dallas Hardware/Inbound**. With the virtual root defined there is no need to notify this trading partner when a change is made to the hierarchy – as long as the administrator updates the trading partner's virtual root.
Mailbox Browser Interface (MBI)	Enables Internet users to access their mailboxes from a standard Web browser. Users can send messages to, retrieve messages from, and search messages in any mailbox for which they have permissions. The MBI also enables users to change their account password. The Mailbox Browser Interface is a Web application, and therefore requires only a Web browser. No proprietary client software is required.
Scheduled Batch Processing	Documents are collected from internal systems and external trading partners. All documents are processed together on a schedule, such as at the end of the day or week. For example, in Automated Clearing House (ACH) handling in the banking industry, messages containing transactions are received during the course of a day and placed into one or more mailboxes. At the end of the day, all transactions are processed. Same-bank transactions are processed internally. Transactions with other banks are sent out for processing.
Asynchronous Document Processing	A hub may provide a trading partner with an inbound mailbox. The trading partner may submit documents containing EDI transactions to that mailbox, where the document is processed. Each submission is processed one time. For example, an electronics supplier wants to process purchase orders as soon as they arrive. The electronics supplier instructs its trading partners to send purchase orders to a mailbox. When orders arrive, a business process extracts the order from the mailbox and passes it to a back-end application for order processing.
Document Publishing	Documents, such as a product catalog, may be published using a mailbox. Authorized trading partners retrieve the document using a browser-based, secure interface. After a period of time, the document expires and is no longer available for retrieval. The following scenarios illustrate ways to publish documents to a mailbox. ◆ A hardware supplier publishes a price list for a sale to their trading partners. The hardware supplier places the price list in a mailbox and grants trading partners access to the mailbox. The price list can be extracted (downloaded) until the end of the sale. ◆ An insurance company publishes a document of all claims processed for its clients of the past year. The company adds the claim detail to the mailboxes of the individual clients and allows clients to extract claim details for one year.
File Copying	Files can be copied to and from the Mailbox through the Connect:Direct Server adapter or the FTP Server adapter.
Routing Rules	Initiate action automatically when a message is added to a mailbox.

Integrating Mailboxes with Your Application

Integrating Mailboxes with Services

You can integrate the Mailbox feature with any application service or adapter by designing business process models using the Graphical Process Modeler. In addition, Mailbox provides ready-to-use integration with the EDIINT AS2 protocol. This support is provided through special pre-built business process models and an enhanced AS2 Setup Wizard.

The FTP Server adapter is tightly integrated with the mailbox subsystem. The Connect:Direct Server adapter can be used to copy files to and from the Mailbox.

Integrating Mailboxes into Business Processes

You have several options when integrating mailboxes with the rest of the application. One option is integrating the mailboxes with business processes. There are two primary methods you can use:

- Invoking the Mailbox services from a business process
- Specifying an application business process using a routing rule

Integration Examples

Following are examples of how you can integrate the mailbox into application business processes:

Integration Type	Example
Event-Driven Integration	You can use the mailbox for event-driven near real-time integration. Set up an automatic routing rule that searches a specific mailbox for a message name pattern. When the routing rule is evaluated, the message in the designated mailbox is matched, and a designated application business process is triggered. The business process can access the contents of the message and perform automation functions like back-end systems processing or notification to an interested party. Event-driven processing is useful when your business requirements dictate that documents arriving in a mailbox should be processed as soon as possible after arrival.

Integration Type	Example
Time-Driven Integration	You can use the mailbox for time-driven integration with your business processes. To do this, set up a business process that runs on a time schedule and uses the Mailbox Query service to search the mailbox for specific message criteria. When matching messages are found, the next step in the business process is started. The business process can do anything with the matched message, such as extract it and pass it to another application or notify a person that the message is available for them. This application of the mailbox is useful where scheduled processing is important such as end of month payments. Messages received in the mailbox are processed at the next scheduled run of the business process.
Document Publishing	You can use the mailbox to publish documents for a specified period of time. Create a business process to add a document to a mailbox and set the extract policy ExtractableUntil, specifying the date you want the document to expire. Give permissions to this mailbox to anyone that will view the document. Users can extract the document until the date you specified has passed. A common application of this is making a catalog available to customers, until the catalog expires.

Mailbox Services

Following are the Mailbox services.

- *Mailbox Add Service*
- *Mailbox Extraction Services*
- *Mailbox Query Service*
- *Mailbox Delete Service*
- *Mailbox Delete Mailbox Service*
- *Mailbox Scheduled Delete Service*

Mailbox Add Service

The Mailbox Add service enables you to add messages to a particular mailbox. The service enables the specification of a message name, the mailbox where the message should be added, and the extraction policy. Before the Mailbox Add service runs, it verifies a user's permission to use a mailbox.

One of three extraction policies is assigned to a message when it is added to a mailbox. These policies control when extraction of a message is allowed. The following table describes the extraction policies:

Policy	Description
Extract a limited number of times	Carries a count, which is reduced each time the document is extracted. Following are two ways you can use this policy: ◆ When the count is one, the message is like a normal letter placed into a drop-box. After the message is extracted once, it is no longer available. ◆ When the count is greater than one, the message is available to multiple users. The extraction succeeds, but after the count goes to zero, no one can extract the message.
Extractable until some future date	Enables extraction until the date is reached and disables extraction after the date is passed. This policy is like a coupon that expires on a certain date.
Extractable (or not) until further notice	Enables or disables all extractions until an administrator changes the policy.

Mailbox Extraction Services

Extraction is the term for reading a message from a mailbox, typically into the primary document of a business process. Extracting a message within a business process consists of two steps:

1. The Mailbox Extract Begin service verifies permissions, availability and extractability. If the operation is allowed, the data is provided to the business process.
2. After the business process has finished processing the data, the extraction can be completed by invoking either the Mailbox Extract Abort service or the Mailbox Extract Commit service. If there is an error after the Mailbox Extract Begin service, the Mailbox Extract Abort service is invoked, which restores the extractable count to the original value as if the Mailbox Extract Begin service never took place. If no errors occur, the Mailbox Extract Commit service is invoked, which formally completes the extraction.

If business processes do not need this failure handling, you can combine the Mailbox Extract Begin service and the Mailbox Extract Commit service into a single service by setting a parameter in the Mailbox Extract Begin service.

When a business process executes the Mailbox Extract Begin service, a message “hold” table tracks the processing of a message by a particular business process. Access to a message is controlled by the extraction policy.

It is possible that a user begins to extract a message, but then decides that it is not possible to process the document. For example, a business process may extract a message and send it to a trading partner over the network. If the transfer fails, the extraction does not succeed (to prevent one of the limited copies of the message from being extracted).

Mailbox Query Service

The Mailbox Query service enables you to select a similar grouping of messages. For example, a user can use the Mailbox Query service to find messages added between two dates. A user must have permission to query a mailbox.

The Mailbox Query service supports multiple parameters, including:

- Mailbox path
- Message name pattern
- Message ID
- User ID
- Start date and time
- End date and time
- Messages extractable
- Order by
- Ascending/descending

Mailbox Delete Service

The Mailbox Delete service enables you to remove outdated or obsolete messages. This service supports a parameter list similar to that of the Mailbox Query service. The user must either have permission on each of the mailboxes, or must have the mailbox global delete.permission, which allows the holder to delete messages from any mailbox.

