Sterling Standards Library

Using AS2 and the AS2 Edition

Version 7.0

Sterling Commerce
An IBM Company

Contents

Overview of the AS2 Edition

Overview of Using AS2 and the AS2 Edition

The application enables you to send and receive AS2 messages either through the application user interface or through the AS2 Edition. The AS2 Edition combines the strengths of the application with Applicability Statement 2 (AS2) EDIINT technology, a protocol for securely exchanging data with non-repudiation of receipt over the Internet.

The AS2 Edition is a message management system enabling the exchange of a variety of documents between trading partners using secure AS2 EDIINT technology. The AS2 Edition uses the Internet as a transport mechanism, ensures privacy and security of documents exchanged, and provides a means of non-repudiation. The AS2 Edition extends your investments by sending and receiving documents and interacting with your existing processes. Basically, you put a document into a specific mailbox or directory to send it to a specific partner and you receive documents from partners in partner-specific mailboxes or directories.

This section explains what the AS2 Edition is and what you need to know to interact with the product. This section also gives an overview of the steps you must take from installation to exchanging documents with your AS2 trading partners.

Is AS2 Edition Right for Your Implementation?

The AS2 Edition contains all the application components necessary to configure a basic AS2 implementation. The AS2 Edition may not be suitable for all environments. We recommend that you carefully evaluate whether your needs will be met by the AS2 Edition or if you require an advanced implementation that will necessitate you writing custom business processes to use the EDIINT services. You will require a custom implementation for any of the following reasons:

- You need to trade messages with many trading partners.
- You want to integrate directly with the translator or any other application subsystem, instead of simply doing input and output to mailboxes or to the file system.
- You want to write either more simple or different processes for performance reasons (for example, you do not want to use the JDBC service or the AS2_TRADEPART_INFO table (the application-specific database

table for mapping directories or mailboxes to contracts) because foregoing these components will improve performance).

- You need to exchange AS1 messages.

AS2 Components

The AS2 Edition has the following components that are embedded in the application. These components are also available to AS2 users of the application (those AS2 users who are not using the AS2 Edition but rather using the application to meet their AS2 needs):

- Predefined business processes to send messages and check for acknowledgements (MDNs)—these business processes contain built-in error notification mechanisms that are able to send e-mails if MDNs are not received or if a negative MDN is received
- Services
- Browser-based user interface to configure and manage AS2 trading partners
- Database table (AS2_TRADEPART_INFO) that enables the mapping of directories and mailboxes to trading partner contracts
- Default AS2 URL (ApplicationIP_ADDRESS:port/b2bhttp/inbound/as2), which invokes the business process EDIINTParse and is designed to work both with and without the AS2 Edition to verify whether the sender/recipient are in the AS2_TRADEPART_INFO database table and, if so, perform application-specific handling in addition to message parsing

The predefined business processes and the services leverage the EDIINT implementation and enable you to exchange documents with your trading partners through AS2.

The AS2 Edition uses either the application file system (directories) or mailboxes for processing business documents inbound and outbound. These mailboxes and directories are created by the AS2 wizard. This enables you to put a document into a specified mailbox or directory to send it to a particular trading partner and you receive documents from partners though partner-specific mailboxes and directories.

Note: While mailboxes are displayed in the AS2 Edition Wizard, the AS2 Edition functionality does not support them. AS2 Edition users should not select the mailbox options in the wizard.

AS2 Predefined Business Processes

The AS2 implementation uses predefined business processes (in conjunction with predefined services) to implement the AS2 EDIINT protocol. These predefined business processes are automatically installed and configured when you install the AS2 Edition or the application.

The AS2 implementation uses these predefined business processes along with services to build and trans-mit messages to trading partners. Data files are collected from the file system or extracted from mailboxes. After the application collects files from the file system or extracts files from mail-boxes, it launches business processes that:

- Encapsulate the data files into AS2-compliant messages.
- Attempt to transmit those messages through HTTP or HTTPS.
- Potentially process responses or acknowledgements to those messages.

The application provides business processes for sending messages and checking for acknowl-edgements (MDNs). These business processes contain built-in error notification mechanisms that can continue to send e-mails if an MDN is not received, or if a negative MDN is received.

Existing predefined AS2 business processes include enhanced retry logic for each partner, and a parameter that enables you to specify how many files to retrieve from a partner's file system dur-ing each scheduled interval. This enables the application to stop send attempts to a partner's system when it is down. This limits how many processes the system starts at any one time, and prevents the application from overloading itself and your partner's system.

These business processes can detect several types of errors and can inform users and restage data files if errors occur. The business processes attempt to retry in the following situations:

- When what is potentially a transient HTTP error is detected based on the return code (408, 503, or 504).
- When an asynchronous Message Disposition Notification (MDN) is requested, and the MDN does not show up in the MDN timeout interval.
- When you are collecting and saving data using the file system, a scheduled business process, AS2 File System Adapter.bpml, invokes the Schedule_<TP Name>_FS.bpml, which collects data files from the file system. The EDIINT Message Service is used to build AS2 messages and process acknowledge-ments. The HTTPClientSend business process is used to transmit messages using HTTP. The Wait service is used to wait for acknowledgements or for an interval to expire before a retry, and the EDIINT Acknowledge Check Service is used to check for acknowledgements.

The following steps summarize the activities completed by business processes when sending messages:

1. Business processes send messages requesting synchronous receipts, asynchronous receipts, or no receipts.
2. Based on the receipt options specified for a trading partner, the business processes handle busi-ness documents, as appropriate.
3. The following provide an overview of activities completed by predefined business processes when receiving messages:
   - Business processes parse messages, generate and send receipts.
   - Using the File System adapter, the business processes extract business documents.
   - Predefined business processes run up to three times if the message transaction is not completed within a specified amount of time. The AS2 Edition enables you to monitor the predefined busi-ness processes and perform manual activities, such as starting and stopping predefined business processes.

The following types of business processes enable document transactions with the AS2 Edition:

- Extraction business process
- Message sending business process

AS2 Extraction Business Process

The application provides one extraction predefined business process, the AS2Extract business process. The AS2Extract business process writes a business document that is attached to a message to an inbound folder for a trading partner by completing the following process:

1. The AS2Extract business process calls the JDBC adapter to obtain the name of the trading partner inbound folder from the AS2TradingPartnerInfo table.
2. The AS2Extract business process calls the File System adapter to write the business document to a file in the inbound folder.

The following table describes the extraction business processes:

Business Process	Description
EDIINTParse	Parses messages; is configured on the default application AS2 URL (Applica-tionIP_ADDRESS:port/b2bhttp/inbound/as2). EDIINT Parse invokes the default instance of the EDIINT Header Scanning service and uses the value of the AS2-To header to attempt to find the appropriate row in the AS2TradingPartnerInfo database table. If the row is found, the value con-figured for "Wait for MDN" prompts the default instance of the EDIINT Pipeline service whether to build an MDN. If the EDIINT Pipeline service does not build an MDN, it propagates the MDN building information to the business process called to handle the payload data (either AS2Extract or MailboxAS2Add). **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files. **Note:** The AS2 Edition includes a configured URL that runs the EDIINTParse business process on both the base port and the base port + 33.
AS2Extract	Extracts business payload data to the trading partner's inbound subdirectory. Deter-mines whether a Message Disposition Notification (MDN) must be built and sent before extracting payload data. If an MDN must be built and sent, the default instance of the EDIINT MDN Building service is invoked to build the MDN. The process for sending the MDN is then initiated synchronously and data is extracted if the process for sending the MDN completes suc-cessfully. **Note:** MDNs are only built and sent by the EDIINT MDN Building service if you are using deferred extraction. Otherwise, they are built and sent by the EDIINT Pipeline service.
MailboxAS2Add	Extracts business payload data to the trading partner's inbound mailbox. Deter-mines whether an MDN needs to be built and send before extracting payload data. If the MDN does need to be built and sent, the default instance of the EDIINT MDN Building services is called to build the MDN, and the process for sending the MDN is then invoked synchronously. If the process for sending the MDN completes successfully, the payload data is extracted.

AS2 Message Sending Business Processes

The application provides business processes for sending messages. Depending on which message disposition notification (MDN) option you choose when configuring your trading partner information, the application selects the appropriate business process to send data to a trading partner.

The message sending processes and mailbox routing rules are input/output specific—that is, there is one set of processes using documents from file system directories and one set of processes using documents from mailboxes. If you are using file system input/output, you use one of the file system business processes. If you are using the mailbox input/output, you use one of the mailbox business processes. Both the file system and mailbox business processes use throttling. Then, if a lock is set by an associated business process, the business process responsible for creating (spawning) the business process to send the documents will not attempt to create more sending business process instances while the lock is set. Once the application determines that the trading partner is able to accept messages, the backlog of messages (messages that were unable to be sent while the database lock was in place) are cleared in a manner so that your trading partner is not bombarded with many messages all at once.

Note: Please note that the mailbox and file systems behave differently when a message is in error: While using file system, the message is moved to the error directory. While using mailbox, the message remains in the mailbox and the Extractable Count of the message in the Outbound Mailbox does not decrease.

You can set a Max Files to Collect parameter in the business process to ensure that any back-log of messages is cleared in an orderly manner.

The following table describes each message sending business process:

Business Process	Description
AS2SendNoMDN	Builds a message with a file collected from the file system for which no MDN is requested, calls AS2SendAndProcessNoMDN to send the message, verifies whether a final notification needs to be sent and, if so, invokes the EDIINTErrorNotification business process **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
AS2SendAndProcess NoMDN	Sends a message from the file system when no MDN is expected. Verifies whether an intermediate notification needs to be sent after each failed send attempt and, if so, invokes EDIINTErrorNotification. Waits for the configured retry interval and requeues a message up to the maximum configured number of times to handle transient errors and when the trading partner's system is down. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
AS2SendSyncMDN	Builds a message with a file collected from the file system for which a synchronous MDN is expected, calls AS2SendAndProcessSyncMDN to send the message, verifies whether a final notification needs to be sent and, if so, invokes the EDIINTErrorNotification business process. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
AS2SendAndProcess SyncMDN	Sends the message from the file system and processes the MDN when a synchronous MDN is expected. Verifies whether an intermediate notification needs to be sent after each failed send attempt and, if so, invokes the EDIINTErrorNotification business process. Waits for the con-figured retry interval and requeues a messages up to the maximum configured number of times to handle transient errors and when the trading partner's system is down. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
AS2SendAsyncMDN	Builds a message with a file collected from the file system for which an asynchronous MDN is expected, calls AS2SendAndProcessAsyncMDN to send the message, verifies whether a final notification needs to be sent and, if so, invokes the EDIINTEr-rorNotification business process.

Business Process	Description
	Note: This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
AS2SendAndProcess AsyncMDN	Sends the message from the file system and processes the MDN when an asynchronous MDN is expected. Verifies whether an intermediate notification needs to be sent after each failed send attempt and, if so, invokes the EDIINTErrorNotification business process. Waits for the configured retry interval and requeues a messages up to the maximum configured number of times to handle transient errors and when the trading partner's system is down. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
EDIINTErrorNotification	Sends email notifications when errors occur in the send process. Uses the BP MetaData service to obtain the parent ID of its parent process, the TimeStamp service to obtain the current time, and provides additional information to the SCLT service to construct the notification message. **Note:** You must complete E-mail notification parameters (E-mail address, E-mail Host, and E-mail Port) if you want to receive e-mail notifications.
MailboxAS2SendNo MDN	Builds and sends a message from a mailbox when no MDN is expected. Also uses throttling if a trading partner is "down" or unable to accept messages (based on a connection failure or a non-transient HTTP error code) by setting a lock in the database. Verifies whether a final notifica-tion needs to be sent and, if so, invokes the EDIINTErrorNotification business process. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendNo MDNSpawner	Launches the MailboxAS2SendNoMDN. The MailboxAS2SendNoMDN builds messages, calls the MailboxAS2SendAndProcessNoMDN processes to do the sending, sends intermediate notifications, and sets locks. The MailboxAS2SendAndProcessNoMDN processes then return control to the MailboxAS2SendNoMDN processes, which may send a final error notification if the trading partner's configuration requires. If a lock is set by the MailboxAS2SendNoMDN business process, this spawning process will not attempt to create more sending process instances while the lock is set. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendSync MDN	Builds and sends a message from a mailbox when a synchronous MDN is expected. Also uses throttling if a trading partner is "down" or unable to accept messages (based on a connection failure or a non-transient HTTP error code) by setting a lock in the database.

Business Process	Description
	Note: This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendSync MDNSpawner	Launches the MailboxAS2SendSyncMDN, which builds messages, calls the MailboxAS2SendAndProcessSyncMDN processes to do the sending, sends intermediate notifications, and sets locks. The MailboxAS2SendAndProcessSyncMDN processes then return control to the MailboxAS2SendSyncMDN processes, which may send a final error notification if the trading partner's configuration requires. If a lock is set by the MailboxAS2SendSyncMDN business process, this spawning process will not attempt to create more sending process instances while the lock is set. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendASyncMDNSpawner	Launches the MailboxAS2SendAsyncMDN, which builds messages, calls the MailboxAS2SendAndProcessAsyncMDN processes to do the sending, sends intermediate notifications, and sets locks. The MailboxAS2SendAndProcessAsyncMDN processes then return control to the MailboxAS2SendAsyncMDN processes, which may send a final error notification if the trading partner's configuration requires. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendAndProcessNoMDN	Verifies whether an intermediate notification needs to be sent after each failed send attempt and, if so, invokes the EDIINTErrorNotification business process. Waits for the configured retry interval and requeues a messages up to the maximum configured number of times to handle transient errors and when the trading partner’s system is down.
MailboxAS2SendAsyncMDN	Builds a message from the mailbox when an asynchronous MDN is expected. Verifies whether a final notification needs to be sent and, if so, invokes the EDIINTErrorNotification business process. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendAnd ProcessAsyncMDN	Sends the message from the mailbox and processes the MDN when an asynchronous MDN is expected. Verifies whether an intermediate notification needs to be sent after each failed send attempt and, if so, invokes the EDIINTErrorNotification business process. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.

Business Process	Description
MailboxAS2SendSync MDN	Builds a message from the mailbox when a synchronous MDN is expected. Verifies whether a final notification needs to be sent and, if so, invokes the EDIINTErrorNotification busi-ness process. Waits for the configured retry interval and requeues a messages up to the maximum configured number of times to handle transient errors and when the trading partner's system is down. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
MailboxAS2SendAnd ProcessSyncMDN	Sends the message from the mailbox and processes the MDN when a syn-chronous MDN is expected. Verifies whether an intermediate notification needs to be sent after each failed send attempt and, if so, invokes the EDIINTErrorNotification business process. Waits for the configured retry interval and requeues a messages up to the maximum configured number of times to handle transient errors and when the trading partner's system is down. **Note:** This business process uses the EDIINT Pipeline service instead of the EDIINT Message service because of the ability of the former service to handle large and high-concurrency files.
HTTPSyncSend	Sends a synchronous MDN using the EDIINT Message service or EDIINT Pipeline service.
HTTPAsyncSend	Sends an asynchronous MDN using the EDIINT Message service or EDIINT Pipeline service.
SMTPSend	Sends an SMTO (mailto) MDN using the EDIINT Message service or EDIINT Pipe-line service.

AS2 Message Sending Business Process Description

Each business process completes the following process:

1. The business process calls the JDBC adapter to obtain the MDN information for a trading partner. This information consists of the error directory, the receipt time-out value, and the retry interval value.
2. The business process calls the EDIINT Pipeline service (or in rare cases, the EDIINT Message service) to build a message for a trading partner.
3. The business process invokes the HTTPClientSend business process to send the message to the trading partner. The HTTPClientSend business uses the HTTP Client Begin Session Service, HTTP Client POST Service, and HTTP Client End Session Service. If the send request fails, the process attempts to resend the message based on the time interval (seconds) defined by the Retry Interval configured in the partner profile. If needed, this step repeats a total of "n" times where "n" is the Max Retries configured.
   - If the send request is successful, the AS2SendSyncMDN process calls the EDIINT Pipeline service to parse the response, which should be a valid message disposition notification.
   - If the send request fails, an error is written to the error log.

4. The AS2SendSyncMDN and the AS2SendASyncMDN business processes call the EDIINT Acknowledge Check service periodically to check whether the message has been acknowledged. These calls continue until the receipt time-out interval expires.
   - If the message is acknowledged, the EDIINT Acknowledge Check service completes successfully.
   - If the message is not acknowledged, the EDIINT Acknowledge Check service waits for the time period set in the Retry Interval parameter. If the retry interval expires and the message is still not acknowledged, the process retries from step 1 in this process. If the retry fails “n” times where “n” is the Max Retries configured, an error indicating that the service failed is written to an error log in your trading partner’s error folder on your AS2 Edition system. A second error is written to the trading partner error log containing the original collected file under another name.

Message Disposition Notifications

A message disposition notification (MDN) is a receipt document that contains the original message ID of a message and status information about the original message.

Electronic Data Interchange-Internet Integration (EDIINT) is a family of protocols developed by the Internet Engineering Task Force (IETF) for securely packaging and transporting messages containing business data over the Internet, using S/MIME.

There are two types of EDIINT:

- AS1, which uses SMTP, POP, and IMAP as the transport
- AS2, which uses HTTP as the transport

Within a business process in the application, the EDIINT Message service builds and parses EDIINT AS1 and AS2 messages. The EDIINT Pipeline service on the other hand builds and parses only AS2 messages, including plain text, signed, and encrypted data.

MDNs that conform to the EDIINT specifications can contain a cryptographic hash calculated over the content of the message after EDIINT processing.

An MDN can be either:

- Signed – Contains an encrypted digital signature of the receiver.
- Unsigned – Contains only the original message ID and not a digital signature.

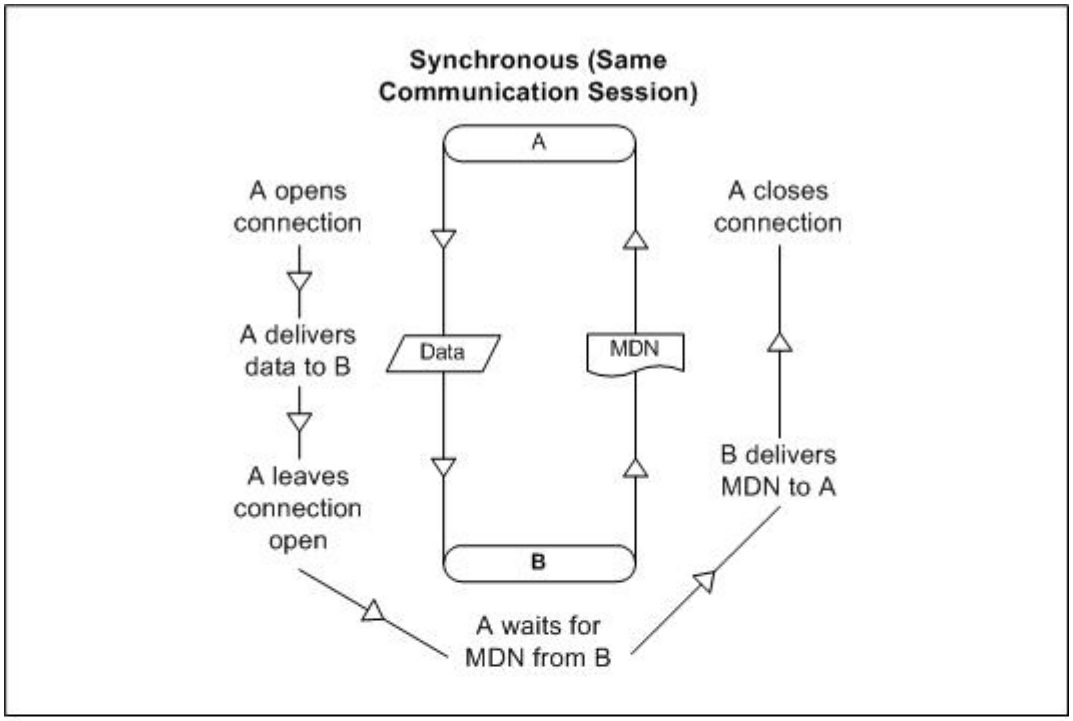
Signed MDNs that conform to the EDIINT specifications can provide non-repudiation of receipt in addition to message status information. A valid digital signature over an EDIINT MDN shows that the MDN was sent by the trading partner possessing the relevant key pair. It also shows that the signed area of the MDN (which includes the cryptographic hash calculated over the received content) was not altered after signing. A message sender compares the hash in the MDN with the hash calculated when the message was generated. If the hashes match, the sender knows that the receiver received the content and has the MDN to demonstrate the status.

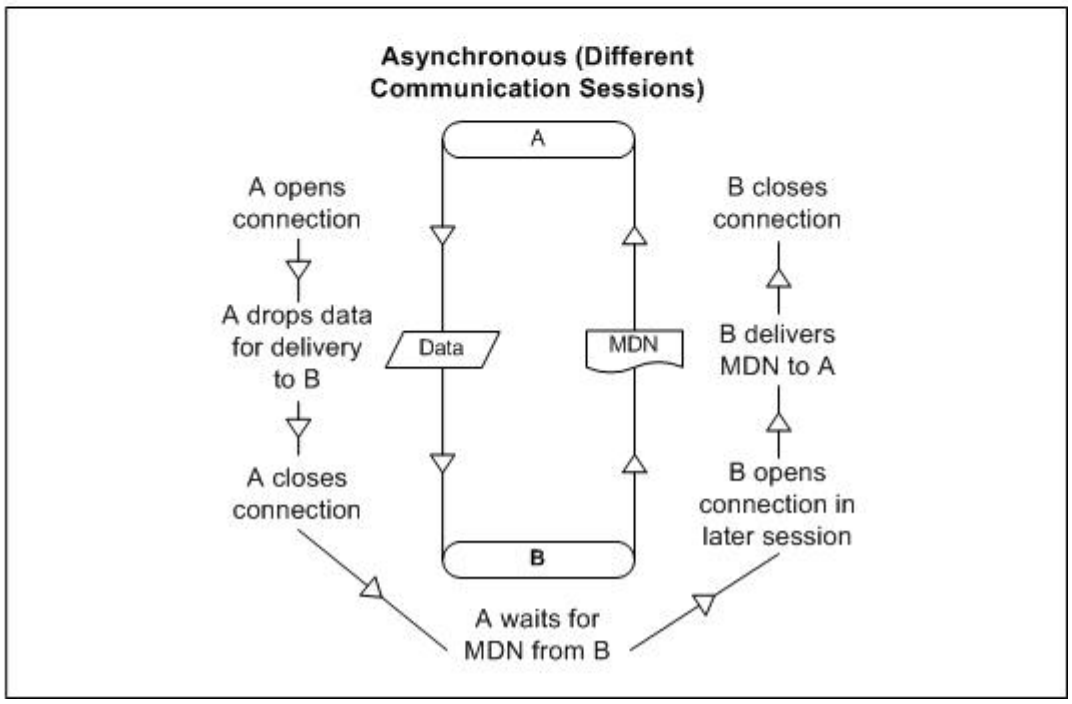
Whether signed or not, MDNs do not show that the received message content conforms to EDI or other business document formatting requirements.

