Informatica® B2B Data Exchange
10.4.0

Administrator Guide

Table of Contents

Preface

Use the *B2B Data Exchange Administrator Guide* to administer the B2B Data Exchange Operation Console. Learn about applications, event types, user policies, and schedules. You can also learn how to manage documents, repositories, dashboards, and reports.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.

- View product availability information.

- Create and review your support cases.

- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

C H A P T E R   1

Product Overview

This chapter includes the following topics:

Introduction

B2B Data Exchange facilitates the transfer and processing of structured and unstructured documents for trading partners. You can use B2B Data Exchange to manage the flow and transformation of documents and to manage the trading partners that send and receive the documents.

Use B2B Data Exchange to customize the processing of similar types of documents using the same transformation logic for different trading partners. You create workflows that define the transformation logic to process different types of documents. Then, create a profile to associate a partner with a workflow and define the document processing requirements for the partner.

For example, you create a workflow to process EDI documents for two partners. One partner requires acknowledgement and the other does not. You can create a profile for the first partner to use the workflow to process EDI documents. Set up parameters for the profile to allow for document acknowledgement. Then create a profile for the second partner to use the same workflow to process EDI documents but without acknowledgment. In this way, you can customize the way a workflow is used to process documents for each partner.

You can use the B2B Data Exchange Operation Console to customize and monitor document processing. Use the Operation Console to manage partners, workflows, and profiles and to monitor the events generated during document processing. You can also use the Operation Console to administer B2B Data Exchange users and roles, manage system properties, and set console preferences.

B2B Data Exchange Components

B2B Data Exchange includes the following components:

- Data Exchange Server. The Data Exchange Server manages document processing in B2B Data Exchange. It sends the inbound documents to PowerCenter for processing. After PowerCenter processes the documents, the Data Exchange Server takes outbound documents and puts them in the correct location to send to a partner.

- Data Exchange Repository. The Data Exchange Repository resides in an Oracle or SQL Server database. The repository database tables contain the metadata required to process documents. When you create or modify partners, profiles, and other objects, the Operation Console saves metadata to the repository. The

Data Exchange Server reads the metadata in the repository to determine the requirements for processing documents.

- Operation Console. The Operation Console is a web application that customizes and monitors document processing for partners. It also administers users and resources in B2B Data Exchange. You use a browser to access the Operation Console.

- Command line interface. B2B Data Exchange includes command line utilities that import and export metadata and archive metadata and events.

- Application server. B2B Data Exchange uses the Apache Tomcat servlet container to run the Operation Console. By default, this Tomcat servlet container is installed during the B2B Data Exchange installation.

- JDK. B2B Data Exchange is a Java application and requires the Java Development Kit (JDK). By default, the JDK is installed during the B2B Data Exchange installation.

- Message broker. The Data Exchange server uses the B2B Data Exchange JMS Broker to send documents to PowerCenter for processing and receive documents from PowerCenter after processing. The B2B Data Exchange JMS Broker is installed during B2B Data Exchange installation.

B2B Data Exchange uses the following products to complete document processing:

- PowerCenter. B2B Data Exchange uses real-time processing to process documents. For more information about PowerCenter and its components, see the Informatica PowerCenter documentation. You can use an Unstructured Data transformation in a PowerCenter workflow process to process documents. Data transformations convert complex data from one structure or format to another.

B2B Data Exchange Architecture

The following figure shows the components of B2B Data Exchange and how they interact:

Figure 1. B2B Data Exchange Components
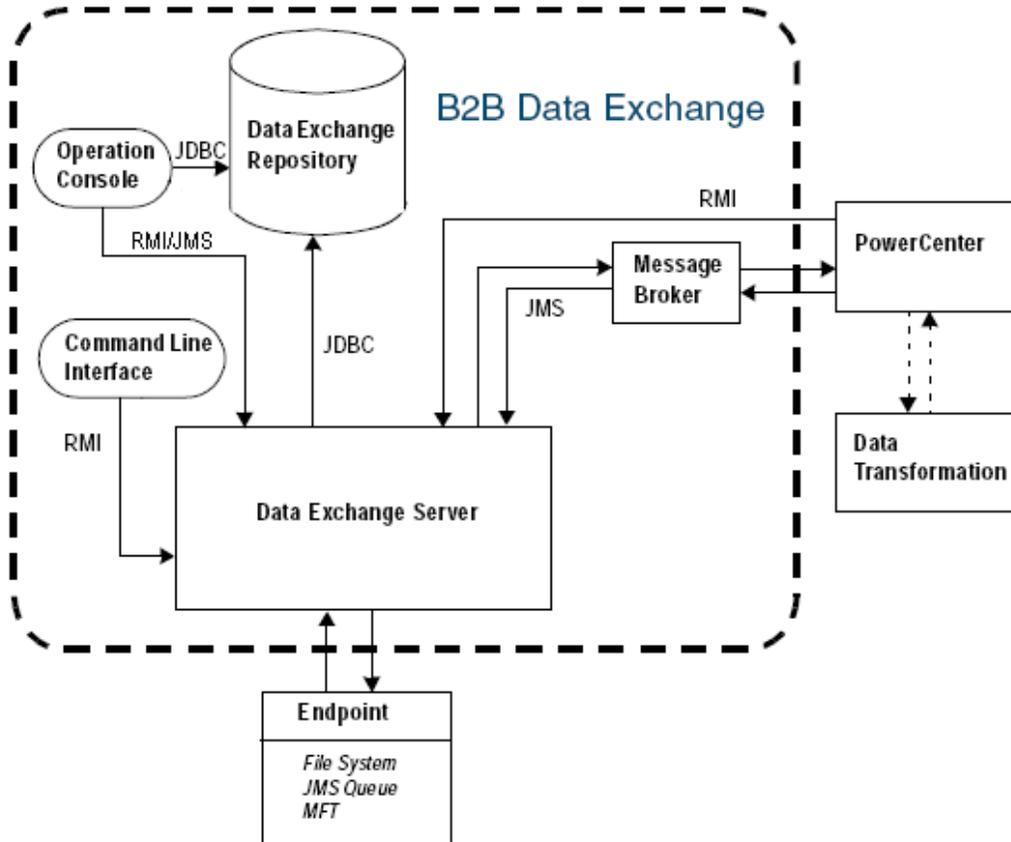
When you install B2B Data Exchange, you provide the information to connect to a database for the Data Exchange Repository. The installer connects to the database and creates the tables and views required for the repository.

The Data Exchange Server reads the metadata from the Data Exchange Repository for information on how to process documents. It determines the parameters required for a workflow based on the information saved in the repository.

B2B Data Exchange uses the Data Transformation Engine to convert documents from one format to another. You can include Unstructured Data transformations in the PowerCenter workflows you build to process Data Exchange documents.

The B2B Data Exchange endpoints determine where the Data Exchange Server reads the documents to be processed and writes the documents after processing. Documents can consist of text files in a file system or messages in a queue. For more information about endpoints, see the *B2B Data Exchange Operator Guide*.

Operation Console

The following figure shows the components of the B2B Data Exchange Operation Console:

Figure 2. B2B Data Exchange Operation Console
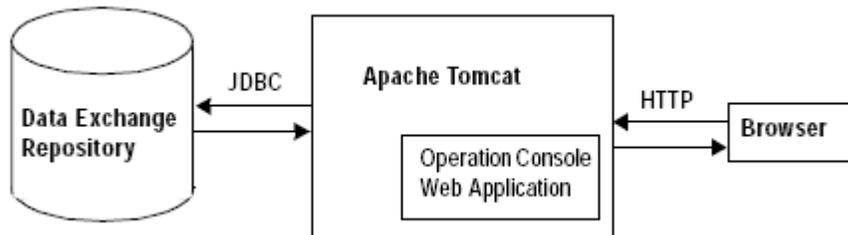
The Operation Console is a web application that is deployed within an application server. B2B Data Exchange uses Apache Tomcat to run the Operation Console. When you create and edit objects in the Operation Console, the application server saves the metadata in the Data Exchange Repository. The Data Exchange Server reads the metadata in the Data Exchange Repository to determine how to process Data Exchange documents.

CHAPTER 2

Security

Security Overview

B2B Data Exchange security protects the B2B Data Exchange infrastructure against unauthorized access to or modifications of B2B Data Exchange services and resources.

Infrastructure security includes the following aspects:

- Control B2B Data Exchange server shutdown and startup by restricting remote shutdown and startup to specific clients in your organization.
- A secret token authorizes calls from PowerCenter workflows to the B2B Data Exchange server through B2B Data Exchange transformations. You can define a custom token to replace the default system token.

Restrict Remote B2B Data Exchange Server Shutdown and Startup

You can define a list of clients from which users can remotely shut down and start up the B2B Data Exchange server.

Users can still ping the B2B Data Exchange server from any client in the network.

If you do not define the list, users can shut down and start up the server from any client in the network.

Shutdown and startup from the local host are enabled regardless of whether or not you define the list.

Configuring Clients for Remote Server Shutdown and Startup

1. On the B2B Data Exchange server, open the following security configuration file:

       <DXInstallationDir>\conf\security\dx-security-config.properties

2. In the security configuration file, in the `dx.security.dxcontrol.whitelist` property, enter the IP addresses of the clients from which users can remotely shut down and start up the B2B Data Exchange server, separated by a semi colon.

For example:

```
dx.security.dxcontrol.whitelist=192.168.1.1;192.168.1.2;192.168.1.3;fe80::3516:cd0c:6
f8:df39%19;
```

Define a Custom Secret Token for Calls to the B2B Data Exchange Server

Customize the secret token that B2B Data Exchange uses to authorize calls from PowerCenter workflows to the B2B Data Exchange server through B2B Data Exchange transformations.

The token you define replaces the default system token.

Defining a Custom Secret Token

1. In your PowerCenter Integration Service, create the following environment variable:

    ```
    dx.security.flowservice.shared_secret
    ```

    Assign the environment variable a value that will act as the shared secret between server and client.

2. On the B2B Data Exchange server, open the following security configuration file:

    ```
    <DXInstallationDir>\conf\security\dx-security-config.properties
    ```

3. In the security configuration file set the value of the property `dx.security.flowservice.shared_secret` to the shared secret that you assigned in step 1.

CHAPTER 3

Applications

This chapter includes the following topics:

Applications Overview

An application is a group of related B2B Data Exchange workflows. A B2B Data Exchange workflow represents a PowerCenter workflow. The developer creates a workflow in the Operation Console for every PowerCenter workflow that processes B2B Data Exchange documents.

You can associate a workflow with an existing application. For example, processing a document can involve multiple steps. If a separate PowerCenter workflow is required for each step, you can group the B2B Data Exchange workflows that represent these workflows into one application.

Creating an Application

Applications are optional. If you use applications in workflows, you must create the applications before you create the workflows.

1. In the Navigator, click **Partner Management** > **Applications**.
2. Click **New Application**.

   A row appears at the bottom of the list of applications.
3. Enter the name of the application.

   The application name can contain up to 60 characters and can include spaces and special characters.
4. Click **Save**.

Editing an Application

You can edit the name of an application.

Click **Partner Management** > **Applications**, and then click the **Edit** icon for the application you want to edit. Modify the application name, and then click the **Save** icon.

Deleting an Application

You can delete an application and all its dependent objects.

Before you delete an application, you must delete all dependent objects such as workflows.

1. In the Navigator, click **Partner Management** > **Applications**.
2. Click the **Delete** icon for the application you want to remove, and then confirm the deletion.

   If the application has dependent objects, the Operation Console displays a warning.
3. Expand the object list and review all dependent objects.

4. Perform one of the following actions:
   - Click **Delete all** to delete the application and all its dependent objects
   - Click **Cancel**, and then delete the dependent objects individually. After you delete the dependent objects, delete the application.

CHAPTER 4

Partner and Account Information

This chapter includes the following topics:

Partner and Account Information Overview

The ability to customize partner and account information answers the need of many customers to keep track of partner and account information beyond that which B2B Data Exchange contains. For example, a customer might want to keep track of the DUNS Number of its partners. B2B Data Exchange does not contain this information. Use the partner information customization to add information not contained in B2B Data Exchange.

B2B Data Exchange provides one place to store extended partner information and another place to store extended account information. B2B Data Exchange displays the extended partner information in the Additional Information tab of the Partner screen and the extended account information in the Additional Information tab of the Account screen. Both additional information tabs are, by default, blank. You can customize the content of these tabs to meet unique customer needs.

You design the Partner > Additional Information form using the Partner screen. Similarly, you design the Account > Additional Information form using the Account screen. Each of these screens contains a Forms Designer tool that enables you to add fields, format them, and collect them into groups of various kinds, such as columns and tabs.

You are encouraged to read the Forms Designer documentation in conjunction with the following material on customizing partner and account information. For more information about the Forms Designer, see the *B2B Data Exchange Developer Guide*

Customizing Partner Information

This section explains how to customize the Additional Information form of the Partner screen. It explains how to add and delete attributes and how to save the design of the form. Grouping attributes and arranging them on the form are covered in the Forms Designer documentation. For more information on the Forms Designer, see the *B2B Data Exchange Developer Guide*.

When attributes are added to the Additional Information form, they apply to all partners.

1.   In the Navigator, click Administration > Partner Attributes >Designer.

     The Forms Designer screen opens.
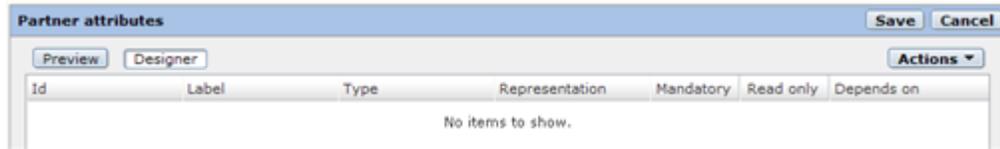
     This screen contains the list of attributes that are displayed in the Update Partner Screen > Additional Information tab. The System Administrator is responsible for populating this list. By default, it is empty. The forms contains the following actions:

Action	Description
Edit	Edit the attribute properties.
Create Attribute	Create an attribute.
Delete Attribute	Delete an attribute.
Create Tab	Create a tab.
Create Column	Create a column.
Create Header	Create a header.
Create Disclosure	Create a disclosure group.
Delete Group	Delete the selected tab, column, header, or disclosure.
Move to Group	Move the selected attribute to a group.

2.   To add an attribute to the form:

     a.   Click Actions > Create Attribute.

     b.   Enter the Id of the attribute.

     c.   Enter the label of the attribute.

     d.   Enter the description of the attribute.

     e.   If the attribute is mandatory, check the box.

     f.   If the attribute is read-only, check the box.

     g.   Select the attribute type from the list.

     h.   Select the representation of the attribute from the list.

     i.   Enter any default value of the attribute.

     j.   If the representation of the attribute is a drop-down list, a radio button, a list, or a checkbox, enter the possible values that the attribute can have in the Values box. Enter one value per line and press Enter to go to the next line.

     k.   If the attribute has the Entry Field representation, you can enter optional minimum and maximum values.

l.   To define a relationship between two attributes, check the box labelled "This group/field should be." Select enabled/disabled. Select a field from the list that controls the behavior of this field. Select specific/any value and fill in a specific value.

An example of a relationship is: This group/field should be **enabled** when parameter **Test** has **specific** value **yes**.

3.   Other actions can be performed on the form. For more information about the Forms Designer, see the *B2B Data Exchange Developer Guide*.

4.   Click Preview to see a preview of the form.
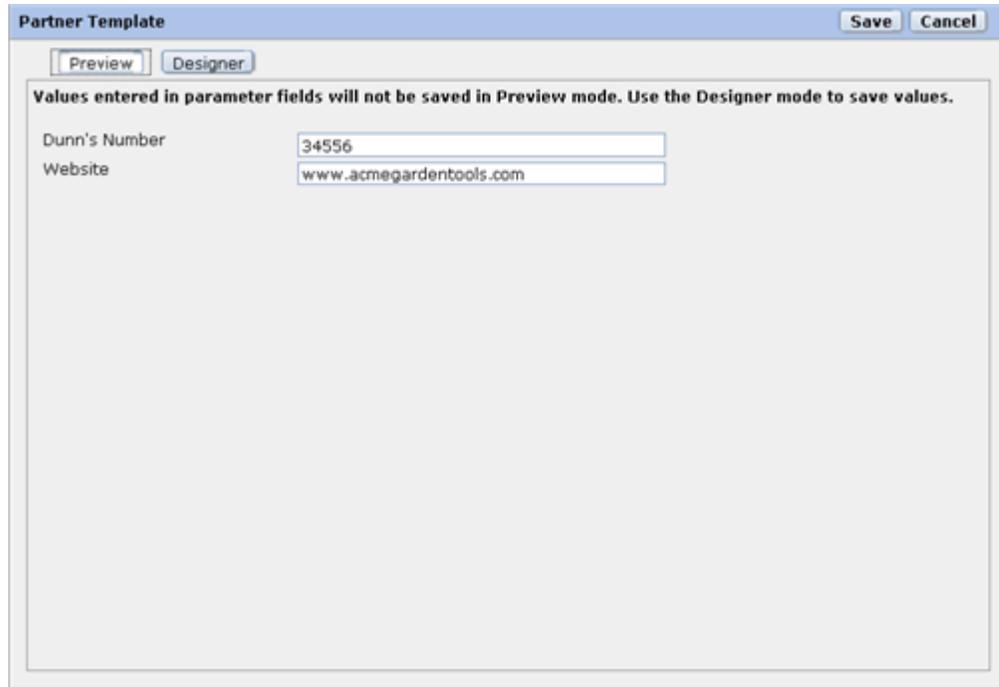
5.   Click Save to save the form.

Customizing Account Information

1.   On the Navigator, click Administration > Account Attributes.

2.   Follow the procedure in .

Note that additional information added to the Account screen will apply to existing and new partners.

CHAPTER 5

Events

This chapter includes the following topics:

Events Overview

An event is a representation of a publication or a subscription instance, at a particular stage of the publication or subscription process. The B2B Data Exchange server generates events as it runs and processes publications and subscriptions, and it changes the status of the events as the publication or subscription process progresses. When an application triggers a publication, if the triggered publication has a pre-process, the publication event also tracks the pre-process. When a subscription triggers a post-process, the subscription event also tracks the post-process.

When an application that runs a publication pre-process publishes data or files to the publication repository, the B2B Data Exchange server assigns an event to the publication as follows:

- If the pre-process passes the Publication event ID to the publication process, the publication uses the same event, and the B2B Data Exchange server does not generate an additional Publication event for the publication process.
- If the pre-process does not pass the event ID to the publication process, the B2B Data Exchange server generates another Publication event for the publication process.

If a file publication publishes more than one file, B2B Data Exchange creates a File event for each file that it picks up. B2B Data Exchange creates a Publication event after all the files are picked up.

The Publication event is the root event and the parent event for all of the subscription events that the B2B Data Exchange server generates during the publication process. After the published data is ready for subscribers, the B2B Data Exchange server generates a Subscription child event for each subscriber that needs to consume the published data. The Publication event contains aggregated status information for all Subscription child events.

An event changes status as it is processed. The B2B Data Exchange server changes the status of an event based on a set of event statuses that you define in the Operation Console. As each subscriber consumes the

published data, the child event finishes processing. After all subscribers consume the published data, the B2B Data Exchange server updates the consumption status of the parent event for the publication.

You can manage storage space in the B2B Data Exchange run-time repository by purging events that B2B Data Exchange generates when they are no longer needed.

Event Types

When the B2B Data Exchange server processes documents, it creates events according to the event types that are defined in the Operation Console.

In the Operation Console, you can create custom event types based on your processing requirements. You can then use the custom type in a PowerCenter workflow. You can edit or delete an event type that you create.

The following table describes the default event types:

Event Type	Description
Custom Event	Predefined custom event. You can configure a workflow to generate events of this type. Used by the B2B Data Exchange Server for archiving and monitor events.
File Level Event	Event generated at the start of the processing. This is the parent event for all other events generated during the course of processing the document.
Group Level Event	Event associated with groups included in a document. You can configure a workflow to generate events of this type.
Segment Level Event	Event associated with segments included in a document. You can configure a workflow to generate events of this type.
System Event	Event generated by the B2B Data Exchange server for system notifications. For example, the B2B Data Exchange server generates a system event when a notification delivery fails.
Transaction Level Event	Event associated with transactions included in a document. You can configure a PowerCenter workflow to generate events of this type.

Managing Event Types

Use the Navigator to create, edit, and delete event types. If you define custom event types, you can build PowerCenter workflows that assigns the new event types to events that B2B Data Exchange processes.

1. In the Navigator, click **Events** > **Event Types**.

   The **Event Types** page appears.

2. Choose to create, edit, or delete an event type.

   - To create an event type, click **New Event Type** and enter the name of the event type.

   - To edit an event type, click the **Edit** icon next to the event type that you want to edit and change the event type name. You cannot edit or delete the System Event type.

   - To delete an event type, click the **Delete** icon next to the event type that you want to delete and confirm the deletion.

Event Statuses

The event status indicates the progress of the event while B2B Data Exchange processes it.

The following table describes the default event statuses:

Event Status Type	Description
Complete	Assigned when the event completes processing. Child events might, however, still be processing. Message reconciliation can be completed later.
Critical	Assigned when the event processing produces a critical error.
Delayed	Assigned if message processing is delayed due to processing rules, if message processing waits for a processing rule to release the message, or if message processing waits for a manual release.
Discarded	Assigned when the event is delayed and then discarded due to a processing rule, or discarded manually.
Error	Assigned when the event processing produces an error.
New	This event type is not currently used.
Pending	Assigned while the event waits to be processed. The event is assigned this status from the moment it is created until the status changes.
Rejected	Assigned when a message is rejected.
Reprocessed	Assigned when the event processes again.
Transferring	Assigned while the message transfers from B2B Data Exchange to an outbound endpoint. After the transfer completes, B2B Data Exchange changes the event type to Complete or Error based on the result.

In the Operation Console, you can create custom event statuses and types based on your processing requirements. You can then use the custom status or type in a PowerCenter workflow .

For example, you can create a status that reflects a unique process in your organization, such as Sent for Approval. You can then configure a PoweCenter workflow to set the event to that status until the approval is processed.

You can edit or delete any event status that you create. You can also manually edit an event and set the event status to any status in the Operation Console.

Each event status includes a state property. The state property represents the processing stage for the event.

The state property value determines whether an event appears in the Dashboard charts and reports. For example, only events with a state value of Error appear in the Error Rate by Partner chart and report.

When you create a user-defined event status, assign a value to the state property. Failure to assign state the correct value might result in incorrect Dashboard reports.

Event Status Properties

The event status indicates the processing stage for the event and whether the event encountered errors during processing.