Mailbox Delete Mailbox Service

The Mailbox Delete Mailbox service enables you to delete one or multiple mailboxes, as well as the associated submailboxes, messages, virtual roots, routing rules, and permissions. It is designed to completely and permanently remove mailboxes and everything associated with them. The Mailbox Delete service differs from the Mailbox Delete Mailbox service in that it deletes only *messages* in mailboxes.

You can either delete mailboxes interactively, through the application interface, or at a decision point in a business process, using the Mailbox Delete Mailbox service in a business process.

To delete mailboxes interactively:

1. Go to **Deployment** > **Mailboxes** > **Configuration**.
2. Next to List ALL, click **Go!**
3. Click the delete icon.
4. You have the option to view a report of what was deleted.

Mailbox Scheduled Delete Service

The Mailbox Scheduled Delete service can delete mailbox messages meeting criteria consisting of:

- Message name pattern
- Mailbox
- Extractability status
- Message age

For example, it is possible to create a configuration of the Mailbox Scheduled Delete service to periodically delete all messages more than a week old.

As with all scheduled services for this application, the Mailbox Scheduled Delete service can be configured to run once at a specified date and time, or periodically, such as once a month or twice a week.

Routing Rules for Mailboxes

You can create routing rules to initiate action automatically when a message is added to a mailbox. Automatic routing ensures that the rule is evaluated at least once. When a message is added to a mailbox, any rules established for the Mailbox are evaluated automatically. After evaluating automatic routing rules, the application starts any business processes that the rules are configured to run. The rules do not wait for the business processes to complete. After all routing rules run (according to defined schedules), the messages added to any mailbox since the last automatic routing rule evaluation are removed from the “needs to be routed” table. After messages are removed from that table, they are never again eligible for auto routing.

Manual and scheduled evaluation route all messages that meet the pattern of the rule to be evaluated. If a message is in a mailbox and is included in a rules pattern, that message is routed every time the rule is evaluated.

Manual and scheduled evaluation do not provide a guarantee that message will be delivered at least once. Routing usually occurs once, but if a system outage occurs, the routing does not resume at system start. If you restart the application, the business processes that were started may need to be restarted, depending on whether the processes are restartable or resumable.

After the application evaluates a routing rule, the routed messages are guaranteed to be processed by the routing rule business process.

Routing Rule Pattern and Action

Routing rules consist of two parts: a pattern to specify when the rule applies, and an action to be performed. Routing rules contain string patterns used to match message names. This string can contain wildcard characters. You can restrict the application of the rule to specific mailboxes. When a message name matches the string pattern of a rule, the rule triggers the execution of a designated application business process. That process can perform any processing, including extraction of the message and integration with back-end systems or a notification action. For example, a routing rule may trigger a business process that pages an administrator whenever a message arrives in the Dead Letter mailbox.

Routing Rule Evaluation Modes

A routing rule evaluation mode is used to define when the rule is evaluated. You establish the evaluation mode when you define the routing rule. There are two routing rule evaluation modes—Automatic and Manual.

Automatic routing rule evaluation is carried out by the Mailbox Evaluate All Automatic Rules service. It is a scheduled service, and its frequency is controlled through the application interface. Messages are eligible for automatic evaluation only once as they are added to a mailbox.

All messages are always candidates for manual evaluation of routing rules. A message may be routed multiple times if a routing rule is manually evaluated repeatedly.

There are three ways to manually evaluate a routing rule:

- A routing rule can be manually evaluated within a business process by calling a configuration of the Mailbox Evaluate Routing Rule service.
- A routing rule can be manually evaluated by a scheduled configuration of the Mailbox Evaluate Routing Rule service.
- A routing rule can be manually evaluated interactively through the application interface.

Adjusting the Evaluation Frequency

An administrator may want to reduce the frequency with which mailbox routing rules are evaluated in order to reduce the overhead of the system resources that are consumed each time a service is invoked. Evaluation of the routing rules involves database queries followed by the start of various business processes, as specified in the routing rules. An administrator can balance the need for timely routing of messages against the overhead of the routing process.

Note: Frequency adjustment pertains only to the evaluation of automatic routing rules—not to routing rules, in general.

To adjust the evaluation frequency:

1. From the **Deployment** menu, select **Schedules**.
2. Search for the MailboxEvaluateAllAutomaticRules schedule and click the **edit** icon.
3. Redefine the frequency for routing rule evaluation.

Evaluating a Routing Rule at a Different Frequency

If you have a routing rule that you want evaluated at a different frequency than that of the Mailbox Evaluate All Automatic Rules service, you may use the Mailbox Evaluate Routing Rule service to allow a business process to evaluate a routing rule. This service is schedulable.

The minimum configurable routing interval is one minute (as determined by the application’s scheduler).

To evaluate a routing rule at a different frequency:

1. Create a configuration of the Mailbox Evaluate Routing Rules service that evaluates the appropriate routing rule, and set its schedule to the frequency you want.

   The schedule is configurable from the service definition page.
2. Add this Mailbox Evaluate Routing Rules service configuration to your business process.
3. Designate the routing rule to be evaluated at a different frequency as a manual routing rule, so that it will not be evaluated by the Mailbox Evaluate All Automatic Rules service.

Creating a Routing Rule

When a routing rule is evaluated, Mailbox searches the mailboxes defined in the rule for message names that match the pattern defined in the rule. When a match is found, the routing rule notifies the business process or contract specified in the routing rule. Depending on how the business process is defined, it may extract and process the message, extract the message and pass it to another application for processing, or notify another application to extract and process the message.

If routing rules are set to be evaluated manually, they can be evaluated by a user or a business process.

Use the following procedure to create a routing rule:

1. From the **Deployment** menu, select **Mailboxes** and **Routing Rules**.
2. In the Create section, click **Go!**
3. Specify a Name for the routing rule. This name must be unique for each routing rule. It is used to identify the routing rule in other parts of the application.
4. In the Rule Application page, select the Evaluation Mode:
   - Evaluate Manually – The rule must be evaluated manually or evaluated using a scheduled business process.
   - Evaluate Automatically – The rule is evaluated every minute.
5. Select the Action Type:
   - Business Process – The rule notifies a business process when a match is found.
   - Contracts – The rule notifies a business process associated with a contract when a match is found.
6. Click **Next**.
7. In the Rule Pattern page, use the arrows to add the mailboxes to the **Selected Mailboxes** list.

   All groups in the **Selected Mailboxes** list are searched by the routing rule. Click the double arrow to add all available groups to the **Selected Mailboxes** list.
8. Specify the **Message Name Pattern** and click **Next**.

   This is the message name or pattern that the routing rule searches for in the mailboxes specified. You can use an asterisk for a wildcard. You must specify a mailbox, a message name pattern, or both.

Note: If you do not specify a mailbox within the routing rule configuration, then upon evaluation, the routing rule is evaluated against all mailboxes.

9. In the Rule Action page, select the associated business process (or filter by name) and click **Next**.
10. In the Run Rule as User page, select the user ID that is associated with the routing rule when it is run.