Note: By default, the application uses AS2 version 1.1 in the MDN. If you want to use AS2 version 1.2 in your MDNs, you must change the **AS2VersionForMDN** property in **customer_overrides.properties** file.

MDNs are sent either:

- Synchronously – Returned immediately during the same communication session. As shown in the following diagram, A initiates the connection to B and delivers the data to B. A then leaves the connection open while waiting for an MDN from B during the same communication session. After A receives the MDN, A closes the connection.
- Asynchronously – Returned at a later time during a different communication session. As shown in the following diagram, A initiates the connection to B and drops the data for delivery to B. A closes the connection and does not wait for an MDN from B during the same communication session. In a later session, B initiates a connection to A, receives the data from A, and sends an MDN to A. When the MDN is delivered, B closes the connection.





Reprocessing and Resending Messages with the Original Message ID

The application allows you to easily reprocess messages because the building and sending of messages is all handled by the predefined business processes. This enables you to reprocess and resend messages using the same message identifier by simply restarting the appropriate business process. The business process will automatically use the primary document (message) with the original message identifier.

To restart a business process, navigate to the Business Process Manager and perform a business process restart. see *Running and Stopping Predefined AS2 Business Processes*.

AS2 Services and Adapters

The application uses services within predefined business processes to carry out a range of AS2-related functions.

The EDIINT-related services are available for customized implementations.

The following services enable document transactions with the application and the AS2 Edition:

- HTTP Server adapter
- HTTP Client adapter
- HTTP Client Begin Session service
- HTTP Client POST service
- HTTP Client End Session service
- EDIINT Message service
- EDIINT Acknowledge Check service
- EDIINT Pipeline service
- EDIINT MDN Building service
- EDIINT Header Scanning service
- AS2 File System adapter

Because of our continuing efforts to improve services and adapters to align with new technology and capabilities, the B2B HTTP Server adapter and the B2B HTTP Client adapter have entered the retirement process in the application and are changed to the HTTP Server adapter and the HTTP Client adapter and elated services, respectively.

HTTP Server Adapter

Note: Because of our continuing efforts to improve services and adapters to align with new technology and capabilities, the B2B HTTP Server adapter has entered the retirement process in the application and has been changed to the HTTP Server adapter.

The HTTP Server adapter completes the following actions in the AS2 Edition:

1. Receives messages in the AS2 Edition from a Java™ servlet running in a Web server.

   Caution: The Java servlet provides the HTTP listener service for receiving AS2 messages from trading partners.

2. Runs business processes to handle the messages.

   Caution: The Java servlet can deploy in a demilitarized zone (DMZ) environment, while the AS2 Edition, including the HTTP Server adapter, resides in the secure area behind the DMZ.

HTTP Client Adapter

Note: Because of our continuing efforts to improve services and adapters to align with new technology and capabilities, the B2B HTTP Client adapter has entered the retirement process in the application and is being replaced with the HTTP Client adapter and related services.

The HTTP Client adapter sends messages and asynchronous MDNs to trading partners using the HTTP/HTTPS communication protocols.

EDIINT Message Service

The EDIINT Message service completes the following steps in the AS2 Edition:

1. Builds or parses EDIINT messages.
2. Generates receipts for messages, as necessary.
3. Correlates receipts with messages.

Runs business processes that send receipts and process inbound documents.

EDIINT Acknowledge Check Service

The EDIINT Acknowledge Check service determines whether an MDN acknowledgement has been received for an EDIINT message within a business process in the application. If the MDN acknowledgement is not received within a specific period of time or if a negative MDN is received, the service can cause the business process to fail (or it can continue successfully, depending on the service configuration).

This service is designed to be used in a business process after a message has been sent

You must always include an EDIINT Message service or EDIINT Pipeline service configuration in a business process whenever you include an EDIINT Acknowledge Check service configuration.

EDIINT Pipeline Service

Within a business process, the EDIINT Pipeline service builds and parses only AS2 messages, including plain text, signed, and encrypted data.

Communications services, such as the B2B SMTP Client adapter or the HTTP Client adapter, then send or receive the messages within the business process.

The EDIINT Pipeline service also generates signed or unsigned Message Disposition Notifications (MDNs) when requested to do so and launches the workflow to send MDNs, and will request and process such MDNs too if the contract is so configured. Signed MDNs provide non-repudiation of receipt, which is realized when the original sender of a message verifies the signed receipt coming back from the receiver.

The EDIINT Pipeline service is identical to the EDIINT Message service in terms of functionality except for its added ability to parse large documents (up to 2 GB in size).

EDIINT MDN Building Service

The EDIINT MDN Building service builds a Message Disposition Notification (MDN) based on information in process data and a specified contract ID. This enables you to perform additional custom operations between message parsing and MDN generation so that you can consider the outcome of those operations by reviewing the status code reported in the MDN.

Note: This service is currently not used automatically by the AS2 Edition (the embedded AS2 application) or any predefined business processes—you must create a custom (user-defined) business process to implement it.

EDIINT Header Scanning Service

The EDIINT Header Scanning service parses the header area of messages without loading or examining the entire message, and then outputs the header information to process data.

AS2 Edition File System Adapter

The File System adapter performs the following:

- Monitors an outbound directory configured for a trading partner for documents to send to the trading partner.
- Extracts business documents and error information to appropriate directories configured for a trading partner.

When configuring information about an AS2 trading partner, you configure the File System adapter to monitor the outbound folder for that trading partner. The frequency with which the monitoring occurs is specified during the trading partner configuration.

When monitoring the outbound directory, the File System adapter polls the folder to determine whether any new messages need to be sent to your trading partner. If new documents are in the folder and are ready to be sent, the adapter sends the documents to your trading partner.

Note: You can view the files in the inbound and outbound folders in the File Tracking page (the initial page that opens upon accessing the AS2 Edition). The File Tracking page also displays the error log for outbound documents that the File System adapter could not send because of processing errors.

When documents are received from a trading partner, the File System adapter extracts the documents to the inbound folder configured for the partner.

Transmission Failures

If a transmission attempt fails, the File System adapter extracts an error log and the original document to the error folder configured for the partner.

Note: This process does not work with mailbox input or output.

---

1. The business processes that send messages to trading partners do not retry when errors cannot be interpreted as transient HTTP errors (that is, time-outs because a system is busy at the moment) based on HTTP return codes. These processes use the System Lock service to set a lock when unable to communicate with a trading partner's server.
2. The business processes that send messages to trading partners use the Wait service.
3. The AS2 File System Adapter checks for a lock before invoking the File System Adapter to collect files. If the lock is found, the File System adapter will not be invoked.
4. The AS2 File System Adapter allows you to specify the maximum number of files to collect when invoking the File System adapter to collect files. The use of this value in conjunction with appropriate system sizing allows you to configure your system to be able to clear queued data when a trading partner's server comes back online.

Duplicate Message Processing

EDIINT messages contain message IDs. Message IDs are used to correlate receipts with messages. When a message received from a trading partner is parsed, information about the message, including its message ID, is stored in the database. If a second message is received with the same message ID as a previous message, the application handles the second message as a duplicate. In this case, the application returns the MDN that

it sent for the previous instance of the message to the message sender. The application does not extract the message content to the inbound folder configured for the trading partner.

You can force the AS2 Edition to fully process duplicate messages by completing the following actions:

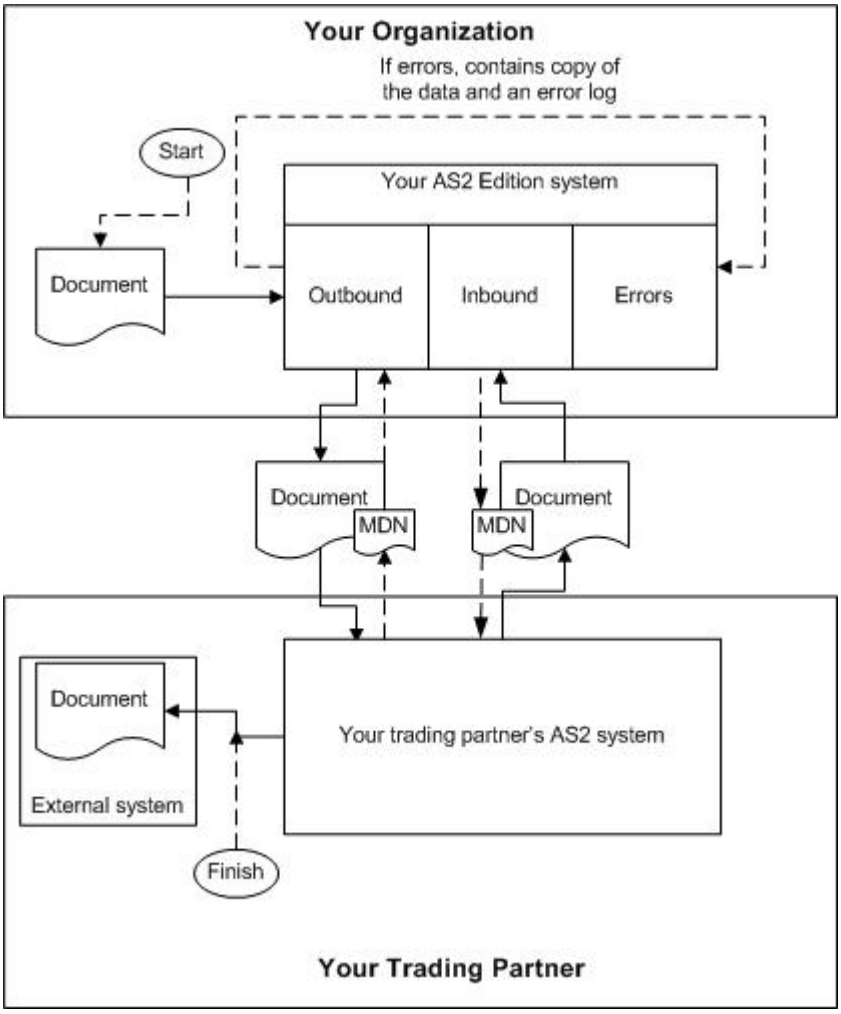
1. Stop the AS2 Edition.
2. Edit the file ediint.properties in the properties directory of your AS2 Edition installation.
3. Add the line ProcessDuplicateMessages = true to the file ediint.properties.
4. Save the file ediint.properties.
5. Start the AS2 Edition.

How the AS2 Edition Works

The AS2 Edition (and using AS2 with the application) works in the following way:

1. You place a document in the Outbound directory or mailbox configured for a trading partner in your AS2 Edition system.
2. The File System adapter or Mailbox adapter checks the trading partner Outbound directory based on the schedule that you have specified.
3. If a document is found in the Outbound directory, the File System adapter (or Mailbox adapter) starts a predefined business process that sends the document to your trading partner's AS2 system.
4. If an error occurs during transmission of your document to your trading partner, a copy of the data and an error log are placed in the Error directory for that trading partner on your system. You can review the error log, make the correction to the data and copy the corrected document to the Outbound directory to be sent to the trading partner.
5. If you requested an MDN, your trading partner's AS2 system returns the MDN to your system. Your AS2 Edition system processes the MDN and updates the EDIINT transaction information for the MDN.
6. If the MDN contains a negative response, a copy of the data and an error log are placed in the Error directory for that trading partner on your system. You can review the error log, make the correction to the data and copy the corrected document to the Outbound directory to be sent to the trading partner.
7. After the document is received by your trading partner, a system external to the application extracts the document for use in another system.

The following figure shows the process described in the preceding steps:



Starting the AS2 Edition in UNIX or Linux

Note: To use AS2 with the application, you need to have the application installed.

To start AS2 Edition in a UNIX or Linux environment, follow these steps:

1. Change the directory to /*install_dir*/bin.
2. Enter `run.sh`.
3. Enter the passphrase that you supplied during installation. If you receive a message about an invalid or corrupt license file, see UNIX/Linux troubleshooting information in the *Installation Guide.*

   When startup is complete, a message like the following is displayed:

   `Open your Web browser to http://host:port/dashboard, where host:port is the IP address and port number where the application resides on your system.`
4. Make a note of the URL address so you can access the application later.

   The system returns you to a UNIX prompt.

Starting the AS2 Edition in Windows

Note: To use AS2 with the application, you need to have the application installed.

To start AS2 Edition in a Windows environment, follow these steps:

1. Do one of the following:
   - Double-click the application shortcut icon on the server desktop. The application starts running.
   - Use Windows Explorer to open the installation directory (c:\sterlingcommerce\si\bin). Then, click on **startWindowsService.cmd**.

   Note: It may take several minutes for the application components to initialize and start up.

   If the application does not start or if you receive a message about an invalid or corrupt license file, see Windows troubleshooting information in the *Installation Guide*.

2. When startup is finished, a message like the following is displayed:

   Open your Web browser to http://host:port/dashboard, where *host:port* is the IP address and port number where the application resides on your system.

   Make a note of the URL address so that you can access the application later.

Starting the AS2 Edition in iSeries

Note: To use AS2 with the application, you need to have the application installed.

To start AS2 Edition in an iSeries environment, follow these steps:

1. Sign onto iSeries with your application user profile.
2. Submit a batch job by entering the following command:

   SBMJOB CMD(QSH CMD('umask 002 ; cd *install_dir*/bin ; ./run.sh')) JOB(SIMAIN)

   Note: The job queue to which you submit the command must allow at least two active jobs. If the maximum number of active jobs is less than two, the application will not start up completely.

   To reduce keying errors at startup, create a command language (CL) program similar to the following example:

   ```
   PGM
   SBMJOB CMD(QSH CMD('umask 002 ; cd install_dir/bin; ./run.sh')) +J
   OB(SIMAIN)
   ENDPGM
   ```

3. Wait for startup to complete, a process that takes 10 to 15 minutes.
4. Startup creates a spool file. When startup is finished, open the QPRINT spool file and check the end of the file for a message about how to connect to the application. For example, you may see a message like the following:

   Open your Web browser to http://*host:port*/dashboard, where *host:port* is the IP address and port number where the application resides on your system.

Make a note of the address so you can access the application later.

Note: It may take several minutes for the application to be available from the Web browser, even after the above URL message has been issued.

5. (Optional) To verify that the application has started normally and completely, view the system through WRKACTJOB and verify that only two QP0ZSPWP jobs (of yours) are left running in your GIS batch subsystem.
6. Prepare your browser to log in to the application. Configure your browser so that there is direct connection between the Web browser and iSeries. Do not configure the browser to use any proxy server between you and iSeries (unless it is a requirement of your network).

Accessing the AS2 Edition

To open the AS2 Edition:

1. Open a browser window.
2. In the Address line, type the following address:

   http://*IP address:port number*/dashboard

   Note: You can either use the IP address or host name to open a login page. Ensure that you separate the IP address (or host name) and port number with a colon (:), for example, http://Application_IPAddress:Installation BasePortNumber+33/dashboard

3. At the login page, type your AS2 Edition user name and password.

   Note: The AS2 Edition generic user name is **as2_user** and the password is **password**. For security purposes, change this user name and password after you have installed AS2 Edition.

Using the AS2 Edition

The following steps illustrate how to begin exchanging documents using the AS2 Edition:

1. Generate or check in one or more system certificates for use by your organization. For more information, see *About Digital Certificates*.
2. Establish or acquire your company's AS2 identifier within your trading partner community. AS2 identifier is an identification number or name that your company uses when communicating with your trading partners.
3. Check out your certificates to files. For more information, see Checking out a System Certificate.
4. If you are going to require inbound SSL, contact Sterling Commerce Customer Support for instructions.
5. Exchange the following information with your trading partners, as appropriate:

   • Certificates
   • AS2 identifiers
   • Server names or IP addresses
   • Server ports
   • Server URLs
   • Agreed-upon algorithms for signing and encryption

- Receipt options

6. Check the trading partner certificates into the application. For information, see Managing Digital Certificates in AS2 Edition.
7. Configure other trading partner settings. For information, see Configuring Organization and Trading Partner Information.

About the AS2 Edition Interface

The AS2 Edition interface enables you to easily navigate the AS2 Edition and quickly enable your organization to exchange documents with your trading partners.

Caution: Use the navigation buttons in the AS2 Edition interface instead of your browser Back and Forward buttons. Using the Back and Forward buttons can cause errors.

The following menu options display the pages that make up the AS2 Edition interface:

Menu Option	Description
File Tracking	Displays the File Tracking page, which is the first page that opens when you access the AS2 Edition. The page provides a link to system logs and after you provide information about your organization, configure your trading partner information, and define file locations for saving documents, this page lists: • Inbound documents from trading partners • Outbound documents to trading partners • Errors that occurred when sending (outbound) documents to trading partners **Note:** The File Tracking page automatically refreshes every 10 seconds. To disable this feature, clear the **Automatically refresh every 10 seconds** check box. If the Multi-Org license is installed, the first page that opens asks which Organization you want to track the files of. As you type the name in the field, a list of possible matches is shown. Make a selection and click Go! The File Tracking page appears.
Business Process	Provides access to the Execution Manager page. The Execution Manager page enables you to: • Monitor predefined business processes. • Perform activities to stop and start business processes, as appropriate.
Central Search	Displays the Central Search page, which enables you to perform basic and advanced searches for: • Live (active) business processes • Active, archived, and restored business processes • EDIINT transaction records for messages that include requests for MDNs
Trading Partners	Displays Trading Partner Configuration pages. Using the Trading Partner Configuration pages, you can establish communication and set preferences, which enable your organization and your AS2 trading partners to exchange documents.
Certificates	Displays the System Certificates pages, which enable you to check in digital certificates for secure document exchange.

Menu Option	Description
Schedules	Displays the Schedules page, which enables you to schedule a business process and search for services, including predefined business processes. After locating a service, you can obtain archiving information about the service, edit the default service schedule to meet your business requirements, and enable or disable the service.

Using AS2 to Support Multi-Organizations

Some businesses have a need to create multiple organizations that they need to represent individually. The AS2 wizard was originally designed to support the creation of only one organization, but with the purchase of a Multi-Org license, users are able to create more than one organization in the AS2 wizard. Users having the Multi-Org license can also create multiple organization and partner profiles for the same identity.

Using the Application with the Sterling Community Manager (SCM)

The application and the Sterling Community Manager (SCM) provide support for setting up an AS2 trading relationship. The SCM-created AS2 resources are updated in the appropriate records in the application database. These records create an AS2 trading relationship with the trading partner, which enables you to use the SCM agreement framework by using an AS2-specific converter.

The AS2 SCM converter has the following functionality:

- Creates trading partner-specific AS2 mailboxes, if they do not currently exist.
- Creates mailboxes routing rules, if they do not currently exist.
- Assigns the /AS2/Organization_Identity_Name/Partner_Identity_Name/Outbound mailbox to the routing rule and creates two mailboxes:
  - /AS2/Organization_Identity_Name/Partner_Identity_Name/Outbound
  - /AS2/Organization_Identity_Name/Partner_Identity_Name/Inbound

  Note: SCM has the option of using mailboxes that exist in the application. If this option is exercised and the mailbox specified has some other name, then the above condition is not applicable.

- Updates AS2 profiles.
- Updates AS2 contracts.
- Creates three AS2 folders for the AS2 File System: the Collection Folder, Extraction Folder, and the Error Log Folder.
- When an Asynchronous MDN is requested through a different URL, a new profile is created.
- SCM question blocks for AS2 enable you to set up partner and sponsor questionnaires, including SSL information.

Auto Complete Lists

Several text box fields in the AS2 wizard now have an automated list to make navigation easier. As you begin to type a word in the text box, a list of possible matches pops up on the screen. The following conditions apply:

- The maximum number of results shown in the list is set to a default value of 500. This limit has been set in a property file and is eligible for customer_overrides.properties configuration, if necessary. The property name is autocomplete2_maxresults.as2.

  Note: This limit is in place to ensure that the system is not overwhelmed with a potentially very large result set. If the server had a very large set of matches (~ 5000), returning all results at the same time could potentially cause an out-of-memory issue or a slow page load time.

- If the number of possible matches exceeds the set limit, the bottom of the list will contain the text "...continue text entry to see additional matches...". This will prompt the user that some matches may not appear in the current list.

A maximum of 15 results are visible at a time to the user, anything over 15 are scrollable.

Import/Export Considerations

There are some important points to consider in regards to import and export behavior of the AS2 wizard profiles for Single-Org users (users who use the default AS2 wizard and don't have a Multi-Org license) and Multi-Org users who have a Multi-Org license and create more than one organization.

- (Single-Org only) For a system without the Multi-Org license (such as, the Single-Org license model) of the AS2 wizard, import of an Organization profile is not allowed if an Organization profile is already present in the system. However, if at the time of import there was no organization profile present in the system, the organization profile being imported would be marked as a default organization. This is useful to the users who want to clean up their system while upgrading and later import their configurations through import files created before upgrade.
- Contracts between Organization and Partner Profiles are needed to setup a communication channel between the two profiles. When importing the organization and partner profiles, contracts should also be imported. If the required contracts have not been imported and you use a Multi-Org license, you will have to manually edit the relationship. If the required contracts have not been imported and you use Single-Org, you will need to edit the partner profile by clicking through all of the edit screens and clicking Finish. Doing this will internally generate the required contracts.
- (Multi-Org only) Relationships get imported or exported along with the Partner Profile, not with the Organization Profile.
- (Multi-Org only) If a new import file is created from Sterling Integrator version 5.1, there are two ways of establishing a working relationship:
  - Import the organizations in a relationship along with the partners. Relationship is established.
  - If only partners are imported, a broken relationship is established because the organization profile was not imported. You will have to manually edit such a relationship and you will be asked to choose an existing organization to link your partner with.