The following table describes the event status properties:

Property	Description
Event Status Name	Name of the event status.
Icon	Optional. Image to display in the **Status** column when you view the event on the **Event List** page.
State	Optional. State of the event during processing. You can choose one or more of the following options: - Final. The event finished processing successfully. - Error. The event encountered an error. If you select Final and Error, the event status indicated that the event finished processing with errors. If you do not select a state property value, the event status represents an intermediate stage in event processing.

Managing Event Statuses

Use the Navigator to create, edit, or delete event statuses.

1. In the Navigator, click **Events** > **Event Status**.

   The **Event Statuses** page appears.

2. Choose to create, edit, or delete an event status.

   - To create an event status, click **New Event Status** and define the event status properties on the **Create Event Status** page.

   - To edit an event status, click the **Edit** icon next to the event status that you want to edit and change the event status properties on the **Edit Event Status** page.

   - To delete an event status, click the **Delete** icon next to the event status that you want to delete and confirm the deletion. You cannot delete a system-defined event status.

Event Attributes

An event attribute is a parameter that you can associate with a workflow to collect business-related information when the associated workflow processes documents. The B2B Data Exchange server saves the information from the workflow to the repository. You can also use event attributes in an advanced search for some objects in the Operation Console.

You create event attributes in the Operation Console based on the information that you want to collect about the event or the document. When you create a workflow in B2B Data Exchange, you select the event attribute to use in the workflow from the list of available event attributes.

You view the event attributes and the values in the **Event Details** section of the **Events** page in the Operation Console. When you perform an advanced search for events, you select from the list of available event attributes to search for an attribute value.

You can use event attributes, for example, to collect the claim number and the claim amount that an insurance company receives from a customer. You include the event attribute value in the workflow that processes the claim. An event attribute that is associated with a workflow is also associated with the profile that uses the workflow.

If you installed the Dashboard and Reports component, you can use event attributes in reports. The B2B Data Exchange developer can use the event attributes to customize the Dashboard and create new Dashboard panels. You can use only numeric event attributes in reports. An event attribute is numeric if the lexical syntax rules in the Java Language Specification define it as a FloatValue.

Event Attribute Properties

Event attributes are parameters that store additional information about the processed events. Use the **Event Attributes** page to view and manage event attributes.

The following table describes the event attribute properties:

Property	Description
Attribute Name	Name of the event attribute.
Description	Optional. Description of the event attribute.
Use for reports	Optional. Determines whether to load the event attributes to the operational data store. The B2B Data Exchange developer can use the event attribute in custom reports that you view in the dashboard. You can load only numeric event attributes to the operational data store.

Managing Event Attributes

Use the Navigator to create, edit, or delete event attributes.

1. In the Navigator, click **Events** > **Event Attributes**.

   The **Event Attributes** page appears.
2. Choose to create, edit, or delete an event attribute.
   - To create an event attribute, click **New Attribute** and define the event attribute properties on the **Create New Attribute** page.
   - To edit an event attribute, click the **Edit** icon next to the event attribute that you want to edit and change the event attribute properties on the **Edit Attribute** page.
   - To delete an event attribute, click the **Delete** icon next to the event attribute that you want to delete and confirm the deletion. If the event attribute is not used in workflows or profiles, B2B Data Exchange deletes the event attribute.

Pending Events Timeout Monitor

B2B Data Exchange contains a mechanism for altering the system administrator and operator when event abnormalities occur.

One of the most useful built-in monitors is the Pending Events Timeout Monitor. This pre-defined monitor alerts system administrators to events that are waiting to be processed for 15 minutes or more. A task that is in the Pending status for 15 minutes or more might have started processing and is taking too long, or its PowerCenter workflow might be down, or another system issue might prevent the task from completing.

The monitor runs every minute.

The pre-defined monitor cannot be deleted, but can be disabled, by setting the execution frequency to Disabled. You can also change the event status time window (by default fifteen minutes).

MIME Type of Event Attachments

You can define the MIME type of a BLOB when you attach the BLOB to an event. The MIME type affects the application used to present the BLOB to the operator.

B2B Data Exchange manages the MIME types in a `mimetypes.properties` file in the `<DX installation directory>/conf` directory. You can edit this file to add an additional MIME type or to change the default value.

If you update the `mimetypes.properties` file, copy it to the `<DX_installation_directory>/conf/META-INF` directory and restart B2B Data Exchange.

CHAPTER 6

Event Archiving

This chapter includes the following topics:

Event Archiving Overview

You can archive events that B2B Data Exchange generates to manage storage space in the runtime repository. You archive events with Data Archive or with the archive command line utility. The archive tool that you choose is based on the requirements in your organization.

Data Archive is an advanced archive tool that archives events and documents to a compressed file store. Use Data Archive to define custom archive projects, schedule archive jobs, and browse archived events and documents that are passed by reference through endpoints in B2B Data Exchange. Archive events with Data Archive to address the following scenarios:

- Short-term archiving. Archive events from the production database, which contains the main Data Exchange document store, to the history database, which stores the archived events and documents in an intermediate document store. You can view and search the archived events from the **Archived Events** page of the Operation Console. Use this method to archive events you need to easily access from B2B Data Exchange but take up too much space in the production database and reduce performance.

- Long-term archiving. Archive events from the main Data Exchange repository or the intermediate repository to an optimized file store, which you can access only from Data Archive or with external viewing tools. Use this method for long term archiving of older events to which you no longer require ongoing access but you need to keep for legal or business compliance purposes.

The archive command line utility is a basic B2B Data Exchange utility that archives events to an XML file and deletes the events from B2B Data Exchange. Use the archive utility if your organization does not require access to archived events. If you archive with the utility, you cannot browse or restore archived events.

Event Archiving Process with Data Archive

Use Data Archive to define archive projects, schedule standalone and recurring archive jobs, and browse archived events and documents in B2B Data Exchange or Data Archive. You can also archive documents that B2B Data Exchange passes by reference.

The archive process with Data Archive typically includes the following stages:

1. Install and configure the B2B Data Exchange accelerator in Data Archive. The accelerator accesses the B2B Data Exchange repository and retrieves events based on the archive project settings that you define in Data Archive. For installation instructions, see the *B2B Data Exchange Installation and Configuration Guide*.

2. Determine the locations of the source and target database. You must store the production database and history database on the same type of database. For example, you cannot archive events from an Oracle database to a Microsoft SQL Server database.

3. Configure the connections to the source and target archive locations. Define general connection properties and database-specific properties based on the archive method that you want to use. You configure the source and target connection properties to archive documents that are passed by reference to the B2B Data Exchange document store.

4. Set up user roles and configure secured access. Create access roles and assign security groups to the source and target archive locations to determine which users can run archive jobs and access archived events in Data Archive. You must create an access role even for a single user. You do not need to create a security group for the target connection.

5. Configure seamless access to the history database. For short-term archiving, create a seamless access layer to link the production database and the history database to view the archived events in the Operation Console.

6. Create the file archive folder. For long-term archiving, create the file archive user, and run a standalone archive job to create the file archive folder.

7. Create and publish the archive project. In the archive project, you define the parameters according to which you want the archive job to archive the events and documents from the source archive location. For example, you can define to archive events of a specific type, status, or partner. Although you can only archive whole event hierarchies, some archive parameters only apply to the root event in the hierarchy.

8. Schedule and run the archive job. The archive job uses the parameters from the archive job that you create and moves the events and documents from the source location to the target location. You can schedule a single immediate job or a recurring job. Each archive scenario requires additional jobs that you run after the main archive job.

9. View the archived events and documents. For short-term archiving, use the **Archived Events** page of the Operation Console to view events that you archive to the history database. For long term archiving, use the Data Discovery portal in Data Archive to browse and search for events that you archive to the file archive.

10. Periodically, rebuild the indexes of the B2B Data Exchange repository schema. You can use the `ALTER INDEX <index name> REBUILD ONLINE` syntax.

Event Archiving with Data Archive Rules and Guidelines

When you use Data Archive to archive events from B2B Data Exchange, consider the following rules and guidelines:

- You must enable the Data Archive process to access the locations that you define in the source and target connections.
- If you move the document store, you must update the location in the **Source / Staging Attachment Location** property for the source connection.
- When you create the archive project, you must select **Archive and Purge** to move documents that B2B Data Exchange passed by reference from the document store. If you select **Archive Only**, the archive job does not copy the documents. If you select **Purge Only**, the archive job deletes the documents.**Purge Only**.
- The archive jobs do not delete documents that B2B Data Exchange stores in temporary folders of the B2B Data Exchange document store. If you no longer require access to the files in the temporary folder, manually delete these files. Do not delete documents that B2B Data Exchange creates on the day that you delete the documents.

Short-Term Event Archiving to the History Database

Use short-term archiving to archive events that you need to easily access in the Operation Console but take up too much space in the B2B Data Exchange repository and reduce performance.

In short-term archiving, you archive events from the production database to the history database. The production database is the main Data Exchange repository. The history database is an intermediate repository that contains the archived events and documents.

You define the source connection properties for the production database and the target connection properties for the history database. You set up the history database user access role and assign the role to users that can access the history database. You add the users to a security group. The history database user must have privileges to create tables, views, and synonyms.

Before you create the archive project and run the archive job, you run the seamless access script to create a seamless access layer that links the production database and the history database. After you run the archive job, you view the archived events on the **Archived Events** page of the Operation Console in the same way you view regular events. You can also assign viewing privileges in B2B Data Exchange to operators based on the policies in your organization. If the history database contains deleted event types, you cannot view the archived events regardless of the viewing privileges.

When you no longer require ongoing access to the archived events and documents, you can use the long term archiving method in Data Archive to archive events from the history database to the file archive. The file archive is a compressed file store that you can access only in Data Archive. Use the long term archiving method to improve performance of the history database and reduce loading time when you view archived events in the Operation Console.

Short-Term Event Archiving Connection Properties

Before you create and run archive jobs from the production database to the history database in Data Archive, you configure source connection properties for the production database and the target connection properties for the history database.

The following table describes the production database source connection properties and the values to enter for short-term archiving:

Property	Description	Value
Application Version	Version of the application.	Must match the installed B2B Data Exchange version.
Source / Staging Attachment Location	Root location of the B2B Data Exchange document store.	Must match the value of the dx.system.document.store.folder system property in B2B Data Exchange.
Target Attachment Location	Location in which to store the archived document store, which contains documents passed by reference.	Must match the value of the dx.archive.document.store.folder system property in B2B Data Exchange.

The following table describes the history database target connection properties and the values to enter for short-term archiving:

Property	Description	Value
Application Version	Version of the application.	Must match the installed B2B Data Exchange version.
Database Link to Source	Link to the metadata tables in the production database.	- For Oracle, consult your database administrator. - For Microsoft SQL Server, use the server link. For more information about server links, see http://msdn.microsoft.com/en-us/library/ms188279.

Short-Term Event Archiving Access Roles Properties

Use the **Assign Role to Entity** section of the **Manage Access Roles** page in Data Archive to set up access roles to each archive location. Set up access roles to determine who can view the archived events and documents. After you create the access roles, you add the roles to security groups and assign the security groups to the source or target connections.

The following table describes the access role properties and the values to enter for short-term archiving:

Property	Description	Value
Application Version	The version of the application.	B2B Data Exchange <version>
Application	The source archive location.	DX_SCHEMA
Entity	The archive entity.	Processing Data

Configuring Seamless Access to the History Database

You create a seamless access layer that links that production database to the history database to view archived events in the Operation Console. You create the tables and indexes of the history database in Data Archive, and run an SQL script to create the seamless access layer.

You must have database administrator privileges for the history database to run the seamless access script.

1. On the **Schedule a Job** page in Data Archive, run the **Create Tables** and **Create Indexes** standalone programs.

    Note: For Microsoft SQL Server, delete the DX_VIEW_ARCHIVE_EVENT table from the history database after you run the **Create Tables** program.

2. In the B2B Data Exchange installation directory, edit the script file for the database on which you store the history database:

Database	Path
Oracle	`<DX installation directory>/ILM-accelerator/sql/` `oracle_seamless_access_script.sql`
Microsoft SQL Server	`<DX installation directory>/ILM-accelerator/sql/` `sqlserver_seamless_access_script.sql`

3. In the &linkName variable, enter the same value as the value of the **Database Link To Source** property in the target connection.

4. In the &databaseName variable, enter the database or schema name for the production database.

5. Save and run the script.

Viewing Archived Events in the Operation Console

After you run a short term archive job in Data Archive, you view the archived events and documents in the Operation Console. You can view the details of the archived events and export the event list.

1. In the Navigator, select **Events** > **Archived Events**.

    The **Archived Events** page the list of events from the history database.

2. To drill down to each archived event, click the event ID.

3. To export the list of events to a CSV file, click **Actions** > **Export to CSV** and save the file.

Long-Term Event Archiving to the File Archive

Use long-term archiving to archive events for which you no longer require ongoing access but must retain for legal or business compliance requirements.

In long-term archiving, you archive events either from the production database to the file archive or from the history database to the file archive. The production database contains Data Exchange document store. The history database contains the archived events and documents in an intermediate repository. The file archive is an optimized file store that contains the archived events and documents to which you can access only from Data Archive or with external viewing tools.

You define the source connection properties for either the production database or the history database, and the target connection properties for the file archive. You set up the file archive user access role and assign the role to users that can access the file archive. You add the users to a security group.

Before you create the archive project and run the archive job, you run a standalone archive to create the file archive folder. After you run the archive job, you view the archived events in the **Data Discovery** portal in Data Archive. You browse for events in the file archive on the **Browse Data** page. Browse for events if you have sufficient information about the event itself, such as the status or the processing start time. You search for events in the file archive with the **Search File Archive** page. Search for events to find events based on associated metadata, such as the related partner or account.

Long-Term Archiving Connection Properties

Before you create and run archive jobs from the production database or the history database to the file archive in Data Archive, you configure source connection properties for the production database or the history database and the target connection properties for the file archive.

The following table describes the production database source connection properties and and the values to enter for long-term archiving:

Property	Description	Value
Application Version	Version of the application.	Must match the installed B2B Data Exchange version.
Source / Staging Attachment Location	Root location of the B2B Data Exchange document store.	Must match the value of the dx.system.document.store.folder system property in B2B Data Exchange.
Target Attachment Location	Temporary location in which to store the archived document store during the archive process. After the archive process ends, the archive job deletes the files.	Must refer to a location with sufficient storage space for the archived document store.

The following table describes the history database source connection properties and the values to enter for long-term archiving:

Property	Description	Value
Application Version	Version of the application.	Must match the installed B2B Data Exchange version.
Source / Staging Attachment Location	Root location of the history database document store.	Must match the value of the dx.archive.document.store.folder system property in B2B Data Exchange.
Target Attachment Location	Temporary location in which to store the archived document store during the archive process. After the archive process ends, the archive job deletes the files.	Must refer to a location with sufficient storage space for the archived document store.

The following table describes the file archive target connection properties and the values to enter for long-term archiving:

Property	Description	Value
Application Version	Version of the application.	Must match the installed B2B Data Exchange version.
File Archive User	User role to use when you create the file archive folder and archive to the file archive. **Note:** The user must be able to send queries to the NPA system data. For more information, consult your file archive service administrator.	sa_user

Long-Term Event Archiving Access Roles Properties

Use the **Assign Role to Entity** section of the **Manage Access Roles** page in Data Archive to set up access roles to each archive location. Set up access roles to determine who can view the archived events and documents. After you create the access roles you add the roles to security groups and assign the security groups to the source or target connections.

The following table describes the access role properties and the values to enter for long-term archiving:

Property	Description	Value
Application Version	The version of the application.	B2B Data Exchange <version>
Application	The source archive location.	DX_SCHEMA
Entity	The archive entity.	FAS Processing Data

Creating the File Archive Folder

Before you create the archive project and run the archive job for long term archiving, you set up the file archive user and run a standalone archive job in Data Archive to create the file archive folder. When you run the archive job, Data Archive uses the location that you defined to archive events to the file archive.

Before you create the archive folder, verify that your machine locale is **English (US)** and that the machine date format is **mm/dd/yyyy**.

1. In the File Archive Service utility, assign the **sa_user** role to the file archive user.

2. On the **Schedule a Job** page in Data Archive, run the **Create Archive Folder** standalone program.

   Data Archive creates the file archive folder.

Viewing Archived Events in Data Archive

After you run a long term archive job in Data Archive, you view the archived events and documents in the Data Discovery portal for Data Archive. You can browse the file archive or search for specific events or documents.

1. In Data Archive, select **Data Discovery**.

2. Choose one of the following options:

Option	Description
Browse Data	Search the file archive according to basic search criteria, such as the file archive folder or database schema.
Search File Archive	Search the file archive according to global search criteria and specific search criteria, such as the type of the event or the partner. Use this option to search for a specific event. Before you search for events, you can define search options on the **Search Options** page.

3. In the list of events, drill down to the details of the event that you want to view.

Viewing Documents Archived by Reference in Data Archive

To view documents that B2B Data Exchanges passed by reference in the file archive, you configure access in Data Archive to the entity that stores the documents. You then specify the document name when you search the file archive.

1. In Data Archive, open the **Manage Access Roles** page and create the access role for the AM_ATTACHMENTS_ENTITY entity.
2. Click **Assign Role to Entity**, and select the application version **B2B Data Exchange**.
3. Select the application **External Attachments** to enable access to the event attachments.
4. In the Data Discovery portal, use the **Search File Archive** page to search for the event to which the document is attached and select to display the **FULL FILE NAME** column in the search results.
5. Copy the name and immediate parent folder for the file that you want to view from the **FULL FILE NAME** column to the clipboard.

   For example, if the full file path is `<doc_store>\documents\by_ref\document.txt`, copy only `by_ref\document.txt`.

6. On the **Search File Archive** page, enter values in the following fields:

Field	Value
Entity	AM_ATTACHMENT_ENTITY
Schema	dbo
Table	AM_ATTACHMENTS

7. In the search rows, define the search criteria:

Criteria	Operator	Description
Attachment Directory	Contains	Immediate parent folder.
Attachment Name	Contains	File name.

8. Click **Search**.
9. Select the file that you want to view and click **Click to view**.

Archive Projects in Data Archive

You manage archive projects in Data Archive. You create short term archiving projects to the history database or long term archiving projects to the file archive.

Before you create the archive project, you configure the source and target connections to the archive locations that you want to use. You set up access roles and assign security groups to the source and target archive locations to determine which users can run archive jobs in Data Archive. Based on the archiving method that you use, you perform additional tasks to prepare Data Archive for the archive process.

When you create the archive project, you define project parameters to control which events and documents to archive. The archive project contains required and optional parameters. Required parameters apply to the entire event hierarchy. Optional parameters apply to the root event in the event hierarchy.

For required parameters that apply to the entire event hierarchy, the archive job archives only event hierarchies in which all events match the parameter. For example, if you select to archive events older than 10 days, the archive job archives event hierarchies in which all events are older than 10 days.

For optional parameters that apply to the root event in the hierarchy, child events of the hierarchy do not need to match the parameter. For example, if you select to archive events with a related partner, the archive job archives event hierarchies in which only the root event has a related partner. The child events in the event hierarchy can have different related partners or no partners.

After you create the archive project, you schedule and run an archive job. The archive job contains the archive project that you created and any additional operations that Data Archive needs to perform to successfully complete the event archiving. For long-term archive jobs, the Load External Attachments archive job reports an error if the B2B Data Exchange document store does not contain any documents.

Archive Project Parameters

When you create the archive project you define the parameters for the accelerator to use when the archive job runs. The archive project parameters are available regardless of the archive method that you use.

The following table describes the archive project parameters:

Parameter	Description
Event Age (days)	Required. Minimum number of days from the event creation date for the entire event hierarchy. For example, if the event was created on March 1, 2014 and the date that the archive job runs in March 10, 2014, the age of the event at the time that the archive job runs is 10 days. Therefore, if the value of the parameter is higher than 10, the archive job does not archive the event. If you enter the value 0 in the parameter, the archive job archives all events that match the other parameter values regardless of the event age. **Note:** All events that B2B Data Exchange generates from 00:00 until 23:59 on the same day have the same event age.
Partner	Related partner for the root event in the event hierarchy.
Account	Related account for the root event in the event hierarchy. **Note:** You can select an account only after you select a partner.
Event Type	Event type for the root event in the event hierarchy.
Event Status	Event status for the root event in the event hierarchy. **Note:** If you do not specify a value, the archive job archives only event hierarchies in which all events reached a final state.

Parameter	Description
Reconciliation Status	Required. Reconciliation status for the entire event hierarchy. You can select one of the following options: - Any. Archives all events that match the other parameter value regardless of the reconciliation status. - Completed. Archives events for which the reconciliation completed successfully. - Completed and Timed-out. Archives events for which the reconciliation completed successfully and events for which the reconciliation did not complete successfully before the timeout limit.
Root Events Without Partners	Required. Instructs the archive job to archive event hierarchies in which the root event has no related partner. If you entered a value in the **Partner** or **Account** parameter, the archive job archives event hierarchies for that partner as well.
Intermediate Documents	Required. Instructs the archive job to archive by reference intermediate documents such as log BLOBS for the entire the event hierarchy. Otherwise, the archive job deletes the documents after the job runs.

Creating an Archive Project

After you configure the source and target connections and set up user access to the archive locations, you create an archive project in Data Archive. In the archive project, you assign the source and target connections to the project, define user roles, and define the archive parameters that determine which events and documents to archive.

1. On the **Manage Archive Projects** page in Data Archive, create an archive project.

2. On the **General Information** page, enter a name for the project and select the **Archive and Purge** action.

3. Select the source and target connections.

4. For long-term archiving, choose to include reference data to ensure archiving of event metadata, such as the partner name or the account number.

   Short-term archiving projects use the database link to retrieve metadata from the production database.

5. On the **Identify Identities** page, click **Add Entity** and choose the entity to which to archive: .

Entity	Description
Processing Data	History database entity. Select for short term archiving.
FAS Processing Data	File archive entity. Select for long term archiving.

6. Assign a user role to the archive project.

7. Define the archive parameters to determine which events and documents to archive.

8. On the **Manage Execution** page, choose whether to publish the project and run the archive job immediately or save the project and schedule the archive job separately.

Scheduling an Archive Job

After you create the archive project, you schedule an archive job that includes the archive project definitions. You also schedule additional archive programs based on the archiving method that you use. You can run the job immediately, at a later time, or as a recurring job.

1. On the **Schedule a Job** page, select the archive project that you want to run and add the program that you want to run.

   For example, to schedule a short term archive job from the production database to the history database, add the **Oracle Production > History** program.

2. Choose additional standalone programs to run based on the archiving method that you use:

Option	Description
Create Indexes	Short term archiving. Generates indexes for the archived data. Enter the same the source and target connections as the main archive job.
File Archive Loader	Long term archiving. Loads the events to the file archive. Leave the **Archive Job ID** field empty.
Load External Attachments	Long term archiving. Loads documents that B2B Data Exchange passes by reference to the file archive. Enter values in the following fields: • In the **Directory** parameter, enter the same value as the value for the **Target Attachment Location** property of the source connection. • In the **Target Archive Store** parameter, enter the same value as the value of the **Target Archive Store** parameter in the main archive job. • In the **Purge After Load** option, select **Yes**. If you run multiple Load External Attachments archive jobs in the same directory, the archive jobs might create duplicate files. To prevent duplicate files, configure source connections for different staging directories.