11. In the **Confirm** page, verify the parameters and click **Finish**.
12. When the system update is complete, click **Return**.

Editing a Routing Rule

Use the following procedure to change one or more routing rule parameters. There are routing rules created by the AS2 wizard. These rules contain the phrase *Routing Rule created automatically by the AS2 Wizard* in the Description column of the search results screen. Editing these system generated rules affects communications with trading partners.

1. From the **Deployment** menu, select **Mailboxes** and **Routing Rules**.
2. Select the routing rule you want to edit using one of the following methods:
   - In the By Mailbox Name field of the Search section, type the mailbox ID associated with the routing rule and click **Go!**
   - In the List section, select the first letter of the routing rule name or select ALL for a list of all routing rules and click **Go!**
3. Identify the routing rule you want to edit and click the **edit** icon in the **Select** column.

   Caution: Rules containing the phrase *Routing Rule created automatically by the AS2 Wizard for xxx* in the Description column are system-generated rules. Editing these rules affects communication with trading partners.

4. In the Rule Application page, select the Evaluation Mode:
   - Evaluate Manually – The rule must be evaluated manually or evaluated using a scheduled business process.
   - Evaluate Automatically – The rule is evaluated with the frequency specified in the Mailbox Evaluate All Routing Rules service.

   Select the Action Type:
   - Business Process – The rule notifies a business process when a match is found.
   - Contracts – The rule notifies a business process associated with a contract when a match is found.
5. Click **Next**.
6. In the Rule Pattern page, use the arrows to add the mailboxes to the **Selected Mailboxes** list.

   All groups in the **Selected Mailboxes** list are searched by the routing rule. Click the double arrow to add all available groups to the **Selected Mailboxes** list.
7. Specify the **Message Name Pattern**.

   This is the message name or pattern that the routing rule searches for in the mailboxes specified. You can use an asterisk for a wildcard. Specify a mailbox, a message name pattern, or both.
8. Click **Next**.
9. In the Rule Action page, select the associated business process (or filter by name) and click **Next**.
10. In the Run Rule as User page, select the user ID to associate with the routing rule when it is run.

11. In the Confirm page, verify the parameters and click **Finish**.
12. When the system update is complete, click **Return**.

Manually Evaluate a Routing Rule

To manually evaluate a routing rule:

1. From the **Deployment** menu, select **Mailboxes** and **Routing Rules**.
2. In the Evaluate Routing Rules section, click **Go!**
3. From the Available Rules list, select the rules you want to evaluate and click the right arrow button to move it to the To Be Evaluated list and click **Next**.
4. Click **Finish**.

   The Update system page opens with an Evaluation Report. To view the message IDs that were evaluated, click the Evaluation Report.

Managing Your Mailbox

Organizing Your Mailboxes

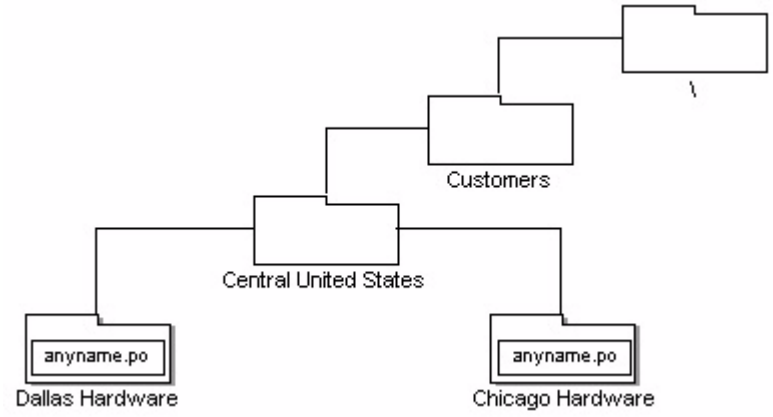
When designing the Mailbox function for your application, you must consider how you will use routing rules and the Mailbox Query service to interact with mailboxes. Routing rules and the Mailbox Query service enable you to search for messages based on mailbox path, mailbox name, and message name. Following are two examples of how routing rules and the Mailbox Query service relate to mailbox organization.

Example 1 – Mailbox Name and Message Name Suffix

Two trading partners, Dallas Hardware and Chicago Hardware, will be sending purchase orders to the mailbox. A routing rule or Mailbox Query service is set up to search for messages in the /Customers/Central United States/Dallas Hardware mailbox and /Customers/Central United States/Chicago Hardware mailbox. They will look for messages with the suffix .po. When matching messages are found, a business process is notified and the Dallas Hardware purchase order is processed.

When the routing rule is evaluated or the Mailbox Query service is run, any messages with the suffix .po that are in the Dallas Hardware or Chicago Hardware mailboxes are identified, extracted and processed by a business process.

The following figure represents a possible organization of mailboxes that uses mailbox name and the message name for routing rules or the Mailbox Query service:

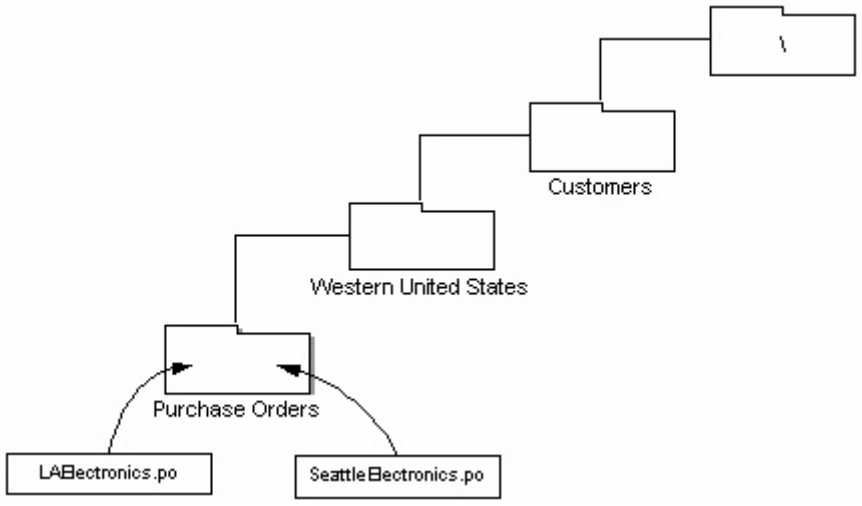


Example 2 – Mailbox Name, Message Name, Message Name Suffix

Two trading partners, Seattle Electronics and LA Electronics, will be sending purchase orders. One routing rule is set up to search for messages in the /Customers/Western United States/Purchase Orders mailbox and will look for messages named SeattleElectronics.po. Another routing rule is set up to search for messages in the /Customers/WesternUnited States/Purchase Orders mailbox and will look for messages named LAElectronics.po. Each will notify a business process.

When the routing rules are evaluated, any messages with the name SeattleElectronics or LAElectronics and suffix .po notify a business process.

The following figure represents a possible organization of mailboxes that uses mailbox name, message base name, and the message suffix for routing rules:



Other Organization Options

There are a variety of ways you can communicate information for using routing rules. This section contains more examples of the type of information you can communicate using mailbox name, mailbox path, and message name.