- (Multi-Org only) If you are using import files older than Sterling Integrator version 5.1, there are two ways of establishing a working relationship:
  - Import the organization profile (profile_ORGANIZATION) along with the partner profile(s). The relationship is established.
  - If only partners are imported, a broken relationship is established because importing the organization profile was not satisfied. You will have to manually edit such a relationship and you will be asked to choose an existing organization to link your partner with.

Managing Digital Certificates

Managing Digital Certificates in the AS2 Edition

The application and the AS2 Edition uses digital certificates to securely transport documents between system components. Before you add your trading partners' information to the AS2 Edition, you must obtain and check in any digital certificates.

To help you manage your digital certificates, the AS2 Edition includes the Certificate Wizard, a stand-alone tool that enables you to generate:

- Private and public keys protected with a passphrase
- A certificate signing request (CSR) to send to a trusted certificate authority (CA)

After the CA authorizes the CSR and issues a digitally-signed certificate, you can then use the Certificate Wizard to generate and validate a key certificate that you check in to the AS2 Edition.

Note: To manage digital certificates in the application (that is, if you are not using the AS2 Edition), see the application documentation for Digital Certificates.

As an AS2 user, you need to check in the following certificates into the application:

- CA certificates
- Trusted certificates
- Self-signed certificates

Digital Certificates

Sterling Integrator provides a Certificate Wizard to help you manage your digital certificates. The system uses the following types of digital certificates:

- CA and trusted certificates – Digital certificates for which the system does not have the private keys. These certificates are stored in standard DER format.
- System certificates – A digital certificate for which the private key is maintained in the system. These certificates are stored with the private key in a secure format.

The following is some basic information about how digital certificates are used:

- Every organization exchanging secure documents must have a certificate. You can use the Certificate Wizard to generate the certificate or it can be generated externally.
- Every trading profile for a trading partner with whom you exchange signed and encrypted documents must have a certificate.
- An organization or trading profile can have only one active certificate at a time. In the case of dual certificates, an organization can have one active pair of certificates; one for signature, one for encryption.
- An organization or trading profile must have an active certificate to successfully exchange signed and encrypted documents.
- An organization or trading profile can have multiple valid certificates.
- Certificates can be used to sign documents you transmit by all transport methods.
- The key length for a certificate does not have to be the same as that of a trading partner certificate.
- Before you set the validity period for the certificate, it is recommended you read and apply the best practice recommendations from the Microsoft PKI Quick Guide. For information about the best practice recommendations for using certificates, see *http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html*.

Supported Digital Certificates

Sterling Integrator supports version 3 X.509 of digital certificates. Digital certificates can be either self-signed or CA-signed:

- A self-signed certificate is a digital certificate that is signed with the private key that corresponds to the public key in the certificate, demonstrating that the issuer has the private key that corresponds to the public key in the certificate.
- A CA-signed certificate is a digital certificate that is signed using keys maintained by certificate authorities. Before issuing a certificate, the CA typically evaluates a certificate requestor to determine that the requestor is in fact the certificate holder referenced in the certificate.

Benefits of Self-signed and CA-signed Digital Certificates

When you and your trading partners are deciding whether to generate a self-signed certificate or purchase a signed certificate from a CA, consider the following:

- You can easily create self-signed certificates using Sterling Integrator. However, these self-signed certificates are not verified by a trusted third party.
- The primary advantage of using certificates from a CA is that the identity of the certificate holder is verified by a trusted third party. The disadvantages include extra cost and administrative effort. If you decide to use a third-party certificate, obtain it from a CA.
- A CA provides a centralized source for posting and obtaining information about certificates, including information about revoked certificates.

By default, the system trusts all CA certificates and self-signed certificates generated by the application. You can, however, specify whether all or some certificates issued by a specific CA should be trusted. You can also explicitly not trust a self-signed certificate of a trading partner.

Expiration Dates for Certificates

If an adapter and servlet are used for inbound communications (for example, receiving AS2 data from trading partners), you must monitor the expiration dates of the system certificates to ensure the certificates are valid. Before the certificates expire, they must be replaced with valid certificates.

Create a Self-Signed Certificate

To create a self-signed certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Next to **Create Self-signed Certificate,** click **Go!**
3. Enter the **Name** of the self-signed certificate.
4. Enter the name of the originating **Organization**.
5. Select the **Country** or origin of the self-signed certificate.
6. Enter a contact **e-mail** address for the person responsible for certificates in the organization and then click **Next**.
7. Enter the **Serial Number** for the certificate.

   The serial number is the number you want to assign to the self-signed certificate.
8. Enter the number of days (**Duration**) that the self-signed certificate is valid.
9. Enter the **IP addresses** of the network interfaces you want to associate with the certificate as the SubjectAltName field.
10. Enter the **DNS Names** of the network interfaces you want to associate with the certificate as the SubjectAltName field.
11. Select the **Key Length**. Select one of the following key lengths:
    - 512
    - 1024 (The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 2048 is the most secure, but also the slowest, and may not work with some applications.)
    - 2048
12. Select the **Signing Algorithm**.
13. Select the **Validate When Used** option. Validation options are:
    - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
    - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
14. Set the **Certificate Signing Bit** by selecting the checkbox.
15. Click **Next**.

16. Review the information about the self-signed certificate.
17. Click **Finish**.

Obtain Trusted Certificate Automatically from Trading Partners

The Certificate Capture Utility automates the process of obtaining an SSL certificate from a trading partner. This method of obtaining certificate information allows a partner to easily connect and save a certificate. If desired, an out-of-band security check can then be made before the certificate is checked into the system as a CA or Trusted certificate.

Before you begin:

- Verify that your partner's host system is SSL-enabled.
- Obtain host and port information for your trading partner's server.
- If FTPS mode will be used, determine whether mode will be explicit or implicit.
- Configure the default SSLCertGrabberAdapter service instance to use the appropriate perimeter server and (HTTPS only) proxy server. See the adapter documentation for details.

To obtain the SSL certificate automatically from a trading partner:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > Certificate Capture Utility**.
2. Next to **Capture Partner Certificate**, click **Go!**
3. Select the connection type for the server and click **Next**.
   - FTPS
   - HTTPS
4. Enter the **Host name** or **IP address**.
5. Enter the **Port** number.
6. Select the connection mode for FTPS (if you are using HTTPS, skip this step):
   - Explicit – SSL negotiation occurs after the FTP connection is established. Default.
   - Implicit – SSL negotiation occurs before the FTP connection is established.
7. Click **Next**.

   The system attempts to connect and retrieve certificates.
8. After the capture is complete, review the summary information and decide which certificates you want to save.
9. Select an encoding method for each certificate and click **Save**. Encoding formats are:
   - BASE64 – Uses BASE64 encoding on the standard DER certificate. Default.
   - DER – Standard format for digital certificates, accepted by most applications.
10. Click **Save** and browse to the location where you want to save the file.
11. Accept the default file name or edit it according to your file naming conventions and click **Save**.
12. After saving, the certificates may be checked in into the system. If you decide to check a certificate into the system:
    a) Verify that each certificate is valid and trusted.

b) Check in the certificate as a CA or a Trusted certificate, depending on function. For Certificate Authority-based trust, you may need to check in the certificate chain, excluding the end user certificate. For direct trust, check in the end user certificate.

Configure Status Information on Certificate Summaries

By default, certificate status information is provided at the end of the summary pop-up window when a hyperlinked certificate name is selected. You have the option to include or exclude the status information. Because the status information is compiled in real time, you may not want to include it.

The VerificationOnPopupInfo property controls whether the status information is displayed in the certificate summary. This property is in the ui.properties file. Values for the VerificationOnPopupInfo property are:

- true - include validation information (default)
- false - do not compile or display validation information in the pop-up window
- (any other value) - include validation information

To prevent the compilation and display of the status information:

1. Open the ui.properties file.
2. Update the value of VerificationOnPopupInfo to be false. For example:

   ```
   VerificationOnPopupInfo=false
   ```

3. Save and close the file.
4. Restart Sterling Integrator.

Configure Thumbprint Displays

In addition to the precomputed SHA1 hash, additional certificate thumbprints can be included in certificate display, confirmation, and summary screens. Hash computations are done on demand when a display is generated.

Additional thumbprints display on application GUI screens, but have no effect upon message handling or system communication.

To configure the system to compute and display additional certificate thumbprints:

1. In the ui.properties file, modify this line:

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   To display more than one additional hash, separate the values with commas. For example:

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

Parameter	Description
hash_algorithm	Name of a hash algorithm to be applied to the certificate thumbprint. Valid values are: • SHA-256 • SHA-384 • SHA-512

2. Save and close ui.properties file.
3. Restart Sterling Integrator.

The Certificate Wizard

Sterling Certificate Wizard

The Sterling Certificate Wizard is a Web-deployed application. The wizard enables you to create the following files:

- Certificate Signing Requests (CSRs) – A file to be sent by e-mail to a certificate authority to request an X.509 certificate.
- Key certificates – A combination of an ASCII-encoded certificate and an ASCII-encoded PKCS12 encrypted private key (key cert.txt). If you generate key certificates using the standard format (default) with certain cipers, the output certificate will error when imported into the Sterling Integrator. It is recommended that you use the PKCS12 Format for the key certificates.
- Trusted root files – The trusted root file (trusted.txt) contains a list of trusted sources that enable the certificate wizard to validate a key certificate and ensure a secure connection.

See the wizard online help for information on generating a Certificate Signing Request (CSR), creating a key certificate, and validating a key certificate.

Download and Install the Sterling Certificate Wizard

To download the Sterling Certificate Wizard:

1. Access Sterling Commerce Customer Center.
2. Log in using your **email address** and **password**.
3. Select **Support Center**.
4. In the **Product Support** panel, select **Sterling**.
5. Under the **Product Updates & Downloads,** select **Sterling Certificate Wizard**.
6. Review the information.
7. Download the Release Notes. The Release Notes contains the information on how to install the Certificate Wizard.
8. Download the operating system specific version of the certificate wizard, by clicking **View/Download**.
9. In the **File Download** dialog box, click **Save**.
10. When the Save As dialog box opens, specify the location to save the file. If the web browser adds a number in brackets to the downloaded file (CertWizard .v1300.Unix.tar[1].z), then you need to rename the file before you download it.
11. Use the instructions in the Release Notes to install the Sterling Certificate Wizard.

Start the Sterling Certificate Wizard

You must download and install the Sterling Certificate Wizard before you can start the wizard.

To start the Sterling Certificate Wizard:

1. Click **Start** > **Programs**.

2. Select **Certificate Wizard (version number)** > **Certificate Wizard**.

   The Certificate Wizard is displayed.

   See the wizard online help for information on generating a Certificate Signing Request (CSR), creating a key certificate, and validating a key certificate.

Generate a Certificate Signing Request (CSR) Using the Certificate Wizard

To generate a CSR using the Certificate Wizard:

1. Start the Certificate Wizard.
2. Select **Generate CSR**.
3. Enter the client computer name in the **Common** field.
4. Enter **Country**, **State/Province**, and **City/Locality**.
5. Enter the **Organization/Company Name**.
6. Enter the **Organization Unit**.
7. Enter your **Email Address**.
8. Click **Next**.
9. If you want the pseudo-random number generator (PRNG) to generate a random number for the public/private key pair, enter any random sequence of characters until processing stops.
10. In the Message dialog box that indicates enough random input is now available (random generated number for the public/private key pair), click **OK** and then click **Next**.
11. Enter the **Private Key Length**.

    Valid values are:

    • 512
    • 768
    • 1024
    • 2048
    • 4096

    The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 4096 is the most secure, but also the slowest, and may not work with some applications.

12. Enter the **Passphrase**.

    Passphrase must not be more than 20 characters in length.

13. Enter the passphase a second time in **Confirm Passphrase**.
14. Click **Next**.
15. Enter the **Key file name**.

    Either accept the default directory or click **Browse** and select another directory to save the PKCS12-formatted private key (privkey.txt is the default file name) file.

16. Enter the **CSR file name**

    Either accept the default directory or click **Browse** to select another directory to save the CSR (csr.txt is the default file name) file.

17. Review the information.

18. Click **Next** to create the CSR.

Create a Key Certificate Using the Certificate Wizard

To create a key certificate using the Certificate Wizard:

1. Start the Certificate Wizard.
2. Select **Key Certificate**.
3. Select the key certificate you want to generate from **Output Keycert/Keystore Format**.
   Valid values are Standard, JKS, and PKCS12.
4. Enter the directory or click **Browse** to select the directory to which you have saved the private key file (privkey.txt).
5. Specify the passphrase associated with the private key in the **Private Key Passphrase**.
6. Enter the directory or click **Browse** to select the directory to which you have saved the Digitally-signed (cert.crt) certificate from the CA.
7. Either accept the default directory or click Browse to select another directory to save the key certificate (keycert.txt) file.
8. Click **Generate** to create the key certificate.

Validate a Key Certificate Using the Certificate Wizard

To validate a key certificate using the Certificate Wizard:

1. Start the Certificate Wizard.
2. Select **Verify Certificate**.
3. Enter the **Passphrase**.
4. Select the key certificates to verify.
   Enter the full path to directory and file name or click **Browse** to select the directory and files.
5. Click **Verify**.
   A message displays that includes the verification results for each file you selected.

CA Certificates

CA Certificates

A CA certificate is a digital certificate issued by a certificate authority (CA). The CA verifies trusted certificates for trusted roots. Trusted roots are the foundation upon which chains of trust are built in certificates. In the application, trusting a CA root means that you trust all certificates issued by that CA. If you elect not to trust a CA root, Sterling Integrator does not trust any certificates issued by that CA.

CA certificates contain a public key corresponding to a private key. The CA owns the private key and uses it to sign the certificates it issues. To validate a trusted certificate, you must first check in a CA certificate.

Root certificates from common CAs are contained in a Java keystore (JKS) in the JVM that ships with Sterling Integrator. This allows users to establish some authority-based trust relationships more easily than if they had to search for and obtain the certificates from a CA Web site.

CA certificates are stored separately from trusted certificates in the product.

From the user interface, you can check in CA root certificates that originate from any of the following sources:

- Common CA root certificates shipped with Sterling Integrator in the JKS keystore.
- Only certificates and trusted certificates are recognized. Certificates and private keys are not visible to the UI.
- SSL certificates imported from trading partners.
- Other certificates obtained externally.

Based on security policies at your site, CA certificates in the JKS keystore can also be checked in through the console. Although CA certificates are public documents, you must be careful about who has rights to add them. Someone could maliciously add a false CA certificate in order to verify false end-user certificates.

CA Certificate Names

The CA certificate name is not part of the content of the certificate. They are generally built from the issuer Relative Distinguished Name (RDN) and serial number of the certificate. However, certificates from the JKS keystore are named with an arbitrary string.

Because the certificate name is stored in the system database and is used as the alias to refer to the certificate in the GUI, you may want to rename CA certificates with shorter or more meaningful names based on your file naming conventions. Certificates can be renamed when checked in or when edited.

Search for CA Certificates

To search for a CA certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Complete one of the following and then click **Go!**
   - Under Search in the **by Certificate Name** field, enter a portion of the name or the entire CA certificate name you are searching for. The CA Digital Certificates page lists all CA certificates that match your search criteria.
   - Under List in the **Alphabetically** field, select **ALL** or the letter that begins the name of the CA certificate you are searching for. Selecting ALL lists all CA certificates. The CA Digital Certificates page lists all CA certificates that match your search criteria.

View CA Certificate Summary Information

When a list of certificates is displayed, you can click the certificate name to view summary information about that certificate. The following fields are configurable in the system.

Certificate Summary Field	Description
System Name	The Certificate Name is the database label. It is used to refer to this certificate in the GUI and the application stores this name in its database. The default name for a certificate from the JKS keystore is an arbitrary string. Names for other certificates are built from the issuer relative distinguished name (RDN) and serial number of the certificate. You can change a certificate name to a shorter or more recognizable name when checking in or editing the certificate.
Thumbprint	Information for the SHA1 hash is included by default. To configure computation and display of thumbprint information for other hashes, edit the ui.properties file.
Status	A real-time check of current status, stating whether certificate dates are valid and the certificate has been verified. To configure whether or not this information is computed at the time of display, edit the ui.properties file.

Although this information applies to summary information for a CA certificate, similar fields appear in summary and confirmation screens for other types of certificates.

Check In CA Certificates from the User Interface

Based on security policies at your site, CA certificates in the JKS keystore can also be checked in through the console.

Before you begin, save any CA certificates that you have obtained externally to a local file.

To check in a CA certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **CA**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Next to **Check in New Certificate**, click **Go!**
3. Select a method to import certificates:

Import method	Next Steps
Import from JVM – Imports from the JKS keystore	1. Click **Import** from **JVM**. 2. Accept the default password that appears in the password field and click **Next**. The default keystore password is supplied by Sun Microsystems. If the password field is empty, the system still uses the default password.
Import from File – Imports certificates saved as a file on a local drive	1. Click **Import** from **File**. 2. Enter the Filename or click **Browse** to select a CA certificate file. Click Next.

Import method	Next Steps
	You may ignore the password that appears in the password field. There is no need to erase the entry.

Available certificates are listed with a summary of identifying information. All certificates are selected by default.

4. Click the check boxes to the left of each entry to select or de-select certificates to import.
5. For each certificate selected, accept the suggested Certificate Name or edit it based on your file naming conventions.
6. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Attempts to construct a chain of trust up to the root for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. If you receive a message stating that the certificate duplicates a certificate already in the database, enter Y or N to indicate whether to import the duplicate.

   This check is done on single certificates only. It does not take place when checking in one or more certificates from a file.

   Certificates are identified by SHA1 hash for purposes of determining duplicates. More than one copy of a certificate can be present in the database, since each will populate a different row and have a distinct object ID. The existing certificate is not overwritten.
8. Review the CA certificate information.
9. Click **Finish**.

Check In CA Certificates from the Console

Common CA certificates are contained in a JKS keystore that is part of the JVM that is shipped with Sterling Integrator. The JKS keystore is located at /install_dir/jdk/jre/lib/security/cacerts.You may also obtain certificates externally.

To import certificates into the Sterling Integrator trusted repository, modify the command at /install_dir/install/bin/ImportCACerts.sh (UNIX) or \install_dir\install\bin\ImportCACerts.cmd (Windows).

Before you begin, save any CA certificates obtained externally to a local file.

To check in a CA certificate at the console:

1. Navigate to the installation directory.
2. Navigate to the bin directory.
3. Enter this command:

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   All certificates in the file are listed, one at a time, with these exceptions:

- Entries containing symmetric or private keys are not processed or listed.
- Only the first certificate in a DER-format file is processed and listed.

4. Following the prompts, enter Y (not case-sensitive) for any certificate you want to import.
5. For each certificate accepted, accept the suggested Certificate Name or edit it based on your file naming conventions.
6. If the certificate label duplicates a label already in the database, enter `Y` or `N` (not case-sensitive) to indicate if you want to change the label.

   Although certificates are not generally identified by label and the database allows label duplicates, some services look up certificates by label. Avoid duplicate labels to avoid the possibility of unexpected behavior.
7. If the certificate duplicates a certificate already in the database (as indicated by the SHA1 hash of the certificate, specify with Y or N whether you want to import the duplicate.

   Certificates are identified by SHA1 hash for purposes of determining duplicates. More than one copy of a certificate can be present in the database, since each will populate a different row and have a distinct object ID. The existing certificate is not overwritten.

Edit CA Certificates

To edit a CA certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **CA**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Using either Search or List, locate the CA certificate you want to edit and click **Go!**
3. Next to the **CA certificate** you want to edit, click **edit**.
4. Enter the Certificate Name.
5. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. Review the CA certificate information.
7. Click **Finish**.

Delete CA Certificates

To delete a CA certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **CA**.

- If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**

2. Next to **Alphabetically**, click **Go!**
3. Next to the CA certificate you want to delete, click **delete**.

Trusted Certificates

Search for Trusted Certificates

To search for a trusted certificate:

1. Choose one:

   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**

2. In the Trusted Digital Certificates page, complete one of the following actions, and then click **Go!**:

   - Under Search in the **by Certificate Name** field, enter a portion of the name or the entire trusted certificate name you are searching for. The Trusted Digital Certificates page lists all of the trusted certificates that match your search criteria.
   - Under **List in the Alphabetically** field, select **ALL** or the letter that begins the name of the trusted certificate you are searching for. The Trusted Digital Certificates page lists all of the trusted certificates that match your search criteria.

Check In Trusted System Certificates

Trusted certificates may originate from the following sources:

• SSL certificates imported from trading partners
• Other certificates obtained externally

Before you begin, save the trusted system certificate to a file on your local computer.

To check in a trusted system certificate:

1. Choose one:

   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**

2. Next to **Check in New Certificate**, click **Go!**
3. Enter the **Filename** or click **Browse** to select the file name of the trusted certificate and then click **Next**.
4. Enter the **Certificate Name**.
5. Verify the name of the trusted certificate you are checking in.

   For each certificate you selected, the Certificate Name field shows a suggested name, followed by a summary of the identifying information in the certificate. You can change the name based on your file naming conventions.

6. If you have more than one trusted certificate contained in the file you selected, select the check box to the left of each certificate to check in each certificate.
7. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Attempts to construct a chain of trust up to the root for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
   - CRL cache – Controls whether the CRL Cache is consulted each time the system certificate is used.
8. Review the trusted certificate information.
9. Click **Finish**.

Edit Trusted Certificates

To edit a trusted certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Using either Search or List, locate the trusted certificate you want to edit and click **Go!**
3. Click **edit** next to the trusted certificate you want to edit.
4. Enter the **Certificate Name**.
5. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Attempts to construct a chain of trust up to the root for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
   - CRL cache – Controls whether the CRL Cache is consulted each time the system certificate is used.
6. Review the certificate information.
7. Click **Finish**.

Delete Trusted System Certificates

To delete a trusted system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Next to **Alphabetically**, click **Go!**

3. Next to the trusted certificate you want to delete, click **delete**.

System Certificates

System Certificate Parameter Definitions

If an adapter and servlet are used for inbound communications (for example, receiving AS2 data from trading partners), you must monitor the expiration dates of the system certificates to ensure the certificates are valid. Before the certificates expire, they must be replaced with valid certificates.