3. Define the job schedule and click **Schedule**.

   If you scheduled the archive job to run at a later time, you can view the job status on the **Manage Jobs** page. After the archive job ends, you can view the job status and results on the **View Job History** page.

Event Archiving Process with the Archive Command Line Utility

Use the archive command line utility to archive events and documents from B2B Data Exchange to an external XML file and delete the events and the documents from B2B Data Exchange.

You can archive the following event types:

- Root events
- Parent and child events
- Events with a final status
- Legacy audit trail events from earlier B2B Data Exchange versions with a status of Completed or Rejected
- Reconciliation events with a Reconciled reconciliation status

The archive specification file contains the parameters according to which you want to archive the events. In the specification file, you can select to archive events for a specific partner or account. You can also archive events based on the event creation date and time. The archive specification file also contains pre-configured rules that you can use to limit the archive criteria. If any event that you want to archive contains reconciliation information, the associated reconciliation event must be with the status Reconciled.

After the archive process completes successfully, B2B Data Exchange generates an event for the archive process with a status of Complete. The event contains a log BLOB that describes the object hierarchies in the archive file, the data that the archive utility purged, and any error that the archive utility generated.

Archive Specification File

The archive specification file contains rules that the archive utility uses to determine which events to archive. You edit the file in a text editor.

The following table describes the archive specification file elements:

Element	Description
Name	Name of the archive rule.
PartnerName	Name of the partner. You can specify a partner name or use one of the following options: - (ALL). Default. Archives events for all partners and events with no partners. - (SYSTEM). Archives system events and legacy audit trail events.
StorageLocation	Absolute path to the directory in which to create the the archive file. The B2B Data Exchange server must be able to access the location in which you store the archive file.

EventAge	Required. The minimum age of the event to be archived based on the last change to the event status. Specify the age in the following format:
	`<NumOfDays>d <NumOfHours>h <NumOfMinutes>m`
	The archive includes events where the status was changed before the specified number of days, hours, and minutes.
	For example:
	`20d 12h 0m`
	This value means that the archive utility includes only events where the event status was changed at least 20 days and 12 hours ago.

ArchiveEvents	Indicates whether to archive events. If you set the PurgeEvents to true, use this element to specify whether the events will be archived before they are deleted from the repository. If you set ArchiveEvents to false, you cannot set the PurgeEvents element to false. Default is true.
PurgeEvents	Indicates whether to delete events from the Data Exchange Repository. You can use this element to delete events from the repository after they are archived. If you set PurgeEvents to false, you cannot set the ArchiveEvents element to false.
IncludeLogBlobs	Indicates whether the log data for log events will be included in the archive. Default is false.

The following example shows the contents of the archive specification file:

```
<ArchiveTask>
<!-- archive events for a particular partner, account combination -->
    <ArchiveRule>
        <Name>Archive Rule One</Name>
        <PartnerName>(ALL)</PartnerName>
        <StorageLocation>c:\temp\archive\all</StorageLocation>
```

```
            <EventAge>1d 0h 0m</EventAge>
            <ArchiveEvents>true</ArchiveEvents>
            <PurgeEvents>true</PurgeEvents>
            <IncludeLogBlobs>false</IncludeLogBlobs>
        </ArchiveRule>
    <!-- archive the Audit Trail and system events -->
        <ArchiveRule>
            <Name>System Events</Name>
            <PartnerName>(SYSTEM)</PartnerName>
            <StorageLocation>c:\temp\archive\system</StorageLocation>
            <EventAge>0d 12h 00m</EventAge>
            <ArchiveEvents>false</ArchiveEvents>
            <PurgeEvents>true</PurgeEvents>
            <IncludeLogBlobs>true</IncludeLogBlobs>
        </ArchiveRule>
    </ArchiveTask>
```

Archive Command Syntax

After you define the archive rules in the specification file, you run the archive utility with the command line. The archive utility creates the archive file and deletes the archived events from B2B Data Exchange.

The archive utility uses the following syntax:

```
archive
<-s|--specification> file
<-u|--user> userID
<-p|--password> user password
[--server "hostname:port"]
```

The following table describes options and arguments for the archive utility commands:

Option	Argument	Description
-s --specification	file	Required. Absolute path and file name of the archive specification file.
-u -user	userID	Optional. User name of an Operation Console user account with archiving privileges. If you use Informatica domain authentication or Informatica domain with Kerberos authentication, the user ID must specify the Informatica security domain, separated by the @ symbol. For example: `Administrator@SecurityDomain`
-U	Environment variable	Optional. Environment variable that contains a user name. User name of an Operation Console user account with archiving privileges. If you use Informatica domain authentication or Informatica domain with Kerberos authentication, the user name must specify the Informatica security domain, separated by the @ symbol. For example: `Administrator@SecurityDomain` **Note:** You must specify at least one of the user name options, -u or -U.
-p --password	user password	Optional. Password of the Operation Console user that runs the archive command. The password must be in clear text.

Option	Argument	Description
-P	Environment variable	Optional. Environment variable that contains a password. Password of the Operation Console user that runs the archive command. The password must be encrypted. Use `dxencrypt` for the encrypted value. **Note:** You must specify at least one of the password options, -p or -P.
--server	"hostname:port"	Optional. Host name and port number of the Data Exchange server. If you do not pass this option, the archive utility connects to the localhost server with the default port 18095. You must enclose the argument in quotation marks, such as: `archive --server "localhost:18095"...`

C H A P T E R   7

User Policies

This chapter includes the following topics:

User Policies Overview

User policies determine which users can log in to B2B Data Exchange and access information that B2B Data Exchange processes.

You manage user policies in the following areas of B2B Data Exchange:

- User authentication. Credentials for B2B Data Exchange user accounts. User authentication controls which users can log in to the Operation Console. You can use native authentication or Informatica domain authentication.

- User groups. Sets of users with permissions and privileges that determine the actions that users can perform in the Operation Console. You must include each user in one or more user groups.

- Categories. Additional permissions that you use to determine which user groups can access objects. You create categories and grant permissions for the categories to user groups. The operator assigns categories to accounts, profiles, and partners.

- Portal user groups. Groups with access privileges to the partner Portal.

User Authentication

User authentication determines the users that can log in to B2B Data Exchange. The user authentication mode controls the location of user accounts and the tools for managing the accounts.

When you install B2B Data Exchange you select a default administrator user name. The password is the same as the user name. Use the administrator account to manage user authentication in one of the following authentication modes:

- B2B Data Exchange native authentication. Stores user accounts in the local B2B Data Exchange repository. Use native authentication for a development or a test environment. When you install B2B Data Exchange, the default password is the same as the user name. Use the Navigator of the B2B Data Exchange Operation Console to manage users in the B2B Data Exchange repository.

- Informatica domain authentication or Informatica domain with Kerberos authentication, depending on the authentication method that your Informatica domain uses. Synchronizes user accounts with the Informatica security domain. Use Informatica domain authentication or Informatica domain with Kerberos authentication for a production environment. Use the Administrator tool of the B2B Data Exchange Operation Console to manage users. Use the Operation Console Navigator to synchronize users between the security domain and the B2B Data Exchange repository and to assign user groups to users.

You can switch between B2B Data Exchange native authentication and Informatica domain authentication or Informatica domain with Kerberos authentication, depending of the authentication method that your Informatica domain uses. If you switch from B2B Data Exchange native authentication to Informatica domain authentication or to Informatica domain with Kerberos authentication, the user synchronization process overrides existing user accounts.

User Account Properties

You define user account details and user group assignments on the **Edit/Create User** page of the Operation Console. In Informatica domain authentication mode, user account details appear in read-only mode and you can define only user group assignments.

The following table describes the user account properties on the **Details** tab:

Property	Description
User ID	Unique identifier for the user account. In Native authentication mode, the user ID and password are identical. You cannot change this property after you create the user account. The maximum character length is 80.
Full Name	Name or description for the user account. The maximum character length is 255.
Email	Optional. Email address for the user account. The maximum character length is 255.

The following table describes the user account properties on the **User Groups** tab:

Property	Description
Available User Groups	List of user groups to which you can assign the user account.
Selected User Groups	List of user group assignments for the user account.

Managing Users in Native Authentication

Manage users on the **Users** page of the Operation Console. When you use native authentication, you manually define a user name and password for users in the Operation Console.

1. In the Navigator, click **Administration** > **Users**.

   The **Users** page appears.

2. Choose to create, edit, or delete a user.

   - To create a user, click **New User** and configure the user properties and user group assignments.
   - To edit an user, click the **Edit** icon next to the user that you want to edit and change the properties or user group assignments for the user. You cannot change the user ID property.
   - To delete an user, click the **Delete** next to the user that you want to delete and confirm the deletion.

You must assign the user account to one or more user groups to define permissions and privileges to the user. You cannot manage permissions for a single user account.

Switching to Native Authentication

Use the command line to switch from Informatica domain authentication or from Informatica domain with Kerberos authentication to B2B Data Exchange native authentication.

1. In the command line, change to the following directory:

   ```
   <DX_Install_Directory>/dx-tools
   ```

2. Run the following command:

   ```
   repoutil

   -c migrateToNative

   -l "<JDBC_URL_for_DX_Repository>"

   -u <DX_Repository_User_Name>

   -p <DX_Repository_Password>

   --sysadmin <DX_System_Administrator_User_Name>

   -t dx
   ```

   The authentication mode changes to native authentication and the system creates the administrative user that you specified in the --sysadmin command.

3. Use the Navigator to create additional users.

Managing Users in Informatica Domain Authentication

When you use Informatica domain authentication or Informatica domain with Kerberos authentication, you can synchronize users in the Informatica security domain with B2B Data Exchange. Use the Operation Console Navigator to synchronize users between the security domain and B2B Data Exchange. You synchronize users after you switch from Native authentication or if user information in the security domain changed.

To synchronize users in the Informatica security domain with B2B Data Exchange, the following conditions must be true:

- The Informatica security domain is configured on the **Security** page of Informatica Administrator.

- At least one security group in the Informatica security domain contains the B2B Data Exchange users to synchronize.
- The B2B Data Exchange system property `dx.authentication.groups` contains the list of groups from the Informatica security domain to synchronize, in the following format:

  ```
  <group name>@<security domain> [;<groupname>@<security domain>]
  ```
- One of the groups that are defined in `dx.authentication.groups` contains the user that performs the synchronization.
- The user that is defined in the B2B Data Exchange system property `pwc.repository.user.name` has privileges to manage users, groups, and roles.
- The B2B Data Exchange user has privileges to synchronize users.

1. In the Navigator, click **Administration** > **Users**.

   The **Users** page appears.

2. Click **Synchronize Users**.

   The **Synchronize Users** page appears.

3. Click **OK** to synchronize users.

4. On the **Edit User** page, verify user group assignments for the users that you synchronize.

Switching to Informatica Domain Authentication

Use the command line to switch from B2B Data Exchange native authentication to Informatica domain authentication.

1. In the command line, change to the following directory:

   ```
   <DX_Install_Directory>/dx-tools
   ```

2. Run the following command:

   ```
   repoutil

   -c migrateToISP

   -l "<JDBC_URL_for_DX_Repository>"

   -u <DX_Repository_User_Name>

   -p <DX_Repository_Password>

   -Ddx.pwc.domain.gateway=<PowerCenter_GatewayHost>:<PowerCenter_GatewayPort>

   -Ddx.pwc.user=<PowerCenter_User_Name>@<Security_Domain>

   -Ddx.pwc.password=<PowerCenter_Password> -t dx
   ```

   The authentication mode changes to Informatica domain and the repoutil deletes all users from the B2B Data Exchange repository.

3. Restart the B2B Data Exchange Operation Console.

4. Synchronize the users from the Informatica platform security domain to the B2B Data Exchange repository.

   For more information, see "Managing Users in Informatica Domain Authentication" on page 43.

Switching to Informatica Domain with Kerberos Authentication

Switch from B2B Data Exchange native authentication or from Informatica domain authentication to Informatica domain with Kerberos authentication.

1. Create a `.properties` file with the following properties:

   - dx.kerberos.initial.administrator=<Kerberos_Domain_System_Administrator_Credentials>
   - dx.kerberos.krb5.file=<File_That_Stores_Keberos_Configuration_Information>
   - dx.kerberos.console.keytab.file=<Location_of_the_Keytab_File_for_the_Operation_Console>
   - dx.kerberos.console.service.principal.name=<SPN_for_the_Operation_Console>
   - dx.pwc.domain.gateway=<PowerCenter_Domain_Gateway_Host_and_Port_Number>

2. Optionally, add the following properties to the file:

   - dx_system_property.pwc.repository.user.name= <User_to_Access_the_PowerCenter_Repository_Service>
   - dx_system_property.pwc.repository.password= <Plain_Text_Password_to_Access_the_PowerCenter_Repository_Service>
   - dx_system_property.pwc.user.name.space=<PowerCenter_Security_Domain>

   For example, if the credentials changed during the upgrade. B2B Data Exchange stores the password in an encrypted form.

3. In the command line, change to the following directory:

   ```
   <DX_Install_Directory>/dx-tools
   ```

4. Run the following command:

   ```
   repoutil

   -c migrateToISPKerberos

   -l "<JDBC_URL_for_DX_Repository>"

   -u <DX_Repository_User_Name>

   -p <DX_Repository_Password>

   -t dx
   --file <Properties_File_You_Created_in_Step_1>
   ```

   For example:

   ```
   repoutil.bat -c migrateToISPKerberos -l "jdbc:informatica:oracle://
   machine1:1521;SID=orcl" -u DX_DB_USER -p DX_DB_PASSWORD -t dx --file
   c:\migrateToISP.properties
   ```

5. If you performed step 2 and added the credential to the properties file, run the following command:

   ```
   repoutil

   -c loadProperties

   --file <Properties_File_You_Created_in_Step_1>

   -u <DX_Repository_User_Name>

   -p <DX_Repository_Password>

   -t dx
   -l "<JDBC_URL_for_DX_Repository>"
   ```

For example:

```
repoutil -c loadProperties --file c:\PowerCenter.properties -u DX_DB_USER -p
DX_DB_PASSWORD -t dx -l "jdbc:informatica:oracle://machine1:1521;SID=orcl"
```

The authentication mode changes to Informatica domain with Kerberos and the repoutil deletes all users from the B2B Data Exchange repository.

6. Synchronize the users from the Informatica security domain to the B2B Data Exchange repository.

User Groups

A user group defines permissions and privileges for B2B Data Exchange user accounts. Permissions control the objects and data that users can access. Privileges control the actions that users can perform on objects.

B2B Data Exchange contains the following default user groups:

- Administrator

- Analyst

- Developer

- Operator

- SysAdmin

You must assign each user to one or more user groups. You cannot edit or delete the default user groups. You can create, edit, and delete additional user groups.

When you create a user group, you assign one or more roles to the user group. Each role defines permissions to access defined types of data and privileges to use defined system functions. You can assign some or all of the permissions and privileges to the user group. The roles are predefined and you cannot create custom roles.

User Group Permissions

You define user group properties on the **Create/Edit User Group** page.

You define permissions to determine the object categories that the users in the group can view or change. When you assign categories to partners, accounts, or profiles, only user groups with permissions to the categories can view or change the objects.

The **Permissions** tab includes the following properties:
User Group Name

Textual name for the user group.

Category permissions

Determines whether to grant the user group read and write permissions to all categories or to specific categories. You can choose from the following options:

- Grant read and write permissions to all categories

- Select specific categories to grant read permissions or both read and write permissions

If you select specific categories, users in the group can access only objects with the selected categories and objects with no category assignments.

User Group Privileges

You define user group properties on the **Create/Edit User Group** page.

You define privileges to determine which actions users in the group can perform on different object types. To assign privileges, you select roles and add or remove privileges as needed.

B2B Data Exchange contains the following roles:

- Administrator
- Analyst
- Developer
- Operator

You select roles and set privileges to the roles on the **Privileges** tab. Each role includes default privileges and some privileges appear in more than one role.

If you create an event type, B2B Data Exchange assigns viewing privileges for that event type to the default user groups. To grant custom user groups access to the event type, you must manually assign viewing privileges to additional user groups that you create.

Administrator Role Privileges

The following table describes the actions that the Administrator role can perform on objects in B2B Data Exchange:

Object	Action
Account Attribute	- View - Edit
Audit Event	- View - Create - Edit - Delete
Authorization Levels	- Edit
Calendar	- View - Create - Edit - Delete
Category	- View - Create - Edit - Delete
Checklist	- View
Checklist Template	- View - Create - Edit - Delete

Object	Action
Endpoint	- View - Create - Edit - Delete
Partner Attribute	- View - Edit
Portal Groups	- View - Create - Edit - Delete
Schedule	- View - Create - Edit - Delete
System Property	- View - Create - Edit - Delete
User	- View - Create - Edit - Delete
User Group	- View - Create - Edit - Delete
Other	- Allow Pause or Resume Dx Server - Archiving - Export Data - Import Data - Managed File Transfer - Synchronize Users

Analyst Role Privileges

The following table describes the actions that the Analyst role can perform on objects in B2B Data Exchange:

Object	Action
Application	- View
Category	- View
Dashboard	- View
Event Attribute	- View

Object	Action
Event Status	- View
Event Type	- View
Event	- View
Partner	- View
Profile	- View
View Events	- Custom Event - File Level Event - Group Level Event - Segment Level Event - System Event - Transaction Level Event
Workflow	- View

Developer Role Privileges

The following table describes the actions that the Developer role can perform on objects in B2B Data Exchange:

Object	Action
Application	- View - Create - Edit - Delete
Event Attribute	- View - Create - Edit - Delete
Event Status	- View - Create - Edit - Delete
Event Type	- View - Create - Edit - Delete
Profile	- View - Edit

Object	Action
System Property	- View - Create - Edit - Delete
Workflow	- View - Edit

Operator Role Privileges

The following table describes the actions that the Operator role can perform on objects in B2B Data Exchange:

Object	Action
Account Attribute	- View
Application	- View
Archived Event	- View
Audit Event	- View
Authorization	- View
Authorization Approve/Reject	- Edit
Calendar	- View - Edit
Category	- View - Create - Edit - Delete
Checklist	- View - Edit
Checklist Template	- View
Dashboard	- View
Endpoint	- View - Create - Edit - Delete
Event Attribute	- View
Event Status	- View
Event Type	- View

Object	Action
Event	- View
MFT Connections	- View - Create - Edit - Delete
MFT Web Users	- View - Create - Edit - Delete
Monitor	- View - Create - Edit - Delete
On-boarding Report	- View
Partner Attribute	- View
Partner	- View - Create - Edit - Delete
Portal Groups	- View
SLA Rule	- View - Create - Edit - Delete
Schedule	- View - Edit
System Property	- View
User	- View
User Group	- View
View Events	- Custom Event - File Level Event - Group Level Event - Segment Level Event - System Event - Transaction Level Event

Object	Action
Workflow	- View
Other	- Allow Endpoint Selection for Event Resend - Allow Profile Selection for Event Reprocess - Allow Source File Selection for Event Reprocess - Allow Source File Selection for Event Resend - Change Event Status - Managed File Transfer - Monitor Full Access - Promote Partner - Reprocess Event - Resend Event - Run Profile

Managing User Groups

Manage custom user groups on the **User Groups** page of the Operation Console.

1. In the Navigator, click **Administration** > **User Groups**.

   The **User Groups** page appears.

2. Choose to create, edit, or delete a custom user group.

   - To create a custom user group, click **New User Group** and configure the permissions and privileges.

   - To edit a custom user group, click the **Edit** icon next to the user group that you want to edit and change the permissions and privileges. You cannot edit or delete default user groups.

   - To delete a custom user group, click the **Delete** icon next to the user group that you want to delete and confirm the deletion.

If you assign user group permissions to specific categories, you assign categories to objects such as partners, accounts, and profiles to link them with the user group.

Portal User Groups

A portal user group defines privileges for B2B Data Exchange Partner Portal users.

You can create, edit, and delete user groups. When you create a user group, you define privileges for the user group. You can assign each portal user to one or more user groups.

You define user group properties on the Create/Edit Portal User Group page.

Managing Portal User Groups

Manage portal user groups in the **Portal User Groups** page of the Operation Console.

Note: If you do not assign a portal user group to a portal user, the portal user can only view the Dashboard in the Partners Portal.

1. In the Navigator, click **Administration** > **Portal User Groups**.

   The **Portal User Groups** page appears.

2. Choose to create, edit, or delete a portal user group.

- To create a portal user group, click **New User Group** and configure the privileges.

- To edit a portal user group, click the name of the user group that you want to edit, or the **Edit** icon next to the user group, and change the privileges.

- To delete a portal user group, click the **Delete** icon next to the user group that you want to delete and confirm the deletion.

3. To assign privileges to a portal user group, in the Privileges tab select the privileges to assign.

- To assign the portal user role, select **Portal User Role**.

- To view the Dashboard in the Partners Portal, click **View Dashboard**. Alternatively, to assign all Dashboard privileges, click **Dashboard**.

- To view the Event List in the Partners Portal, click **View Event List**. Alternatively, to assign all Event List privileges, click **Event List**.

- You can set the following message profile privileges in the Partners Portal:

  - To view message profiles, click **View Message Profiles**

  - To edit message profiles, click **Edit Message Profiles**.

  - Alternatively, to assign all privileges, click **Message Profile**.

  a. To assign the portal user role, select **Portal User Role**.

  Note: You cannot save the portal user group without assigning the portal user role.

  b. To view the Dashboard in the Partners Portal, click **View Dashboard**. Alternatively, to assign all Dashboard privileges, click **Dashboard**.

  c. To view the Event List in the Partners Portal, click **View Event List**. Alternatively, to assign all Event List privileges, click **Event List**.

  d. You can set the following message profile privileges in the Partners Portal:
  - To view message profiles, click **View Message Profiles**
  - To edit message profiles, click **Edit Message Profiles**.
  - Alternatively, to assign all privileges, click **Message Profile**.

  e. You can set the following endpoint privileges in the Partners Portal:
  - To view endpoints, click **View Endpoints**.
  - To edit the password for organization hosted FTP or FTPs endpoints, click **Change Password**.
  - Alternatively, to assign all privileges, click **Endpoint**.

  f. You can set the following file exchange privileges in the Partners Portal:
  - To view file exchanges, click **View File Exchange**.
  - To download files from the portal, click **Download Files**.
  - To upload files to the portal, click **Upload Files**.
  - To delete files on the portal, click **Delete Files**.
  - Alternatively, to assign all privileges, click **File Exchange**.