Mailbox Name

The application provides the capability to build nested mailbox structures. When you create a new mailbox, it must be nested within another mailbox. At a minimum, the virtual root mailbox "/" is a starting point from which to build the mailbox structure. Consider an example where someone creates a mailbox with the name "Inbound" in the "/" virtual root mailbox, and then adds sub-mailboxes to it for specific trading partners:

/Inbound

Company A

Company B

Company C

The mailbox name is the actual name assigned to the mailbox at the time of creation. In this case, the mailbox names are Inbound, Company A, Company B, and Company C. Mailbox names are useful for general communication purposes, for example, informing trading partners about where to send documents they have for you.

The mailbox name can identify information such as trading partner name or the direction of message flow. Following are two examples:

- A message from the trading partner Dallas Hardware may be stored in the Dallas Hardware mailbox.
- A message received from Dallas Hardware Incorporated will be stored in a mailbox named /Customers/Central United States/Dallas Hardware/Inbound, and a message sent to Dallas Hardware Incorporated will be stored in the mailbox /Customer/Central United States/Dallas Hardware/Outbound.

Mailbox Path

For security/privacy reasons, though, you may not want trading partners to be aware of the nesting structure for your mailbox system. In the above example, you may only want Company A, Company B, and Company C to be aware of their own individual mailboxes. The application gives you the flexibility to design your mailbox structure with this concern in mind.

The mailbox name alone is not sufficient for business process activities that perform operations on mailboxes (for example, adding or extracting messages). For these activities, the mailbox path is required. The mailbox path represents the full sequence of mailboxes and sub-mailboxes that specifies the location of a certain, named mailbox.

In the example above, the mailbox path for Company A is:

/Inbound/Company A

Your trading partners do not need to know the mailbox path for their mailbox. However, services used to perform operations on mailboxes require the mailbox path.

The path to a mailbox can identify information such as the category of trading partner. For example, mailboxes for customers from the Central United States may be embedded inside a mailbox named Central United States such as /Customers/Central United States/Dallas Hardware.

Message Name

The message name can be used to communicate information about the message using a suffix, base name, or prefix. Following are three examples:

- A purchase order may be sent with a message name suffix that indicates it is a purchase order, such as 9912234.po.
- A message representing transaction ID 9912234 may have a message name 9912234.po.
- The order-123456767.request and order-123456767.cancellation might be part of an order process, while invoice-234325677.receipt might be part of an invoice process.

Creating a Mailbox and Assigning Permissions

To create a new mailbox and assign permissions to groups and users to operate on this mailbox:

1. From the **Deployment** menu, select **Mailboxes** > **Configuration**.
2. In the Create section, click **Go!**
3. In the Mailbox: Name page, select the parent mailbox in which the mailbox you are creating will be embedded. You can type a partial name in the **Filter by Name** field and click the filter button for a filtered list.

   The root mailbox is denoted by a slash (/).
4. In the **Name** field, type a name for the mailbox you want to create.

   This name is used to identify the mailbox in the application.
5. In the **Description** field, type a short description for the mailbox and click **Next**.

   Use this field to describe the mailbox. This field is not used by any other resource in the system. (This is a required field.)
6. In the Assign Groups page, use the arrows to add the groups to the **Selected Groups** list and click **Next**.

   All groups in the **Selected Groups** list will have permissions on this mailbox. Click the first double arrow to add all available groups to the **Selected Groups** list. You can type a partial group name in the **Filter by Name** field and click the filter button for a filtered list. No groups are required. Groups can be added from the **Accounts** menu.
7. Use the arrows to add users to the **Selected Users** list and click **Next**.

   All users in the **Selected Users** list will have permissions on this mailbox. Click the double arrow to add all available users to the **Selected Users** list. You can type a partial user name in the **Filter by ID** field and click the filter button for a filtered list. No users are required. Users can be added from the **Accounts** menu.

Creating a Submailbox and Assigning Permissions

After you create a mailbox, your can create submailboxes. You can do this by creating a mailbox again or you can create a submailbox. Use the following procedure to create a submailbox:

1. From the **Deployment** menu, select **Mailboxes** > **Configuration**.
2. Open the configuration data of the mailbox you want to edit using one of the following methods:
   - In the By Mailbox Name field of the Search section, type the name or partial name of the mailbox you want to edit and click **Go!**
   - In the Alphabetical section, select the letter the mailbox starts with or select all to pull a list of all mailboxes and click **Go!**
3. A list of available mailboxes opens. Click the **Create sub-mailbox** icon next to the mailbox you want to create a submailbox in.
4. In the Mailbox: Name page, the parent mailbox is specified for you.

   The root mailbox is denoted by a slash (/).
5. In the **Name** field, type a name for the mailbox you want to create.

   This name is used to identify the mailbox in the application.
6. In the **Description** field, type a short description for the mailbox and click **Next**.

   Use this field to describe the mailbox. This field is not used by any other resource in the system. (This is a required field.)
7. In the Assign Groups page, use the arrows to add the groups to the **Selected Groups** list and click **Next**.

   All groups in the **Selected Groups** list will have permissions on this mailbox. Click the first double arrow to add all available groups to the **Selected Groups** list. You can type a partial group name in the **Filter by Name** field and click the filter button for a filtered list. No groups are required. However, if you want administrators to have access using the MBI, you must assign permissions to the Mailbox Browser Interface Group or to the Admin user.
8. In the Assign Users page, use the arrows to add users to the **Selected Users** list.

   All users in the **Selected Users** list will have permissions on this mailbox. Click the double arrow to add all available users to the **Selected Users** list. You can type a partial user name in the **Filter by ID** field and click the filter button for a filtered list. No users are required. Users can be added from the **Accounts** menu.
9. Click **Next**.
10. In the Confirm page, verify your mailbox configuration and click **Finish**.

Editing a Mailbox Configuration

To edit the description and permission assignment of an existing mailbox:

1. From the **Deployment** menu, select **Mailboxes** > **Configuration**.
2. Open the configuration data of the mailbox you want to edit using one of the following methods:
   - In the By Mailbox Name field of the Search section, type the name or partial name of the mailbox you want to edit and click **Go!**
   - In the Alphabetical section, select the letter the mailbox starts with or select all to pull a list of all mailboxes and click **Go!**
3. A list of available mailboxes opens. Click the **Edit** button next to the mailbox you want to edit.
4. In the Mailbox: Name page, change the **Description** field if necessary and click **Next**. (This is a required field.)
5. In the Assign Groups page, use the arrows to add the groups to the **Selected Groups** list and click **Next**.

   All groups in the Selected Groups list will have permissions on this mailbox. Click the first double arrow to add all available groups to the Selected Groups list. You can type a partial group name in the **Filter by Name** field and click the filter button for a filtered list. No groups are required.
6. In the Assign Users page, use the arrows to add users to the Selected Users list.

   All users in the Selected Users list will have permissions on this mailbox. Click the double arrow to add all available users to the Selected Users list.You can type a partial user name in the **Filter by ID** field and click the filter button for a filtered list and click **Next**. No users are required.
7. In the Confirm page, verify your mailbox configuration and click **Finish**.