Parameter	Description
alias	The key name stored in the HSM. Use only alias names containing characters a-z, A-Z, 0-9 or hyphen (-), and whose total length is no longer than the system GUID length.
certname	Name to assign to the system certificate in the database.
Certtype	The certificate type to import. Four types of certificate files are supported: pkcs12, pkcs8, pem, and keystore. Sterling Integrator only supports pem keys encrypted with DES or 3DES. Use keystore to list or import the keystore.
file	Name of the File to import.
keypass	PIN for the slot on the Eracom device.
keystoretype	Keystore type to import. Valid value is CRYPTOKI.
keystoreprovider	Provider type. Eracom is the only HSM supported provider type. Valid values are: • ERACOM • ERACOM.n (if you are importing certificates to a slot other than the first position)
password	Store passphrase for the certificate file.
pkcs12file	Name of the PKCS12 file to import.
pkcs12storepass	Store passphrase used for the generation of the PKCS12 file.
pkcs12keypass	Valid passphrase for the PKCS12 file.
storepass	PIN for the slot on the Eracom device where the keystore resides.
systempass	System passphrase.

Search for System Certificates

To search for a system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. In the system certificates, complete one of the following actions and then click **Go!**
   - Under Search, in the **by Certificate Name** field, enter a portion of the name or the entire system certificate name you are searching for. The System Certificates page lists all of the system certificates containing the full or partial name you typed.
   - Under **List**, in the **Alphabetically** field, select **ALL** or the letter that begins the name of the CA certificate you are searching for. Selecting ALL lists all system certificates. The System Certificates page lists all of the system certificates that match your search criteria.

Edit System Certificates

To edit a system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Using either Search or List, locate the **system certificate** you want to edit and click **Go!**
3. Next to the system certificate you want to edit, click **edit**.
4. Enter the **Certificate Name**.
5. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. Review the system certificate information.
7. Click **Finish**.

Identify System Certificates in Sterling Integrator

To identify a system certificate:

1. From the **Administration Menu**, select **Deployment > Services > Configuration**.
2. In the List section, select the applicable service or adapter type from the **by Service Type** list and click **Go!**
3. From the list of configurations, choose the configuration.
4. Click the **service name** to view configuration information.
5. Review the certificate summary information.

Check the Expiration Date of a System Certificate

If an adapter and servlet are used for inbound communications (for example, receiving AS2 data from trading partners), you must monitor the expiration dates of the system certificates to ensure the certificates are valid.

To check the expiration date of a system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. To view all system certificates, select **All** from the Alphabetical drop-down list and click **Go!**
3. Select the system certificate name you want to view.

   The Certificate Summary is displayed.
4. In the **Description** section of the Certificate Summary, review information provided in the **Valid Dates** field.
5. Review the information provided in the **Status** section to see if the dates are valid and the certificate has been verified.

Export System Certificates in Sterling Integrator

This export command is only applicable to Sterling Integrator system certificates. You cannot use this command to export system certificates on HSM.

To export a system certificate, enter the following command, with the appropriate parameters:

```
./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass
```

Parameter	Description
keyname	Keyname of the system key to export.
pkcs12filename	Name of the file that contains exported information.
pkcs12storepass	Store password that protects the store.
pkcs12keypass	Key password that protects the key.

Delete System Certificates in Sterling Integrator

You should export a copy of the system certificate to your local disk before you delete it. The OpsDrv, OpsKey, and UIKeys are system certificates that cannot be deleted.

To delete a system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner** > **Digital Certificates** > **System**.

- If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**

2. Next to **Alphabetically**, click **Go!**
3. Next to the system certificate you want to delete, click **delete**.
4. Click **Delete** on the Confirm page.

Check Out System Certificates

To export a system certificate, you must check out the certificate. The following procedure exports only the public certificate, not the private key, and provides you with a public certificate to send to a trading partner.

To check out a system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Using either Search or List, locate the system certificate you want to check out.
3. Next to the system certificate you want to check out, click **check out**.
4. In the **Check Out System Certificate** dialog box, select the certificate format and then click **Go!**:
   - PKCS12 – This option formats the digital certificate as a PKCS12 file. You also have the option of entering a Private Key Password and a Key Store Password.
   - BASE64 – This option uses BASE64 encoding on the standard DER certificate.
   - DER – This standard format for digital certificates is accepted by most applications.
5. In the **File Download** dialog box, click **Save**.
6. In the **Save As** dialog box, select the location where you want to save the certificate, and then click **Save**.

   The option to open the certificate is not supported. You must open the certificate within the operating system. If you receive the error message, This is an invalid Security Certificate file, open the file in a text editor and delete any blank lines before -----BEGIN CERTIFICATE-----. Save the edited file and then try to open the file.
7. Click **Close** In the Check Out System Certificate dialog box.

   The System Certificate page is displayed.

PKCS12 System Certificates

Import PKCS12 System Certificates

To import a PKCS12 system certificate:

1. Navigate to /*install_dir*/install/bin.
2. Enter:

```
./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
keypass
```

Check In PKCS12 System Certificates

Before you begin, you need to save the PKCS12 system certificate to a file on your local computer.

To check in a PKCS12 system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. In the System Certificates page, under Check in, next to **PKCS12 Certificate**, click **Go!**
3. Enter the PKCS12 **Certificate Name**.
4. Enter the **Private Key Password**.
   This is the password used to encrypt the PKCS12 certificate.
5. Enter the **Key Store Password**.
   This is the password for the PKCS12 object. It may be the same as the private key password.
6. Enter the **Filename** or click **Browse** to select the file name of the PKCS12 certificate, and then click **Next**.
7. Select the **Validate When Used** option and then click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
8. Review the PKCS12 system certificate information.
9. Click **Finish**.

Pem, Key, and Keystore System Certificates

Import Pem System Certificates

Only pem keys encrypted with DES or 3DES are supported.

To import a pem system certificate:

1. Navigate to /*install_dir*/install/bin.
2. Enter:

```
./ImportSystemCert.sh -pem systempass certname file password
keystoretype keystoreprovider storepass keypass
```

Import Key System Certificates

To import a key system certificate:

1. Navigate to /*install_dir*/install/bin.

2. Enter:

```
./ImportSystemCert.sh -keycert systempass certname file
password keystoretype keystoreprovider storepass keypass
```

Import Keystore System Certificates

To generate a keystore system certificate on an HSM:

1. Navigate to /*install_dir*/install/bin.
2. Enter:

```
./ImportSystemCert.sh -keystore systempass certname
alias keystoretype keystoreprovider storepass keypass
```

Check In Key System Certificates

Before you begin, save the key system certificate to a file on your local computer.

To check in a key system certificate:

1. Choose one:
   - If you use Sterling Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
   - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates.**
2. Next to **Key Certificate**, click **Go!**
3. Enter the **Certificate Name**.
4. Enter the **Private Key Password.**
   This is the password used to encrypt the private key.
5. Enter the **Filename** or click **Browse** to select the file name of the key certificate and click **Next**.
6. Select the **Validate When Used** option and click **Next**. Validation options are:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. Review the key certificate information.
8. Click **Finish**.

Configuring AS2 Organization and Trading Partner Information

Configuring AS2 Organization and Trading Partner Information

To exchange documents between trading partners, the application and the AS2 Edition use predefined business processes that link trading partners together. A trading partner is a company or business entity that participates in the exchange of business application data. To enable the application and the AS2 Edition to run these business processes, you must provide information about each trading partner participating in the business processes, including your organization.

The application allows you to send e-mail notifications to the e-mail address you configure for your AS2 organization. Additionally, you can configure notifications to be sent when retries fail (an intermediate failure of the sending process) and when the entire sending process fails (after the maximum number of retries have been exhausted), and you can configure these notifications for each trading partner. The e-mail notifications include the following details:

- Message identifier for which the notification applies
- URL to which the message should be sent
- Current attempt number for resending the message
- Total number of retry attempts configured for the trading partner to which the message is being sent
- Business process attempting to send the message
- Timestamp of the notification

You can also specify exactly how messages for which delivery fails should be requeued to be resent. Messages are requeued and the sending process retried a specified number of times at the interval you configure.

The application also offers you an option to defer (until the process for returning a Message Disposition Notification (MDN) is complete the extraction of payload data to either the file system or mailbox that you specify, when the sender requests a synchronous MDN. If the process for returning the MDN fails, the payload is not extracted. This option prevents you from introducing duplicate data into the system from a trading partner that terminates the connection prior to receiving the MDN, and then resends the data.

Note: Deferred extraction must not be enabled if duplicate suppression is enabled. Conversely, if deferred extraction is enabled, duplicate suppression must not be enabled. These two features are mutually exclusive.

Upgrade Considerations When Using Identity

If upgrading, the following considerations should be noted:

- If the user edits the organization or partner profile and also modifies the Identity Name in the profile, the existing profile name will be changed to the new naming convention.
- If the user edits the organization or partner profile and does not make any changes in the Identity Name, the existing profile name will be retained.
- The naming convention for profiles and underlying objects (transports, doc exchanges, and so forth) is **AS2_[ORG | PART]_<Identity Name>**.

Before You Begin

Before you configure information about your organization and trading partners:

- Check in digital certificates for the secure transport of data.
- Collect the following information about your organization and trading partners:
  - Name and address information
  - AS2 identifiers
  - The following certificates, as appropriate:
    - System certificates
    - SSL server certificates
    - End-user certificates
  - IP addresses, port numbers, and URLs
  - Agreed-upon algorithms for signing and encryption
  - Passwords

Creating an AS2 Organization

Before you can create trading partners in your system, you must create your organization. An organization is the company or business entity that administers your system. You can have only one organization for each AS2 Edition. This organization is comparable to a profile and an identity in the application. The application and AS2 Edition only allow you to create one organization (representing your company) because the AS2 Edition is limited to a “one hub, many spokes” configuration (that is, you can send AS2 documents to many partners and receive AS2 documents from those partners, but a “many-to-many” trading partner scenario is not supported).

Keep the following in mind as you create your organization information:

- The option to validate the certificate dates is checked when you check the certificate in (or you can go back and edit that setting), but the actual validation is done when the certificate is used, not at check-in time.
- The system will allow the use of certificates that have expired, or have future go-live dates. This is to support both backwards compatibility and scenarios where partners do not provide an updated certificate but need business continuity.
- "Closest non-future Go Live date, or only certificate in the list" policy means that when multiple certificates are provided, the system will choose the certificate with the nearest "go live" date that is not in the future; however, if there is only one certificate, it will use it, even if it has a future go-live date.

- The ordering of certificates in the user interface is currently an option to change the user interface display of the list. This ordering is not used to determine the order in which the system selects certificates.
- Certificates cannot have the same go-live dates.

To create your organization information:

1. From the File Tracking page, select **Trading Partner**.

   Note: If you are not using the AS2 Edition but are instead using the application to send and receive AS2 messages, from the Administration menu, select **Trading Partner** > **AS2**.

2. In the Trading Partners Configurations page, in the Create section next to New AS2 partner or organization, click **Go!**
3. In the AS2 Configuration Type page, select **Organization** and click **Next**.
4. On the New Identity page you can either use an existing Identity or create a new one:
   a) To use an existing identity, select Use Existing Identity and begin typing the name of the identity. A list automatically appears that match your entry. This list contains all the identities available in your system, some of which might not be associated with any of the AS2 profiles. Make a selection and click **Next**.
   b) To create a new Identity, select **Create a New Identity** and click **Next**.
5. In the Organization Details page, complete the fields, as appropriate, and click **Next**.
6. In the Confirm page, verify the information and click **Finish**.

   To edit information about your organization, see *Editing AS2 Organization and Trading Partner Information*.

Creating an AS2 Organization Reference

Organization Details Page

Field	Description
Identity Name	Name of the identity used for the organization profile. Required.This parameter will be populated automatically if the existing identity is chosen. **Note:** You can not enter spaces in this field.
AS2 Identifier	AS2 identifier of your organization. It could be a DUNS number, EDI interchange ID, e-mail address, or another unique string. Required. **Note:** This parameter will be populated automatically if the existing identity is chosen.
Profile Name	Name of the organization profile. Required.
Exchange Certificate	Name of certificate that your organization is using for decryption. Required. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the

Field	Description
	policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
Signing Certificate	Name of the certificate that your organization is using to sign messages. This certificate can be the same as the certificate that you are using for key exchange. Required. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
E-mail Address (optional)	The e-mail address of your organization. Optional. **Note:** You must provide an e-mail address if you want to receive e-mail notifications, because the SMTP client does not perform a record lookup to retrieve the e-mail address.
E-mail Host (optional)	The host name (server) for your organization's e-mail. Optional (except when E-mail Address is used and then E-mail Host is mandatory).
E-mail Port	The port for the e-mail server. Optional. Default is 25.

Creating an AS2 Trading Partner

You must create a Trading Partner record for each trading partner with whom you will be exchanging AS2 documents. Each time you create a partner using the AS2 wizard, it automatically creates two contracts between that partner profile and the organization—one contract for the sending system and one for the receiving system. A contract has a production profile and a consumption profile, and each contract is associated with a business process.

Additionally, each contract has up to four extensions that are used for AS2. These extensions are the identifiers in the contract and may also be the e-mail addresses from the transport mechanism(s). These identifiers are used by the EDIINT Message service and EDIINT Pipeline service to look up contracts.

The contract lookup fails if more than one contract is found for a set of extensions.

Modifying an SCM Managed AS2-Related Resource

You are warned whenever you attempt to modify an SCM-managed AS2-related resource. The following changes are seen in the existing AS2 user interface:

1. When you click Go! next to List all configurations in the AS2 Trading Partner Configurations page, all the AS2 resources that are managed by SCM have the keyword [SCM] appended to their names.
2. When you click the name of the AS2 resource in the AS2 profiles list page, a line is added to the information summary page indicating whether the AS2 resource is managed by SCM.
3. When you attempt to edit an AS2 resource managed by SCM, a warning dialog box is displayed with the options Yes or No with the following information:

```
Stop! This partner related data is now managed
in Sterling Community Manager. Please change
the ______ information in Sterling Community Manager. Changes made
directly to Sterling Integrator are temporary and will be overwritten
when updates from Sterling Community Manager are absorbed. In case
you have a critical need to update it directly, please make sure
that later on you make the same update in the Partner _______information
in Sterling Community Manager as soon as possible. Do
you still want to proceed and make a temporary change?
```

Caution: Any SCM-managed resource in the application cannot be deleted from within the application. The delete option is not displayed in the application for resources with [SCM] tag. The only way that you can delete resources (managed by SCM) can be deleted in the application is by deleting the corresponding agreements in SCM (for which these resources were created in the application).

Migrating an Existing AS2 Envelope to SCM

You need to use the SCM Migration tool to migrate the existing trading partners, envelopes, contracts, and other configuration information from the application to SCM. SCM Migration tool allows you to move your existing information into SCM where you can manage that information going forward. The Migration tools are responsible for the following tasks:

- When presented with a resource set, a program, and a flag that indicates if the program is a template, the Migration tool verifies that a resource set contains exactly the information required by the program, and matches the sponsor data, if any, in the program. For example, if the program contains two inbound X12 envelope blocks and an AS2 block, the Migration tool verifies that those exact resources are in the set.

Note: A resource set is defined as a set of the application resources associated with a single trading partner. A template program is a program that is going to be copied when migrating. A non-template program is a partner program to which a resource set is directly migrated and that has the appropriate sponsor blocks (display steps) populated.

- For a group of resource sets, the Migration tool determines how to partition so that each partition contains only resource sets that contain the same sponsor information.
- For a resource set, the Migration tool creates the MultiApi call necessary to migrate the resource.

Building and Parsing an AS2 Message

When you build an AS2 message, all the information about security preferences, acknowledgement preferences, and transport is pulled from the consumption profile. The identity identifier and the signing key for the document exchange (if the document is signed) are pulled from the production profile.

When you parse an AS2 message, all the information about security preferences, acknowledgement preferences, and transport is pulled from the production profile. The identity identifier and the exchange key for the transport exchange (if the message is encrypted) are pulled from the consumption profile.

Associating SCM-Managed AS2 Trading Partners with the Application

When an AS2 trading partner is created through the SCM application and ported to the application, it is associated with the corresponding identity in the application. It is then viewable in the application Identity summary page. Clicking the link on the display that mentions an AS2 trading partner record associated with the summary displays a dialog box with the same summary information that is displayed if you had clicked on the name of the identity in the list of the existing AS2 profiles.

Creating a Trading Partner

To create a trading partner:

1. From the File Tracking page, select **Trading Partner.**

Note: If you are not using the AS2 Edition but are instead using the application to send and receive AS2 messages, from the Administration menu, select Trading Partner > AS2.

2. In the Trading Partners Configurations page, in the Create section next to New AS2 partner or organization, click **Go!**
3. In the AS2 Configuration Type page, select **Partner** and click **Next**.
4. On the New Identity page you can either use an existing Identity or create a new one:
   a) To use an existing identity, select **Use Existing Identity** and begin typing the name of the identity. A list automatically appears that match your entry. Make a selection and click **Next**.
   b) To create a new Identity, select **Create a New Identity** and click **Next.**

Note: The identity name and AS2 identifier belong to the selected identity itself and thus any changes will affect all profiles belonging to that identity.

5. In the Identification page, complete the fields, as appropriate, and click **Next.**
6. In the HTTP Communication page, complete the fields, as appropriate, and click **Next**.
7. In the Notifications and Retries page, complete the fields, as appropriate, and click **Next.**

Note: These notification options enable you to configure, on a per trading partner basis, the sending of notifications with either each failed send attempt or when all retries have been exhausted.

8. In the Messages page, complete the fields as appropriate and click **Next**:
9. Complete one of the following steps:
   - If you did not select MDN Receipt, go to step 10.
   - If you selected MDN Receipt, in the Receipt page, complete the following fields, as appropriate, and click **Next**:
10. If you need to set up an additional URL for MDNs (if a trading partner wants MDNs sent to a URL that differs from the main AS2 URL), select Setup additional Server Communications and add the URL.

Note: For the application to send AS2 messages, you must have a trading partner profile set up that includes a transport listing any URL to which you need to send AS2 messages (including MDNs). If you need to send asynchronous MDNs to a URL that is different than the trading partner's main URL, you must configure an additional profile (belonging to that trading partner's identity) with the appropriate information.

11. In the Collection page, complete the fields, as appropriate, and click **Next**.

Note: The folders identified in this step are created during the installation of AS2 Edition and are found in the *install_dir*/as2organization/as2partner. By default, an inbound, outbound, and an error folder is created.

12. In the Confirm page, verify the information and click **Finish** to update the AS2 Edition with your trading partner information.

You can test the AS2 profile by going to the Trading Partner Profile screen in the Admin Console and selecting **Test Now** next to the profile you want to verify. The TestNow option enables you to verify that a new or updated trading partner profile is working correctly.

Creating a Trading Partner Reference

Identification Page

Field	Description
Identity Name	Name of the identity used for your trading partner. Required. **Note:** This parameter will be populated automatically if the existing identity is chosen. **Note:** Do not enter spaces in this field.
AS2 Identifier	AS2 identifier of your trading partner. Required. **Note:** This parameter will be populated automatically if the existing identity is chosen.

HTTP Communication Page

Field	Description
Profile Name	Name of the trading partner profile. Required.
End Point	HTTP address or URL to post AS2 messages to for this specific trading partner. For AS2, the end point must be the complete URL to send messages. Contact your trading partner for the value to use in this field. Required. **Note:** The AS2 Edition includes a configured URL that runs the EDIINTParse business process on the base port + 33.
User ID	User name for HTTP basic authentication, if required to log in to the trading partner system. Optional.
Password	Password that is associated with the User ID identified in the previous field for HTTP basic authentication, if required to log in to the trading partner system. Optional.
Response Timeout (seconds)	Number of seconds the HTTP client adapter waits for a response from the trading partner's server before the system times out. Valid value is number of seconds. Required. **Note:** To avoid timing out, set both the Response Timeout and Socket Timeout fields to the same value and ensure that the value is greater than 180 seconds. This ensures the socket remains open for a reasonable amount of time, so it can receive responses.
Firewall Proxy	IP address, port number, login ID, and password of your proxy server if you need to use a proxy server to connect outbound to this trading partner. Separate values with a comma. If used, you must specify both the login ID and password. Optional. **Note:** If you connect through a proxy server, but authentication is not required, the IP address and port number routes the outbound message through the specified proxy server.
Firewall Connect Count	Number of attempts that the application can make to connect to the proxy server before timing out. Optional. The value of Firewall Connect count should be less than 50. **Note:** If the proxy server is used heavily, set the Firewall Connect Count to a high number to reduce the number of time outs.
Socket Timeout (seconds)	Number of seconds that the socket connection can idle before timing out. Valid value is any positive number that is optimal for your system. Optional. **Note:** To avoid timing out, set both the Response Timeout and Socket Timeout fields to the same value and ensure that the value is greater than 180 seconds.
SSL	Whether Secure Sockets Layer (SSL) should be active. SSL is a negotiation between the client and the server that establishes the method of encrypting and decrypting data transmissions. Optional. Valid values are: • None – SSL is not used (default). • Optional – SSL encryption.

Field	Description
	• Must – Uses this protocol configured for SSL encryption. If you select Optional or Must, the asset protection key must enable SSL for the appropriate protocol.
Key Certificate Passphrase	Type a passphrase to be used with this key certificate. Required only if a key certificate is being used for SSL client side authentication and if the SSL parameter is set to Optional or Must.
Cipher Strength	Strength of the algorithms used to encrypt data. Only accepts supported algorithm. Required. Valid values are: • ALL – Includes all cipher strengths (weak and strong as listed below). • WEAK – Required for international e-commerce if government regulations prohibit STRONG encryption from being exported. Includes the following strengths: • Export level RSA 512-bit with 40-bit RC4 and MD5 • Export level RSA 512-bit with 40-bit DES and SHA1 • STRONG – This is the default. Required if SSL option is anything other than None. Includes the following strengths: • RSA with 128-bit RC4 with SHA1 • RSA with 128-bit AES with SHA1 • RSA with 256-bit AES with SHA1 • RSA with 3DES with SHA1 • RSA with 128-bit RC4 with MD5 • RSA with DES with SHA1 **Note:** If you are using an older or retired adapter, the 128-bit and 256-bit AES ciphers might not be available. For more information on the phases of the Retiring process, see *Retiring and Removed Services and Adapters*.
Key Certificate (System Store)	A combination of ASCII-encoded certificate and ASCII-encoded PKCS5 encrypted key. Select a key certificate. Optional. **Note:** You must have already checked the certificate in to the application for it to be displayed in this list. The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You

Field	Description
	cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
CA Certificates	Certificate used to validate SSL server authentication of the trading partner. Required if you selected Must or Optional in the SSL field. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list. For information about checking in self-signed CA certificates, see *Managing Digital Certificates in AS2 Edition*.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.