4. Click **Save**.

Categories

A category controls access to partners, accounts, or profiles. You assign categories to user groups to determine the users that can view or change the objects. Objects without categories are accessible by all users.

A category can represent regional classifications for the partner, account, or profile. For example, you might have a Western sales region that includes California, Oregon, and Washington. You can create a category for each state, and a user group with privileges for sales personnel. Assign the California, Oregon, and Washington categories to the sales user group. Sales personnel in the Western region can access all the partners that are relevant to their work.

You can assign categories to multiple user groups. For example, your customer service department might have a different Western region that includes California, Nevada, Oregon, and Washington. Assign the categories for those states to the customer service user group. Customer service personnel in the Western customer service region can access all the partners that are relevant to their work.

The operator assigns categories to partners, accounts, or profiles. Categories also control access to dependent objects, such as events, monitors, SLA rules, and data in the Dashboard reports. The categories the operator assigns to partners, accounts, or profiles must match the categories that you assign to the user groups.

For more information about assigning categories to partners, accounts, or profiles, see the *B2B Data Exchange Operator Guide*.

Managing Categories

Create, edit, or delete categories on the **Categories** page of the Operation Console.

1. In the Navigator, click **Administration** > **Categories**.

   The **Categories** page appears.
2. Choose to create, edit, or delete a category.

   - To create a category, click **New Category**, enter the name for the category, and click the green checkmark next to the category.

   - To edit a category, click the **Edit** icon next to the category that you want to edit, change the name of the category, and click the green checkmark next to the category.

   - To delete a category, click the **Delete** next to the category that you want to delete and confirm the deletion.

     Note: If you delete a category for an object with no other assigned categories, the object becomes accessible by all users.

CHAPTER 8

Schedules

This chapter includes the following topics:

Schedules Overview

A schedule is used to establish when B2B Data Exchange runs PowerCenter batch workflows.

A PowerCenter batch workflow reads from a file, database, or another customer source. It runs once and stops after completion. You can use file-reading PowerCenter batch workflows to process documents from B2B Data Exchange. You can use the other batch workflows to generate documents for B2B Data Exchange, for example, outbound reports. The B2B Data Exchange administrator can use the scheduling feature to run the batch workflows when required.

Navigating the Schedules Page

This topic describes various actions that you can perform on the Schedules page. You can sort schedules alphabetically based on the name of the schedule. If schedules spans across multiple pages, you can navigate between multiple pages using pagination buttons.

- To navigate to the Schedules page, select **Administration** > **Schedules**
- To sort schedules click the arrow button next to Schedule Name.
  The schedules are listed alphabetically.
- To find a schedule in a particular page, click the pagination buttons in the bottom of the Schedules page.
  - Click the **First** button to navigate to the first page.
  - Click the **Next** button to navigate to the next page.
  - Click the **Previous** button to navigate to the previous page.

- Click the **Last** button to navigate to the previous page.

- Enter a number in the **Page** text box to navigate to the corresponding page number.

- To view a certain number of schedules in the Schedules page, select a number from the **Show** drop-down list.
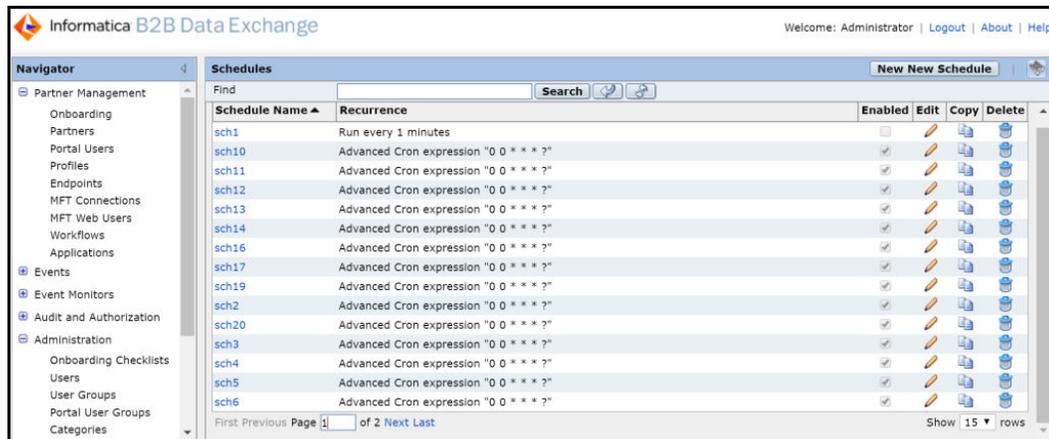
Creating a Schedule

1. In the Navigator, click Administration > Schedules. The Schedule screen appears.
2. Click New Schedule.
3. Enter the Schedule Name.

4. Optionally, enter Comments.
5. Select the Start Time hour and minutes from the drop-down lists or type them in.

6. Select the Recurrence of the schedule:

- If the schedule is a one-time occurrence, check Run Once. Click the Calendar icon and select a date to run the schedule.

- If the schedule is to run every X minutes, check Minutes and enter the run interval in minutes.

- If the schedule is ro run every X hours, check Hours and enter the run interval in hours.

- If the schedule is a daily one, check Daily.

- If the schedule is a weekly one, check Weekly, and then check the desired day of the week.

- If the schedule is a monthly one, check Monthly. If the schedule is to trigger on a given date each month, click Run on day and select the appropriate date. If the schedule is to trigger on a certain weekday each month, for example, the second Tuesday, select these options.

- To define your schedule using a Cron expression, click the Advanced option and enter the Cron expression. Double check the expression very carefully before saving the schedule. An incorrect Cron expression can cause undesirable results.

  Note: B2B Data Exchange does not support schedules shorter than one minute. Schedules shorter than one minute are run once a minute.

7. Using the Status field, select the status of the schedule.

8. Click Save.

Searching Schedules

You can search for a schedule from the list of existing schedules.

Perform the following steps to search a schedule:

1. In the Navigator, click **Administration** > **Schedules**.

   The Schedule page appears.

2. Enter the name of the schedule in the **Find** text box and click **Search.**

   Schedules that match with the text that you have entered displays.

3. Click the **Reload Default Search Results** button.

   The search result is cleared and the list of schedules appears.

4. Click the **Refresh Search Results** button.

   The search results are updated.

Editing a Schedule

To edit a schedule, click Administration > Schedules and click the Edit icon for the schedule you want to edit. Modify the schedule properties and click the Save icon.

Deleting a Schedule

1. In the Navigator, click Administration > Schedules.
2. Click the Delete icon for the schedule you want to remove and confirm the deletion.

CHAPTER 9

B2B Data Exchange Administrative Tasks

This chapter includes the following topics:

B2B Data Exchange Administrative Tasks Overview

Your organization might need to approve actions that operators perform in the Operation Console. Use the Operation Console to manage authorization levels for B2B Data Exchange users. When you set authorization levels for users and objects, operators with authorization privileges can approve or reject actions that other operators perform on the objects in the Operation Console. In addition, administrators can examine access logs to track and analyze actions that users perform in the Operation Console.

You can also use the Operation Console to create calendars that manage event monitoring notifications. B2B Data Exchange uses event monitors to track partner events. Event monitors track events based on the event type and status. When you create a calendar, you can specify holidays and other dates so that B2B Data Exchange sends monitoring notifications after the holiday.

Authorization Levels

Your organization may need to monitor and regulate actions that operators perform on certain objects that directly affect business functions. When you set authorization levels for the objects, operators with authorization privileges can approve or reject actions that other operators perform on the objects in the Operation Console, such as editing or deleting partners or accounts.

Operator actions on the object may require approval by one or two operators with authorization privileges. You define the authorization levels for each object type, and assign authorization privileges to specific operators based on the organization needs. For example, to require approval by two operators each time an

operator edits a partner, set the authorization level for the **Partner** object type and the **Edit** action type to **Second Level**.

Only operators that did not perform the actions can approve the actions. In addition, if the action requires approval by two operators, a different operator must perform each approval level. If the action requires approval by two operators, the request remains pending until the second operator approves the request. If an operator edits an object, that object is locked for editing while the action request is pending and a message indicates that the object contains pending actions. If an operator creates an object, the object is not visible to other operators while the action request is pending.

When an operator deletes an object with related objects, the approval for the parent object applies to all related objects even if the related objects require a different approval level. For example, if an operator with authorization privileges approves an action request to delete a partner with a profile that requires second level approval, B2B Data Exchange deletes that profile without requiring second level approval. Actions that B2B Data Exchange receives from external tools, such as the Web Services API or the command line utilities, do no require approval and override actions that operators perform in the Operation Console.

Authorization Level Properties

You define authorization levels for each object and action type. If you enable authorization, each action that the operator performs on the specified object type requires approval by one or two operators with authorization privileges.

You define authorization levels to require approval when operators create, edit or delete the partner, account, or profile object types. For example, your organization may not require approval to create a partner, but may require approval from two operators to delete a partner.

Note: You cannot modify the authorization levels if any operator action is pending approval.

The following table describes the authorization level properties:

Authorization Level	Description
None	No approval required.
First Level	Requires approval by one operator.
Second Level	Requires approval by two operators.

Setting Authorization Levels

You set the authorization levels to require approval by one or two operators with authorization privileges for each action that operators perform on the object type.

1. In the Navigator, click **Administration** > **Authorization Levels**.

    The **Authorization Levels** page displays the object types and the authorization levels for each operator action.

2. Set the authorization level for each object type and action type to **None**, **First Level**, or **Second Level**, based on the organization requirements or policies.

3. To enable operators to approve or reject actions, assign authorization privileges to operators based on the organization requirements and policies in the **User Group** page.

Viewing Access Logs

You can examine the access logs to track and analyze actions that users perform in the Operation Console and Partners Portal.

To track and analyze the user actions on a specific day, check the `localhost_access_log.<date>.txt` log files at the following directory: `<DXInstallationDir>/DataExchange/tomcat/logs`. The date is in the format `yyyy-mm-dd`.

To view expanded details about user activity that include login activity, check the `dx-console.log` files at the same directory: `<DXInstallationDir>/DataExchange/tomcat/logs`.

Calendar Management

You can set up multiple calendars with different holiday and weekend schedules. For each calendar, indicate which days of the week are weekend days and which dates are holidays. You can set the holiday dates for the current year and for the next six years.

To create a calendar with weekend days and holiday dates similar to an existing calendar, copy a calendar, modify the dates, and save it with a new name.

Creating a Calendar

1. In the Navigator, click Administration > Calendars.
2. Click New Calendar.
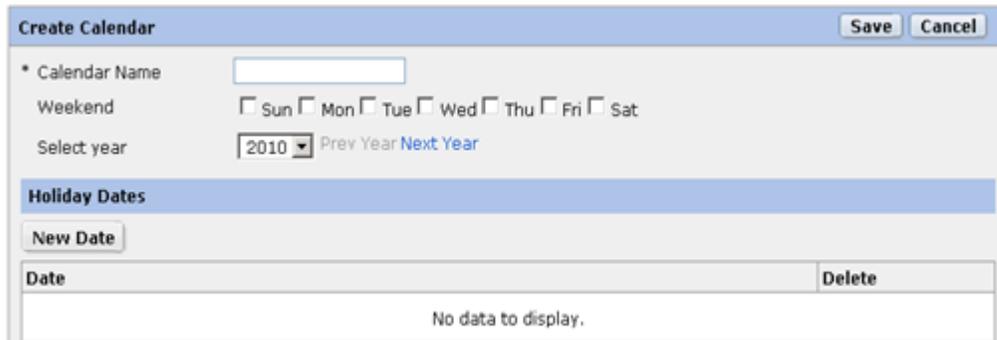
3. Enter a name for the calendar.
4. Select the days of the week to designate as weekend (non-working) days.
5. To select dates to designate as holidays, select the calendar year and click New Date.

   A calendar displays the current month and year.
6. Select a date from the calendar.

   You can click the left or right arrows to view the previous or next year or month.
7. Repeat steps 5 and 6 to add more holiday dates.
8. Click Save.

Copying a Calendar

To copy a calendar, click Administration > Calendars and click the Copy icon for the calendar that you want to edit. Enter a new name. Modify the weekend days and holiday dates. Click Save.

Editing a Calendar

To edit a calendar, click Administration > Calendars and click the Edit icon for the calendar you want to edit. Modify the weekend days and holiday dates and click Save.

Deleting a Calendar

To delete a calendar, click Administration > Calendars and click the Delete icon for the calendar you want to remove. Confirm the deletion.

Setting Date and Time Format

Use the Navigator to configure the format to use when the Operation Console displays the date and time.

1. In the Navigator, click **Administration** > **Preferences**.
2. Select the date and time format for the Operation Console.
3. Click **Save**.

CHAPTER 10

On-boarding Checklist Template

This chapter includes the following topics:

On-boarding Checklist Template Overview

Partner on-boarding is the organizational process that transforms a new trading agreement into a working connection for a new partner. On-boarding partners to send and receive messages with the organization with B2B Data Exchange. The on-boarding process often involves multiple roles within the organization, each of which has to perform tasks to implement the trading agreement. Some of these tasks are performed in the B2B Data Exchange environment. Other tasks are carried out in other systems, for example, CRM and Accounting.

An on-boarding checklist template contains the tasks that the B2B Data Exchange operator must accomplish in order to complete the on-boarding process.

Administrators use the Operator Console to create, edit, and delete functions in on-boarding checklist templates. The administrator customizes an on-boarding checklist from the checklist template for a specific partner.

After the administrator creates a template, an operator uses an on-boarding checklist to implement and monitor the on-boarding tasks that are performed for the partner so that the partner can send and receive messages with B2B Data Exchange.

Creating an On-boarding Checklist Template

1. In the Navigator, click Administration > On-boarding Checklists.

   The On-boarding Checklist Templates screen appears.

On-boarding Checklist Templates		New Template		
Name	**Description**	**Publish**	**Edit**	**Delete**
EDI partners		⊙	✎	🗑
HIPPA 4010		⊙	✎	🗑
HIPPA 5010		⊙	✎	🗑
Test1		⊙	✎	🗑
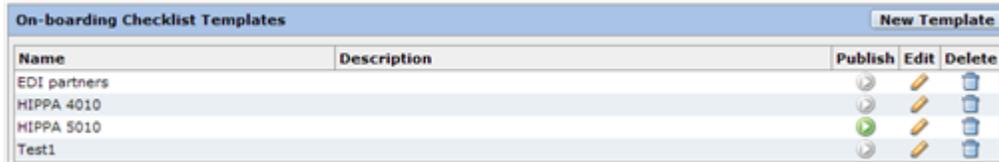
2. Click New Template.

   The Create New Checklist Template screen opens:

Create new Checklist template	Save	Cancel

   * Name
   Description

   Tasks
   Add Task

Name	**Description**	**Up**	**Down**	**Edit**	**Delete**
	No data to display.				
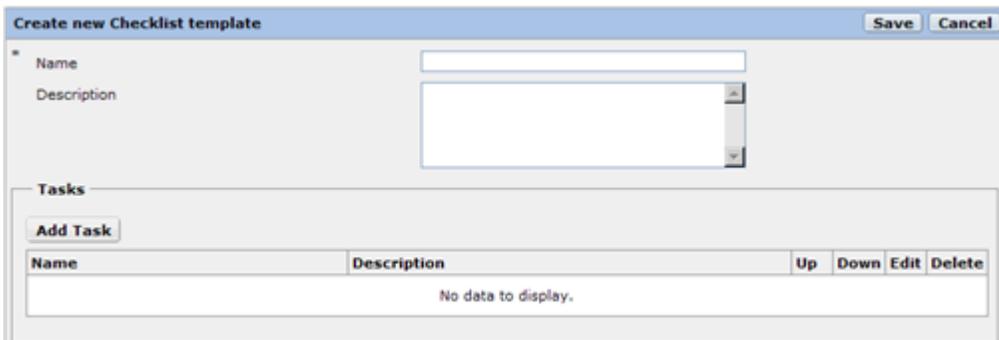
3. Enter a name for the new template.

4. Optionally, enter a description for the template.

5. Click Add Task.

6. In the Create Task dialog box, enter the following fields:

Field	Description
Name	The name of the task.
Action	Action is either a link to a B2B Data Exchange screen (for example, Create Profile) or a reference to a task that needs to be implemented outside of B2B Data Exchange, for example, "Open a user in the Accounting System."
Description	Optional description of the action.

7. Click OK.

8. Continue adding tasks to the on-boarding checklist template. When you have finished, click Save.

9. To make a checklist available for use by the operators, you need to publish it.

   To publish a checklist, in the On-boarding Checklist Template screen, click its Publish icon.

   Note: Editing a published template does not update all the published checklist instances that are based on the this template.

Editing an On-boarding Checklist Template

1. On the Navigator, click Administration > On-boarding Checklists.

2. On the On-boarding Checklist Templates screen, click the Edit icon for the desired template.

   The Edit Checklist Template screen appears:

3. To rearrange the order of the tasks, click the Up and Down icons.

4. To edit a task, click the Edit icon.

   The Create Task screen opens.

5. Edit the data in the Create Task window and click OK.

6. To delete a task, in the Edit Checklist click the Delete icon of the task. Confirm the deletion.

7. Click Save.

   Note: If you edit a published template, there is no need to re-publish it.

Deleting an On-boarding Checklist Template

To delete a template, click Administration > On-boarding Checklists and click the Delete icon for the template that you want to remove. Confirm the action.

CHAPTER 11

System Properties

This chapter includes the following topics:

System Properties Overview

System properties affect the configuration of B2B Data Exchange. You can use system properties to change how B2B Data Exchange operates and how it processes documents. The installer creates and initializes the system properties.

If you installed the Dashboard and Reports component, see "Dashboard and Reports System Properties" on page 128 for a description of the dashboard and reports system properties.

To create topic tables from sources that exist in Enterprise Data Catalog, you must configure Enterprise Data Catalog system properties. Fo more information about Enterprise Data Catalog system properties, see "Enterprise Data Catalog System Properties" on page 70.

Note: If the system property name ends with `.password`, B2B Data Exchange stores the system property value as an encrypted string.

General System Properties

General system properties determine B2B Data Exchange behavior, such as authentication mode and document store location.

The following table describes general system properties:

System Property	Description
dx.audit.trail.generate.view.events	Indicates whether the B2B Data Exchange server generates an audit record when users view any of the following objects: - Calendar - Event - User - User group - Profile - Workflow - Partner Default value is False.
dx.authentication.groups	Names of the Informatica domain security groups to synchronize. If you do not specify a value, the Informatica domain security domain synchronizes only the administrator user account that you define when you install B2B Data Exchange. You can define multiple security groups separated by semicolons. You must enter the authentication group name and domain name in the following format: `<group>@<InformaticaSecurityDomain>[;<group>@<InformaticaSecurityDomain>]*` For example: B2B@Native
dx.authentication.mode	Active authentication mode.
dx.archive.document.store.folder	Location to store the history database. The history database contains archived events and related documents that you archive from the B2B Data Exchange document store with Informatica Data Archive. If you do not enter a value, you cannot view the archived events in the **Archived Events** page of the Operation Console.
dx.console.url	Web address for the operation console. You must include a host name and a port that are accessible from the Advanced Exception Handling module, for example http://localhost:18080/dxconsole. In a high availability configuration, set this property to a logical server name.
dx.endpoint.mft.delta.max.results	Maximum number of transfers that the Managed File Transfer scheduler handles in each run. The scheduler runs every 10 seconds. Default value is 500.

System Property	Description
dx.gui.events.show.with.children	Default behavior for advanced search and for event lists in the Operation Console. Set one of the following values: - True. The Operation Console includes child events in advanced search results and displays child events on the **Event List** by default. - False. The Operation Console includes only root events in advanced search results and displays only root events on the **Event List** page by default. B2B Data Exchange does not create this system property during the installation process. To change the default value of this system property, manually add it and set the value. If you do not add the system property, the default behavior is to include only root events.
dx.system.account.uniqueness	Indicates whether an account is unique within the scope of the partner or within the scope of B2B Data Exchange. You can set the following values: - Partner. The account is unique within the scope of the partner. The B2B Data Exchange server determines the profile based on the application, partner, and account number. - System. The account is unique within the scope of B2B Data Exchange. The B2B Data Exchange server determines the profile based on the application and account number. Default value is System.
dx.system.document.store.folder	Directory to store all documents associated with a document reference. You set up this directory during installation. After installation, do not change this system property in the console. Use the repository utility to change the document store directory and all references to the directory.

Endpoint System Properties

Endpoint system properties determine endpoint settings and default behavior.

The following table describes endpoint system properties:

System Property	Description
dx.endpoint.file.prefix.path	The path to the File Receive and File Send endpoint paths when the Use Endpoint Root Directory checkbox is checked. You must restart the B2B Data Exchange server to apply the change.
dx.endpoint.file.scan.interval	The frequency in seconds of the file endpoint scan interval. Every x seconds, each inbound file endpoint is scanned once. You must restart the B2B Data Exchange server to apply the change.
dx.endpoint.hdfs.file.prefix.path	Path to the root directory of the Hadoop file system (HDFS) to use when an operator selects **Use HDFS root directory**.
dx.endpoint.hdfs.fs.default.name	Connection string for the HDFS server in the following format: `hdfs://<server name>:<port number>`

System Property	Description
dx.endpoint.hdfs.username	Name of the user with directory privileges for the HDFS server. **Note:** You can only store documents in HDFS servers that do not require password authentication.
dx.endpoint.jms.factory.initial	Connection factory to use for the JMS provider.
dx.endpoint.jms.provider.url	JNDI provider URL. This URL must match the jndiProviderURL attribute of the JMS endpoints in the B2B Data Exchange configuration file. You must restart the B2B Data Exchange server to apply the change.
dx.endpoint.mft.inbox.path	Path to the buffer where Managed File Transfer stores incoming files temporarily until B2B Data Exchange reads the files. It is recommended to store the buffer on the same file system as the document store. By default, the Mft-in directory is located in the document store directory. You can choose to set this property to a network path. 1. In the Windows Control Panel, open **Administrative Tools** > **Services**. 2. Right-click the Informatica Managed File Transfer service and click **Properties**. 3. On the Logon tab, configure an account with network access to the paths that you want to set. You must restart the B2B Data Exchange server to apply the change.
dx.endpoint.mft.incorrect.pattern.error.event	Determines whether to create an error event if B2B Data Exchange receives a file through Managed File Transfer that does not match any endpoint file pattern.
dx.endpoint.mft.password	Internal password for Managed File Transfer. Use the password for edit and view only operations. You must restart the B2B Data Exchange server to apply the change. Default value is **dxadmin**.
dx.endpoint.mft.purge.transfers.days	Retention period in days of VLTransfers entries. If you enter 0, purging is disabled. To improve performance when you process a large number of documents, reduce the retention period to 10 days. You must restart the B2B Data Exchange server to apply the change. Default value is 90.
dx.endpoint.show.hidden	Determines whether to display hidden endpoints, such as the Web Service Receive endpoint.
dx.jms.maxwait	Maximum time that an outbound JMS endpoint waits before it reports an error for failed transmissions.
dx.jms.message.dedup.window	Maximum time that B2B Data Exchange tracks delivery for internal messages.
dx.jms.message.ttl	Maximum time that can pass from when B2B Data Exchange creates an internal message to when B2B Data Exchange processes the message.
java.naming.provider.url	JNDI provider URL. This URL must match the jndiProviderURL attribute of the JMS endpoints in the B2B Data Exchange configuration properties file.