Assigning Mailbox Permissions

Permissions for individual mailboxes are assigned when you create the mailbox. You can add mailbox permissions when you create a group or user account or you can edit a group to add mailbox permissions after the mailbox is created.

Trading partners communicating using the Connect:Direct Server adapter and FTP Server adapter must have a user account with ó, with the appropriate permissions on mailboxes that they are trying to access.

Assigning Mailbox Permissions to User Accounts

You can assign mailboxes to user accounts. You can do this at the time you create the user account or you can edit a user account to add mailbox permissions.

1. From the **Accounts** menu, select **User Accounts**.

   The Accounts page opens. You can either create a new user account or edit an existing account, if necessary.
2. To create a new user account, in the Create section, next to Create a new account, click **Go!**
3. Complete the fields in the User ID page, and click **Next**.
4. Complete the fields in the Groups page and click **Next**.

5. In the Permissions page, find the mailbox or mailboxes that you want to grant permissions to in the **Available** list and move them to the **Assigned** list. Then click **Next**.
6. When you are finished updating the user account, click **Save** or **Finish**.

Assigning Mailbox Permissions to Groups

After you assign a group permissions to a mailbox, you can dynamically grant permissions to new users by adding them to the group. To add mailbox permissions to a group:

1. From the **Accounts** menu, select **Groups**.
2. In the Assign Permissions page, search for the mailbox that you want to grant permissions to.
3. When you are finished updating the group, click **Save** or **Finish**.

Assigning Users to Mailbox Groups

There are two predefined mailbox groups, the Mailbox Browser Interface Users group and the Mailbox Administrators group. All users that interact with mailboxes through the MBI, must be added to the Mailbox Browser Interface Users group. All users that administer mailboxes must be added to the Mailbox Administrators group. The Mailbox Administrators group has the Mailbox Browser Interface Users group as a subgroup, so users do not need to be added to it separately. Following are descriptions for each group:

- Mailbox Browser Interface Users Group – Users in this group have permissions to access the Mailbox Browser Interface (MBI) business processes and templates. External or internal trading partners that add files to and extract files from the mailbox should be placed in this group.
- Mailbox Administrators Group – Users who are part of the Mailbox Administrators group are also (automatically) part of the Mailbox Browser Interface Users group. So making a user part of the Mailbox Administrators group gives the user access to the Mailbox Browser Interface without the need to assign the latter group, explicitly. The user ID Admin is, by default, part of the Mailbox Administrators group.

To add users to these groups:

1. From the **Accounts** menu, select **User Accounts**.
2. You can either create a new user account or edit an existing account.
3. To create a new user account, in the Create section, next to Create a new account, click **Go!**
4. To edit an existing account, search by name or find it in a list. Click the **edit** icon.
5. Complete the fields in the User ID page and click **Next**.
6. In the Groups page, move either the Mailbox Browser Interface Users group or the Mailbox Administrators group from the **Available** list to the **Assigned** list and click **Next.**
7. When you are finished updating the user account, click **Save** or **Finish**.

Creating Virtual Roots

To support limited visibility into the mailbox hierarchy, mailboxes are visible to the end user as a relative path, while administrators see the mailbox in an absolute or full path. This concept is referred to as the *virtual root*.

When a Mailbox Add service is invoked with a mailbox name, the mailbox name is appended to the virtual root mailbox associated with the user ID to obtain the absolute name of the mailbox to which the message should be added. The absolute path to the mailbox is never disclosed to the sender.

When a Mailbox Query service is invoked, only mailboxes that are under the virtual root of the user and for which the user has permissions can be searched.

This is useful for security reasons if you do not want to disclose the full path to a mailbox. It is also valuable for mailbox maintenance. If you change the organization of your mailbox, the virtual root does not change, so the change is transparent to the user.

A trading partner using the new FTP Server adapter must have a virtual root mailbox to have an FTP session.

To create a virtual root:

1. From the **Deployment** menu, select **Mailboxes** > **Virtual Roots**.
2. In the Create section, click **Go!**
3. Specify the User ID that you want to create the virtual root for and click **Next**.

   You can type a partial user ID in the **Filter by ID** field and click the filter button for a filtered list.
4. Specify the mailbox that you want to be the virtual root of the User ID and click **Next.**

   You can type a partial mailbox name in the **Filter by Name** field and click the filter button for a filtered list.
5. Click **Finish**.

Editing Virtual Roots

You can change the virtual root of a user ID. This does not impact any other system resource and does not impact how the user interacts with the mailbox. To change the virtual root of a user ID:

1. From the **Deployment** menu, select **Mailboxes** > **Virtual Roots**.
2. Select the virtual root you want to edit using one of the following methods:
   - In the By User ID field in the Search section, type the User ID that you want to change the virtual root for and click **Go!**
   - In the List section, select the first letter of the user ID, or select ALL for a list of all virtual roots and click **Go!**
3. Identify the virtual root you want to edit and click **edit** in the **Select** column.
4. In the User ID page, click **Next**.

5. Select the **Mailbox Name** and click **Next**.
6. Click **Finish**.

Searching for Messages

The Mailbox feature enables you to search all mailboxes for messages. Criteria you can search on include: mailbox, message name pattern, from date and time, to date and time, processing status, and message ID.

Use the following procedure to perform a search:

1. From the **Deployment** menu, select **Mailboxes** > **Messages**.
2. On the Message Management page, specify the criteria you want to search on and click **Go!** The default for all fields is All. You can type a partial name of a mailbox and click the filter button to filter by name and shorten the list.
3. A list of matching messages opens. The following table describes the content of each column:

Column Title	Description
Select	Contains the icon for editing a message.
Name	Message name. Displayed as hyperlink by default. **Note:** If the Extractable Count = 0, the hyperlink does not open the message. To remove the hyperlink and display the message name as text, see Display Message Name as Text.
ID	Message ID assigned by the mailbox.
Created	Date and time the message was created.
Size	Size of the message in KB.
Mailbox	Mailbox location of the message.
Extract Policy	Extraction policy associated with the account.
Policy Value	Value associated with the Extract Policy.
Locked by BP	Indicates the business process that has the message locked, if any.

Display Message Name as Text

To remove the hyperlink from the message name and display the name as text only:

1. From **Deploy** > **XSLT**, search for MBIList.
2. Click on **Source Manager**.

3. Edit the MBIlist file to remove the action element containing:

```
<a href=
/mailbox/mybp/FormToXML?bpDest=MBIDocView&amp;MessageId={MessageId}&amp;fil
ename={MessageName}&amp;bpResolverTimeout=360 target= _blank > </a>
```

4. Enter a description and click **Next**.
5. Select the version you modified, and click **Save**.
6. Click **Finish**.
7. Open the MBI and verify the Message Name link is disabled.

Suppressing Duplicate Messages

The Mailbox feature can suppress duplicate messages, providing a model similar to traditional file systems (for example, UNIX). In this mode, when a message is added to a mailbox, the system determines whether a message with that same name is already present in the mailbox. If so, then the old message is "deleted" before the new one is added. The document associated with the old message is of course not deleted—only the message referencing the document (content) is deleted. The document is still retrievable through correlation search and archival search.