Notification and Retries Page

Field	Description
Retry Interval (sec)	The interval (in seconds) after which messages will be requeued and an attempt will be made to resend them (after a send failure). Default is 300. Required.
Max Retries	The maximum number of retries that should be attempted after repeated send failures. Required. Default is 5.
Notify on Immediate Failures	Select this check box to be notified immediately after a send attempt fails. Default is selected (this functionality is turned on).
Notify on Final Failure	Select this check box to be notified after the maximum number of retries (Trading Partner Max Retries) have been exhausted. Default is selected (this functionality is turned on).
Store AS2 Messages in File System	Stores your AS2 messages in the directories you choose. Required. AS2 messages are stored in the directories you choose or, by default are stored in: <*Path to Install_dir*>/as2partner/<Organization Identity Name>/<Partner Identity Name>/Outbound

Field	Description
	<*Path to Install_dir*>/as2partner/<Organization Identity Name>/<Partner Identity Name>/Inbound <*Path to Install_dir*>/as2partner/<Organization Identity Name>/<Partner Identity Name>/error **Note:** When you are configuring a large number of AS2 partners or relationships using the AS2 wizard, we do not recommend that you choose the option to store messages for those partners or relationships in file system directories. Using file system directories with a large number of AS2 partners or relationships may cause Out Of Memory errors to occur due to the large number of schedules that are required. Instead, we recommend that you use the option to store messages in mailboxes since this avoids the need for additional schedules.
Store AS2 Messages in Mailbox	Store AS2 Messages in the mailbox. If you select this option, you are asked to select default or custom mailboxes. **Note:** You must have a Mailbox Edition license to access the Mailbox feature. AS2 messages are stored in the mailboxes you choose or, by default are stored in: /AS2/<<Organization Identity Name>/<Partner Identity Name>/Outbound /AS2/<<Organization Identity Name>/<Partner Identity Name>/Inbound **Note:** When you are configuring a large number of AS2 partners or relationships using the AS2 wizard, we do not recommend that you choose the option to store messages for those partners or relationships in file system directories. Using file system directories with a large number of AS2 partners or relationships may cause Out Of Memory errors to occur due to the large number of schedules that are required. Instead, we recommend that you use the option to store messages in mailboxes since this avoids the need for additional schedules.

Messages Page

Field	Description
Payload Type	Payload is the document at the inner level of the message. The payload type describes the message format for transporting documents. Optional. Valid values are: • Plain Text – Payload is not signed and it is not encrypted. • Signed Detached – Payload is signed with a detached signature, according to the EDIINT specifications. • Encrypted – Payload is encrypted according to the EDIINT specifications. • Signed Detached Encrypted – Payload is signed with a detached signature and then encrypted, according to the EDIINT specifications. This is the default.
MIME Type	How to package the lowest level of payload content (the document at the inner level of a message) to be sent. MIME type helps to implement the EDIINT specification correctly, and provides some flexibility, because receiving programs might expect a specified MIME type and sub-type. The MIME type value is used as the Content-type value in the header of the payload section of the message. Optional.

Field	Description
	Valid values are: • Text – For XML or text • Application – For EDI, or any other type of data (this is the default) • Message • Image • Video • Audio
MIME Sub Type	How to package the lowest level of payload content (the document at the inner level of a message) to be sent. The MIME sub type value combined with the MIME type value creates the Content-type values in the header of the payload section of the message. For example, Content-Type: Application/EDI-X12, where Application is a MIME type and EDI-X12 is the MIME sub type. Optional. Valid values are: • EDI-X12 (this is the default) • EDIFACT • EDI-Consent • Octet-stream – For any type of data • XML • Plain
Compress Data	Level to compress the payload. Optional. Valid values are: • None • Low • Medium • High • Default (this is the default)
Exchange Certificate	Name of the trading partner encryption certificate. Use the trusted certificate that this specific trading partner sent to you. You must check in the trading partner certificate prior to setting up the trading profile. Optional. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. The default value is the Not Before Date.

Field	Description
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
Signing Certificate	Name of the signing certificate that your trading partner sent you. This certificate can be the same as the exchange certificate, if your trading partner uses the same certificate for both encryption and signing. Use the trusted certificate that this specific trading partner sent to you. You must check in the trading partner certificate prior to setting up the trading profile. Required. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
Encryption Algorithm	If you selected a payload type requiring encryption, identifies the encryption algorithm to use. • Triple DES 168 CBC with PKCS5 padding • 56-bit DES CBC with PKCS5 padding (default) • 128-bit RC2 CBC with PKCS5 padding • 40-bit RC2 CBC with PKCS5 padding
Signing Algorithm	Algorithm to use to sign messages to the trading partner. Optional. Valid values are MD5 and SHA1 (Secure Hash Algorithm). The default is SHA1. This field is required if you select a payload type requiring a signature.
MDN Receipt	Whether you request Message Disposition Notifications (MDNs) for messages from your trading partner. Select the check box to view the MDN page. Clear the check box to disable viewing.

Receipt Page

Field	Description
Receipt Signature Type	Type of signing algorithm requested on receipts. Valid values are None (default), MD5, and SHA1. Selection of a value other than None makes the EDIINT Message service request a signed Message Disposition Notification (MDN) when sending messages to the trading partner.
Receipt Timeout	Timeout value in seconds for receipt of expected MDNs. Required. Default is 300.
Wait for synchronous MDN process to complete before extracting data	When selected (and when the sender requests a synchronous MDN), defers the extraction of payload data to the file system or mailbox until the process for returning the MDN is complete. Optional. Default is not selected. **Note:** This option prevents duplicate data that results if a trading partner terminates the connection before receiving a requested MDN and then resends the data. If such data is resent using a different message identifier, the duplicate data cannot be detected unless you have duplicate detection enabled in the translator. **Note:** Deferred extraction (this parameter) must not be enabled if duplicate suppression is enabled in the EDIINT Pipeline service. Conversely, if deferred extraction (this parameter) is enabled, duplicate suppression must not be enabled in the EDIINT Pipeline service. These two features are mutually exclusive. **Note:** We recommend that you do not select this option if you are performing asynchronous MDN delivery because the performance penalties can be substantial. Use this option only for synchronous MDN delivery.
Delivery Mode	Delivery mode for MDNs. Optional. Valid values are: • Synchronous – Requests a synchronous receipt. This the default mode. • Asynchronous HTTP – Request an asynchronous receipt over HTTP. If you select this option, you must put the complete URL identifying where the partner should send the receipt in the Receipt to Address field. • Asynchronous HTTPS – Request an asynchronous receipt over HTTPS. If you select this option, you must put the complete URL identifying where the partner should send the receipt in the Receipt to Address field. • Asynchronous SMTP – Request an asynchronous receipt over SMTP. If you select this option, you must put the complete URL identifying where the partner should send the receipt in the Receipt to Address field.
Receipt to Address	If you are using EDIINT AS2 requesting asynchronous MDNs, you must type the complete URL where you want your trading partner to send the MDN. This may be your usual AS2 URL. Optional. **Note:** The AS2 Edition includes a configured URL that runs the EDIINTParse business process on the base port + 33.
Setup additional Server Communication	Enables you to configure additional transport profiles for a trading partners that requests asynchronous MDNs over HTTP/HTTPS to a URL other than their standard AS2 message URL. The application will not send receipts to URLs that have not been configured in the system. Select this option if your trading partner requests asynchronous HTTP/HTTPS receipts to a URL other

Field	Description
	than their primary AS2 URL. If you select this, repeat steps 5 through 7 again for each additional transport profile.

Collection Page

Field	Description
Collection folder	Directory that contains outgoing (outbound) documents to your trading partners. Required. The default directory is *Install_dir*/as2partner/<*Organization_Identity_Name*>/Partner_Identity_Name/outbound. **Note:** If the trading partner set up that is being created is with the organization that was existing before upgrade, then the collection directory structures will follow old convention which is *install_dir*/as2partner/<*Partner_Name*>/outbound.
Extraction folder	Directory that contains incoming (inbound) documents from your trading partner. Required. The default directory is *install_dir*/as2partner/<*Organization_Identity_Name*>/<*Partner_Identity_Name*>/inbound. **Note:** If the trading partner set up that is being created is with the organization that was existing before upgrade, then the extraction directory structures will follow old convention which is *install_dir*/as2partner/<*Partner_Name*>/inbound.
Error log folder	Directory to which errors are written for outgoing (outbound) documents that contain errors (for example, if the AS2 Edition cannot send a document because of an invalid IP address, the AS2 Edition generates an error log and saves it in this folder). Required. The default directory is *install_dir/*as2partner/<*Organization_Identity_Name*>/<*Partner_Identity_Name*>/error. **Note:** If the trading partner set up that is being created is with the organization that was existing before upgrade, then the error log directory structures will follow old convention which is *install_dir*/as2partner/<*Partner_Name*>/error.
Max files to Collect	The number of files that are picked up from the collection folder each time that the scheduled business process executes. Valid values range from 0 to 500. The default value is All. Optional.
Run service based on a timer every	Hours and minutes for which to run the File System adapter. The default time is five minutes. Required.
Use Message File Name to Save File	Attempts to use the filename specified for the document in the message received from the trading partner to save the file. If your trading partner sends multiple messages with the same included filenames, existing files with the same names (that is, files currently in the inbound directory) may be overwritten.
Include File Name in Message	Includes the name of the file in the message when building messages to send to a trading partner. Valid values are: • None – Does not provide a file name in the message. This is the default. • File Name Only – Provides only the file name in the message.

Field	Description
	• Full Path – Provides the full path to the file in the message.

Note: Monitor the document status by accessing the File Tracking page.

Mailbox Page

Field	Description
Use Default Inbound/Outbound Mailboxes	Whether to use the default inbound and outbound mailboxes. The default mailboxes are: /AS2/<*Organization Identity Name*>/<*Partner Identity Name*>/Inbound and /AS2/<*Organization Identity Name*>/<*Partner Identity Name*>/Outbound
Select Existing Parent Mailbox	If desired, 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 (/). Creates two mailboxes with the format Parent Mailbox/Inbound and Parent Mailbox/Outbound, where Parent Mailbox is the mailbox you selected. **Note:** If a message has been received and there is a problem putting it in the inbound mailbox, the received message will be located in the dead letter mailbox.

Editing AS2 Organization and Trading Partner Information

You can edit the information for your AS2 organization or trading partner after you have entered it. This may be necessary, for example, if you are negotiating a contract and you or your trading partner wants to change some of the information.

Note: Ensure that you do not skip any screens when editing the AS2 partner profiles.

Editing Organization Information

To edit organization information:

1. From the File Tracking page, select **Trading Partner**.

   Note: If you are not using the AS2 Edition but are instead using the application to send and receive AS2 message, from the **Administration** menu, select **Trading Partners** > **AS2**.

2. In the **Search Profiles by Identity** field, you can search several ways, which include:
   - Typing the Identity name. A list automatically appears with a list of profiles that match your entry.
   - Using a partial search by typing only a few characters. A list automatically appears with a list of profiles that match your entry.
   - Not typing anything in the field. This will list all the AS2 profiles in the system.
3. In the list, locate the organization you want to edit and click **edit**.
4. Update your organization information as necessary and click **Next**.

5. Click **Finish** to update the organization with your changes.

Editing Trading Partner Information

To edit trading partner information:

1. From the File Tracking page, select **Trading Partners**.

   Note: If you are not using the AS2 Edition but are instead using the application to send and receive AS2 message, from the **Administration** menu, select **Trading Partners** > **AS2**.

2. In the **Search Profiles by Identity** field, you can search several ways, which include:
   - Typing the Identity name. A list automatically appears with a list of profiles that match your entry.
   - Using a partial search by typing only a few characters. A list automatically appears with a list of profiles that match your entry
   - Not typing anything in the field. This will list all the AS2 profiles in the system.
3. Update your trading partner information as necessary and click **Next**.

   Note: The identity name and AS2 identifier belong to the selected identity itself and thus any changes will affect all profiles belonging to that identity.

4. Click **Finish** to update the trading partner information with your changes

Deleting Trading Partner Information

You can delete the trading partner information when it becomes obsolete. This may be necessary, for example, if a trading partner is lost, or when two trading partners merge.

Note: You can delete only trading partner information and not organization information. AS2 Edition will not work without an organization definition. You cannot delete an AS2 resource managed by SCM from within the application.

To delete trading partner information:

1. From the File Tracking page, select **Trading Partner**.

   Note: If you are not using the AS2 Edition but are instead using the application to send and receive AS2 message, from the **Administration** menu, select **Trading Partners** > **AS2**.

2. In the Trading Partners page, under List, next to Lis all configurations, click **Go!**
   In the AS2 Profiles page, a list of trading partners displays.
3. In the list, locate name of the trading partner whose information you want to delete and click **delete**.
4. In the message prompting you to confirm your intent to delete, complete one of the following actions:
   - Click **OK** to continue the deletion.
   - Click **Cancel** to cancel the deletion.
5. In the Delete Resources page, review the information and click **Next**.

Caution: When you click **Delete**, you completely remove this trading partner from the database. This action cannot be undone.

6. In the Confirm page, click **Delete** to complete the deletion.

Deleting AS2 Resources When an SCM AS2 Delete Agreement is Received by the Application

SCM is used to manage the AS2-related resources in the application. When those resources are managed by SCM, a system warning is displayed if you attempt to edit these resources. When you terminate an agreement in SCM, resources associated with that agreement are deleted in the application. Additionally, the row for the partner is deleted from the AS2_TRADEPART_INFO database table when an SCM AS2 Delete Agreement is received by the application.

Using Communities

A community is a collection or grouping of trading partners for the purpose of achieving a common goal. The goal is defined and enforced by the creator of the community (the host). For example, you can create a group of partners (manufacturers) from whom the host (a retailer) wishes to purchase items. The host can create a separate community for each department (toys, hardware, clothing, groceries, home and garden), one for purchasing resale items (all departments), and one for purchasing maintenance items and services (third-party in-store sub-retailers, facilities maintenance, janitorial services). Community Management tools enable you to quickly and easily create trading partner relationships, including contracts.

You do not need to set up a community to use AS2 with the application.

Creating a New Community

To create a new community:

1. From the Community Management menu, select **Communities > Create Community.**
2. On the community information page, complete the fields as appropriate and click **Next.**
3. Select a **Protocol Type** from the list.
4. Complete the AS2 protocol information page as appropriate, and click **Next.**
5. Click **Next**.

Caution: You can add only one AS2 profile to a community. If you try to add more than one AS2 profile, an error message is displayed. Click **Back** until you reach the Protocols page, then delete all but one AS2 profile. Complete the add community process as normal.

6. You can add a document type to this community for tracking purposes. Otherwise, click **Next** to bypass. Complete the document information page as appropriate and click **Add Document.**
7. Review the document information and click **Next**.
8. You can add more documents at this time. Click **Add**, otherwise, click **Next**.
9. Review and confirm the community information and click **Finish**.
10. Click **Return** to continue.

Creating a New Community Reference

Community Information Page

Community Information Fields	Description
Community Name	New name of the community you are adding. This should be a unique name since you might add more communities. Required.
EDI ID	Your company's EDI ID. Required.
Contact Name	Name of person at your company responsible for this community. Required.
Company's Name	Your company's name. Cannot contain spaces. Required.
Company's Address	Your company's mailing address. Required.
City	Your company's city. Required.
State	Your company's state. Required.
Postal Code	Your company's postal code. Required.
Phone	Your company's phone number. Required.
Country	Trading partner country. Optional.
Time Zone	Trading partner time zone. Optional.
Email	Your company's e-mail address. Required.

AS2 Protocol Information

AS2 Fields	Description
Protocol Type	Protocol this community will accept. Required.
Protocol Name	Unique name for this profile. Required.
End Point	URL. Optional.
End Point IP	Server IP address. Optional.
End Point Port	Port number. Optional.

AS2 Fields	Description
Response Timeout	Number of seconds to wait for a response before ending the session. Optional.
Firewall Proxy	IP address of your firewall proxy. Optional.
Firewall Connection Cnt	Timeout of firewall. Optional.
Socket Timeout	Number of seconds to wait for remote response to a command before ending the session. Optional.
User ID	Unique user ID for this profile. Use only if you want to add security. Optional.
Password	Unique password for this profile. Use only if you want to add security to the Join Community process. Optional.
Send MDN receipt	When receiving an AS2 transmission, send receipt notify. Optional.
Storage Type	Store AS2 message using filesystem or mailboxing. Required.
System Certificate	Additional authentication when transmitting an AS2message. Optional.

Document Information Page

Document Type Fields	Description
Document Name	Name of this document. Required.
Document Type	Document type. Required.
Standard	Standard. Optional.
Version	Version. Optional.
Direction	Document direction - inbound or outbound. Required.

Joining a Community Using the Discovery Location

Note: Before you start this procedure, you need to know the Discovery Location URL.

To join a community using the Discovery Location:

1. From the Community Management menu, click **Communities** > **Join Community**.
2. Select **Discovery Location** and click **Next**.
3. Type or paste the Discovery URL and access code provided by your trading partner, then click **Next**.

4. Select the community you want to join, review the community details, then click **Next**.
5. Select the trading partner to use with this community. Only valid trading partners are listed. If one does not exist, you can create one. Click **Next**.
6. Review and confirm the protocol information populated based on what the community sponsor has entered on their system, then click **Next**.
7. For AS2 you are asked how you would like to store the community protocol (mailbox or file system). Make a selection and click **Next**.
8. Confirm the summary information and click **Finish**.
9. Click **Return** to continue.

Joining a Community Manually

Note: Because you are manually entering your trading partner's information into your system, and there is no synchronization of profile information, your trading partner must also add your trading partner profile information on their side to correspond with yours, and create a contract for this trading relationship.

To manually join a community:

1. From the Community Management menu, click **Communities > Join Community**.
2. Select **Manually Enter Community** and click **Next**.
3. Complete the community information page according to the following table and click **Next**.
4. Select a communications protocol to be used with this trading partner.
5. Complete the AS2 protocol information page and click **Next**.
6. Click **Next**.

Caution: You can add only one AS2 profile to a community. If you try to add more than one AS2 profile, an error message is displayed. Click **Back** until you reach the Protocols page, then delete all but one AS2 profile. Complete the add community process as normal.

7. You can add a document type to this community for tracking purposes. Otherwise, click **Next** to bypass. Complete the document information page according to the following table and click **Add Document**.
8. Review the document information and click **Next**.
9. You can add more documents at this time. Click **Add**, otherwise, click **Next**.
10. Review and confirm the community information and click **Next**.
11. Select or create the trading partner profile you will use with this community and click **Next**. If you choose to create a new profile, type your information in the following fields and click **Next**.
12. Select a communications protocol to be used with this trading partner. The list of protocols is populated by entries made when you created the community this trading partner will join.
13. Based on the protocol selected, you might be required to provide additional information. Type any required information and click **Next**.
14. Review and confirm the community information and click **Finish**.
15. Click **Return** to continue.

Joining a Community Manually Reference

Community Information Page

Community Information Fields	Description
Community Name	Name of the community you want to join. Must be typed exactly as it appears in the system. Required.
EDI ID	The community host's ID. Required.
Contact Name	Name of person at the community's host responsible for this community. Required.
Company's Name	The community host's company name. Cannot contain spaces. Required.
Company's Address	The community host's mailing address. Required.
City	The community host's city. Required.
State	The community host's state. Required.
Postal Code	The community host's postal code. Required.
Phone	The community host's phone number. Required.
Email	The community host's e-mail address. Required.

AS2 Protocol Information

AS2 Fields	Description
Protocol Type	Protocol this community will accept . Required.
Protocol Name	Unique name for this profile. Required.
End Point	URL. Optional.
End Point IP	Server IP address. Optional.
End Point Port	Port number. Optional.
Response Timeout	Number of seconds to wait for a response before ending the session. Optional.
Firewall Proxy	IP address of your firewall proxy. Optional.

AS2 Fields	Description
Firewall Connection Cnt	Timeout of firewall. Optional.
Socket Timeout	Number of seconds to wait for remote response to a command before ending the session. Optional.
User ID	Unique user ID for this profile. Use only if you want to add security. Optional.
Password	Unique password for this profile. Use only if you want to add security to the Join Community process. Optional.
Send MDN receipt	When receiving an AS2 transmission, send receipt notify. Optional.
Storage Type	Store AS2 message using filesystem or mailboxing. Required.
System Certificate	Additional authentication when transmitting an AS2message. Optional.

Document Information Page

Document Type Fields	Description
Document Name	Name of this document. Required.
Document Type	Document type. Required.
Standard	Standard. Optional.
Version	Version. Optional.
Direction	Document direction (Inbound or Outbound). Optional.

Trading Partner Profile Page

Trading Partner Profile Fields	Description
Trading Partner Name	Name for this trading partner profile (cannot contain spaces). Required.
EDI ID	Your identifier. Optional.
Address	Your mailing address. Optional.
City	Your city. Optional.

Trading Partner Profile Fields	Description
State	Your state. Optional.
Postal Code	Your postal code. Required.
Phone	Your phone number. Required.
Country	Your country. Optional.
Time Zone	Your time zone. Optional.
Email Address	Your e-mail address. Required.

Joining a Community Using Onboarding

To complete the online registration, do the following:

1. Type your invite information and click **Next**.
2. From the list, select the community you want to join and click **Next**. There might be only one community to choose from.
3. Type your profile information and click **Next**.
4. From the list, select the AS2 protocol.
5. Complete the following information and click **Next**.
6. Confirm your profile information and click **Finish**.

   Registration is complete. You will receive a confirmation e-mail shortly from your community administrator that registration is complete.
7. Click **Return** to continue.