Enterprise Data Catalog System Properties

Enterprise Data Catalog system properties define the information to access Enterprise Data Catalog.

The following table describes Enterprise Data Catalog system properties:

System Properties	Description
edc.login.username	User name of the Enterprise Data Catalog resource.
edc.login.password	Password of the user account of the Enterprise Data Catalog resource.
edc.url	The URL of the Enterprise Data Catalog resource.
edc.supported.column.types	Comma separated class types of Enterprise Data Catalog. For example, `com.infa.ldm.etl.pc.OutputTransformationPort`, `com.infa.ldm.relational.Column`
edc.supported.table.types	Comma separated table types of Enterprise Data Catalog. For example, `com.infa.ldm.relational.Table`

Event Monitor System Properties

Event monitor system properties determine the structure and the content of event monitor emails.

The following table describes event monitor system properties:

System Property	Description
dx.monitor.max.notifications	The maximum number of notifications that is allowed to be sent from a specific monitor. If the maximum number of notifications is exceeded, the monitor switches to batch mode delivery. The default for the maximum value is 100.
dx_email_bcc_field	List of recipient email addresses separated by semicolons.
dx_email_body_field	Character string that replaces the body text of the built-in email. Maximum length is 255 characters.
dx_email_body_file	Path to a template file that contains a custom body of the email. .
dx_email_cc_field	List of recipient email addresses separated by semicolons.
dx_email_from_field	String that replaces the From field of the email.
dx_email_mimetype	MIME type of attachments to the email message. Default is "text/html"; charset=UTF-8.
dx_email_subject_field	Subject field of the email.
dx_email_to_field	List of recipient email addresses separated by semicolons.

System Property	Description
dx.mft.console.url	URL of the MFT console.
dx.smtp.login	Login name of the B2B Data Exchange SMTP server administrator account.
dx.smtp.password	Password of the B2B Data Exchange SMTP server administrator account.
dx.smtp.port	Port number of the B2B Data Exchange SMTP server.
dx.smtp.server	URL of the B2B Data Exchange SMTP server.
dx.smtp.ssl	Determines whether the B2B Data Exchange SMTP server communicates through SSL or not. - False: The B2B Data Exchange SMTP server does not communicate through SSL. - True: The B2B Data Exchange SMTP server communicates through SSL. By default: False.
dx.smtp.client.secret	Include the Client Secret if the application is a confidential client.
dx.smtp.clientId	The ID assigned to Managed File Transfer (client). This property is used as part of the topic's subscription ID.
dx.smtp.use.o365	To connect to the Office365 SMTP server.

Informatica Intelligent Cloud Services Properties

Data Integration system properties define the connection settings for Informatica Intelligent Cloud Services (Cloud Data Integration).

The following table describes Cloud Data Integration system properties:

System Property	Description
dx.iics.max.poll.time.minutes	Maximum polling time to update the event status. If no event status update is received within this time, the event will timeout.
dx.iics.object.prefix	When B2B Data Exchange creates a Cloud Data Integration object, such as a task or connection, the name of the object is prefixed by this parameter.
dx.iics.runtime.environment	Environment name of the Cloud Data Integration secure agent.
dx.iics.url	URL for Data Integration.
dx.iics.username	Name of the user with read, update, execute, and delete privileges for Cloud Data Integration mass ingestion tasks.
dx.iics.password	Password for the user with access privileges to Cloud Data Integration.

After you change the system properties, restart B2B Data Exchange.

Informatica Managed File Transfer Properties

Informatica Managed File Transfer system properties determine Informatica Managed File Transfer access, download location, and project execution timeout.

The following table describes general system properties:

System Property	Description
infamft.api.username	Name of a user from a user account with privileges to run Informatica Managed File Transfer projects. The credential is used to execute Informatica Managed File Transfer projects.
infamft.api.password	Password of the user defined for the **infamft.api.username** property. The credential is used to execute Informatica Managed File Transfer projects.
infamft.console.url	URL address for Informatica Managed File Transfer.
infamft.download.location	Specifies a temporary local directory to which Informatica Managed File Transfer downloads files.
infamft.project.execution.timeout	Determines the timeout period for an Informatica Managed File Transfer endpoint to complete a project run. If the endpoint project does not complete the run within this time period, B2B Data Exchange generates an error.
infamft.webuser.unassociated.error.event	Determines whether or not to create an error event when B2B Data Exchange receives a file from an MFT Web User that is not associated with any endpoint in B2B Data Exchange.

Partners Portal System Properties and Variables

After you install the Partners Portal, use the Partners Portal system properties to define the Partners Portal and Portal user invitation email.

The following table describes the Partners Portal system properties:

System Property	Description
dx.portal.block.upload.file.extensions	List of file types that cannot be uploaded to Partners Portal, separated by commas.
dx.portal.email.bcc.field	List of recipient email addresses separated by semicolons.
dx.portal.email.body.field	Character string that replaces the body text of the built-in email. Maximum length is 255 characters.

System Property	Description
dx.portal.email.body.file	Path to the file containing the custom body of the email.
dx.portal.email.cc.field	List of recipient email addresses separated by semicolons.
dx.portal.email.from.field	String that replaces the From field of the email.
dx.portal.email.mimetype	MIME type of attachments to the email message. Default is `text/html; charset=utf-8`
dx.portal.email.subject.field	Subject field of the email.
dx.portal.endpoint.mask	List of endpoints types that are masked from portal user, separated by commas.
dx.portal.event.hierarchy.limit	Maximum number of events to display when you view the hierarchy of child events related to an event.
dx.portal.event.limit	Maximum number of events to display in the Monitoring Event tab of the Partners Portal.
dx.portal.profile.parameters.tab	Specifies the name of the tab where you select the workflow parameters that the Partners Portal displays for message profiles. The default setting is `portal parameters`.
dx.portal.upload.size.limit.mb	Maximum file size, in MB, that can be uploaded to the Partners Portal.
dx.portal.url	Web address for the Partners Portal. The property has a default value of http://localhost:18080/dx-portal. If you select a different port or host during installation, you must correct this address manually. In a high availability configuration, set this property to a logical server name.

The following table describes the variables that you use to create a template for the body of the Portal user invitation email:

System Property	Description
$dx_portal_change_password_link	URL to the Partners Portal page to change the user password.
$dx_portal_link	URL to login to the Partners Portal page, based on the system property dx.portal.url.
$dx_portal_user_id	User ID of the Portal user.
$dx_portal_full_user_name	Full name of the Portal user.

For example, the email template contains the following statement with the $dx_portal_user_id variable:

```
User name: $dx_portal_user_id
```

The User ID is defined as `TRice@contact.com`.

When the Portal user is invited to use the Partners Portal, the email sent to the Portal user contains the following statement:

```
User name: TRice@contact.com
```

PowerCenter System Properties

PowerCenter system properties determine PowerCenter domain and connection management.

The following table describes PowerCenter system properties:

System Property	Description
pwc.domain.gateway	Name of the Informatica security domain gateway. The value of this property appears in the following format: `host_1:port_1(;host_2:port_2)`
pwc.domain.name	Name of the domain where PowerCenter is installed.
pwc.integration.service.name	Name of the PowerCenter Integration Service to run batch workflows.
pwc.repository.jdbc.url	JDBC connection URL for the PowerCenter repository database. Applicable for PowerCenter repositories that are hosted on Oracle or Microsoft SQL Server databases.
pwc.repository.jdbc.name	Database name of the PowerCenter repository database. Applicable for PowerCenter repositories that are hosted on Oracle or Microsoft SQL Server databases.
pwc.repository.jdbc.password	Password for the PowerCenter repository database. Applicable for PowerCenter repositories that are hosted on Oracle or Microsoft SQL Server databases.
pwc.repository.password	Password for the PowerCenter Repository Service. **Note:** You must restart the B2B Data Exchange Operation Console after you change the password for the PowerCenter Repository Service.
pwc.repository.service.name	Name of the PowerCenter Repository Service.
pwc.repository.user.name	Name of the PowerCenter Repository Service user.
pwc.retry.interval.sec	Time interval in seconds that the B2B Data Exchange server waits to retry running a workflow in an error state.
pwc.retry.max.count	Maximum number of times that the B2B Data Exchange server retries running a workflow if a failure occurs.

System Property	Description
pwc.user.name.space	Name of the security domain that stores the PowerCenter repository user. If you use Informatica domain authentication, change the default to grant access to the PowerCenter repository. Default value is Native.

pwc.webservices.url	URL or Web address of the PowerCenter Web Services Hub.
	
	The WebServices hub cannot persist the sessionID values across multiple hubs. This is a current limitation with the hub (from platform). Any Pending DX events must be re-submitted in the event of a load balancer or hub failure.
	
	The request from the Data Exchange at any point of time must be routed to one Web service Hub.
	
	For example:
	
	`http://localhost:7333/wsh/services/BatchServices/`
	`DataIntegration`
	
	Note: If a node that makes the batch service calls fails, update the property to the URL of another node manually. Batch service calls do not function if you link to the load-balancer URL.

Advanced Exception Handling System Properties

General system properties determine triggers for advanced exception handling.

The following table describes advanced exception handling system properties:

System Property	Description
issue.tracking.assignee	Default assignee for exception handling issues.
issue.tracking.event.issue.type	Default issue type used for all issues based on non-reconciliation monitors.
issue.tracking.factory.class	Factory class for the issue tracking system.
issue.tracking.project.key	Default project name used for tracking exception handling issues.
issue.tracking.reconciliation.issue.type	Default issue type for all issues based on reconciliation monitors.
issue.tracking.reporter	Default Advanced Exception Handling module reporter value.
issue.tracking.transition.reopen	Advanced Exception Handling module reopen transition name.
issue.tracking.url	Base URL for the Advanced Exception Handling module, for example http://localhost:8080
issue.tracking.user, issue.tracking.password	Login credentials to connect to the Advanced Exception Handling module.

Custom system properties with a name in the format issue.tracking.XYZ.field are added to the issue attributes of an exception handling issue when it is created.

Managing System Properties

Use the Navigator to create, edit, and delete system properties. If the system property name ends with `.password`, B2B Data Exchange stores the password as an encrypted string and displays asterisks in the **Value** column.

1. In the Navigator, click **Administration** > **System Properties**.

   The **System Properties** page appears.

2. Choose to create, edit, or delete a system property.

   - To create a system property, click **New Property** and enter the name and default value for the property.

   - To edit a system property, click the **Edit** icon next to the system property that you want to edit and change the property name or default value.

   - To delete a system property, click the **Delete** icon next to the system property that you want to delete and confirm the deletion.

CHAPTER 12

Repository Management

This chapter includes the following topics:

Repository Management Overview

The B2B Data Exchange repository contains information about objects and events. The operational data store stores aggregated data about publication events and subscription events.

You can use the import and export command line utility to export repository objects to an XML file or import the objects from the XML file to another repository. When you export objects, you create an export specification file to define the objects to export from B2B Data Exchange. When you import objects, you create an import specification file to specify the objects to import and the conflict resolution for duplicate objects.

You can use the repository command line utility to perform maintenance actions on the B2B Data Exchange repository.

Import and Export Utility

Use the import and export utility to export objects from the B2B Data Exchange repository to an XML file and import the objects from the XML file back to the B2B Data Exchange repository.

For example:

- Export objects from a test environment and then import them to the production environment.
- Export object metadata for temporary backup.

To run the import and export utility, you must have the following permissions and privileges:

- Read and write permissions for all objects.
- Export privileges to run the export process and import privileges to run the import process.

If you do not have the required permissions and privileges, B2B Data Exchange aborts the import or the export process.

You can export and import all objects or choose the export/import objects in a specification XML file. The utility exports or imports objects based on the information in the specification file. If you export objects with dependent objects, the export process exports the dependent objects to the export XML file.

If you import objects for which you defined event or reconciliation monitors, the monitors run immediately after you import the objects unless you disabled the monitors before you exported the objects. Scheduled objects are imported in a disabled state and you must enable the objects before they can run. For example, if you import a scheduled profile you need to enable the profile before it can run according to the schedule.

You can find the import and export utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

The directory also contains the export-all and import-all batch scripts. Use the scripts to export or import all objects. If you use the scripts, you do not need to create a specification file.

You can find sample specification files in the following directory:

```
<DXInstallationDir>\dx-tools\samples
```

Export-All and Import-All Batch Scripts

Use the export-all and import-all batch scripts to export and import all objects in the B2B Data Exchange repository. You do not need a specification file to export or import all objects.

You can find the batch scripts in the following directory:

```
<DXInstallationDir>\dx-tools\
```

The following list describes the batch scripts.

export-all

Exports all objects from the B2B Data Exchange repository to an export XML file. The script sets the import specification file to:

```
samples/export-all-specification-sample.xml
```

import-all

Imports all objects from the export XML file into the B2B Data Exchange repository. The script sets the import specification file to:

```
samples/import-all-specification-sample.xml
```

The following list describes parameters and arguments for the export-all and import-all batch scripts.

-f or --file

Argument: ImportFile or ExportFile

Required. Absolute path and file name of the object import file or export file. If you run the import command, this is the file from which to import objects. If you run the export command, this is the file to which to export objects.

-u or --user

Argument: UserID

Optional. Identifier of the B2B Data Exchange user account to use when the import and export utility accesses the B2B Data Exchange repository.

The user account must have the following privileges:

- Data Access permissions to all the data in the repository. The user must be a member of a user group for which the permission option **Grant read and write permissions to all categories** is selected.
- Export Data. Required when you export objects.
- Import Data. Required when you import objects.

If you use Informatica domain authentication or Informatica domain with Kerberos authentication, enter the full user ID in the following format:

```
user@domain
```

-U

Argument: Environment variable.

Optional. Environment variable that contains a user name.

User name of an Operation Console user account with Manage Data privileges to run the import or export command. To run the import command, the user account must have the Import Data privilege. To run the export command, the user account must have the Export Data privilege.

If you use Informatica domain authentication or Informatica domain with Kerberos authentication, the user name must specify the Informatica security domain, separated by the @ symbol. For example:

```
Administrator@SecurityDomain
```

Note: You must specify at least one of the user name options, -u or -U.

-p or --password

Argument: password.

Optional. Password of the B2B Data Exchange user account to use when the import and export utility accesses the B2B Data Exchange repository.

-P

Argument: Environment variable.

Optional. Environment variable that contains a password.

Password for the Operation Console user that runs the import or the export command. The password must be encrypted. Use dxencrypt for the encrypted value.

Note: You must specify at least one of the password options, -p or -P.

--server

Argument: "hostname:port"

Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the import and export utility connects to the localhost server with the default port 18095. You must enclose the argument in quotation marks. For example:

```
--server "localhost:18095"
```

--test

Optional. Runs the import or export command and generates a report with a list of objects to export or import without exporting or importing the objects. Use this parameter to test the import or export specification file.

The import and export utility creates the report in the same directory as the specification file. The name of the report file is the same as the name of the specification file with a log suffix in the following format:

```
<SpecFileName>.log.xml
```

Repository Objects to Export and Import

You can export or import all objects or specify the export/import object types. When you export or import objects with dependent objects, the import and export utility exports the metadata for the dependent objects. When you create the export or the import specification file, you specify the object type to export or import.

The utility does not export or import event attachments.

The following table describes the parent and dependent object types that you can export and import:

Object	Type	Dependent Objects
Account	account	Profiles, workflows, applications, monitors, endpoints, account attributes and account values, event attributes, categories
Application	application	None
Endpoint	endpoint	Schedules
Event Attribute	eventattribute	None
Event Status	eventstatus	None
Event Type	eventtype	None
Holiday Calendar Section	calendarsection	None
Monitor	monitor	Workflow, profile, partner, holiday calendar section, user names, user group names, event type, event status, categories
Partner	partner	Accounts, profiles, workflows, applications, monitors, holiday calendar sections, endpoints, partner attributes and values, event attributes, categories
Profile	profile	Workflow, partner, account, applications, event attributes, categories, workflow parameters and values
Schedule	schedule	None
User	user	User group names
Workflow	workflow	Event attributes, application

Export Specification File

The export specification file contains instructions on which objects to export from the B2B Data Exchange repository. You use the sample specification file structure to create the import specification file.

When the import and export utility exports an object, it exports all the dependent objects to retain the validity of the exported objects. For example, if you export a workflow, the import and export utility exports

associated event attributes.For example, when you export an application, the utility exports associated publications and subscriptions.

Note: When you export an event monitor, the import and export utility does not export the user accounts configured to receive notification from the monitor.

You can use the (ALL) token to export all object of the same type from the repository. You enter the token instead of the object name.

The following example shows the contents of the export specification file:

```
<!-- The order of the object selections does not matter (can be in any order)-->
<ExportSpecification>
    <!-- The minumum number of elements is one -->
    <!-- Export MyOwnEventType -->
    <ObjectSelection type="eventtype">
       <Name>MyOwnEventType</Name>
    </ObjectSelection>

    <!-- Export super event status-->
    <ObjectSelection type="eventstatus">
       <Name>SuperEventStatus</Name>
    </ObjectSelection>

    <!-- Export all the event types -->
    <ObjectSelection type="eventtype">
       <Name>(ALL)</Name>
    </ObjectSelection>

    <!-- Export the flow template, that automatically includes the preprocessing
    templates, applications, and event property keys ? -->
    <ObjectSelection type="flowtemplate">
       <Name>SomeFlowTemplate</Name>
    </ObjectSelection>

    <!-- Export a profile with all its dependencies -->
    <ObjectSelection type="profile">
       <Name>Profile_X</Name>
    </ObjectSelection>

    <!-- Export a delayed processing rule -->
    <ObjectSelection type="delayedprocessingrule">
       <Name>DefaultProcessingRule</Name>
    </ObjectSelection>

    <!-- Export a partner and all its dependencies and related objects
    (such as profiles and delayed processing rules) -->
    <ObjectSelection type="partner">
       <Name>IceSave</Name>
    </ObjectSelection>

    <!-- Export of an account, including its depedendencis and related objects -->
    <ObjectSelection type="account">
    <!-- The partner tag is required, as otherwise we cannot be certain to
    select the correct account -->
       <Partner>IceSave</Partner>
       <!-- the name tag now acts as a selector for the account number -->
       <Name>123456789.123456789</Name>
    </ObjectSelection>
</ExportSpecification>
```

You must use valid XML names in the export specification file. The following table describes the special characters that you must encode:

Special Character	Encoded Character
<	&lt
>	&gt
&	&amp

Import Specification File

The import specification file contains instructions on which objects to import into the B2B Data Exchange repository. You use the sample specification file structure to create the import specification file.

The import specification file defines how to resolve conflicts when an object that you want to import exists in the B2B Data Exchange. The import and export utility determines whether an object exists in the B2B Data Exchange based on the object name.

The following table describes the conflict resolution types you can set:

Conflict Resolution Type	Description
cancel	Cancels the import process. No objects are imported.
overwrite	Overwrites the object in the B2B Data Exchange repository with the object from the export file. If you choose to overwrite existing objects, the utility performs partial validation during the import process. For example, the utility does not verify whether the user objects have associated categories. Information about missing objects appears in the import log file. If you choose to overwrite objects that do not exist, the utility creates the objects.
reuse	Retains the object in the B2B Data Exchange repository if the object name matches the object in the export XML file, and does not import of the object from the export file.
skip	Skips the object in the export XML file and does not check whether the object exists in the B2B Data Exchange repository.
default	Applies the conflict resolution that you set at the parent level of the specification file. For example, if you set the object type resolution to **reuse**, you can create an element for a specific object name and set the resolution type to **default**. The import and export utility applies the object type resolution to the specific object.

Conflict resolution types are case sensitive.

You can specify the conflict resolution for all objects, for a type of object, or for a specific object. The following elements define the scope of the resolution that you can perform:

- DefaultResolution. Applies the conflict resolution you set to all objects to import. You can define set the default resolution to any type except for default.

- ObjectTypeResolutions. Applies the conflict resolution you set to objects of the same type. Use the type attribute to specify the object types.

- ObjectResolution. Applies the conflict resolution you set to specific object names. Use the name element to specify the object names.

The following example shows the contents of an import specification file that defines the conflict resolution for objects and object types:

```
<!-- The import specification requires a particular order of the elements -->
<ImportSpecification>
    <!-- Default resolution in case a particular object has not been specified. -->
    <!-- Specifying 'default' here is an error -->
    <!-- This element is required -->
    <DefaultResolution>cancel</DefaultResolution>

    <!-- Definitions of the resolutions per object type.
    If none are specified then the empty element tag has to be supplied
    -->
    <!-- This element is required, but does not need to contain child elements -->
    <ObjectTypeResolutions>
        <!-- multiple entries are allowed. Be aware that multiple entries
        for the same type can result in unpredictable behaviour -->
        <ObjectTypeResolution type="flowtemplate">overwrite</ObjectTypeResolution>

        <!--The value 'default' revers to the default resolution as defined above -->
        <ObjectTypeResolution type="account">default</ObjectTypeResolution>
    </ObjectTypeResolutions>

    <!-- A specific object resulotion for a profile -->
    <ObjectResolution type="profile">
        <Resolution>reuse</Resolution>
        <Name>ProfileName</Name>
    </ObjectResolution>

    <!-- A specific object resulotion for a flow template. In this case the default
    resolution of the object type flow template is used. -->
    <ObjectResolution type="flowtemplate">
        <Resolution>default</Resolution>
        <Name>workflowName</Name>
    </ObjectResolution>

    <!-- A specific object resulotion for an account. In this case the default
    resolution of the object type account is used. -->
    <ObjectResolution type="account">
        <Resolution>default</Resolution>
        <Partner>PartnerName</Partner>
        <Name>AccountNumber</Name>
    </ObjectResolution>
```

You must use valid XML names in the export specification file. The following table describes the special characters that you must encode:

Special Character	Encoded Character
<	&lt
>	&gt
&	&amp

Import and Export Utility Command Syntax

Use the import and export utility command syntax to define the scope, location, and permissions for the import or export process and for the management of private keys that are used for authentication in SSH FTP connections.

The import and export utility uses the following syntax:

```
importexport
<-c|--command> command
<-f|--file> exportfile
<-s|--specification> specfile
<-u|--user> userID
<-p|--password> user password
[--server "hostname:port"]
[--test]
```

For example:

```
importexport import -f "C:\Users\Administrator\DX_backup\exported_entities.xml" -s C:/dx-
tools/samples/import-all-specification-sample.xml -u Administrator -p Administrator
```

The following list describes parameters and arguments for the import and export utility commands.