To suppress duplicate messages:

1. Using your favorite editor, open the *install_dir*/properties/mailbox.properties.in file.
2. Set the value for the disallowDuplicateMessages property to **true**. Example:
   `disallowDuplicateMessages=true`
3. Run the command **setupfiles.sh / .cmd**
4. Restart the application for changes to the mailbox.properties.in file to take effect.

Note: Message names are limited to 100 characters for DB2 on z/OS. All other platforms support 255 character message names.

Allowing Duplicate Messages in /DeadLetter

The FTP Server adapter places failed uploads in the DeadLetter mailbox. To monitor failed uploads, you may wish to retain these duplicate messages, while still disallowing duplicates in the rest of the system. The disallowDeadLetterDuplicateMessages property in the mailbox.properties.in file allows duplicates in the Deadletter mailbox only, overriding the mailbox-wide property disallowDuplicateMessages.

To allow duplicate messages in the /Deadletter mailbox only:

1. Using your favorite editor, open the *install_dir*/properties/mailbox.properties.in file.
2. Set the value for the disallowDuplicateMessages property to **true**. Example:
   `disallowDuplicateMessages=true`

3. Retain the default value for the disallowDeadLetterDuplicateMessages parameter. Example: `disallowDeadLetterDuplicateMessages=false`
4. Run the command **setupfiles.sh / .cmd**
5. Restart the application for changes to the mailbox.properties.in file to take effect.

Updating Extractability of a Message

After a message is added to the mailbox, you can update the extractability policy or policy value. To update the extractability of a message:

1. From the **Deployment** menu, select **Mailboxes** > **Messages**.
2. Specify the criteria you want to search on and click **Go!** The default for all fields is All.
3. Identify the message that you want to change the extraction policy value and click **Edit**. The Info page opens for the message.
4. Specify the new extract policy and policy value. The following table describes the available policies and policy values:

Policy	Description
Extractable	Enables either unlimited extractions or no extractions. Valid values are: ◆ No – The message cannot be extracted. ◆ Yes – No limit to how many times the file can be extracted.
Extractable Until	Enables unlimited extractability until a certain date. This is ideal for publishing time-sensitive documents such as price lists of catalogs. Valid value is any future date.
Extractable Count	Enables a message to be extracted a specific number of times. This policy is ideal for automated processes that use a file a limited number of times. This is the default policy. Valid value is any integer. The default is 1. **Note:** If an IOException occurs during extraction, including a Cancel by the user, a business process is initiated to increment the Extractable Count. For files smaller than 100Kb, the entire file is already transmitted, so the business process is not initiated. The Extractable Count must be manually incremented for the message to be extractable again.

5. Click **Finish**.

Note: Extractability settings affect message visibility and extractability in various ways for various communications protocols, such as, AS2, FTP, Connect:Direct. For example, by default, the FTP Server adapter adds messages with an extractable policy value of yes/no and an extractability value of yes. This policy causes Mailbox to mimic a traditional file system. Messages added through AS2 use an extractable policy value of N times with an extractability value of 1. This policy supports

transactional processing of AS2 messages. Be aware of how users will access messages before changing policy settings.

Resubmitting a Message for Automatic Routing

After a message is added to the mailbox, you can update the extractability policy or policy value. To resubmit a message for automatic routing:

1. From the **Deployment** menu, select **Mailboxes** > **Messages**.
2. Specify the criteria you want to search on and click **Go!** The default for all fields is All.
3. Identify the message that you want resubmit and click **Edit**. The Info page opens for the message.
4. Select **Resubmit message for automatic routing** and click **Next**.
5. Click **Finish**.

Archiving Messages

The application supports the archiving of mailbox messages as part of the overall archiving process for business processes and documents. Since mailbox messages are represented internally as business process documents, there are certain precautions that Mailbox takes to protect mailbox messages from being archived and inaccessible.

Mailbox messages and the business process responsible for executing the Mailbox Add service are protected from archiving and remain in the application's database tables until their corresponding mailbox message is deleted. They can be deleted by the Mailbox Delete service or the Mailbox Scheduled Delete service. This protection ensures that the message is available as long as it is needed. After a message is deleted from a mailbox, the message is archived along with the business process the next time an archive takes place when the configured archive life span expires.

Restoring Messages

After a business process and its associated message is archived, you can restore the archive and audit the business process and associated message. To restore the message:

1. From the **Operations** menu, select **Archive Manager**.
2. In the Restore Manager section, click **Go!**
3. In the **Command Line** field, type the location for the restore_wrapper.sh script and the location where the data is restored.

4. In the **Working Directory** field, specify the *install_dir*/bin directory, where install_dir is the directory where the application is installed, and click **Go!**

   This restores all archived business processes. For processes that added or extracted mailbox messages, the associated messages are restored with the business process.

Searching for Correlations to Business Processes

You can perform a correlation search to determine which business process accessed a particular mailbox message. You can search on mailbox path, message ID, message name, and creation date. To search for correlations:

1. From the **Business Process** menu, select **Advanced Search > Correlation**.
2. Depending on the search criteria you want to use, specify Any, All, or any combination of the following and click **Go!**

Search Criteria	Name	Value
Mailbox path	Mailbox_MailboxPath	Mailbox ID of messages you want to audit.
Message ID	Mailbox_MessageID	Message ID of message you want to audit.
Message Name	Mailbox_MessageName	Name of the message you want to audit.
Creation Date and Time	Mailbox_CreateDateTime	Creation date and time of the message you want to audit.

   The Correlation Search Results page opens, indicating the number of business processes that matched. You can click the number identifying how many business processes were found. The Multiple Document page opens with the list of matched documents in the left pane.
3. In the Correlation Search page, from the Location list, select one of the following options:
   - Live Tables – Display correlations of live (active) instances.
   - Archive Tables – Display correlations of instances that you have archived in.
   - Restore Tables – Display correlations of instances that you have restored from an offline location.
4. Click a document name to view the contents.
5. Click **Info** in the Status column to view document details.

Note: Correlation entries for mailbox events are truncated to 90 characters on DB2 z/OS platforms. Message names in DB2 z/OS correlation entries have trailing extra characters truncated, while MailboxPath correlation entries have leading extra characters truncated.

Auditing Restored Messages

After archived business processes are restored, you can audit the messages using the central search feature. You can search for messages using the mailbox path, message ID, message name, and creation date. To audit restored messages:

1. From the **Business Process** menu, select **Monitor** > **Advanced Search > Correlation**.
2. In the Correlation Search page, specify **Type** as **ANY** and **Location** as **Restore Tables**. Depending on the search criteria you want to use, specify Any, All, or any combination of the following, and click **Go!**

Search Criteria	Name	Value
Mailbox path	Mailbox_MailboxPath	Mailbox ID of messages you want to audit.
Message ID	Mailbox_MessageID	Message ID of message you want to audit.
Message Name	Mailbox_MessageName	Name of the message you want to audit.
Creation Date and Time	Mailbox_CreateDateTime	Creation date and time of the message you want to audit.

   The Correlation Search Results page opens, indicating the number of business processes that matched.
3. Click the number identifying how many business processes were found. The Multiple Document page opens with the list of matched documents in the left pane.
4. Click a document name to view the contents.