Joining a Community Using Onboarding Reference

Invite Information Page

Invite Information Fields	Description
User ID	ID you want to use to log in and access your community profile information. Required.
First Name	Your company contact first name. Required.
Last Name	Your company contact last name. Required.
Password	Create a password to use to log in and access your community profile information. Required.

Invite Information Fields	Description
Confirm Password	Type your password again. Required.
Email Address	Your company contact e-mail address. Required.

Profile Information Page

Profile Information Fields	Description
Trading Partner Name	Name for this trading partner profile (cannot contain spaces). Required.
EDIID	Trading partner identifier. Optional.
Address	Trading partner mailing address. Optional.
City	Trading partner city. Optional.
State	Trading partner state. Optional.
Postal Code	Trading partner postal code. Required.
Phone	Trading partner phone number. Required.
Country	Trading partner country. Optional.
Time Zone	Trading partner time zone. Optional.
Email Address	Trading partner e-mail address. Required.

AS2 Information

AS2 Fields	Description
End Point	URL. Optional.
End Point IP	Server IP address. Optional.
End Point Port	Port number. Optional.
Response Timeout	Number of seconds to wait for a response before ending the session. Optional.
Firewall Proxy	IP address of your firewall proxy. Optional.

AS2 Fields	Description
Firewall Connection Cnt	Timeout of firewall. Optional.
Socket Timeout	Number of seconds to wait for remote response to a command before ending the session. Optional.
User ID	Unique user ID for this profile. Use only if you want to add security. Optional.
Password	Unique password for this profile. Use only if you want to add security to the Join Community process. Optional.
Certificate	Additional authentication when transmitting an AS2 message. This option may not be available. Optional.

Editing the HTTP Server Adapter

Caution: Because of our continuing efforts to improve services and adapters to align with new technology and capabilities, the B2B HTTP Server adapter has entered the retirement process in the application and is being replaced with the HTTP Server adapter.

To edit the HTTP Server adapter properties:

1. From the File Tracking page, select Trading Partners.

   Note: If you are not using the AS2 Edition, from the Administration menu, select **Deployment** > **Services**.

2. In the Trading Partner Configurations page, under Edit, next to Edit HTTP Server Adapter, click **Go**!

   Note: If you are not using the AS2 Edition, from the Services menu, select **Configuration**. Then from List by service type, select **HTTP Server Adapter** and click Go!.

3. In the Name page, update the fields as appropriate and click **Next**.
4. In the HTTP Connection Properties page, update the fields, as appropriate, and click **Next**.
5. In the HTTP Connection Properties: SSL Settings page, update the fields, as appropriate, and click **Next**.

   Note: This page is only displayed if you set **Use SSL** to **Must**.

6. In the URI page, complete one of the following steps:
   - To add a new uniform resource identifier (URI), click **add** next to New URI.
   - To edit an existing uniform resource identifier (URI), click **edit** next to the URI you want to edit.
   - To delete an existing uniform resource identifier (URI), click delete next to the URI you want to delete and go to step 8. To take no action on the URIs page, click **Next**.
7. In the URIs: Specification page, update the fields and click **Next**.
8. In the Confirm page, complete the following steps:

a) Verify the changes you made to the HTTP Server adapter.
b) Click **Enable Service for Business Processes**, if you want to enable the service for use with business processes.
c) Click **Finish** to update the AS2 Edition with your changes.

Editing the HTTP Server Adapter Reference

Name Page

Field	Description
Name	Name of this adapter. No action necessary.
Description	Meaningful description for this adapter, for reference purposes. Required.
Select a Group	Specifies a group to associate with this configuration. Valid values are: • None – no group association. This is the default. • Create New Group – Creates a new group to associate with this configuration. • Select Group – Select from the list an existing group to associate with this configuration.

HTTP Connection Properties Page

Field	Description
HTTP Listen Port	The port number on which the Perimeter server process listens for connections from external trading partner HTTP clients. If a local-mode Perimeter server is chosen, this listen port is bound on the local computer. Valid values are 1 through 65536. On many operating systems, only the root user can bind on ports 1 through 1024. Required.
Perimeter Server Name	List of available Perimeter servers, including local-mode Perimeter servers. Required. Default is local-mode Perimeter server.
Total Business Process queue depth threshold	Indicates the maximum number of queued business processes allowed for this adapter. If a value other than 0 is specified, the adapter will limit the number of business process requests put on the queue. If the SUM of business processes on all the queues is less than the queue threshold value, processing occurs normally. For example, a queue threshold of 500 will stop a request if queue 4 has 300 business processes, queue 6 has 200, and queue 7 has 3. If the threshold is exceeded, the adapter will return a Service Unavailable message, which will trigger senders to retry later. Valid value is any integer. 0 indicates no threshold.
Document Storage	Where to store the body of the request document. Valid values are: • System Default • Database • File System Default is System Default. Required. **Note:** For more information about document storage types, see Managing Services and Adapters.
User Authentication Required	Whether to enable HTTP basic authentication. Valid values are: • Yes - A connection must pass HTTP basic authentication to be serviced.

Field	Description
	• No - HTTP basic authentication is not to be used. Default is Yes. Required.
Use SSL	Whether SSL Server authentication must be enabled or not. Valid values are: • Must - SSL is enabled • None - SSL is disabled Default is Must. Required. **Note:** User Authentication without SSL will result in a weak security configuration.

SSL Information

Field	Description
System Certificate	Select a system certificate from the list. This is the private key that the SSL server will use. Required if Use SSL is Must.
Cipher Strength	Specifies the strength of the algorithms (cipher suites) used to encrypt data. Valid values are: • STRONG - Required if Use SSL is Must • ALL - All cipher strengths are supported • WEAK - Often required for international trade, because government regulations prohibit STRONG encryption from being exported Default is STRONG. Required if SSL is checked.
CA Certificate	Move one or more CA Certificates to the use column. These are the digital security certificates that the SSL server will use to authenticate the client. Optional.

Specifications Page

Field	Description
URI	Uniform resource identifier representing incoming requests. Required.
Launch Business Process or WAR	Corresponding business process or a WAR file associated with the URI. Required.
Enter WAR File Path	Specifies WAR file to be launched by URI. Valid value is any accessible path. Required if WAR File is selected for Launch BP or WAR File field.
Business Process	Specifies business process to be launched by URI. Select from the list of available business processes. Required if BP is selected for Launch BP or WAR File field.
Send Raw Messages	Whether the raw message is presented to the business process. The term raw denotes that the primary document associated with the business process contains HTTP headers. Valid values are: • Yes - Both the HTTP headers and the entity body are copied to the body of the business process document before the business process is started. This setting is required for EDIINT AS2, RosettaNet, and ebXML.

Field	Description
	• No - Just the HTTP entity body is copied to the body buffer of the business process document. The headers are not available to the business process. Default is No. Required if BP is selected for Launch BP or WAR File field. **Note:** Any business process that uses the EDIINT Message service requires raw messages.
Run BP in sync mode	Whether to invoke Web services in synchronous mode. Valid values are: • Yes - HTTP Server Adapter bootstraps the BP in synchronous mode. HTTP Server Adapter executes the BP in the same thread. • No - HTTP Server Adapter bootstraps the BP asynchronous mode. Default is No. Required if BP is to be run in synchronous mode.

Configuring AS2 Multiple Organizations

Configuring AS2 Multiple Organizations

Some businesses have a need to create multiple organizations that they need to represent invidivually. The AS2 wizard was originally designed to support the creation of only one organization, but with the purchase of a Multi-Org license, users are now able to create more than one organization in the AS2 wizard. Users without a Multi-Org license will use the default AS2 wizard where only one organization can be created; however, there is no restriction on the number of Trading Partners that can be created.

Configuring the AS2 wizard with a Multi-Org license is a 3 step process that sets a working communication channel between an organization and its partner (Steps 1 and 2 are interchangeable):

1. Create an Organization profile
2. Create a Trading Partner profile
3. Create a Relationship between the two profiles from step 1 and 2

For additional information on configuring AS2 to support multiple organizations see *Creating AS2 Multiple Organization*. For additional information on configuring AS2 organizations, see *Configuring AS2 Organization and Trading Partner Information*.

Using an Existing Identity in the AS2 Multiple Organization Wizard

Users can now use an existing Identity to create a new organization or partner profile. An Identity is created in the Advanced Trading Partner Profile and describes the trading partner and contains information referenced when a business process involving the trading partner is run. A trading partner can have more than one Identity to represent the different ways it does business.

Separate profiles are used for organization information and partner information, each with their own delivery channel, doc exchange, transport, etc. A given identity can be used to create any number of organization and partner profiles.For additional information about Identity, see *Advanced Trading Partner Profile*.

If the user edits the organization or partner profile and modifies the Identity name, then:

• All the dependent profile objects will get renamed accordingly
• The filesystem directories will remain unchaged

- The mailbox directories will remain unchanged

Before You Begin

Before you configure information about your organization and trading partners:

- Check in digital certificates for the secure transport of data.
- Collect the following information about your organization and trading partners:
  - Name and address information
  - AS2 identifiers
  - The following certificates, as appropriate:
    - System certificates
    - SSL server certificates
    - End-user certificates
  - IP addresses, port numbers, and URLs
  - Agreed-upon algorithms for signing and encryption
  - Passwords

Creating AS2 Multiple Organization

To create your organization information:

1. From the Administration menu, select **Trading Partner > AS2.**
2. In the Trading Partners Configurations page, in the Create New section next to New AS2 partner or organization, click **Go!**
3. In the AS2 Configuration Type page, select **Organization** and click **Next**. The New Identity page appears.
4. On the New Identity page you can either use an existing Identity or create a new one:
   a) To use an existing identity, select **Use Existing Identity** and begin typing the name of the identity. A list automatically appears that match your entry. This list contains all the identities available in your system, some of which might not be associated with any of the AS2 profiles. Make a selection and click **Next**.
   b) To create a new Identity, select **Create a New Identity** and click **Next.**
5. In the Organization Details page, complete the fields, as appropriate, and click **Next**:
6. In the Confirm page, verify the information and click **Finish.**
7. To edit information about your organization, see *Editing AS2 Organization* and Trading Partner Information and *AS2 Relationships*.

Creating an AS2 Multiple Organization Reference

Organization Details Page

Field	Description
Identity Name	Name of the identity used for your organization. You can not enter spaces in this field. Required. **Note:** If the option of using an existing identity is selected, this field is populated automatically.
AS2 Identifier	AS2 identifier of your organization. It could be a DUNS number, EDI interchange ID, e-mail address, or another unique string. Required. **Note:** If the option of using an existing identity is selected, this field is populated automatically.
Profile Name	Name of the organization profile. Required.
Exchange Certificate	Name of certificate that your organization is using for decryption. Required. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
Signing Certificate	Name of the certificate that your organization is using to sign messages. This certificate can be the same as the certificate that you are using for key exchange. Required. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.

Field	Description
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
E-mail Address (optional)	The e-mail address of your organization. Optional. **Note:** You must provide an e-mail address if you want to receive e-mail notifications, because the SMTP client does not perform a record lookup to retrieve the e-mail address.
E-mail Host (optional)	The host name (server) for your organization's e-mail. Optional.
E-mail Port	The port for the e-mail server. Optional. Default is 25.

Creating an AS2 Trading Partner for Multiple Organizations

For additional information about creating an AS2 Trading Partner, see *Creating an AS2 Trading Partner*.

To create a trading partner:

1. From the Administration menu, select **Trading Partner > AS2.**
2. In the Trading Partners Configurations page, in the Create New section next to New AS2 partner or organization, click **Go!**
3. In the AS2 Configuration Type page, select **Partner** and click **Next**. The New Identity page appears.
4. In the New Identity page you can either use an existing Identity or create a new one:
   a) To use an existing identity, select **Use Existing Identity** and begin typing the name of the identity. A list automatically appears that match your entry. Make a selection and click **Next**.
   b) To create a new Identity, select **Create a New Identity** and click **Next.**
5. In the Identification page, complete the fields, as appropriate, and click **Next**.
6. In the HTTP Communication page, complete the fields, as appropriate, and click **Next**.
7. In the Messages page, complete the fields as appropriate and click **Next**.
8. Complete one of the following steps:
   • If you did not select MDN Receipt, go to step 10.
   • If you selected MDN Receipt, in the Receipt page, complete the fields, as appropriate, and click **Next**.

9. If you need to set up an additional URL for MDNs (if a trading partner wants MDNs sent to a URL that differs from the main AS2 URL), select Setup additional Server Communications and add the URL.

   Note: For the application to send AS2 messages, you must have a trading partner profile set up that includes a transport listing any URL to which you need to send AS2 messages (including MDNs). If you need to send asynchronous MDNs to a URL that is different than the trading partner's main URL, you must configure an additional profile (belonging to that trading partner's identity) with the appropriate information.

10. On the Confirm page, verify the information and click **Finish** to update AS2 with your trading partner information.

Creating an AS2 Multiple Organization Trading Partner Reference

Identification Page

Field	Description
Identity Name	Name of identity used for your trading partner. Do not enter spaces in this field. Required. **Note:** If the option of using an existing identity is selected, this field is populated automatically.
AS2 Identifier	AS2 identifier of your trading partner. Required. **Note:** If the option of using an existing identity is selected, this field is populated automatically.

HTTP Communication Page

Field	Description
Profile Name	Name of your trading partner profile. Required.
End Point	HTTP address or URL to post AS2 messages to for this specific trading partner. For AS2, the end point must be the complete URL to send messages. Contact your trading partner for the value to use in this field. Required. **Note:** The AS2 Edition includes a configured URL that runs the EDIINTParse business process on the base port + 33.
User ID	User name for HTTP basic authentication, if required to log in to the trading partner system. Optional.
Password	Password that is associated with the User ID identified in the previous field for HTTP basic authentication, if required to log in to the trading partner system. Optional.
Response Timeout (seconds)	Number of seconds the HTTP client adapter waits for a response from the trading partner's server before the system times out. Valid value is number of seconds. Required.

Field	Description
	Note: To avoid timing out, set both the Response Timeout and Socket Timeout fields to the same value and ensure that the value is greater than 180 seconds. This ensures the socket remains open for a reasonable amount of time, so it can receive responses.
Firewall Proxy	IP address, port number, login ID, and password of your proxy server if you need to use a proxy server to connect outbound to this trading partner. Separate values with a comma. If used, you must specify both the login ID and password. Optional. **Note:** If you connect through a proxy server, but authentication is not required, the IP address and port number routes the outbound message through the specified proxy server.
Firewall Connect Count	Number of attempts that the application can make to connect to the proxy server before timing out. Optional. The value of Firewall Connect count should be less than 50. **Note:** If the proxy server is used heavily, set the Firewall Connect Count to a high number to reduce the number of time outs.
Socket Timeout (seconds)	Number of seconds that the socket connection can idle before timing out. Valid value is any positive number that is optimal for your system. Optional. **Note:** To avoid timing out, set both the Response Timeout and Socket Timeout fields to the same value and ensure that the value is greater than 180 seconds.
SSL	Whether Secure Sockets Layer (SSL) should be active. SSL is a negotiation between the client and the server that establishes the method of encrypting and decrypting data transmissions. Optional. Valid values are: • None – SSL is not used (default). • Optional – SSL encryption. • Must – Uses this protocol configured for SSL encryption. If you select Optional or Must, the asset protection key must enable SSL for the appropriate protocol.
Key Certificate Passphrase	Type a passphrase to be used with this key certificate. Required only if a key certificate is being used for SSL client side authentication and if the SSL parameter is set to Optional or Must.

Cipher Strength	Strength of the algorithms used to encrypt data. Only accepts supported algorithm. Required. Valid values are
	• ALL – Includes all cipher strengths (weak and strong as listed below).
	• WEAK – Required for international e-commerce if government regulations prohibit STRONG encryption from being exported. Includes the following strengths:
	  • Export level RSA 512-bit with 40-bit RC4 and MD5
	  • Export level RSA 512-bit with 40-bit DES and SHA1
	• STRONG – This is the default. Required if SSL option is anything other than None. Includes the following strengths:
	  • RSA with 128-bit RC4 with SHA1

Field	Description
	• RSA with 128-bit AES with SHA1 • RSA with 256-bit AES with SHA1 • RSA with 3DES with SHA1 • RSA with 128-bit RC4 with MD5 • RSA with DES with SHA1 : **Note:** If you are using an older or retired adapter, the 128-bit and 256-bit AES ciphers might not be available. For more information on the phases of the Retiring process, see *Retiring and Removed Services and Adapters*.
Key Certificate (System Store)	A combination of ASCII-encoded certificate and ASCII-encoded PKCS5 encrypted key. Select a key certificate. Optional. **Note:** You must have already checked the certificate in to the application for it to be displayed in this list. The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
CA Certificates	Certificate used to validate SSL server authentication of the trading partner. Required if you selected Must or Optional in the SSL field. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list. For information about checking in self-signed CA certificates, see Managing Digital Certificates in AS2 Edition.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.

Field	Description
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.

Messages Page

Field	Description
Payload Type	Payload is the document at the inner level of the message. The payload type describes the message format for transporting documents. Optional. Valid values are: • Plain Text – Payload is not signed and it is not encrypted. • Signed Detached – Payload is signed with a detached signature, according to the EDIINT specifications. • Encrypted – Payload is encrypted according to the EDIINT specifications. • Signed Detached Encrypted – Payload is signed with a detached signature and then encrypted, according to the EDIINT specifications. This is the default.
MIME Type	How to package the lowest level of payload content (the document at the inner level of a message) to be sent. MIME type helps to implement the EDIINT specification correctly, and provides some flexibility, because receiving programs might expect a specified MIME type and sub-type. The MIME type value is used as the Content-type value in the header of the payload section of the message. Optional. Valid values are: • Text – For XML or text • Application – For EDI, or any other type of data (this is the default) • Message • Image • Video • Audio
MIME Sub Type	How to package the lowest level of payload content (the document at the inner level of a message) to be sent. The MIME sub type value combined with the MIME type value creates the Content-type values in the header of the payload section of the message. For example, Content-Type: Application/EDI-X12, where Application is a MIME type and EDI-X12 is the MIME sub type. Optional. Valid values are: • EDI-X12 (this is the default) • EDIFACT

Field	Description
	• EDI-Consent • Octet-stream – For any type of data • XML • Plain
Compress Data	Level to compress the payload. Optional. Valid values are: • None • Low • Medium • High • Default (this is the default)
Exchange Certificate	Name of the trading partner encryption certificate. Use the trusted certificate that this specific trading partner sent to you. You must check in the trading partner certificate prior to setting up the trading profile. Optional. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
Signing Certificate	Name of the signing certificate that your trading partner sent you. This certificate can be the same as the exchange certificate, if your trading partner uses the same certificate for both encryption and signing. Use the trusted certificate that this specific trading partner sent to you. You must check in the trading partner certificate prior to setting up the trading profile. Required. **Note:** The Configure Certificates link enables you to open a common window displaying all certificates list that you may use. This window is used to select multiple certificates for the purpose of seamless transition from one certificate to the other when its validity expires and to select the policy for this certificate. The default policy is Closest non-future Go Live Date or the only certificate in the list.

Field	Description
Selection policy	This is a default policy which returns the certificate with the closest non-future Go Live Date. Default value is Closest non-future Go Live Date or the only certificate in the list.
Go Live Date	This is the date when the certificate becomes valid and is ready for use by the application. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Go Live Date that precedes the Not Before Date in the digital certificate. The default value is the Not Before Date.
Not After Date	This is the date beyond which the certificate is no longer valid. Using this parameter results in less system down time for both you and your trading partner when your certificates expire. You cannot specify a Not After Date that succeeds the termination date in the certificate. The default value is Not After Date.
Encryption Algorithm	If you selected a payload type requiring encryption, identifies the encryption algorithm to use. • Triple DES 168 CBC with PKCS5 padding • 56-bit DES CBC with PKCS5 padding (default) • 128-bit RC2 CBC with PKCS5 padding • 40-bit RC2 CBC with PKCS5 padding
Signing Algorithm	Algorithm to use to sign messages to the trading partner. Optional. Valid values are MD5 and SHA1 (Secure Hash Algorithm). The default is SHA1. This field is required if you select a payload type requiring a signature.
MDN Receipt	Whether you request Message Disposition Notifications (MDNs) for messages from your trading partner. Select the check box to view the MDN page. Clear the check box to disable viewing.

Receipt Page

Field	Description
Receipt Signature Type	Type of signing algorithm requested on receipts. Valid values are None (default), MD5, and SHA1. Selection of a value other than None makes the EDIINT Message service request a signed Message Disposition Notification (MDN) when sending messages to the trading partner.
Receipt Timeout	Timeout value in seconds for receipt of expected MDNs. Required. Default is 300.
Wait for synchronous MDN process to complete before extracting data	When selected (and when the sender requests a synchronous MDN), defers the extraction of payload data to the file system or mailbox until the process for returning the MDN is complete. Optional. Default is not selected. **Caution:** This option prevents duplicate data that results if a trading partner terminates the connection before receiving a requested MDN and then resends the data. If such data is resent using a different message identifier, the duplicate data cannot be detected unless you have duplicate detection enabled in the translator.

Field	Description
	Note: Deferred extraction (this parameter) must not be enabled if duplicate suppression is enabled in the EDIINT Pipeline service. Conversely, if deferred extraction (this parameter) is enabled, duplicate suppression must not be enabled in the EDIINT Pipeline service. These two features are mutually exclusive. **Note:** We recommend that you do not select this option if you are performing asynchronous MDN delivery because the performance penalties can be substantial. Use this option only for synchronous MDN delivery.
Delivery Mode	Delivery mode for MDNs. Optional. Valid values are: • Synchronous – Requests a synchronous receipt. This the default mode. • Asynchronous HTTP – Request an asynchronous receipt over HTTP. If you select this option, you must put the complete URL identifying where the partner should send the receipt in the Receipt to Address field. • Asynchronous HTTPS – Request an asynchronous receipt over HTTPS. If you select this option, you must put the complete URL identifying where the partner should send the receipt in the Receipt to Address field. • Asynchronous SMTP – Request an asynchronous receipt over SMTP. If you select this option, you must put the complete URL identifying where the partner should send the receipt in the Receipt to Address field.
Receipt to Address	If you are using EDIINT AS2 requesting asynchronous MDNs, you must type the complete URL where you want your trading partner to send the MDN. This may be your usual AS2 URL. Optional. **Note:** The AS2 Edition includes a configured URL that runs the EDIINTParse business process on the base port + 33.
Setup additional Server Communication	Enables you to configure additional transport profiles for a trading partners that requests asynchronous MDNs over HTTP/HTTPS to a URL other than their standard AS2 message URL. The application will not send receipts to URLs that have not been configured in the system. Select this option if your trading partner requests asynchronous HTTP/HTTPS receipts to a URL other than their primary AS2 URL. If you select this, repeat steps 5 through 7 again for each additional transport profile.