-c or --command

Argument: command

The command to run. Specify one of the following commands:

- export. Exports specific objects from the B2B Data Exchange repository based on the export specification file you create. The utility saves the exported objects in an XML file that you can import back into the B2B Data Exchange repository.

- import. Imports specific objects from the export XML file into the B2B Data Exchange repository based on the import specification file you create.

-f or --file

Argument: ImportFile or ExportFile

Required. Absolute path and file name of the object import file or export file. If you run the import command, this is the file from which to import objects. If you run the export command, this is the file to which to export objects.

-s or --specification

Argument: SpecFile

Required. Absolute path and file name of the import or export specification file.

-u or --user

Argument: UserID

Optional. Identifier of the B2B Data Exchange user account to use when the import and export utility accesses the B2B Data Exchange repository.

The user account must have the following privileges:

- Data Access permissions to all the data in the repository. The user must be a member of a user group for which the permission option **Grant read and write permissions to all categories** is selected.

- Export Data. Required when you export objects.

- Import Data. Required when you import objects.

If you use Informatica domain authentication or Informatica domain with Kerberos authentication, enter the full user ID in the following format:

```
user@domain
```

-U

Argument: Environment variable.

Optional. Environment variable that contains a user name.

User name of an Operation Console user account with Manage Data privileges to run the import or export command. To run the import command, the user account must have the Import Data privilege. To run the export command, the user account must have the Export Data privilege.

If you use Informatica domain authentication or Informatica domain with Kerberos authentication, the user name must specify the Informatica security domain, separated by the @ symbol. For example:

```
Administrator@SecurityDomain
```

Note: You must specify at least one of the user name options, -u or -U.

-p or --password

Argument: password.

Optional. Password of the B2B Data Exchange user account to use when the import and export utility accesses the B2B Data Exchange repository.

-P

Argument: Environment variable.

Optional. Environment variable that contains a password.

Password for the Operation Console user that runs the import or the export command. The password must be encrypted. Use `dxencrypt` for the encrypted value.

Note: You must specify at least one of the password options, -p or -P.

--server

Argument: "hostname:port"

Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the import and export utility connects to the localhost server with the default port 18095. You must enclose the argument in quotation marks. For example:

```
--server "localhost:18095"
```

--test

Optional. Runs the import or export command and generates a report with a list of objects to export or import without exporting or importing the objects. Use this parameter to test the import or export specification file.

The import and export utility creates the report in the same directory as the specification file. The name of the report file is the same as the name of the specification file with a log suffix in the following format:

```
<SpecFileName>.log.xml
```

Exporting Objects from the B2B Data Exchange Repository

Use the import and export utility to export specific objects from the B2B Data Exchange repository to an export XML file. You create an export specification file and specify the object types or names to export.

Note: You can also use the export-all batch script to export all objects. You do not need to create a specification file to export all objects.

1. Create the export specification XML file based on the sample specification file and set the conflict resolutions.

   You can edit the file in a text editor.

2. Save the export specification XML file in a shared directory accessible to the B2B Data Exchange server.

3. From the command line, run the **export** command of the import and export utility with the required parameters.

   The utility creates the following files:

   - Object XML file. Contains the metadata of the exported objects. This file also contains the metadata of dependent objects.

   - Log XML file. Contains the export process steps and information about missing objects.

Do not edit the object XML file. If you change, add, or remove content from the file, the import and export utility might not import the objects correctly.

Importing Objects into the B2B Data Exchange Repository

Use the import and export utility to import specific objects into the B2B Data Exchange repository from the export XML file. You create an import specification file and set the conflict resolution to perform if an object from the export XML file already exists in the B2B Data Exchange repository.

Note: You can also use the import-all batch script to import all objects. You do not need to create a specification file to import all objects.

1. Verify that the export XML file is stored in a shared directory accessible by the B2B Data Exchange server.

2. Create the import specification XML file based on the sample specification file and set the conflict resolutions.

   You can edit the file in a text editor.

3. Save the import specification XML file in a shared directory accessible to the B2B Data Exchange server.

4. From the command line, run the import command of the import and export utility with the required parameters.

   The utility creates an import log file that contains the import process steps and information about missing objects.

Import and Export Endpoints Rules and Guidelines

Consider the following rules and guidelines when you import and export endpoints:

- B2B Data Exchange creates system workflows to store Managed File Transfer endpoint parameter values.

  Note: Do not skip the import of system-generated workflows when importing Managed File Transfer endpoints.

- Non-Managed File Transfer endpoints are imported as-is, depending upon each endpoint status.

- After you import JMS endpoints from version 9.1 or earlier, you must re-enter the password for each endpoint to enable B2B Data Exchange to securely connect to the JMS queue.

List Objects Utility

Use the list objects utility to list objects such as endpoints, profiles, and schedules. To run the list objects utility, you must have view privilege. If you do not have the required permissions and privileges, B2B Data Exchange aborts this process.

You can find the listObjects utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

List Objects Batch Script

Use the listObjects batch script to get the list of all objects, such as endpoints, profiles, and schedules in the B2B Data Exchange repository. You do not need a specification file to list all objects.

The following is an example of a sample batch script to list the endpoints object:

```
listObjects.bat -u <username> -p <password> -t endpoints -f /data/endpoints.xml
```

The following list describes parameters and arguments for the listObjects batch script.

-t or --type

Argument: objectType

Required. List the object type. Specify one of the following commands:

- Endpoints. Lists the name, type, status, partner name, account name, and schedules associated with the endpoints in the specified file
- Profiles. Lists the name, status, partner name, account name, and schedules associated with the profiles in the specified file.
- Schedules. Lists the name, status, and cron expression associated with the schedules in the specified file.

-f or --file

Argument: objectType

Required. The file path where the objects are saved.

-u or --user

Argument: UserID

Optional. Identifier of the Operation Console user account with the List {objects} privileges, where {objects} are endpoints, profiles, or schedules.

-U

Argument: Environment variable

Optional. Environment variable that contains the UserID value.

UserID of an Operation Console user account with List {objects} privileges where {objects} are endpoints, profiles, or schedules.

If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol.

For example:

```
Administrator@SecurityDomain
```

You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.

-p or --password

Argument: password

Optional. Password of the Operation Console user that executes the listObjects command. This option contains the clear text password.

You must specify at least one of the password options, -p or -P to determine the UserID required to execute this command.

-P

Argument: Environment variable

Optional. Environment variable that contains the password value.

Password for the Operation Console user that executes the listObjects command. The password must be encrypted.

You must specify at least one of the password options, -p or -P to determine the user's password required to execute this command.

--server

Argument: "hostname:port"

Optional. Environment variable that contains the password value.

Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the utility connects to the localhost server with the default port 18095. The argument must be enclosed in quotation marks.

For example:

```
listObjects.bat --server "localhost:18095"
```

Similarly, the following is an example of a sample batch script to list profiles and schedules:

```
listObjects.bat -u <username> -p <password> -t profiles -f /data/profiles.xml
listObjects.bat -u <username> -p <password> -t schedules -f /data/schedules.xml
```

Enable and Disable Objects Utility

Use the enable and disable utility to enable or disable objects such as endpoints, profiles, and schedules in the B2B Data Exchange repository.

To run the enable and disable objects utility, you must have the following privileges:

- Edit Endpoint privilege to enable or disable endpoints.
- Edit Profile privilege to enable or disable profiles.

- Edit Schedule privilege to enable or disable schedules.

If you do not have the required permissions and privileges, B2B Data Exchange aborts the enable or the disable process.

You can find the enable and disable utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

Enable and Disable Utility Command Syntax

Use the enable and disable objects utility command syntax to enable or disable endpoints, profiles, and schedules, in the B2B Data Exchange repository. You do not need a specification file to enable or disable all objects.

You can find the batch scripts in the following directory:

```
<DXInstallationDir>\dx-tools\
```

The enable and disable utility uses the following syntax:

```
enabledisableobjects
<-c, --command <command>
<-t, --type <type>
<-f, --file <ListObjectFile>
<-u, --user <userID>
<-U, <Environment variable>
<-p, --password <user password>
<-P, <Environment variable>
<--server, --server <"hostname:port">
```

The following is an example of a sample batch script to enable the endpoints:

```
enabledisableobjects.bat -u <username> -p <password> -c enable -t endpoints -f /data/
endpoints.xml
```

The following list describes parameters and arguments for the enable and disable utility commands.

-c or --command

Argument: command

Required. The command to run. Specify one of the following commands:

- enable. Enables the specified object from the object list file in the B2B Data Exchange repository.
- disable. Disables the specified objects from the object list file in the B2B Data Exchange repository.

-t or --type

Argument: type

Required. The object type to enable or disable. Specify one of the following commands:

- endpoints. Enables or disables the endpoint list..
- profiles. Enables or disables the profile list.
- schedules. Enables or disables the schedule list.

-f or --file

Argument: ListObjectFile

Required. The file path where the list of objects are saved.

-u or --user

Argument: UserID

Optional. User ID of an Operation Console user account with the Manage Data privileges to perform the enable or disable command. The user account must have the Edit Data privilege to run this command. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol.

For example:

```
Administrator@SecurityDomain
```

You must specify at least one of the user name options, -u or -U, to determine the UserID required to execute this command.

-U

Argument: Environment variable

Optional. Environment variable that contains the UserID value.

UserID of an Operation Console user account with Manage Data privileges to perform the enable or disable command. The user account must have the Edit Data privilege to run this command. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol.

For example:

```
Administrator@SecurityDomain
```

You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.

-p or --password

Argument: password

Optional. Password of the Operation Console user that executes the enable or disable command. This option contains the clear text password.

You must specify at least one of the password options, -p or -P to determine the UserID required to execute this command.

-P

Argument: Environment variable

Optional. Environment variable that contains the password value.

Password for the Operation Console user that executes the listObjects command. The password must be encrypted.

You must specify at least one of the password options, -p or -P to determine the user's password required to execute this command.

--server

Argument: "hostname:port"

Optional. Environment variable that contains the password value.

Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the utility connects to the localhost server with the default port 18095. The argument must be enclosed in quotation marks.

For example:

```
enabledisableobjects.bat --server "localhost:18095"
```

Similarly, the following is an example of a sample batch script to enable profiles and schedules:

```
enabledisableobjects.bat -u <username> -p <password> -c enable -t profiles -f /data/
profiles.xml
```

```
enabledisableobjects.bat -u <username> -p <password> -c enable -t schedules -f /data/
schedules.xml
```

You can use the following XML sample files to enable profiles, schedules, and endpoints:

profiles.xml

You can use the following XML sample file to enable profiles:

```
<profiles>
          <profile>
             <name>Profile1</name>
             <status>disabled</status>
             <account>Account1</account>
             <partner>DefaultPartner</partner>
          </profile>
          <profile>
             <name>Profile2</name>
             <status>disabled</status>
             <account>Account1</account>
             <partner>DefaultPartner</partner>
          </profile>
       </profiles>
```

schedules.xml

You can use the following XML sample file to enable schedules:

```
<schedules>
           <schedule>
             <name>RunEveryOneMin</name>
             <cronExpression>0 0/1 * * * ?</cronExpression>
             <status>enabled</status>
           </schedule>
           <schedule>
             <name>scheduleForTesting2</name>
             <cronExpression>0 0/5 * * * ?</cronExpression>
             <status>enabled</status>
           </schedule>
           <schedule>
             <name>scheduleForTesting3</name>
             <cronExpression>0 0/10 * * * ?</cronExpression>
             <status>enabled</status>
           </schedule>
       </schedules>
```

Where 0 0/1 * * * ?, 0 0/5 * * * ?, and 0 0/10 * * * ? refers to the schedule running every minute, every 5 minutes, and every 10 minutes respectively.

endpoints.xml

You can use the following XML sample file to enable endpoints:

```
<endpoints>
           <endpoint>
             <name>TestHostedReceiveEP</name>
             <status>enabled</status>
             <account>Account_HostedEP</account>
             <partner>DefaultPartner</partner>
             <type>InfaMftEndpoint</type>
             <direction>Receive</direction>
           </endpoint>
           <endpoint>
             <name>TestHostedSendEP</name>
             <status>enabled</status>
             <account>Account_HostedEP</account>
             <partner>DefaultPartner</partner>
```

```
                                      <type>InfaMftEndpoint</type>
                                      <direction>Send</direction>
                              </endpoint>
                              <endpoint>
                                      <name>TestRemoteReceiveEP</name>
                                      <status>enabled</status>
                                      <account>AccountWithDefaultEP</account>
                                      <partner>DefaultPartner</partner>
                                      <type>InfaMftEndpoint</type>
                                      <direction>Receive</direction>
                              </endpoint>
                              <endpoint>
                                      <name>TestRemoteSendEP</name>
                                      <status>enabled</status>
                                      <account>AccountWithDefaultEP</account>
                                      <partner>DefaultPartner</partner>
                                      <type>InfaMftEndpoint</type>
                                      <direction>Send</direction>
                              </endpoint>
                      </endpoints>
```

For more information about listObjects batch script, see .

Enable and Disable Schedules Utility

Use the enable and disable schedules utility to enable or disable all schedules in the B2B Data Exchange repository. To run the enable and disable schedules utility, you must have the edit schedule privilege. If you do not have the required permissions and privileges, B2B Data Exchange aborts the enable or the disable schedule process.

You can find the enable and disable schedules utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

Enable and Disable Schedules Command Syntax

Use the enable and disable schedules utility command syntax to enable all schedules, in the B2B Data Exchange repository. You do not need a specification file to enable or disable all objects.

You can find the batch scripts in the following directory:

```
<DXInstallationDir>\dx-tools\
```

The enable and disable schedules utility uses the following syntax:

```
enabledisableschedules
<-f, <enable/disable>
<-u, --user <userID>
<-U, <Environment variable>
<-p, --password <password>
<-P, <Environment variable>
<--server, --server <"hostname:port">
```

The following is an example of a sample batch script to enable the endpoints:

```
enabledisableschedules.bat -u <username> -p <password> -f enable
```

The following list describes parameters and arguments for the enable and disable schedules utility commands.

-f

Argument: enable/disable

Required. The command to run. Specify one of the following commands:

- enable. Enables the schedules from the list file in the B2B Data Exchange repository.
- disable. Disables the schedules from the list file in the B2B Data Exchange repository.

-u or --user

Argument: UserID

Optional. User ID of an Operation Console user account with the Edit Schedule privilege to perform the enable or disable all command. The user account must have the Edit Data privilege to run this command. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol.

For example:

```
Administrator@SecurityDomain
```

You must specify at least one of the user name options, -u or -U, to determine the UserID required to execute this command.

-U

Argument: Environment variable

Optional. Environment variable that contains the UserID value.

UserID of an Operation Console user account with Edit Schedule privileges to perform the enable or disable all command. The user account must have the Edit Data privilege to run this command. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol.

For example:

```
Administrator@SecurityDomain
```

You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.

-p or --password

Argument: password

Optional. Password of the Operation Console user that executes the enable or disable all command. This option contains the clear text password.

You must specify at least one of the password options, -p or -P to determine the UserID required to execute this command.

-P

Argument: Environment variable

Optional. Environment variable that contains the password value.

Password for the Operation Console user that executes the enable or disable all command. The password must be encrypted.

You must specify at least one of the password options, -p or -P to determine the user's password required to execute this command.

--server

Argument: "hostname:port"

Optional. Environment variable that contains the password value.

Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the utility connects to the localhost server with the default port 18095. The argument must be enclosed in quotation marks.

For example:

```
archive --server "localhost:18095"
```

B2B Data Exchange Repository Utility

Use the B2B Data Exchange repository utility to create, upgrade, and maintain the B2B Data Exchange repository and the operational data store.

For example, you can use the repository utility to create the repository if you did not create the repository during installation. You also use the repository utility to change the document store directory or the user authentication mode.

The repository utility is a command-line utility. You can find the utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

Note: Before you run the repository utility you must stop the B2B Data Exchange Operation Console service and the B2B Data Exchange server service. After you run the repository, restart the services.

Repository Utility Command Syntax

Use the repository utility syntax to define the actions that you want to perform on the B2B Data Exchange repository.

The repository utility uses the following syntax:

```
repoutil
<-c|--command> command
<-t|contentType> contentType
<-l|--url> "url"
<-u|--user> user
<-p|--password> password
[--authmode mode]
[--sysadmin name]
[--docStore docStore]
[--file file]
[--forceDelete]
[-Ddx.kerberos.initial.administrator]
[-Ddx.pwc.domain.gateway]
[-Ddx.kerberos.krb5.file]
[-Ddx.kerberos.console.keytab.file]
[-Ddx.kerberos.console.service.principal.name]
```

The following table describes the repository utility options and arguments:

Options	Argument	Description
- c --command	command	Required. Command to run on the repository. Enter one of the following commands: - createContent. Initializes the repository. Use this command after you run the repository utility with the deleteContent command. - CreateOdsContent. Initialized the operational data store. Use this command after you run the repository utility with the deleteODSContent command - createSchema. Creates the tables and views in the repository. - createOdsSchema. Creates the tables and views in the operational data store. - deleteContent. Removes all content from the repository. If you use this command, you must run the repository utility with the createContent command before you can use the repository again. - deleteOdsContent. Removes all content from the operational data store. If you use this command, you must run the repository utility with the createOdsContent command before you can use the operational data store again. - deleteSchema. Deletes all tables and views in the repository. - deleteOdsSchema. Deletes all tables and views in the operational data store. - loadProperties. Loads and sets B2B Data Exchange system properties and event attributes in the B2B Data Exchange repository. - migrateToISP. Switches the authentication mode to Informatica domain authentication and deletes all user information from the B2B Data Exchange repository. For details see the section "Switching to Informatica Domain Authentication". You can synchronize B2B Data Exchange with the Informatica security domain when you switch authentication modes. Create a `.PROPERTIES` file with the properties dx.authentication.groups, dx.pwc.domain.gateway, dx.pwc.user, and dx.pwc.password, and enter the file path in the `--file` command to load the properties from the file. You can also synchronize the users after you switch authentication modes on the **Users** page of the Operation Console. - migrateToISPKerberos. Switches the authentication mode to Informatica domain with Kerberos authentication. Deletes synchronized users from the B2B Data Exchange repository and adds the system administrator that is defined by the command argument `-Ddx.kerberos.initial.administrator`.

Options	Argument	Description
		For details see the section "Switching to Informatica Domain with Kerberos Authentication".
		- migrateToNative. Switches the authentication mode to B2B Data Exchange native authentication and deletes synchronized users from the B2B Data Exchange repository. For details see the section "Switching to Native Authentication".
		- moveDocumentStore. Moves the document store directory to a different location. Enter the absolute file path of the location to which you want to move the document store in the `--file` command.
		- upgradeSchema. Upgrades the repository to the latest version.
		- upgradeOdsSchema. Upgrades the operational data store to the latest version.
		- verifyContents. Verifies the contents of the B2B Data Exchange repository.
-t --contentType	contentType	Required. Specifies on which repository the command runs. Specify one of the following options: - dx. B2B Data Exchange repository. - dx_ods. Operational data store.

-l
 -- url
	"url"	Optional. JDBC URL for the B2B Data Exchange repository or for the operational data store. You must enclose the URL in quotation marks. For example:
		 `repoutil -c createContent -l "jdbc:informatica:oracle://`
		 `//oracle_1:1521;SID=orcl"...`

-u --user	user	Optional. User name for the database account to use when the utility connects to the B2B Data Exchange repository or for the operational data store.
-p --password	password	Optional. Password for the database account to use when the utility connects to the B2B Data Exchange repository or for the operational data store.
--authMode	mode	Optional for the createContent command. The argument determines the authentication mode to set. Specify one of the following options: - native. Native authentication. - isp. Informatica platform authentication.
--sysadmin	name	Required for the following commands: - migrateToNative - createContent if the --authMode parameter value is native Creates an administrator user account that you use to log in to the Operation Console. By default, the password for the administrator user account is the same as the user name. If --authMode has the value "isp", this option is ignored.

Options	Argument	Description
--docStore	docStore	Required for the moveDocumentStore command. Absolute path of the directory to which to move the document store. The directory must have the same access permissions as the current directory. You cannot move the document store to a subdirectory of the current document store directory. For example, if current document store directory is `c:\DocStore`, you cannot move the document store to the following directory: `c:\DocStore\newstore` If the repository utility fails when you run the moveDocumentStore command, you can resume the move with the same value in the --docStore command. On Windows operating systems, you must use forward double slashes (//) in the file path.
--file	file	Optional for the loadProperties, migrateToISPKerberos, migrateToISP, and verifyContents commands. Enter the following file name in the command: The commands use the file to determine the connection properties of the publication repository. Each property must appear on a separate line in the following format: `<propertyName>=<propertyValue>`
--configFile	propertyFile	Optional for all the repository commands. Points to the location of the B2B Data Exchange configuration property file. If not specified, B2B Data Exchange loads the file from the following location: `<DXInstallationDir>/conf/dx-configuration.properties`
--createVersion	version	Optional. If you run the createSchema command, you can use this option to specify the version of the product for which to create the repository. The product version consists of numbers separated by periods. For example: 9.5.1. By default, the product version is set to the latest version.
--forceDelete		Optional for the deleteSchema command. Deletes the repository schema regardless of errors. By default, the deleteSchema command does not delete the repository schema if it encounters errors.

-Ddx.kerberos.initial.administrator	user	Required for the migrateToISPKerberos command. Kerberos user that exists in the Informatica security domain, in the following format:
		
		`<username>@<SECURITY_DOMAIN>`
		
		You must enter `<SECURITY_DOMAIN>` in uppercase letters. For example:
		
		`Administrator@DEVELOPMENT.COM`

Options	Argument	Description
-Ddx.pwc.domain.gateway	host	Required for the migrateToISPKerberos command. Gateway machine to the Informatica domain. For example: `host:6005`
-Ddx.kerberos.krb5.file	file	Required for the migrateToISPKerberos command. Location of the Kerberos configuration file. This file usually resided in the same location as the PowerCenter configuration file.
-Ddx.kerberos.console.keytab.file	file	Required for the migrateToISPKerberos command. Location of the keytab file. If B2B Data Exchange is installed on the same machine as the PowerCenter Administrator Console, the keytab file is the same file that is used for the service principal `HTTP/<hostname>@<domain>`, the file `webapp_http.keytab`. If B2B Data Exchange is installed on a different machine than the PowerCenter Administrator Console, the keytab file must contain the credentials for the service principal `HTTP/<DXhostname>@<domain>`.

-Ddx.kerberos.console.service.principal.name	name	Required for the migrateToISPKerberos command. Service principal host name in the following format:
		
		`HTTP/<FQDN>@<REALM NAME>`
		
		For exampe:
		
		`HTTP/`
		`webserver.development.com@DEVELOPMENT.COM`

Event Utility

Use event utility to execute actions for events during the publication or subscription process. You can use REST API and command line utility to reprocess, resend, discard, or change an event status.