Monitoring EDIINT Activity

You can monitor AS2 EDIINT tracking for AS2 transfers that use the Mailbox feature. This information is only be available if AS2 is configured to use Mailbox.

Note: The EDIINT search function is only intended to track documents with MDNs. Therefore, if an AS2 is configured not to request MDNs or if your partner chooses not to receive MDNs, the tracking information is not displayed in the EDIINT search. The MDN is controlled by the sender, so if your partner does not request it, you are unable to view that partner's documents information using this search.

1. From the **Business Process** menu, select **Advanced Search > EDIINT**.
2. In the EDIINT Transaction Search page, specify the AS2 messages you want to search for. Specify Any, All, or any combination of the following and click **Go!**

Search Criteria	Description
Contracts	Search for AS2 transactions associated with a contract.

Search Criteria	Description
Status	Search for AS2 transactions with a specific status.
Type	Search for AS1 or AS2 transactions.
Start date	Search for transactions according to the date the transfer started.
End date	Search for transactions according to the date the transfer ended.

3. Click the message ID to view the details. The EDIINT Transaction Detail page opens. The following fields are specific to Mailbox:

Field	Description
Mailbox	Mailbox associated with the transaction
Mailbox Message ID	Message ID assigned to the message
Mailbox Message Name	Name of the message in the mailbox

Viewing Dead Letter Mailbox Contents and Status

The Dead Letter mailbox stores messages that could not be added to a regular mailbox. The Dead Letter mailbox is located under the root mailbox as /DeadLetter. You can view information about messages using the following:

- To view the contents of the Dead Letter mailbox, see *Searching for Messages* on page 25.
- To view the status report, including user ID of the message originator, the original intended destination, and the reason for the failure. See *Searching for Correlations to Business Processes* on page 29.

Configuring an AS2 Trading Partner to Use Mailbox

The Mailbox feature provides ready-to-use integration with the EDIINT AS2 protocol. This section describes how to configure your AS2 profile to use Mailbox. When configuring your AS2 profile using the AS2 wizard, you encounter two fields that you must select to use the mailbox.

To set up an AS2 trading partner to use the Mailbox feature:

1. From the **Trading Partner** menu, select **AS2**.
2. Start the AS2 wizard one of two ways:
   - In the Create section, click **Go!** to create a new trading profile.
   - To edit an existing trading profile, click **Go!** in the List section and click **Edit** on the Profile.
3. In the New Identity: AS2 Configuration Type: Identification page, select **Store Messages in Mailbox**.

4. In the AS2 Configuration Type Mailbox page, select one of the following options:
   - Use default Inbound/Outbound Mailboxes. Creates two mailboxes with the format AS2/*Name*/Inbound and AS2/*Name*/Outbound, where *Name* is the name given to the trading partner in the AS2 Configuration Type: Identification page.
   - Select Existing Parent Mailbox. Enables you to select a parent mailbox where the mailbox you are creating will be embedded. If you do not want to embed the mailbox, select the slash (/). This creates two mailboxes with the format *Parent Mailbox*/Inbound and *Parent Mailbox*/Outbound, where *Parent Mailbox* is the mailbox you select to embed the mailbox you are creating.

   All failed messages are placed in the /DeadLetter mailbox.

Deleting Mailboxes

The Mailbox Delete Mailbox service enables you to delete one or multiple mailboxes, as well as the associated submailboxes, messages, virtual roots, routing rules, and permissions. It is designed to completely and permanently remove mailboxes and everything associated with them. The Mailbox Delete service differs in that it deletes only *messages* in mailboxes.

You can either delete mailboxes interactively, through the application interface, or at a decision point in a business process, using the Mailbox Delete Mailbox service in a business process.

To delete mailboxes interactively:

1. Go to **Deployment** > **Mailboxes** > **Configuration**.
2. Next to List ALL, click **Go!**
3. Click the delete icon.
4. You have the option to view a report of what was deleted.

   You can also delete mailboxes by using the Mailbox Delete Mailbox service.

Mailbox Browser Interface (MBI)

Configuring the Mailbox Browser Interface

The MBI is a Web application that can reside inside your secure network or in the DMZ of your company network.

To run the MBI inside your secure network, no configuration is required. An HTTP Server adapter configuration (named MBI HTTP Server adapter) comes with the application and enables clients on the same network as the application to access the Mailbox Browser Interface.

To run the MBI in a DMZ, an HTTP Server adapter must be configured that uses a remote perimeter server.

Incoming URL requests are passed from the HTTP Server adapter, which runs preconfigured business processes. These business processes use a variety of Mailbox services and return results to the browser that the original request came from.

After a Perimeter Server has been configured in the application, its name is available to the HTTP Server adapter configuration, in the Perimeter Server Name list on the HTTP Connection Properties page.

To configure the MBI to run in the DMZ:

1. Set up a perimeter server in the DMZ.
2. Configure a new Perimeter Server in the application.

   The port specified in the Perimeter Server configuration must *not* be the HTTP listen port (to which trading partners are expected to connect), which is specified in a subsequent stage.
3. Ensure that the remote perimeter server is running.
4. Clone the MBI HTTP Server adapter configuration.
   a. From the **Deployment** menu, select **Services** > **Configuration**.
   b. In the **Service Name** field, type **MBI HTTP** and click **Go!**
   c. In the Search Results page, find the entry that corresponds to the MBI HTTP Server adapter and click **Copy**.
   d. Give the adapter a new unique name, and click **Next**.
   e. For the **HTTP Listen Port**, specify the port that the HTTP client (typically the trading partner) is expected to connect to. This port must not be used by a different application on the computer that the remote perimeter server is installed on. No two HTTP Server adapter configurations can listen on the same port on the same remote perimeter server computer.

f. From the **Perimeter Server Name** list, select the name of the Perimeter Server (previously configured) that corresponds to the specific remote perimeter server to be used. The name is in the format *node & name*, where *name* is what you specified. Click **Save**.

g. On the **Confirm** page, verify that all parameters are as specified. Ensure the **Enable Service for Business Process** check box enabled.

h. Click **Finish**.

5. If you have access to the computer on which the remote perimeter server is running, log in to that computer and run the following command:

   `netstat -an | grep <httpListenPort>`

   where <*httpListenPort*> is the port previously specified. If a row is found that reads LISTEN, the HTTP Server adapter is ready to handle requests from external clients.

6. Verify that the HTTP Server adapter is listening and that the Mailbox Browser Interface is configured correctly by pointing an HTTP browser to the following URL:

   http://<*host*>:<*httpListenPort*>/mailbox

   where <*host*> is the IP address or host name of the computer where the remote perimeter server is running and <*httpListenPort*> is the port previously specified. A dialog opens, requesting the user name and password to use with the Mailbox Browser Interface. If instead the browser encounters an error, verify that <*httpListenPort*> is being listened on. If it is listening, verify that some other application has not reserved this port. To do this, disable the HTTP Server adapter and verify that this port is not being listened on. If it is, find the application that has the port bound and shut it down. Alternately, select a different HTTP Listen Port and try again.