Testing the AS2 Profile

You can test the AS2 profile by going to the Trading Partners Configuration screen in the Admin Console and selecting **Test Now** next to the profile you want to verify. The TestNow option enables you to verify that a new or updated trading partner profile is working correctly. For additional information about TestNow, see *Using the AS2 and HTTP TestNow Feature*

Creating an AS2 Relationship for Multiple Organizations

A new concept of Relationship has also been introduced for users with a Multi-Org license while using the AS2 wizard. A Relationship is an entity where users define the rules explicitly needed for a message transfer

between two parties: organization and partner. From the main page of AS2 wizard, relationships can be either created or searched. Relationships do not have names, they are a mapped combination of the names of the organization and partner.

There can be multiple organizations/partner profiles for a given identity; however, the number of relationships between a given pair of identities and AS2 identifiers is limited to only one. When creating or editing a relationship you will have to choose whether to use filesystem or mailbox for storing the messages. Based on the choice the user will have to provide the details of filesystem or mailbox.

To create a relationship:

1. From the Administration menu, select **Trading Partner > AS2.**
2. In the Trading Partners Configurations page, in the Create New section next to AS2 trading relationship, click **Go!**
3. In the AS2 Relationship page, complete the fields, as appropriate, and click **Next**.
4. In the Notifications and Retries page, complete the fields, as appropriate, and click **Next.**

   Note: These notification options enable you to configure, on a per trading partner basis, the sending of notifications with either each failed send attempt or when all retries have been exhausted.

5. In the Collection page, complete the fields, as appropriate, and click **Next**.

   Note: The folders identified in this step are created when an AS2 relationship is saved and are found in the *install_dir/as2partner/<Organization Identity Name>/<Partner Identity Name>* Prior to an upgrade, the the collection and extraction directory structures follow this convention: *install_dir/as2partner/<Partner Identity Name>*.By default, an inbound, outbound, and an error folder is created. If you create a relationship using storage type as a mailbox and an error appears indicating that Mailboxes are in use and a relationship cannot be created, then delete the existing mailbox directory and proceed with creating the new relationship.

   When you choose a mailbox, you can select either the default or customized mailboxes.

6. In the Confirm page, verify the information and click **Finish** to update AS2 with your trading partner information.

Creating an AS2 Relationship for Multiple Organizations Reference

AS2 Relationship Page

Field	Description
Organization	Name of the organization. Required. **Note:** As you type, a list appears with matching entries. Double-click an entry to select it.
Partner	Name of the trading partner. Required. **Note:** As you type, a list appears with matching entries. Double-click an entry to select it.

Notifications and Retries Page

Field	Description
Retry Interval (sec)	The interval (in seconds) after which messages will be requeued and an attempt will be made to resend them (after a send failure). Default is 300. Required.
Max Retries	The maximum number of retries that should be attempted after repeated send failures. Required. Default is 5.
Notify on Immediate Failures	Select this check box to be notified immediately after a send attempt fails. Default is selected (this functionality is turned on).
Notify on Final Failure	Select this check box to be notified after the maximum number of retries (Trading Partner Max Retries) have been exhausted. Default is selected (this functionality is turned on).
Wait For Synchronous MDN Process To Complete Before Extracting Data:	Select this check box to wait for the synchronous MDN process to complete before extraction of data.
Store AS2 Messages in File System	Stores your AS2 messages in the directories you choose in this procedure. Required. AS2 messages are stored in the directories you choose or, by default are stored in: <*Path to Install_dir*>/as2partner/<Organization Identity Name>/<Partner Identity Name>/outbound <*Path to Install_dir*>/as2partner/<Organization Identity Name>/<Partner Identity Name>/inbound <*Path to Install_dir*>/as2partner/<Organization Identity Name>/<Partner Identity Name>/error **Note:** If the relationship that is being created is with the organization that was existing before upgrade then the collection and extraction directory structures will follow old convention. For example, for the collection folder, the directory structure would be as follows:*Path to Install_dir*/as2partner/*Partner Identity Name*/Outbound
Store AS2 Messages in Mailbox	Store AS2 Messages in Mailbox. **Note:** You must have a Mailbox Edition license to access the Mailbox feature. AS2 messages are stored in the mailboxes you choose or, by default are stored in: AS2/<Organization Identity Name>/<Partner Identity Name>/Outbound AS2/<Organization Identity Name>/<Partner Identity Name>/Inbound AS2/<Organization Identity Name>/<Partner Identity Name>/error

Collection Page

Field	Description
Collection folder	Directory that contains outgoing (outbound) documents to your trading partners. Required. The default directory is *install_dir*/as2partner/<*Organization Identity Name*>/<*Partner Identity Name*>/outbound.
Extraction folder	Directory that contains incoming (inbound) documents from your trading partner. Required. The default directory is *install_dir*/as2partner/<*Organization Identity Name*>/<*Partner Identity Name*>/inbound.
Error log folder	Directory to which errors are written for outgoing (outbound) documents that contain errors (for example, if the AS2 Edition cannot send a document because of an invalid IP address, the AS2 Edition generates an error log and saves it in this folder). Required. The default directory is *install_dir*/as2partner/<*Organization Identity Name*>/<*Partner Identity Name*>/error.
Max files to Collect	The number of files that are picked up from the collection folder each time that the scheduled business process executes. Valid values range from 0 to 500. The default value is All. Optional.
Run service based on a timer every	Hours and minutes for which to run the File System adapter. The default time is five minutes. Required.
Use Message File Name to Save File	Attempts to use the filename specified for the document in the message received from the trading partner to save the file. If your trading partner sends multiple messages with the same included filenames, existing files with the same names (that is, files currently in the inbound directory) may be overwritten.
Include File Name in Message	Includes the name of the file in the message when building messages to send to a trading partner. Valid values are: • None – Does not provide a file name in the message. This is the default. • File Name Only – Provides only the file name in the message. • Full Path – Provides the full path to the file in the message.

Mailbox Page

Field	Description
Use Default Inbound/Outbound Mailboxes	Whether to use the default inbound and outbound mailboxes. The default mailboxes are: /AS2/<*Organization Identity Name*>/<*Partner Identity Name*>/Inbound and /AS2/<*Organization Identity Name*>/<*Partner Identity Name*>/Outbound
Select Existing Parent Mailbox	If desired, 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 (/). Creates two mailboxes with the format Parent Mailbox/Inbound and Parent Mailbox/Outbound, where Parent Mailbox is the mailbox you selected. **Note:** All failed messages are placed in the Dead Letter Mailbox.

Editing AS2 Organization, Trading Partner Information, and AS2 Relationships

You can edit the information for your AS2 organization, trading partner, or AS2 relationship information after you have entered it. This may be necessary, for example, if you are negotiating a contract and you or your trading partner wants to change some of the information.

Note: Ensure that you do not skip any screens when editing the AS2 partner profiles.

Editing Organization Information for Multiple Organizations

To edit organization information:

1. From the Administration menu, select **Trading Partners** > **AS2**.
2. In the **Search Profiles by Identity** field, you can search several ways, which include:
   - Typing the Identity name. A list automatically appears with a list of profiles that match your entry.
   - Using a partial search by typing only a few characters. A list automatically appears with a list of profiles that match your entry.
   - Not typing anything in the field. This will list all the AS2 profiles in the system.
3. Click **Go!**
4. In the list, locate the organization you want to edit and click **edit**.
5. Update your organization information as necessary and click **Next**.
6. Click **Finish** to update the organization with your changes.

Editing Trading Partner Information for Multiple Organizations

To edit trading partner information:

1. From the Administration menu, select **Trading Partners** > **AS2**.
2. In the **Search Profiles by Identity** field, you can search several ways, which include:
   - Typing the Identity name. A list automatically appears with a list of profiles that match your entry.
   - Using a partial search by typing only a few characters. A list automatically appears with a list of profiles that match your entry
   - Not typing anything in the field. This will list all the AS2 profiles in the system.
3. Click **Go!**
4. In the list, locate the trading partner you want to edit and click **edit**.
5. Update your trading partner information as necessary and click **Next**.
6. Click **Finish** to update the trading partner information with your changes.

Editing Relationship Information for Multiple Organizations

To edit relationship information:

1. From the Administration menu, select **Trading Partners > AS2**.
2. In the **Search Relationships** field, you can search several ways, which include:
   - Typing the Organization and Partner name in the respective boxes. A list automatically appears with a list of profiles that match your entry.
   - Using a partial search by typing only a few characters. A list automatically appears with a list of relationships that match your entry
   - Not typing anything in the field. This will list all the AS2 profiles in the system.
3. Click **Go!** In the list, locate the relationship you want to edit and click **edit**.
4. In the list, locate the relationship you want to edit and click **edit**.
5. Update your relationship information as necessary and click **Next**.
6. Click **Finish** to update the relationship information with your changes.

Deleting Organization, AS2 Trading Partner, or Relationship Information

You can delete an organization, trading partner, or relationship information when it becomes obsolete.

Note: When you delete an organization or a partner, it also deletes all the relationships associated with it.

Deleting Organization Information

To delete organization information:

1. From the Administration menu, select **Trading Partner > AS2**.
2. In the Search Profiles by Identity area, begin typing the name of the Organization, a list automatically appears that match your entry.
3. Double-click a selection and click **Go!**
4. Identify the organization you want to delete and click **delete**.
5. In the message prompting you to confirm your intent to delete, complete one of the following actions:

   Note: When you click **delete**, you will be recommeneded to export and save a copy to offline storage. You can decide if you want to do so.

   - Click **OK** to continue the deletion.
   - Click **Cancel** to cancel the deletion.
6. In the Delete Resources page, review the information and click **Next**.

   Note: When you click **Delete**, you completely remove this organization from the database. Deleting an organization will delete all the associated resources and any dependant relationship(s). This action cannot be undone.
7. In the Confirm page, click **Delete** to complete the deletion.

Deleting AS2 Trading Partner Information

You can delete the trading partner information when it becomes obsolete. This may be necessary, for example, if a trading partner is lost, or when two trading partners merge.

Note: AS2 Edition will not work without an organization definition. You cannot delete an AS2 resource managed by SCM from within the application. The organization information can be deleted in a multi-org scenario..

To delete trading partner information:

1. From the File Tracking page, select **Trading Partner**.

   Note: If you are not using the AS2 Edition but are instead using the application to send and receive AS2 messages, from the Administration menu, select **Trading Partner > AS2**.

2. In the Trading Partners page, under Search Profiles by Identity area, begin typing the first few letters of the trading partner name, a list automatically appears that matches your entry. Select the trading partner name and click**Go!**
3. Identify the trading partner whose information you want to delete and click **delete**.
4. In the message prompting you to confirm your intent to delete, complete one of the following actions:

   Note: When you click **delete**, you will be recommeneded to export and save a copy to offline storage. You can decide if you want to do so.

   • Click **OK** to continue the deletion.
   • Click **Cancel** to cancel the deletion.

5. In the Delete Resources page, review the information and click **Next**.

   Note: When you click **Delete**, you completely remove this trading partner from the database. This action cannot be undone.

6. In the Confirm page, click **Delete** to complete the deletion.

Deleting Relationship Information

To delete relationship information:

1. From the Administration menu, select **Trading Partner > AS2**.
2. In the Search Relationships area in the Organization and Partner fields, begin typing the names of the Organization and Partners you set up a relationship with. A list automatically appears that match your entry.
3. Double-click a selection and click **Go!**
4. In the list, locate the relationship you want to delete and click **delete**.
5. In the message prompting you to confirm your intent to delete, complete one of the following actions:

   • Click **OK** to continue the deletion.
   • Click **Cancel** to cancel the deletion.

6. In the Delete Resources page, review the information and click **Next**.

Note: When you click **Delete**, you completely remove this relationship from the database. Deleting a relationship does not affect its associated profiles (organization and partner). Deleting a relationship does not delete the filesystem/mailbox directories. The user will have to manually delete these items.This action cannot be undone.

7. In the Confirm page, click **Delete** to complete the deletion.

Tracking and Managing AS2 Document Exchange

Tracking AS2 Documents

The application provides information about inbound and outbound documents and any designated outbound documents that cannot be processed because of an error. Viewing the information about documents can help you determine if further action is necessary.

The Current Documents feature offers the following benefits:

- You can monitor document processing to ensure documents are processing successfully, and take corrective action if necessary.
- If a problem document is noted, you can view document details with one click to see what happened.
- By default, the page is automatically refreshed every minute for the most current information.
- You can change the number of documents displayed per page, change the name of the document displayed to something more meaningful—for example, document type—and enable detailed document tracking.

To access Current Documents, go to **Business Processes > Current Documents**. The following information is available on the Current Documents page:

- Up to a week of processed documents is displayed. To view documents older than one week, use the **Advanced Search > Documents** feature.
- Documents are generally listed in the order received, with the most current documents at the top.
- Select Automatically refresh every minute to get current information. Deselect this option to disable the automatic refresh.
- Last update date and time displays when the page was last refreshed.

Note: To modify file locations, see *Editing Trading Partner Information*.

To track documents:

Field Name	Description
Status	Green or red traffic light indicates the processing status of the document: • Green status indicates no errors or warnings occurred during processing. • Red status indicates errors or warnings were encountered during processing.
Document	Name of the document processed. This can be changed in the business process so that a meaningful name will appear instead of the default. Most pre-configured business processes already have the document name established. Click the document name to view the contents. **Note:** You can change the meta data for your service to display a more meaningful document name, such as the document type, in Current Documents instead of the default name. The default display is the Body Name, if available, otherwise it is the document ID. Some services, such as EDI documents (EDIFACT, for example), are already configured to display the document type. Contents will not be viewable if encrypted or obscured.
Proc. ID	Processing ID assigned by the application as an identification number. Click the Processing ID to view Business Process Details.
Sender ID	ID of the document sender as found in the document. If no ID is found, Sender ID is None.
Receiver ID	ID of the document receiver as found in the document. If no ID is found, Receiver ID is None.
Correlations	Click the Correlations icon to view document correlations.
Details	If document tracking is enabled at the business process level, you can view the document history by clicking on Details from the Current Documents page.

Changing the Number of Documents Displayed When Tracking Documents

Current Documents displays the most recent 15 documents that have been processed. You can change this and display more than 15 documents per page by making an adjustment on the My Account page.

To change the number of documents displayed:

1. Select **Accounts > My Account**. The My Account page is displayed.
2. In the Preferences section, next to Page Size for Current Documents, select the number of documents you want to display on each page. Remember that the larger number you select, the more you will have to scroll to see all of the documents displayed, and the system may take longer to display results.
3. Click **Save**. Your changes are saved. Log out the application and then log back in to see the change in preferences.

Running and Stopping Predefined AS2 Business Processes

Predefined business processes associated with a document that contains errors may continue to run unnecessarily. Using the Business Processes page, you can not only obtain general and detailed processing information about predefined business processes, you can also run and stop business process and any subprocesses. After reconciling document errors, you can then use the Business Processes to run the business process again.

To access the Business Processes page and perform activities for predefined business processes:

1. From the Administration Menu, select **Business Processes > Manager**.
2. In the Business Processes page, use the following fields and columns to view business process information and perform other activities, as appropriate:

Field/Column	Description
Name	Name of the business process.
Execute	Run the business process and any subprocesses.
Stop All	Stop the business process and any subprocesses waiting to run.
Date	Date and time the business process ran.
Life Span	Expiration time of the business process and archiving details.
Username	User associated with the business process.

Searching for Business Process (Basic)

In the application, you can use the Central Search pages to perform basic and advanced searches for information about:

• Additional live (active), archived, and restored predefined business processes
• EDIINT transaction records for business processes that included EDI interchange processing

To perform a basic search for a business process:

1. From the **Administration** menu, select **Business Processes > Central Search**.
2. In the Central Search page, specify any combination of the following search criteria, and then click **Go!**

- Business Process – Display business processes by names containing specified characters or strings.
- Status – Display business processes that resulted with a success or error outcome.
- Start Date From/Start Date To – Display business processes run within specific start dates and times.

3. In the Central Search Results page, click the number link that indicates the number of matches. The Monitor page opens, listing the business processes that match your search criteria. For information about the Monitor page, see *Viewing General Processing Information*.

Searching for Business Process (Advanced)

In the application, you can use the Central Search pages to perform basic and advanced searches for information about:

- Additional live (active), archived, and restored predefined business processes
- EDIINT transaction records for business processes that included EDI interchange processing

You can conduct advanced searches for business processes under a variety of characteristics. You can search for:

- Business Processes in the application
- EDIINT transactions
- Correlations

The application also enables you to search for business processes by:

- Location of business process
- Business process ID
- Business process name

To conduct an advanced search for a business process in the application:

1. From the **Administration** menu, select **Business Processes > Central Search.**
2. In the Central Search page, under Advanced Search, ensure that the application is selected in the list and click **Go!**
3. In the Business Process Monitor Advanced Search page, specify any combination of the following search criteria, as appropriate:

Field	Description	Action
Search Location		
Select the area to search from	Business processes maintained in a specific location.	Select one of the options: • Live Tables – Display live (active) business processes. • Archive Tables – Display data for business processes that are archived. • Restored Tables – Display data for business processes that have been restored from an offline location.
Search Using Business Process ID		

Field	Description	Action
Process ID	ID assigned by the AS2 Edition to identify a business process.	Type the ID for the business process.
Search Using Business Process Name		
Business Processes	List of business processes currently maintained in the application and the AS2 Edition.	Select a business process from the list.
System Business Processes	The system business processes (that is, business processes that complete or have completed system operations).	Select a system business process from the list.
State	Current or final state of a business process.	The default value is ALL (displays all business processes). Maintain the default value or select one of the following options: • Completed • Waiting • Active • Halted • Halting • Interrupted_Man • Interrupted_Auto • Terminated
Status	Current or final status of a business process.	The default value is ALL (displays all business processes). Maintain the default value or select one of the following options: • Success • Error
Start date/time range	Business processes running or completed within the specified start dates and times.	Type a starting date and time range and select **AM** or **PM**

4. Click **Go!** The Monitor page opens, listing the business processes that match your search criteria.

Searching for EDIINT Transaction Records

To search for EDIINT transaction records for business processes that included EDI interchange processing:

1. From the **Administration** menu, select Business Processes > Advanced Search > EDIINT.
2. In the EDIINT Transaction Search page, complete one of the following:
   - Click **Go!** to view all EDIINT transaction records.
   - Search for specific EDIINT transaction records. Specify any combination of the following search criteria and click **Go!**
     - Contracts – Display the records whose contract name corresponds to the specified contract.

- Status – Display the records whose status corresponds to the specified status. Statuses include ALL, Processed without errors, Processed with errors, Pending, Expired, and MIC Invalid.

  Note: The status displayed is the status of the MDN as it relates to the received transaction. This status does not signify the result of the HTTP transfer of the MDN.

- Type – Display the records whose Internet security protocol type corresponds to the specified type. Search parameters include ALL, AS1, and AS2.
- Start Date From and Start Date To – Display the records generated starting on the specified start dates and time.
- End date/time range – Display the records generated prior to the specified end dates and time.

Searching for Correlations

To search for correlations of business processes or documents that have been configured with name-value pairs (using the Correlation service):

1. From the **Administration** menu, select **Business Processes > Advanced Search > Correlation**.
2. In the Central Search page, under Advanced Search, select **Correlation**, and then click **Go!**
3. In the Correlation Search page, from the **Type** field, select either **Document** or **Business process**.
4. From the **Location** field, 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 the application.
   - Restored Tables – Display correlations of instances that you have restored from an offline location.
5. To refine your search, select up to five names. Typically, the following options display:
   - SenderID
   - ReceiverID
   - Standard
   - Version
   - FunctionalID
   - TransactionSetID
   - ControlNumber
   - Date/Time
   - AcknowledgementRequested
   - AcknowledgementStatus
6. In the Value fields, type the value that corresponds with each of the selected names, and then click **Go!**
7. In the Correlation Search Results page, click the number link that indicates the number of matches in the application.

   The Monitor page opens, listing the business process instances that match your search criteria.

Searching for EDI Correlations

The application enables you to find and correlate an AS2 message with an EDI document or data, group, or transaction through a link in the EDI Correlation Search details—a **Document Correlation** information link that displays detailed interchange information about AS2 messages.

If you are using AS2, the Document Correlation link enables you using AS2 to quickly and easily view interchange details about AS2 messages, and to see the correlation between an AS2 message and a corresponding EDI document or data.

To search for AS2 correlations:

1. From the Application **Administration** menu, select **Business Process > Monitor > Advanced Search > EDI Correlation**.
2. In the Search Option area, specify any combination of the following search criteria, as appropriate:

Field	Description	Action
All Level Options		
Location	EDI correlations maintained in a specific location.	Select one of the following options: • Live Tables – Display live (active) EDI correlations. • Restored Tables – Display EDI correlations restored from an offline location.
Search Level Type	EDI processing level.	Select one of the following options: • Interchange – For the search query, display results from the interchange level. • Group – For the search query, display results from the group level. • Transaction – For the search query, display results from the transaction level.
Test Mode	Mode of the application system where documents that contain the EDI correlations were created.	Select one of the following options: • Any (default) • Test • Production • Information • Interchange is a test • Syntax only test • Echo request • Echo response
Direction	Flow of the documents that contain the EDI correlations.	Select one of the following options: • Any (default) • Inbound • Outbound
Sender ID	ID for the organization that is sending documents.	Type the identifier of the sender.