Connecting Trading Partners to the MBI

For your trading partners to use the MBI you must do the following:

- Create a new user account for each trading partner.
- Assign trading partners to the **Mailbox Browser Interface Users** group.
- Provide each trading partner the URL of your Web server.
  - If your MBI application resides inside your secure network, use the following URL:

    http://<*SIhost*>:<*MBIport*>/mailbox

    where <*SIhost*> is the IP address or host name of the computer where the application's Web application is installed and <*MBIport*> is the port that the MBI HTTP Server adapter listens on. To find the <*MBIport*>, complete the following steps:

    a. From the **Deployment** menu, select **Services** > **Configuration**.

    b. In the Service Name field, type **MBI HTTP** and click **Go!**

    c. In the Search Results page, find the entry that corresponds to the MBI HTTP Server adapter and click the name of the adapter.

    d. The HTTP Listen Port is the <*MBIport*>

- If you installed the MBI to run in the DMZ, use the following URL:

  http://<*host*>:<*httpListenPort*>/mailbox

  where <*host*> is the IP address or host name of the computer where the remote perimeter server is running and <*httpListenPort*> is the port previously specified. A dialog opens, requesting the user name and password to use with the Mailbox Browser Interface. If instead the browser encounters an error, verify that <*httpListenPort*> is being listened on. If it is listening, verify that some other application has not reserved this port. To do this, disable the HTTP Server adapter and verify that this port is not being listened on. If it is, find the application that has the port bound and shut it down. Alternately, select a different HTTP Listen Port and try again.

✦ Provide each trading partner an initial user ID and password.

Trading partners can obtain information about using the MBI by clicking **Help** after logging in.

Changing Your Password in the MBI

To change your Mailbox password:

1. On the Navigation bar, click **Change Password**.
2. Type your old password in the **Old Password** field.
3. Type the new password in the **New Password** and **Confirm New Password** fields and click **Change**.

   Your password must be at least six characters long and cannot contain any of the following characters:

   ! @ # % ^ * ( ) + ? ,] [{ } | ; > < " &

   The application supports external authentication. If a user is set up as an external user, then the password is stored in an external LDAP repository. In that case, the application does not own the password, and cannot change it. For external users, the Mailbox Browser Interface does not display the Change Password option.

Keeping Permissions Secure in the MBI

If multiple users share a computer, the following must be performed between user sessions:

1. Log off from the application.
2. Clear the browser cache.
3. Close the browser session.

This procedure ensures that each user has the correct permissions.

Searching for Messages in a Mailbox

The Search page is the first page that opens when you log in to Mailbox. The page is also available from the navigation bar by clicking **Search** or **Home**. From the Search page, you can search for messages in any or all mailboxes that you have permission to search. To search a mailbox:

1. On the Navigation bar, click **Search**.
2. Specify the search criteria as described in the following table:

Field	Description
Mailbox	Mailbox you want to search or select **All** to search all mailboxes you have permission to search. Required. To filter your search, use **MailboxPath lookup**. Type part of the path name in the Filter window to reduce the size of the list beneath it. Click on the path name you want and it populates the Mailbox field.
Message Name	Message name or partial message name for your search. You can use the asterisk (*) as a wildcard. Optional.
Message ID	Message ID for your search. Optional.
From	Beginning date and time range for your search. Optional. Date format is *yyyy-mm-dd*. Time format is *hh:mm:ss AM/PM.*
To	Ending date and time range for your search. Optional. Date format is *yyyy-mm-dd*. Time format is *hh:mm:ss AM/PM.*

3. Click the **Search** button.
4. Do one of the following:
   - Click the message name to view the message in a browser window without extracting the message.
   - Click the **Extract** button to extract the message.

Search Results

From the Search Results page, you can sort the search results by clicking on any of the following column headings: Name, ID, Created, Size, or Mailbox. The Search Results page contains the following information:

Column	Description
Extract	Click to download the message (file) to your computer.
Name	Name of the message. Click to view the message in a browser window.
ID	Message ID assigned by the Mailbox.
Created	Date and time the message was created.

Column	Description
Size	Size of the message in bytes.
Mailbox	Name of the mailbox containing the message.
Extract Policy	Policy that is used to govern the extractability of the message: ◆ Count – Message is extractable a specific number of times (specified in Policy Value column). ◆ Until – Messages are extractable until a specified date (specified in the Policy Value column). ◆ Extractable – If Policy Value is Yes, the message is infinitely extractable. If Policy Value is No, the message is not extractable.
Policy Value	Identifies the values for the policy identified in Extract Policy.

Sending a Message to a Mailbox

To send a message to a mailbox:

1. On the Navigation bar, click **Send**.
2. Specify the send criteria as described in the following table:

Field	Description
Mailbox	Mailbox that you want to send the message to. Required. To filter your search, use **MailboxPath lookup**. Type part of the path name in the Filter window to reduce the size of the list beneath it. Click on the path name you want and it populates the Mailbox field.
Filename	The path and file name of the file you want to send. Click **Browse** to navigate to the directory where the message is located. Required. The following characters cannot be used in the name: \ / : * ? " < > | % ! **Note:** Message names are limited to 100 characters for DB2 on z/OS. All other platforms support 255 character message names.
Rename File	Use this option if you want to modify the name of the file or messsage. The following characters cannot be used in the name: \ / : * ? " < > | % !

3. Click **Send**.

   If the file is successfully added, the Send page opens. If the file was not successfully added, an error message displays.

Note: When Mailbox Duplicate Suppression is turned on, an existing message (with the same name as a new message) is removed, and a new message is added. When Mailbox Duplicate Suppression is turned off, messages with the same name can be added.

Viewing a Message from a Mailbox Without Extracting

To view a message from a mailbox:

1. On the Navigation bar, click **Search**.
2. Specify the search criteria as described in the following table:

Field	Description
Mailbox	Mailbox you want to search or select **All** to search all mailboxes you have permission to search. Required.
Message Name	Message name or partial message name for your search. You can use the asterisk (*) as a wildcard.
Message ID	Message ID for your search.
From	Beginning date and time range for your search. Date format is *yyyy-mm-dd*. Time format is *hh:mm:ss AM/PM.*
To	Ending date and time range for your search. Date format is *yyyy-mm-dd*. Time format is *hh:mm:ss AM/PM.*

3. Click the **Search** button.
4. Identify the message you want to view and click the message name.

Extracting a Message from a Mailbox

To extract a message from a mailbox:

1. On the Navigation bar, click **Search**.
2. Specify the search criteria as described in the following table:

Field	Description
Mailbox	Mailbox you want to search or select **All** to search all mailboxes you have permission to search. Required.
Message Name	Message name or partial message name for your search. You can use the asterisk (*) as a wildcard.

Field	Description
Message ID	Message ID for your search.
From	Beginning date and time range for your search. Date format is *yyyy-mm-dd*. Time format is *hh:mm:ss AM/PM.*
To	Ending date and time range for your search. Date format is *yyyy-mm-dd*. Time format is *hh:mm:ss AM/PM.*

3. Click the **Search** button.
4. Identify the message you want to extract and click the associated icon in the **Extract** column.
   - If the message is extractable, you are prompted to save the file.
   - If the message is not extractable, the extraction fails and an error message displays. Click **Back** to return to the previous page.
5. Click **Refresh** (on your Browser) to refresh the page and view the updated extraction value.

Index

P

Q

R

S

T

U

V

X