Field	Description	Action
Receiver ID	ID for the receiving organization.	Type the identifier of the receiver.
Sender ID Qualifier	Qualifier used with the Sender ID to define the organization that is sending documents.	Type the qualifier of the sender.
Receiver ID Qualifier	Qualifier used with the Receiver ID for the receiving organization.	Type the qualifier of the receiver.
Start Date	Documents in progress or completed after the specified start date and time.	Using the following formats, type a starting date and time range and select AM or PM: • Date – MM/DD/YYYY • Time – HR:MN:SC **Note:** Defaults to a range of the last 24 hours.
End Date	Documents in progress or completed before the specified end date and time.	Using the following formats, type an end date and time range and select AM or PM: • Date – MM/DD/YYYY • Time – HR:MN:SC **Note:** Defaults to a range of the last 24 hours.
Interchange Level Options		
Interchange Control Number	Sequential number, located at the beginning and end of an interchange, used to verify that all interchanges sent have been received and that the information in the interchange is complete.	Type the control number that references the interchange.
Standard	EDI standard you agree to use for a trading partnership.	Type the name of the standard (including CHIPS or Fedwire).
Acknowledgement Status	Status of an expected acknowledgement at the interchange level.	Select one of the following options: • Any (default) • Waiting • Accepted • Accepted with Errors • Rejected • OverDue • Received • None • Manually Accepted
Compliance Status	Status of compliance checking at the interchange level.	Select one of the following options: • Any (default)

Field	Description	Action
		• OK • NOT OK
Start Date	EDI correlations generated or completed for documents at the interchange level after the specific start date and time. This date is compared with the interchange date/time in the data.	Using the following formats, type a starting date and time range and select AM or PM: • Date – MM/DD/YYYY • Time – HR:MN:SC **Note:** Defaults to a range of the last 24 hours.
End Date	EDI correlations generated or completed for documents at the interchange level before the specific end date and time. This date is compared with the interchange date/time in the data.	Using the following formats, type an end date and time range and select AM or PM: • Date – MM/DD/YYYY • Time – HR:MN:SC **Note:** Defaults to a range of the last 24 hours.
Group Level Options		
Functional Group ID	ID of the functional group indicated in the document.	Type the ID of the functional group.
Group Control Number	Sequential number, used to verify that all groups sent have been received and that the information in the group is complete.	Type the control number that references the group.
Acknowledgement Status	Status of an expected acknowledgement at the group level.	Select one of the following options: • Any (default) • Waiting • Accepted • Accepted with Errors • Rejected • OverDue • Received • None • Manually Accepted • Partially Accepted
Compliance Status	Status of compliance checking at the functional group level.	Select one of the following options: • Any (default) • OK • NOT OK
Start Date	EDI correlations generated or completed for documents at the group level after the specific start date and time. This date is compared with the group date/time in the data.	Using the following formats, type a starting date and time range and select A.M. or P.M.: • Date – MM/DD/YYYY • Time – HR:MN:SC

Field	Description	Action
		Note: Defaults to a range of the last 24 hours.
End Date	EDI correlations generated or completed for documents at the group level before the specific end date and time. This date is compared with the group date/time in the data.	Using the following formats, type an end date and time range and select A.M. or P.M.: • Date – MM/DD/YYYY • Time – HR:MN:SC **Note:** Defaults to a range of the last 24 hours.
Transaction Level Options		
Transaction Set ID	ID of the transaction set indicated in the document.	Type the ID of the transaction set.
Compliance Status	Status of compliance checking at the transaction set level.	Select one of the following options: • Any (default) • OK • NOT OK
Message Repair Status	Status of message repair (for SWIFT documents only).	Select one of the following options: • Any • Ready for Edit • Ready for Resend • Aborted • Resent

3. Click **Go!** to display the EDI correlation records that match your search criteria.
4. In the EDI Correlation Interchange Results page, click **info** in the Detail column for the AS2 interchange for which you want to view details.
5. In the EDI Correlation Interchange/Group/Transaction Detail Results page, click **info** to the right of Document Correlations.
6. For SWIFT documents, on the EDI Correlation Transaction Results page, click **info** in the Detail column for the document you want to edit.
7. In the Document Correlation Details page, view details about the AS2 message you selected, and to see the correlation between the AS2 message and corresponding EDI document or data. The details available include:
   - time stamp
   - scope
   - process ID
   - document name
   - data value

Searching for BPSS Correlations

To search for BPSS correlations that define a standard structure of the activities within a business process:

1. From the Administration menu, select **Business Processes > Advanced Search > BPSS Correlation**.
2. In the BPSS Tracking page, from the **Location** field, select one of the following options:
   - Live Tables – Display BPSS correlations of live (active) business processes.
   - Archive Tables – Display BPSS correlations of business processes that you have archived in the application.
   - Restored Tables – Display BPSS correlations of business processes that you have restored from an offline location.
3. To refine your search, specify any combination of the following search criteria.
   - Transaction Type – Display the records of the activities that completed the specified transaction.
   - Trading Partner – Display the records of the activities that associated with the trading partner specified.
   - Status – Display the records of the activities that resulted with a success or error transaction.
   - Start date/time range – Display the records of activities completed within the specified start dates and times.
4. Click **Go!** to display the BPSS correlation records that match your search criteria.

General Processing Information

The Monitor page refreshes automatically and displays the ten most recent business processes to run and their processing information. If a business process does not display in the Monitor page, you can perform a search to locate the business process. For more information, see *Searching for AS2 Business Processes and Other Information*.

When monitoring active and recent business processes, the application uses two status indicators to indicate further action is required:

Status Indicator	Active Business Process	Recent Business Process
	Encountering no errors or warnings at this point of the execution.	Encountered no errors during execution.
	• Waiting for other activities to complete before continuing execution. • Encountering errors or warnings during execution.	Encountered errors or warnings during execution.

In the Monitor page, use the following fields and columns to view general processing information about business processes and perform other activities, as appropriate:

Field/Column	Description
Automatically refresh every minute	Default time to refresh the list of the 10 most recent business processes. To disable this feature, clear the check box.

Field/Column	Description
Status	Indicator of the status of an active or recently executed business processes. For more information, see *Viewing EDIINT Duplication Transaction Detail Information*.
ID	Number assigned by the AS2 Edition to identify an business processes. Click the number to display the Business Process Details page. For more information, see *Viewing EDIINT Duplication Transaction Detail Information*. .
Name	Name of an business processes. Click the name to view the BPML code that makes up the business processes.
State	Current state of a business process. The following list shows possible states in the order of precedence during branch processing: • Active/Running • Completed • Terminated • Waiting • Interrupted • Halting/Halted
Started	Date and time a business process started.
Ended	Date and time a business process ended.
Expires	Information about when a business process expires. Click Info to display the expiration information, including whether the data for a business process is archived after it expires.
Parent/Child	Parent or child business process that is referenced when running a business process. Click the up arrow to view a parent business process. Click the down arrow to view a child business process.

Detailed Processing Information

From the Monitor page, you can access the Business Process Detail page. The Business Process Detail page provides you with a step-by-step progress report on a specific business process. From the Business Process Detail page, you can also perform activities, such as stopping or restarting a business processes.

In the Business Process Detail page, use the following fields to review detailed processing information and perform activities, as appropriate:

Field/Column	Description
Name	Name of a business process for which you are viewing details. Click the name to view the BPML code that makes up the business process.
Instance ID	Number assigned by the AS2 Edition to identify a business process.

Field/Column	Description
Status	Current status of a business process. Possible status levels are: • Success • Error
State	Current state of a business process. The following list shows possible states in the order of precedence during branch processing: • Active/Running • Completed • Terminated • Waiting • Interrupted • Halting/Halted
Activities	List of activities to complete for a business process, including an activity to generate an XML report. The activities available in this field are determined by whether a business process is currently active or stopped. Possible activities are: • Restart – Continues running a business process • Stop – Stops running a business process • Terminate – Cancels a business process and all remaining active and waiting subprocesses • XML report – Generates an XML report that describes the business process If you terminate an active business process, the State field may indicate messages in the following order: Halting > Halted > Terminated.
Step	Current step of a business process.
Service	Name of the service running for a current step. Click the service name to view settings for a service in a business process.
Status	Current status of the steps in a business process. Possible status levels are: • Success • Error
Advanced Status	Service details about any errors that occurred for a step in a business process, when applicable. Click the message to display information.
Started	Date and time the step of a business process started.
Ended	Date and time the step of a business process ended.
Status Report	Status report that provides the results of a service. To view the status report, click **info**.
Document	Business process document that this service is processing (that is, the primary document). To view the document, click **info**.

Field/Column	Description
Instance Data	Contents of the process data generated after a specific step in a business process. In addition, this field links to any messages going to or coming from a service. To view the information, click **info**.

EDIINT Transaction Information

In the EDIINT Transaction Summary page, use the following fields and columns to view general processing information about business processes and perform other activities, as appropriate:

Field/Column	Description
Status	Indicator of the status of the EDIINT transaction.
ID	Number assigned by the AS2 Edition to identify. Click the number to display the Business Process Details page.
Duplicates	Number of messages with duplicate message IDs. Click the number to display the EDIINT Duplicate Transaction Summary page. When a message with a duplicate message ID is received, a record for a duplicate message is created. This record contains the transaction information for the instance of the message prior to reception of the duplicate. The current transaction record is updated with information about the duplicate, which is the latest instance of the message.
Created	Date and time this transaction record was created. Records are created when messages are built or received.
State	Current state of the EDIINT transaction: • Processed with errors - An error occurred processing the message. These are usually EDIINT specific errors returned in MDNs, such as decryption failures. • Processed without errors - The message was processed successfully. • Pending - An acknowledgement has not yet been received for a message. • Expired - An acknowledgement was not received for the message in the required amount of time. • MIC Invalid - The cryptographic hash in an MDN did not match the one calculated by the system when the message was created.
Contract	Contract associated with the EDIINT transaction.
Type	Type of communication protocol used. AS2 indicates AS2 protocol.
Acknowledged	Date and time that the message was acknowledged

Viewing EDIINT Duplicate Transaction Summaries

From the EDIINT Transaction Summary page, click the number in the Duplicates column to access the EDIINT Duplicate Transaction Summary page. The EDIINT Duplicate Transaction Summary page provides you with

a list of documents that have duplicate message IDs. From the EDIINT Duplicate Transaction Summary page, you can refine the detail of your search by clicking the ID number for each duplicate document.

EDIINT Duplicate Transaction Summaries Fields

In the EDIINT Duplicate Transaction Summary page, use the following fields to review detailed processing information, as appropriate:

Field/Column	Description
Status	Indicator of the status of the EDIINT transaction.
ID	Number assigned by the AS2 Edition to identify an business processes. Click the number to display the Business Process Details page.
Duplicates	Number of messages with duplicate message IDs. Click the number to display the EDIINT Duplicate Transaction Summary page. When a message with a duplicate message-ID is received, a record for a duplicate message is created. This record contains the transaction information for the instance of the message prior to reception of the duplicate.
Created	Date and time this transaction record was created. Records are created when messages are built or received.
State	Current state of the EDIINT transaction: • Processed with errors - An error occurred processing the message. These are usually EDIINT specific errors returned in MDNs, such as decryption failures. • Processed without errors - The message was processed successfully. • Pending - An acknowledgement has not yet been received for a message. • Expired - An acknowledgement was not received for the message in the required amount of time. • MIC Invalid - The cryptographic hash in an MDN did not match the one calculated by the system when the message was created
Contract	Contract associated with the EDIINT transaction.
Type	Type of communication protocol used. AS2 indicates AS2 protocol.
Acknowledged	Date and time that the message was acknowledged

Viewing EDIINT Duplicate Transaction Detail Information

From the EDIINT Duplicate Transaction Summary page, click the ID number to access the EDIINT Duplicate Transaction Detail page. The EDIINT Duplicate Transaction Detail page provides you with additional details about the business process. From the EDIINT Duplicate Transaction Detail page, you can click the Message-ID to view the message, and click the MDN Message-ID to view the MDN.

EDIINT Duplicate Transaction Detail Information

In the EDIINT Duplicate Transaction Detail page, use the following fields to review detailed process information and perform activities, as appropriate:

Field/Column	Description
ID	Number assigned by the AS2 Edition to identify the EDIINT transaction.
Record created	Date and time that this record was created.
Message-ID	Identification string of the message.
State	Current state of the EDIINT transaction: • Processed with errors - An error occurred processing the message. These are usually EDIINT specific errors returned in MDNs, such as decryption failures. • Processed without errors - The message was processed successfully. • Pending - An acknowledgement has not yet been received for a message. • Expired - An acknowledgement was not received for the message in the required amount of time. • MIC Invalid - The cryptographic hash in an MDN did not match the one calculated by the system when the message was created
Acknowledged	Date and time that the message was acknowledged.
MDN Message-ID	Identification string of the MDN.
Disposition	The disposition of the message according to the MDN.
SHA1 MIC	Security string information.
Contract	Contract associated with the message.
Type	Type of transmission protocol used with the message.
Sender	Sender of the message.
Recipient	Recipient of the message.
Output Documents	A link to the business documents extracted from the message, if business documents were extracted from the message. This field does not appear if a document was not extracted from the message. If processing of duplicate messages is not enabled and this transaction is not the first instance of the message, no documents will be extracted from the message.

Viewing EDIINT Duplicate Transaction Messages

From the EDIINT Duplicate Transaction Detail page, click the Message-ID string to access the EDIINT Transaction Message contents. The Message page displays showing the contents of the message sent in the transaction.

Viewing EDIINT Duplicate Transaction MDNs

From the EDIINT Duplicate Transaction Detail page, click the MDN Message-ID string to access the EDIINT Transaction MDN contents. The MDN page displays showing the contents of the MDN sent in the transaction.

Viewing EDIINT Transaction Detail Information

From the EDIINT Transaction Summary page, click the ID number to access the EDIINT Transaction Detail page. The EDIINT Transaction Detail page provides you with additional details about the EDIINT transaction. From the EDIINT Transaction Detail page, you can click the Message-ID to view the message, click the MDN Message-ID to view the MDN, or change the state of the business process.

EDIINT Transaction Detail Information

In the EDIINT Transaction Detail page, use the following fields to review detailed process information and perform activities, as appropriate:

Field/Column	Description
ID	Number assigned by the AS2 Edition to identify the EDIINT transaction.
Record created	Date and time that the record was created.
Message-ID	Identification string of the message.
State	Current state of the EDIINT transaction: • Processed with errors - An error occurred processing the message. These are usually EDIINT specific errors returned in MDNs, such as decryption failures. • Processed without errors - The message was processed successfully. • Pending - An acknowledgement has not yet been received for a message. • Expired - An acknowledgement was not received for the message in the required amount of time. • MIC Invalid - The cryptographic hash in an MDN did not match the one calculated by the system when the message was created
Acknowledged	Date and time that the message was acknowledged.
MDN Message-ID	Identification string of the MDN.
Disposition	Status of the transaction. For example, processed or waiting.
SHA1 MIC	Security string information.
Contract	Contract associated with the message.
Type	Type of transmission protocol used with the message.
Sender	Sender of the message.

Field/Column	Description
Recipient	Recipient of the message.
Input Documents	A link to the business document used to create the message if the transaction is for a message created by this system. This field does not appear if the message was created by a trading partner's system.
Output Documents	A link to the business documents extracted from the message, if business documents were extracted from the message. This field does not appear if no documents were extracted from the message. If processing of duplicate messages is not enabled and this transaction is not the first instance of the message, no documents are extracted from the message

Viewing EDIINT Transaction Messages

From the EDIINT Transaction Detail page, click the Message-ID string to access the EDIINT Transaction Message contents. The Message page displays showing the contents of the message sent in the transaction.

Viewing EDIINT Transaction MDNs

From the EDIINT Transaction Detail page, click the MDN Message-ID string to access the EDIINT Transaction MDN contents. The MDN page displays showing the contents of the MDN sent in the transaction.

Viewing System Logs

You can view system logs to monitor the operational status of the application and the AS2 Edition and its components and the activities occurring within the system.

To view the system logs:

1. From the Administration Menu, select **Operations** > **System** > **Logs**.
2. In the System Logs page, select the appropriate log file. The log opens.

Note: The interface displays only the last 2500 lines of a log file. To view the entire log file, you must have Read permissions for the file system where the log file is located. Open the log file (located at the installation path on your hard drive), with a text editor.

Managing Schedules

Depending on your business needs, you may need to change your service or business process schedules. After you have created a schedule, you can enable, disable, or edit the service schedule when necessary.

Creating a Business Process Schedule

You can schedule a business process to run or you can choose to run the business process manually. If you schedule your business process, you can take advantage of the following advanced scheduling capabilities:

- Schedule your business process to run on specific days of the week – Schedule different processes to run on different days, reserving system resources and scheduling business processes around the critical events of your organization. For example, you can run the business process only on Monday through Friday, or Monday, Wednesday, and Friday. This includes the ability to schedule the system resource intensive business processes to run on weekends when network or system traffic is low.
- Schedule your business process to run based on specifically selected hours – Much like the ability to run on the weekends or specific days of the week; provides further granularity in scheduling your business processes by selecting specific hours or ranges of hours range of hours to run.
- Schedule exclusions – You can set exceptions within the scheduler to exclude peak days or processing hours.

To set up a business process schedule:

1. From the Administration Menu, select **Deployment > Schedules.**
2. Next to Schedule a Business Process, click **Go!**
3. In the Select BP page, select the business process for which you want to set up the scheduled run time from the Business Process field, and then click **Next**.
4. In the Schedule Settings page, indicate whether to use a 24-hour clock display (that is, Military time numbers 24 hours of the day from 1 to 24, rather than repeating the cycle of 12 hours twice).
5. To specify how you want to schedule your business process to run, complete one of the following steps, and then click **Next**:
   - To set a timer to for running your business process, select **Run based on timer**.
   - To schedule your business process to run on a daily basis, select **Run daily**.
   - To schedule your business process to run on specific weekdays, select **Run based on day(s)** of the week.
   - To schedule your business process to run on specific days during the month, select **Run based on day(s) of the month**.
6. Based on the selections you made in step 5., complete one of the following steps:
   a) If you are setting up a timer:
      1. In the **Hour(s)** field, type the number of hours in which the business process should run (for example, if you want the business process to run every 2 hours, type 2).
      2. In the **Min(s)** field, type the number of minutes in which the business process should run (for example, if you want the business process to run every 30 minutes, type 30. However, if you specified 2 in the Hour(s) field and specified 30 in the Min(s) field, the business process runs every 2.5 hours.).

   b) If you are running the business process daily, based on days of the week, or days of the months, and using a timer:
      1. To specify a time interval, select **Check here to select time interval**.
      2. In the **From** and **To** fields, type the time to start and end the interval.
      3. In the **Select Day(s)** field, select the number of days in between intervals. This field is only available if you choose Run based on day(s) of the week or month.
      4. From **Every**, **Hour(s)**, and **Min(s)** lists, select how long the interval lasts.
      5. Click **add** to specify the scheduled time you run the business process.

c) If you are not using a time interval:

1. In the **From** field, type the time to start and end the interval.
2. In the **Select Day(s)** field, select the number of days in between intervals.
3. From **Every**, **Hour(s)**, and **Min(s)** lists, select how long the interval lasts.
4. Click **add** to specify the scheduled time you run the business process.

7. To run the business process at startup, next to the scheduling interval you selected in step 4, ensure that the **At startup** check box is selected, and then click Next.
8. To indicate exclusion dates that business process should not run, complete the following steps:
   a) In the **Months** field, select the month not to run the business process.
   b) In the **Days** field, select the day of the month in which not to run the business process.
   c) Click **add** to specify the exclusion dates for the schedule, and then click **Next**.
9. Click **Finish** to add the schedule for the business process to the application.

Searching for a Service Schedule

You can search for a service schedule to verify the schedule information or to edit the service schedule.

To search for a service schedule:

1. From the Administration Menu, select **Deployment > Schedules**.
2. In the Schedules page, do you know the name of the service you want to locate?
   - If Yes, under Search, in the by Name field, type the name of the service, and then click **Go!**
   - If No, under List, select from the by Scheduler Type list a search method, and then click **Go!** Search Methods include:

     All - Lists all services and business processes that have schedules.
     Services - Lists only services that have schedules.
     Business Processes - Lists only business processes that have schedules.

   The Schedules page displays showing a list of the services that matched your search criteria.

Enabling or Disabling a Scheduled Service

After you have created a service schedule you can enable or disable the service schedule depending on your business needs.

To enable or disable a scheduled service:

1. From the Administration Menu, select **Deployment > Schedules**.
2. Do you know the name of the service you want to edit?
   - If Yes, under Search, in the by Name field, type the name of the service, and then click **Go!**
   - If No, under List, select from the by Scheduler Type list a search method, and then click **Go!** Search Methods include:

     All – Lists all services and business processes that have schedules.

Services – Lists only services that have schedules.

Business Processes – Lists only business processes that have schedules.

3. In the Schedules page complete one of the following actions:
   - To enable a scheduled service, under Enabled, click the check box next to the service you want to enable. Ensure that the check box is selected.
   - To disable a scheduled service, under Enabled, clear the check box next to the service you want to disable. Ensure that the check box is cleared.
4. In the message box indicating Status change will affect only the service associated schedule!, click **OK.**

Editing a Service Schedule

Predefined services run according to a schedule. You can edit a service schedule to meet your business requirements.

To edit a service schedule:

1. From the Administration Menu, select **Deployment > Schedules**.
2. Do you know the name of the service you want to edit?
   - If Yes, under Search, in the by Name field, type the service name. Click **Go!**
   - If No, under List, select from the by Scheduler Type list a search method, and then click **Go!**Search Methods include:

     All – Lists all services and business processes that have schedules.

     Services – Lists only services that have schedules.

     Business Processes – Lists only business processes that have schedules.
3. In the Schedules page, click edit next to the schedule you want to edit.
4. In the Schedule Settings page, do you want the service to use a schedule?
   - If No, select Do not use schedule, and then click **Next**.
   - If Yes, select one of the following: **Run service based on timer every**, **Run service daily at**, or **Run service weekly on**, and complete the hour, minute, time of day, or day of week fields, appropriate to your selection.
5. Do you want to run the service at startup?
   - If Yes, next to the scheduling interval you selected in step 4, select the At startup check box, and then click Next.
   - If No, next to the scheduling interval you selected in step 4, clear the At startup check box (or leave the check box clear if not selected), and then click **Next**.
6. In the Confirm page, complete the following steps:
   a) Verify the schedule information. If information is not correct, click Back, make the needed corrections.
   b) Select **Enable Service for Business Processes** if you want to enable the service.
   c) Click **Finish** to save the changes to the service schedule.

Legal Notices

Copyright

Index

U