Note: Data access restrictions apply to all actions that users perform according to the permissions that you assign to them.

Event Utility REST APIs

Use Event Utility REST APIs to perform the commands available for executing event utility actions.

You can reprocess, resend, discard, or change an event status.

Reprocess Event Utility REST API

Use the Reprocess Event Utility REST API to reprocess an event according to the event ID, username, and password. This API uses the POST method.

Use the following URL for the REST API call:

```
POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/eventUtils
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.
- `<portNumber>` is the port number of the B2B Data Exchange server. The utility connects to the localhost server with the default port 19553.

The following table describes the request body objects:

Object	Arguments
command	Specify the action to execute.
username	Specify which user to execute reprocess.
password	The password used to connect to the server.
passwordEncrypted	Optional. Enter the encrypted password.
eventID	ID of the event to reprocess.
file	Optional. To select a different file to reprocess, enable the **Allow Source File Selection for Event Reprocess** privilege for the user.
changeSourceDocument	Optional. Indicates whether the file is uploaded.
profileId	Optional. To select a different profile to reprocess, enable the **Allow Profile Selection for Event Reprocess** privilege for the user.

Note: The **Allow Source File Selection for Event Reprocess** and **Allow Profile Selection for Event Reprocess** privileges are enabled by default for the user to reprocess an event. Optionally, the user can manually deselect these privileges.

The following table describes the response body objects:

Object	Arguments
responseStatus	Status of the reprocess.
responseExtraMessage	Details of the reprocess.
responseType	Type of action executed.

Request Body Example

The following code shows the request body syntax:

```
{
   "command":"reprocess",
   "username":"DX_MFT"
   "passwordEncrypted":"1234",
   "eventID":"100004",
   "file":"C:\\Assembly_copy\\readme.txt",
```

```
            "changeSourceDocument":"true",
        "profileId":"1001",
        }
```

Response Body Example

The following code shows the response body syntax:

```
    {
        "responseStatus":"SUCCESS",
        "responseExtraMessage":"Successfully, submitted for reprocessing with
    eventId=100004, blobId=null, Uploaded Files=file
        [originalFileName=readme.txt, contentType=text/plain,
    uploadedFileName=upload63758764301336854760.tmp], profileId=1001",
        "responseType":"/eventUtils"
    }
```

Resend Event Utility REST API

Use the Resend Event Utility REST API to resend an event according to the event ID, username, and password. This API uses the POST method.

Use the following URL for the REST API call:

```
    POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/eventUtils
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.

- `<portNumber>` is the port number of the B2B Data Exchange server. The utility connects to the localhost server with the default port 19553.

The following table describes the request body objects:

Object	Arguments
command	Specify the action to execute.
username	Specify which user to execute resend.
password	The password used to connect to the server.
passwordEncrypted	Optional. Enter the encrypted password.
eventID	ID of the event to resend.
file	Optional. To select a different file to resend, enable the **Allow Endpoint Selection for Event Resend** privilege for the user.
changeSourceDocument	Optional. Indicates whether the file is uploaded.
endpointName	Optional. Enter the endpoint name. Enable the **Allow Endpoint Selection for Event Resend** privilege to select different endpoints.

Note: The **Allow Endpoint Selection for Event Resend** privilege is enabled by default for the user to resend an event. Optionally, the user can manually deselect the privilege.

The following table describes the response body objects:

Object	Arguments
responseStatus	Status of the resend.
responseExtraMessage	Details of the resend.
responseType	Type of action executed.

Request Body Example

The following code shows the request body syntax:

```
{
    "command":"resend",
    "username":"DX_MFT"
    "passwordEncrypted":"1234",
    "eventID":"100004",
    "file":"C:\\Assembly_copy\\readme.txt",
            "changeSourceDocument":"true",
    "endpointName":"1001"
    }
```

Response Body Example

The following code shows the response body syntax:

```
{
    "responseStatus":"SUCCESS",
    "responseExtraMessage":"Successfully, submitted for resending with eventId=100004,
blobId=null, Uploaded Files=file
    [originalFileName=readme.txt, contentType=text/plain,
uploadedFileName=upload63758764301368547 60.tmp], profileId=1001",
    "responseType":"/eventUtils"
    }
```

Discard Event Utility REST API

Use the Discard Status Event Utility REST API to discard an event according to the event ID, username, and password. This API uses the POST method.

Use the following URL for the REST API call:

```
POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/eventUtils
```

- <hostName> is the host name or IP address of the B2B Data Exchange server.

- <portNumber> is the port number of the B2B Data Exchange server. The utility connects to the localhost server with the default port 19553.

The following table describes the request body objects:

Object	Arguments
command	Specify the action to execute.
username	Specify which user to execute discard.
password	The password used to connect to the server.

Object	Arguments
passwordEncrypted	Optional. Indicates whether the password used to connect to the server is encrypted.
eventID	ID of the event to discard.

The following table describes the response body objects:

Object	Arguments
responseStatus	Status of the discard.
responseExtraMessage	Details of the discard.
responseType	Type of action executed.

Request Body Example

The following code shows the request body syntax:

```
{
   "command":"discard",
   "username":"DX_MFT"
   "passwordEncrypted":"1234",
   "eventID":"100010"
       }
```

Response Body Example

The following code shows the response body syntax:

```
{
   "responseStatus":"SUCCESS",
   "responseExtraMessage":"Event discarded",
   "responseType":"/eventUtils"
}
```

Change Status Event Utility REST API

Use the Change Status Event Utility REST API to change an event status according to the status name, event ID, username, and password. This API uses the POST method.

Use the following URL for the REST API call:

```
POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/eventUtils
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.
- `<portNumber>` is the port number of the B2B Data Exchange server. The utility connects to the localhost server with the default port 19553.

The following table describes the request body objects:

Object	Arguments
command	Specify the action to execute.
username	Specify which user to execute status change.
password	The password used to connect to the server.
passwordEncrypted	Optional. Indicates whether the password used to connect to the server is encrypted.
eventID	ID of the event to change the status of.
statusName	Specify the status to change the event to.

The following table describes the response body objects:

Object	Arguments
responseStatus	Status of the status change.
responseExtraMessage	Details of the status change.
responseType	Type of action executed.

Request Body Example

The following code shows the request body syntax:

```
{
    "command":"changestatus",
    "username":"DX_MFT"
    "passwordEncrypted":"1234",
    "eventID":"100010",
    "statusName":"Complete"
        }
```

Response Body Example

The following code shows the response body syntax:

```
{
    "responseStatus":"SUCCESS",
    "responseExtraMessage":"Event status changed to Complete",
    "responseType":"/eventUtils"
}
```

Event Utility Action Commands

Use command line utility to perform the commands available for executing event utility actions.

You can reprocess, resend, discard, or change an event status.

Reprocess Event

Reprocess an event using the `reprocess` command. The reprocessed event appears on the Event List. Navigate to the `<C:\Assembly_copy\dx-tools>` directory and type:

eventutils.bat -c <reprocess> [-com <comment>] -eid <eventID> [-f <file>] [-p <password>] [-pid <profile>] [--server <hostname:port>] [-u <loginname>]

Note: The **Allow Source File Selection for Event Reprocess** and **Allow Profile Selection for Event Reprocess** privileges are enabled by default for the user to reprocess an event. Optionally, the user can manually deselect these privileges.

The `reprocess` command accepts the following parameters:

Parameter Name	Description	Mandatory	Default Value
-c	Command to execute reprocess.	Yes	None
-com	Comments for new status.	No	None
-eid	Event ID.	Yes	None
-f	File name of the document to reprocess.	No	None
-p	Password for the user login name.	Yes	None
-pid	Profile ID.	No	None
--server	The DX engine server location. The format is: server_name[:port].	Yes	localhost: 18095
-u	The user login name that holds the required privileges.	Yes	None

Resend

Resend an event using the `resend` command. The resent event appears on the Event List. Navigate to the `<C:\Assembly_copy\dx-tools>` directory and type:

eventutils.bat -c <resend> [-com <comment>] -eid <eventID> [-f <file>] [-p <password>] [--server <hostname:port>] [-u <loginname>]

Note: The **Allow Endpoint Selection for Event Resend** and **Allow Profile Selection for Event Resend** privileges are enabled by default for the user to resend an event. Optionally, the user can manually deselect these privileges.

The `resend` command accepts the following parameters:

Parameter Name	Description	Mandatory	Default Value
-c	Command to execute resend.	Yes	None
-com	Comments for new status.	No	None
-eid	Event ID.	Yes	None
-ept	Endpoint name for resend event.	No	None

Parameter Name	Description	Mandatory	Default Value
-f	File name of the document to resend.	No	None
-p	Password for the user login name.	Yes	None
--server	The DX engine server location. The format is: server_name[:port].	Yes	localhost: 18095
-u	The user login name that holds the required privileges.	Yes	None

Discard

Discard an event using the `discard` command. The discarded event appears on the Event List. Navigate to the `<C:\Assembly_copy\dx-tools>` directory and type:

eventutils.bat -c <discard> [-com <comment>] -eid <eventID> [-p <password>] [--server <hostname:port>] [-u <loginname>]

The `discard` command accepts the following parameters:

Parameter Name	Description	Mandatory	Default Value
-c	Command to execute discard.	Yes	None
-com	Comments for new status.	No	None
-eid	Event ID.	Yes	None
-p	Password for the user login name.	Yes	None
--server	The DX engine server location. The format is: server_name[:port].	Yes	localhost: 18095
-u	The user login name that holds the required privileges.	Yes	None

Change Event Status

Change an event status using the `changestatus` command. The changed event status appears on the Event List. Navigate to the `<C:\Assembly_copy\dx-tools>` directory and type:

eventutils.bat -c <changestatus> [-com <comment>] -eid <eventID> [-p <password>] [--server <hostname:port>] [-st <Completed>] [-u <loginname>]

The `changestatus` command accepts the following parameters:

Parameter Name	Description	Mandatory	Default Value
-c	Command to execute change status.	Yes	None
-com	Comments for new status.	No	None
-eid	Event ID.	Yes	None

Parameter Name	Description	Mandatory	Default Value
-p	Password for the user login name.	Yes	None
--server	The DX engine server location. The format is: server_name[:port].	Yes	localhost: 18095
-st	New status name for changing event status.	Yes	None
-u	The user login name that holds the required privileges.	Yes	None

Export Audit Events Utility

Use the audit export utility to export the audit events to XML. To run the audit export utility, you must enable the view auditing privilege. If you do not have the required permissions and privileges, B2B Data Exchange aborts this process.

You can find the auditExport utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

Export Audit Events Script

Use the auditExport batch script to export the audit events to XML.

The following is an example of a sample batch script to export audit event object:

```
auditExport.bat -u <username> -p <password> -f /data/exportfile.xml
```

The following table describes parameters and arguments for the auditExport batch script.

Parameter Name	Argument	Description	Mandatory
-c or -command	command	Specify the command to execute. You can specify one of the following commands: - start. Starts to export the specified audit event object in the B2B Data Exchange repository. - abort. Stops exporting the audit event object in the B2B Data Exchange repository.	No
-from or -from_date	date	List the object type. Search for audit records created on and after the specified date. The supported date formats are "dd/MM/yyyy HH:mm:ss" and "dd/MM/yyyy".	No
-to or --to_date	-to or --to_date	List the object type. Search for audit records created on and before the specified date. The supported date formats are "dd/MM/yyyy HH:mm:ss" and "dd/MM/yyyy".	No
-name or --ObjectName	name	The name of the object.	No

Parameter Name	Argument	Description	Mandatory
-type or --ObjectType	type	List the object type. Specify one of the following commands: - Partner - Account - Profile - Endpoint - UserGroup - User - Monitor - PortalUser	No
-act or --ActionType	action	List the action type. Specify one of the following commands: - Create - Edit - Delete	No
-f or --filename	file	The file in which the audit report is saved. The parameter is mandatory for the start command.	No
--server	"hostname:port"	The location of the Data Exchange Engine server. Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the utility connects to the localhost server with the default port 18095. The argument must be enclosed in quotation marks. For example: `auditExport.bat --server "localhost:18095"`	No
-u or --user	userID	Identifier of the Operation Console user account. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol. For example: `Administrator@SecurityDomain` You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.	No
-U	Environment variable	Environment variable that contains the UserID value. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol. For example: `Administrator@SecurityDomain` You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.	No

Parameter Name	Argument	Description	Mandatory
-p or --password	password	Password of the Operation Console user. This option contains the clear text password. You must specify at least one of the password options, -p or -P to determine the UserID required to execute this command.	No
-P	Environment variable	Environment variable that contains the password value. Password for the Operation Console user that executes the auditExport command. The password must be encrypted. You must specify at least one of the password options, -p or -P to determine the user's password required to execute this command.	No

The following is an example of a sample batch script to export the audit report:

```
auditExport.bat -f "path/file.xml" -from "18/12/2003 12:55:43" -to "21/03/2021" -name
"Objects"  -type "Partner" -act "Edit" -u sys -p sys  -c abort
```

Run Endpoints Utility

Use the run endpoint utility to run an inbound endpoint. To run an inbound endpoint utility, you must enable the Run Endpoint privilege.

You can find the runendpoint utility in the following directory:

```
<DXInstallationDir>\dx-tools\
```

Run Endpoints Script

Use the runendpoint batch script to run inbound endpoints.

The following is an example of a sample batch script to run an endpoint object:

```
runendpoint.bat -e <endpointname> -u <loginname> -p <password>
```

The following table describes parameters and arguments for the runendpoint batch script.

Parameter Name	Argument	Description	Mandatory
-e or --endpointName	name	The name of the endpoint.	Yes
--server	"hostname:port"	Environment variable that contains the password value. Optional. Host name and port number of the B2B Data Exchange server. If you do not enter an argument, the utility connects to the localhost server with the default port 18095. The argument must be enclosed in quotation marks. For example: `runendpoint.bat --server "localhost:18095"`	No
-u or --user	userID	Identifier of the Operation Console user account with run endpoint privileges. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol. For example: `Administrator@SecurityDomain` You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.	No
-U	Environment variable	Environment variable that contains the UserID value with run endpoint privileges. If you use Informatica platform authentication, the user ID must specify the Informatica security domain, separated by the @ symbol. For example: `Administrator@SecurityDomain` You must specify at least one of the user name options, -u or -U to determine the UserID required to execute this command.	No
-p or --password	password	Password of the Operation Console user. This option contains the clear text password. You must specify at least one of the password options, -p or -P to determine the UserID required to execute this command.	No
-P	Environment variable	Environment variable that contains the password value. Password for the Operation Console user that executes the auditExport command. The password must be encrypted. You must specify at least one of the password options, -p or -P to determine the user's password required to execute this command.	No

The following is an example of a sample batch script to run an endpoint:

```
runendpoint.bat -e PRAD -u sys -p sys --server localhost:18095
```

CHAPTER 13

Document Management

This chapter includes the following topics:

Document Management Overview

When you use B2B Data Exchange to process large document files, you can store the files in the B2B Data Exchange document store and pass a file reference to the PowerCenter Integration Service.

The B2B Data Exchange developer can use an Unstructured Data transformation to process the associated files from the document store. When you view an event in the Operation Console for a document reference, you can view the file that is associated with the event.

To use a document reference to point to a large document, configure the following components:

- **Document store directory.** A directory where the document associated with a document reference is stored. The directory must be accessible to B2B Data Exchange and to PowerCenter.

- **Data by reference indicator.** An indicator that specifies whether you are passing the document data or a reference to the document.

Document Store

The document store is a directory where B2B Data Exchange can store files to process. The directory must be accessible to the B2B Data Exchange server, the Apache Tomcat server, and the PowerCenter Integration Service with the same file path.

You specify the document store directory during B2B Data Exchange installation. If you do not specify a directory, the installer uses the following default directory for the document store: `<DXInstallationDir>\dx-data`

After the installation, B2B Data Exchange saves the path to the document store in the document.store.folder system property. You use the repository utility to change the document store directory after installation.

Note: Do not change the value in the system property. If you change the value, you create a file path conflict and B2B Data Exchange and PowerCenter cannot access the document store.

The files remain in the document store until you delete or archive the associated event. To protect the files, manually back up the document store directory.

Document Store Folder Structure

After you install B2B Data Exchange, the B2B Data Exchange server creates sub-folders in the document store directory. In addition to the files, the sub-folders store logs and temporary files that B2B Data Exchange creates during processing.

The B2B Data Exchange creates the following sub-folders in the document store directory:

/tmp

Directory that stores temporary files that B2B Data Exchange creates during processing.

Note: B2B Data Exchange does not delete temporary files. You must manually clean up the directory periodically. Do not delete temporary files that were created during the last 24 hours before you clean up the directory.

/documents

Directory that stores the files to process. When you pass a reference to PowerCenter, the path must point to files in this directory.

/eventLogs

Directory that stores event logs when you run the B2B Data Exchange server in debug mode. Use the event logs for troubleshooting.

Document Store Permissions

You configure permissions for components that need to access the document store. The Operation Console and the PowerCenter Integration Service must have permissions to access the directory.

Do not grant permissions to PowerCenter workflow to write to the /documents sub-folder. PowerCenter workflows must write all files to the /tmp sub-folder.

The following table describes the component permissions to configure:

Component	Permissions
Operation Console	Requires read permission to the following directory: `<DocumentStoreDir>/documents`

PowerCenter Integration Service	- Requires create and write permissions to the following directory:
	  `<DocumentStoreDir>/tmp`
	- Requires read permission to the following directory:
	  `<DocumentStoreDir>/documents`

Changing the Location of the Document Store

Use the B2B Data Exchange repository utility to change the location of the document store directory. The utility changes the value in the system property, updates all the path references in the B2B Data Exchange repository, and moves all files to the new directory.

To prevent data loss, perform the following actions before you run the repository utility to change the location of the document store directory:

- Shut down all B2B Data Exchange services.

- Verify that B2B Data Exchange workflows are not running.

- Verify that there are no JMS messages that contain document references in any B2B Data Exchange JMS queues.

▶ In the B2B Data Exchange repository utility, run the `moveDocumentStore` command with the following syntax in a single line:

```
repoutil -c moveDocumentStore -t dx -l <B2B Data Exchange repository jdbc URL> -u
<user name> -p <password> --docStore <new document store location>
```

The following example shows a repoutil script for moving the document store in a node that uses a UNIX operating system:

```
./repoutil.sh -c moveDocumentStore -t dx
-l "jdbc:informatica:oracle://xsvcshacl03:1521;ServiceName=drep02_taf" -u dxadmin -p
mypassword --docStore="/u02/app/infa_shared/DX_doc_store"
```

For more information about the repository utility, see the section "B2B Data Exchange Repository Utility".

Note: Do not move the document store manually. If you manually move the document store, B2B Data Exchange will not reference document attachments for events correctly.

Large Document Files

To process a large B2B Data Exchange document, complete the following steps:

1. Verify that B2B Data Exchange, Apache Tomcat, and PowerCenter, can use the same file path to access the document store directory you set during the B2B Data Exchange installation.

2. In B2B Data Exchange Operation Console, verify that the value of the system property document.store.folder is the document store directory you set during installation.

3. When creating a file-receipt endpoint using the Endpoint screen, turn on the Pass by Reference flag on. For more information, see the *B2B Data Exchange Operator Guide*.

4. In the PowerCenter Designer, when you build a mapping to process the document, include a JMS source and target and call the B2B Data Exchange transformations and the Unstructured Data transformation.

   Configure the following PowerCenter objects:

   - **JMS source definition.** Add the DXDataByReference property to the JMS properties in the source and target definitions. If the JMS message contains a document reference, the DXDataByReference property is true.

   - **DX_Get_Document_File_Path transformation.** Use this transformation convert the document reference in the JMS source to a file path that can be used to access the associated file in the document store.

   - **DX_Generate_Temporary_File transformation.** Use this transformation to generate an output file for the Unstructured Data transformation.

- **Unstructured Data transformation.** Call this transformation to use the Data Transformation service to transform the document to the required format. You can also use the Unstructured Data transformation to split a large document.

- **DX_Aggregate transformation.** If you split a large document, call this transformation to combine the transformed data segments into one document.

- **API calls: createDocument and addEventDocument.** Use these calls to attach the output file to an event as a new target document.

- **JMS target definitions.** Send the new document to the JMS target. Add the DXDataByReference property to the JMS properties in the target definition. If the JMS message contains a document reference, set the DXDataByReference property to true.

5. In B2B Data Exchange Operation Console, after you run the workflow, verify that an event has been created for the large document processed. You can view the source document in the Source Data section of the event details page and the target document in the Target Data section of the event details page.

DataByReference Indicator

PowerCenter needs to determine whether the document it receives or sends contains the document data or a reference to the document. When you send a document to a PowerCenter workflow to process, you must indicate whether you are sending a document or a reference to a document. When you pass documents from PowerCenter after processing, you must also indicate whether you are passing a document or a reference to a document.

B2B Data Exchange uses the following ports and properties to indicate whether the document it sends or receives is the document data or a reference to the document:

- DXDataByReference port
- DXDataByReference property
- passDataByReference property

DXDataByReference Port

Each Data Exchange transformation that has a DXData port also has a DXDataByReference port. When you pass a document to the transformation in the DXData port, you must indicate whether the data is a document or a document reference. If the value of the DXDataByReference port is true, the DXData port contains a document reference. If the value is null or the value is false, the DXData port contains the document data.

DXDataByReference Property

When the Data Exchange Server sends a JMS message to PowerCenter for processing, the JMS message header contains the DXDataByReference property to indicate whether the JMS message body contains a document or a document reference. If the DXDataByReference property is true, the JMS message body contains a document reference. If the value is false, the JMS message body contains the document data as a BLOB.

When PowerCenter sends a JMS message to B2B Data Exchange, the JMS message header should also contain the DXDataByReference property. By default, if the JMS message header does not contain the property, B2B Data Exchange assumes that the JMS message body contains document data.

PassDataByReference Property

The Data Exchange Server can forward documents passed to the file, JMS, or Managed File Transfer endpoints as documents or document references. In the configuration file, set the passDataByReference property to indicate how to forward the documents received in the endpoints.

You can set the passDataByReference property to one of the following values:

- **True.** If the endpoint receives a document, the Data Exchange Server converts the document to a document reference and forwards the document reference. If the endpoint gets a document reference, the Data Exchange Server forwards the document reference unchanged.

- **False.** If the endpoint receives a document, the Data Exchange Server forwards the document unchanged. If the endpoint gets a document reference, the Data Exchange Server converts the document reference to a document and forwards the document.

- **Passthrough_as_is.** The Data Exchange Server forwards the documents or document references in the endpoints unchanged. This value is valid for JMS endpoints only.

Document Storage in a Hadoop File System (HDFS)

You can instruct B2B Data Exchange to store documents that pass through File Receive and Managed File Transfer endpoints in a Hadoop file system (HDFS). Store documents in HDFS to enable future analysis or processing without the need for additional space in the main Data Exchange repository.

You define the HDFS server location, name, and user name in system properties. The operator can select to store the documents that B2B Data Exchange processes through the endpoint in HDFS in the File Receive or Managed Transfer File endpoint properties. For Managed File Transfer endpoints, the option is relevant only for incoming files. B2B Data Exchange copies the file to HDFS in the background after the endpoint processes the file, which does not affect the processing performance.

You can change the HDFS version to which B2B Data Exchange connects based on the installed HDFS version.

Note: B2B Data Exchange connects only to HDFS versions that do not require password authentication.

Changing the Hadoop Version on Windows

You can configure B2B Data Exchange on the Windows operating system to connect to a different HDFS version.

1. Shut down the B2B Data Exchange service and close the Operation Console.
2. Open `<DXInstallationDir>\bin\dxhadoop.bat` in a text editor.

   The file displays a list of commands to connect to a specific HDFS version. The line that contains the version to which B2B Data Exchange connects appears in the following format:

   ```
   set DX_HADOOP_CLASS_PATH=%DX_HOME%\hadoop\<selected version>\lib\*
   ```

   The other supported HDFS versions appear in the following format:

   ```
   :: set DX_HADOOP_CLASS_PATH=%DX_HOME%\hadoop\<supported version>\lib\*
   ```

3. To instruct B2B Data Exchange to connect to a different HDFS version, remove the two colon (::) comment indicator at the beginning of the line that contains the HDFS version to which you want B2B Data Exchange to connect.

4. Add two colons (::) as comment indicators at the beginning of the line that contains the HDFS version to which you no longer want B2B Data Exchange to connect.

    Note: If you select more than one HDFS version, the connection may fail.

5. Open `<DXInstallationDir>\conf\wrapper.hadoop.conf` in a text editor.

    The file displays a list of commands to connect to a specific HDFS version. The line that contains the version to which B2B Data Exchange connects appears in the following format:

    ```
    wrapper.java.classpath.6=./hadoop/<selected version>/lib/*.jar
    ```

    The other supported HDFS versions appear in the following format:

    ```
    # wrapper.java.classpath.6=./hadoop/<supported version>/lib/*.jar
    ```

6. To instruct B2B Data Exchange to connect to a different HDFS version, remove the number sign (#) comment indicator at the beginning of the line that contains the HDFS version to which you want B2B Data Exchange to connect.

    Note: The HDFS versions that you define in the `wrapper.hadoop.conf` file and the `dxhadoop.bat` file must be identical.

7. Add a number sign (#) as a comment indicator at the beginning of the line that contains the HDFS version to which you no longer want B2B Data Exchange to connect.

    Note: If you select more than one HDFS version, the connection may fail.

8. Save and close the `wrapper.hadoop.conf` file and the `dxhadoop.bat` file.

9. Restart the B2B Data Exchange service and open the Operation Console.

Changing the Hadoop Version on UNIX

You can configure B2B Data Exchange on the UNIX operating system to connect to a different HDFS version.

1. Shut down the B2B Data Exchange service and close the Operation Console.

2. Open `<DXInstallationDir>\bin\dxhadoop.sh` in a text editor.

    The file displays a list of commands to connect to a specific HDFS version. The line that contains the version to which B2B Data Exchange connects appear in the following format:

    ```
    DX_HADOOP_CLASS_PATH=$DX_HOME/hadoop/<selected version>/lib/*
    ```

    The other supported HDFS versions appear in the following format:

    ```
    #DX_HADOOP_CLASS_PATH=$DX_HOME/hadoop/<supported version>/lib/*
    ```

3. To instruct B2B Data Exchange to connect to a different HDFS version, remove the hash sign (#) comment indicator at the beginning of the line that contains the HDFS version to which you want B2B Data Exchange to connect.

4. Add a hash sign (#) as a comment indicator at the beginning of the line that contains the HDFS version to which you no longer want B2B Data Exchange to connect.

    Note: If you select more than one HDFS version, the connection may fail.

5. Restart the B2B Data Exchange service and open the Operation Console.

C H A P T E R   1 4

B2B Data Exchange Utilities

This chapter includes the following topics:

B2B Data Exchange Utilities Overview

The B2B Data Exchange utilities perform administrative tasks for B2B Data Exchange from the Windows or UNIX command line. The utilities include different commands on Windows and UNIX operating systems.

B2B Data Exchange includes the following utilities:

B2B Data Exchange services

Starts and stops all B2B Data Exchange services. The utility is available on Windows operating systems.

The utility is in the following location: `<DXInstallationDir>/bin/dxservices`

B2B Data Exchange console

Starts and stops the Operation Console service. The utility is available on Windows and UNIX operating systems.

The utility is in the following location: `<DXInstallationDir>/bin/dxconsole`

B2B Data Exchange server

Starts and stops the B2B Data Exchange server. The utility is available on Windows and UNIX operating systems.

The utility is in the following location: `<DXInstallationDir>/bin/dxserver`

B2B Data Exchange JMS Broker

Starts and stops the Operation Console service. The utility is available on Windows and UNIX operating systems.

The utility is in the following location: `<DXInstallationDir>/bin/dxactivemq`

B2B Data Exchange Services Utility

The B2B Data Exchange services utility starts, stops, and manages the registration of all B2B Data Exchange services. The utility is available only on Windows operating systems.

You can also start and stop all B2B Data Exchange services from the Start menu.

Command Syntax

The B2B Data Exchange services utility uses the following syntax:

```
dxservices
<start|stop|install|remove>
```

The following table describes the B2B Data Exchange services utility commands:

Command	Description
start	Starts all B2B Data Exchange services.
stop	Stops all B2B Data Exchange services.
install	Registers all B2B Data Exchange services to the Windows registry with default settings.
remove	Removes all B2B Data Exchange services from the Windows registry.

B2B Data Exchange Console Utility

The B2B Data Exchange console utility starts and stops the Apache Tomcat server.

B2B Data Exchange uses the Apache Tomcat server to send commands between the Operation Console Web client and the B2B Data Exchange server.

On Windows operating systems, you can start the Apache Tomcat server as an application or as a Windows service.

The Apache Tomcat server creates temporary files in the following directory:

```
<DXInstallationDir\DataExchange\tomcat
```

B2B Data Exchange does not delete the temporary files. You must manually clean up the directory periodically. Do not delete temporary files that were created during the last 24 hours before you clean up the directory.

Windows Command Syntax

On Windows operating systems, the B2B Data Exchange console utility uses the following syntax:

```
dxconsole
<start|stop|install|svcstart|svcstop|remove>
```

The following table describes the B2B Data Exchange console utility commands:

Command	Description
start	Starts the Apache Tomcat server as an application.
stop	Stops the Apache Tomcat server.
install	Registers the Apache Tomcat server to the registry as a Windows service.
svcstart	Starts the Apache Tomcat server Windows service.
svcstop	Stops the Apache Tomcat server Windows service.
remove	Removes the Apache Tomcat server Windows service from the registry.

UNIX Command Syntax

On UNIX operating systems, the B2B Data Exchange console utility uses the following syntax:

```
dxconsole.sh
<start|stop>
```

The following table describes the B2B Data Exchange console utility commands:

Command	Description
start	Starts the Apache Tomcat server.
stop	Stops the Apache Tomcat server.

B2B Data Exchange Server Utility

The B2B Data Exchange server utility starts, stops, and manages the B2B Data Exchange server service.

The B2B Data Exchange server is the main component that manages document processing in B2B Data Exchange.

When you run the B2B Data Exchange server utility, you can specify the host name and port number of the B2B Data Exchange server. If you do not specify the host name and port number, the utility uses the local host and default port that you specify during installation.

On Windows operating systems, you can start the B2B Data Exchange as an application or as a Windows service.

By default, the B2B Data Exchange server creates temporary files in one of the following directories:

```
Windows: <SystemDrive>\temp
UNIX: /tmp or /var/tmp
```

B2B Data Exchange does not delete the temporary files. You must manually clean up the directory periodically. Do not delete temporary files that were created during the last 24 hours before you clean up the directory.

Windows Command Syntax

On Windows operating systems, the B2B Data Exchange server utility uses the following syntax:

```
dxserver
<start [port]|
 stop [host][port]|
 install|
 svcstart|
 svcstop|
 remove|
 console|
 ping [host][port]|
 pingjms|
 status>
```

The following table describes the B2B Data Exchange server utility commands:

Command	Description
start	Starts the B2B Data Exchange server. You can use the default port number or specify a port number.
stop	Stops the B2B Data Exchange server. You can use the default host name and port number or specify a host name and port number.
install	Registers the B2B Data Exchange server as a Windows service to the registry.
svcstart	Starts the B2B Data Exchange server Windows service.
svcstop	Stops the B2B Data Exchange server Windows service.
remove	Removes the B2B Data Exchange server Windows service from the Windows registry.
console	Starts the B2B Data Exchange server as an application. This command is the same as the Start menu option.
ping	Pings the B2B Data Exchange server. You can use the default host name and port number or specify a host name and port number.
pingjms	Tests all JMS endpoints in the repository and determines whether the B2B Data Exchange server can connect to the JMS service.

status	Returns the status of the B2B Data Exchange server Windows service. Returns one of the following values:
	- Not installed
	- Starting
	- Started
	- Stopping
	- Stopped
	The following example shows the output message that the status command can return:
	
	`The B2B Data Exchange server service`
	`is not installed.`

UNIX Command Syntax

On UNIX operating systems, the B2B Data Exchange server utility uses the following syntax:

```
dxserver.sh
<start [port]|
 stop [host][port]|
```

```
ping [host][port]|
pingjms>
```

The following table describes the B2B Data Exchange server utility commands:

Command	Description
start	Starts the B2B Data Exchange server. You can use the default port number or specify a port number.
stop	Stops the B2B Data Exchange server. You can use the default host name and port number or specify a host name and port number.
ping	Pings the B2B Data Exchange server. You can use the default host name and port number or specify a host name and port number.
pingjms	Tests all JMS endpoints in the repository and determines whether the B2B Data Exchange server can connect to the JMS service.

B2B Data Exchange JMS Broker Utility

The B2B Data Exchange JMS Broker utility manages the messages that B2B Data Exchange send and receives from PowerCenter.

Use the B2B Data Exchange JMS Broker utility to start or stop the B2B Data Exchange JMS Broker.

On Windows operating systems, you can start the B2B Data Exchange JMS Broker as an application or as a Windows service.

Windows Command Syntax

On Windows operating systems, the B2B Data Exchange JMS Broker utility uses the following syntax:

```
activemq
<start|stop|install|svcstart|remove>
```

The following table describes the B2B Data Exchange JMS Broker utility commands:

Command	Description
start	Starts the B2B Data Exchange JMS Broker as an application.
stop	Stops the B2B Data Exchange JMS Broker.
install	Registers the B2B Data Exchange JMS Broker to the registry as a Windows service.
svcstart	Starts the B2B Data Exchange JMS Broker Windows service.
svcstop	Stops the B2B Data Exchange JMS Broker Windows service.
remove	Removes the B2B Data Exchange JMS Broker Windows service from the registry.

UNIX Command Syntax

On UNIX operating systems, the B2B Data Exchange JMS Broker utility uses the following syntax:

```
activemq.sh
<start|stop>
```

The following table describes the B2B Data Exchange JMS Broker utility commands:

Command	Description
start	Starts the B2B Data Exchange JMS Broker.
stop	Stops the B2B Data Exchange JMS Broker.

CHAPTER 15

DX Toggle Server REST API

This chapter includes the following topics:

DX Toggle Server REST API Overview

DX Toggle Server is used to control the endpoints on any node in the B2B Data Exchange server. For instance, DX Toggle Server can pause only inbound endpoints, pause all endpoints, and resume all endpoints.

Use the DX Toggle Server REST APIs to get status of the B2B Data Exchange server, pause, and resume endpoints.

Note: You must enable the "Allow Pause or Resume DX Server" privilege to pause and resume endpoints using REST API.

Server Status REST API

Use the Server Status REST API to get the status of the B2B Data Exchange endpoints. This API uses the GET method.

Use the following URL for the REST API call:

```
GET https://<hostName>:<portNumber>/dx-server-rest-api/v1/dx_server_status
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.
- `<portNumber>` is the port number of the B2B Data Exchange server. The default port is 19553.

For example, `https://myserver:19553`

The Server Status REST API returns one of the following responses:

- `RUNNING`. Endpoints are running successfully.
- `INBOUND_EP_BINDINGS_STOPPED`. Inbound endpoints are paused.

- `INBOUND_ALL_EP_BINDINGS_STOPPED`. All inbound and outbound endpoints are paused.

Pause Inbound Endpoints REST API

Use the Pause Inbound REST API to pause any new files from being picked up from the B2B Data Exchange inbound endpoints. This API uses the POST method.

Use the following URL for the REST API call:

```
POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/pause_inbound_dx_endpoints
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.
- `<portNumber>` is the port number of the B2B Data Exchange server. The default port is 19553.

For example, `https://myserver:19553`

You can provide a request body to the REST API call. The following table describes the request body objects:

Object	Arguments
username	The username (login name) used to connect to the mailbox server.
password	The password to connect to the mailbox server.
isPasswordEncrypted	Indicates whether the password is encrypted. Run the dxpasswd.bat or dxpasswd.sh command to encrypt the password.

When the endpoints are paused, the Pause Inbound REST API returns a `INBOUND_EP_BINDINGS_STOPPED` response.

Request Body Example

The following code shows the request body syntax:

Key	Value	Description
username	sys	-
password	sys	-
isPasswordEncrypted	false	-

Response Body Example

The following code shows the response body syntax:

```
INBOUND_EP_BINDINGS_STOPPED
```

Pause All Endpoints REST API

Use the Pause All REST API to pause all new files (inbound and outbound) from being picked up from the B2B Data Exchange endpoints. This API uses the POST method.

Use the following URL for the REST API call:

```
POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/pause_all_dx_endpoints
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.

- `<portNumber>` is the port number of the B2B Data Exchange server. The default port is 19553.

For example, `https://myserver:19553`

You can provide a request body to the REST API call. The following table describes the request body objects:

Object	Arguments
username	The username (login name) used to connect to the mailbox server.
password	The password to connect to the mailbox server.
isPasswordEncrypted	Indicates whether the password is encrypted. Run the dxpasswd.bat or dxpasswd.sh command to encrypt the password.

When all the endpoints are paused, the Pause All Inbound REST API returns a `INBOUND_ALL_EP_BINDINGS_STOPPED` response.

Request Body Example

The following code shows the request body syntax:

Key	Value	Description
username	sys	-
password	sys	-
isPasswordEncrypted	false	-

Response Body Example

The following code shows the response body syntax:

```
INBOUND_ALL_EP_BINDINGS_STOPPED
```

Resume All Endpoints REST API

Use the Resume All Inbound REST API to resume all the B2B Data Exchange endpoints. This API uses the POST method.

Use the following URL for the REST API call:

```
POST https://<hostName>:<portNumber>/dx-server-rest-api/v1/resume_all_dx_endpoints
```

- `<hostName>` is the host name or IP address of the B2B Data Exchange server.
- `<portNumber>` is the port number of the B2B Data Exchange server. The default port is 19553.

For example, `https://myserver:19553`

You can provide a request body to the REST API call. The following table describes the request body objects:

Object	Arguments
username	The username (login name) used to connect to the mailbox server.
password	The password to connect to the mailbox server.
isPasswordEncrypted	Indicates whether the password is encrypted. Run the dxpasswd.bat or dxpasswd.sh command to encrypt the password.

When all the endpoints are resumed, the Resume All Inbound REST API returns a `RUNNING` response.

Request Body Example

The following code shows the request body syntax:

Key	Value	Description
username	sys	-
password	sys	-
isPasswordEncrypted	false	-

Response Body Example

The following code shows the response body syntax:

```
RUNNING
```

CHAPTER 16

Dashboard and Reports Management

This chapter includes the following topics:

Dashboard and Reports Management Overview

The Dashboard displays personalized visual reports about information that B2B Data Exchange processes. Use the Dashboard to view summary information about B2B Data Exchange event processing, such as the number of events for certain partners or the error rate for specific accounts.

Most of the reports in the Dashboard are based on key performance indicators (KPIs) that B2B Data Exchange retrieves from the operational data store. KPIs provide measurable information about events that B2B Data Exchange processes. The operational data store is a repository that contains aggregated information solely for reporting purposes.

The Dashboard displays the aggregated event information in panels that you view in the **Dashboard** page of the Operation Console. You install and configure the operational data store when you install B2B Data Exchange.

The following table describes the default KPIs that the Dashboard uses for reports:

KPI	Description
Message processing time	Duration in minutes of the time it takes for the event to reach a final state.
Number of events	Number of events that B2B Data Exchange processes.
Number of error events	Number of error events that reached a final state.

The operational data store event loader is a PowerCenter workflow that collects KPIs from the B2B Data Exchange repository according to specified parameters and loads aggregated events to the operational data store. You import the workflow to PowerCenter after you install the B2B Data Exchange Dashboard and Reports component. The workflow runs at scheduled intervals, and you can change certain aspects of the

workflow behavior. For example, you can configure the number of retry attempts for each event load process in case of failure or the number of minutes to wait between event load processes.

If you use service level agreement (SLA) rules to manage and track violations, the SLA violation detector searches the operational data store for violations according to the SLA rules that you define. If the SLA violation detector finds violations, it stores the violation information in proprietary SLA reports and displays the violations in the **SLA Violations** panel of the Dashboard.

In Dashboard and reports system properties, you change certain aspects of the Dashboard behavior. For example, you can choose to show the Dashboard when users log in to the Operation Console. or configure the error rate range in the Error Rate panelIn the Operation Console, you select specific event attributes to load to the operational data store as KPIs, and the B2B Data Exchange developer can create custom Dashboard panels based on the event attributes.

The Dashboard contains tabs in which to display the panels. Each panel displays event information from the operational data store or the run-time B2B Data Exchange repository based on filters that you apply. You can drill to display the events from each panel in the **Event List** page. For more information about specific Dashboard panels, see the *B2B Data Exchange Operator Guide*.

Note: The operational data store stores aggregated copies of events from the run-time repository. If you archive events from the run-time repository, you cannot drill to display events from operational data store panels in the **Event List** page.

The B2B Data Exchange developer can use Logi Info Studio to customize existing Dashboard panels or create new Dashboard panels based on default or custom KPIs.

Dashboard and Reports System Properties

After you install the Dashboard and Reports component, you can use system properties to modify certain aspects of the Dashboard behavior.

The following table describes the Dashboard and reports system properties:

System Property	Description
dx.dashboard.url	Connection string to the dashboard server, in the following format: `http://<hostname>:<port>/<dashboard name>` If you use HTTPS to connect to the Operation Console, the URL must match the value of the property. Otherwise, the Dashboard does not appear. For example: `https://myhost:18443/dx-dashboard`
dx.dashboard.max.timewindow	Maximum time frame in hours that Operation Console users can select to display unresolved error events in the Dashboard. Default is 96.
dx.dashboard.jdbc.username	User name for the operational data store database.
dx.dashboard.jdbc.password	Password for the operational data store in an encrypted string database. If you change the password you must encrypt the string with the password encryption utility and use the encrypted string.

System Property	Description
dx.dashboard.jdbc.url	Location of operational data store. The location must be different from the B2B Data Exchange repository.
dx.dashboard.show.at.startup	Determines whether to show the Dashboard when users log on to the Operation Console. Default is True.
dx.dashboard.errorrate.threshold.low	Maximum error event percentage to display in the green area of the Error Rate Gauge panel. Any percentage higher than this value is displayed in the orange area. Default is 25.
dx.dashboard.errorrate.threshold.high	Maximum error event percentage to display in the orange area of the Error Rate Gauge panel. Any percentage higher than this value is displayed in the red area. Default is 75.
dx.dashboard.sla.detection.midnight.latency	Time after midnight in minutes from which to start the calculation level. For example, if you define an SLA rule with a calculation level of a single day, you can set the value to 60 minutes to start the calculation at 01:00 instead of midnight. Available for SLA rules in which violations are reported at the end of the time frame. Default is 120.
dx.first.day.of.week	Numeric representation of the first day of a calendar week. For example, the value 1 represents Sunday. Use this property to determine the first day of the week when you define an SLA rule with a calculation level of a week. For example, if you define Monday as the first day of the week, violations are reported for a week that starts on Monday and ends on Sunday. Default is 2.
dx.ods.latency.seconds	Number of seconds between the time the event finished processing and the time that the event load process starts. The operational data store event loader loads events for which the processing time difference in seconds is equal or greater than this value. For example, if you increase the latency to 60 seconds, the event loader only loads events that finished processing at least 60 seconds before the load process starts. Default is 0.
dx.ods.row.limit.thousands	Number of thousands of events to load in each batch when the total number of events is higher than this value. If the total number of events to load is less than the value in this property, the operational data store event loader runs one batch. If you set the row limit to 0, the event loader runs one batch regardless of the number of events. Default is 500. Must be numeric and greater than or equal to 0.

Operational Data Store Event Loader

The operational data store loader is a PowerCenter workflow that collects event information from the run-time B2B Data Exchange repository and then loads the aggregated events to the operational data store. The Dashboard retrieves the aggregated event information and displays it in panels based on the selected KPI.

You can change workflow parameters that affect the workflow behavior. For example, you can choose how long to wait between each event load process and how many retry attempts to perform before failing the workflow. Do not change any internal workflow parameters.

The workflow determines which events to load based on the difference between the time that the event finished processing and the time that the scheduled load process starts. Use the dx.ods.latency.seconds system property to determine the time to wait before the workflow loads the event after the time the event finished processing. Increase the latency if you experience clock sync issues or if you expect events with longer processing time.

If you process a large volume of events, you can change B2B Data Exchange system properties to minimize bottlenecks and to increase performance during the event load process. The workflow loads events in batches. Use the dx.ods.row.limit.thousands system property to determine the number of events to include in each batch.

You import the operational data store event loader to PowerCenter after you install the B2B Data Exchange Dashboard and Reports component with the main B2B Data Exchange installation. For more information, see the *B2B Data Exchange Installation and Configuration Guide*.

Note: If a PowerCenter session fails, the operational data store event workflow might not display a failed status. Monitor the PowerCenter session to verify the success of the run.

Operational Data Store Event Loader Configuration

Configure the operational data store event loader variables and parameters to modify certain aspects of the workflow behavior. You can only modify the variables and parameters listed in this section. All other variables and parameters are for internal use.

The following table describes the DX_ETL workflow variables and parameters that you can modify:

How to Access	Property	Description
Workflow menu > **Edit** > **Variables tab**	$$WF_Last_Load_End_Time	Last date and time until which the event loader loaded the events to the operational data store. The event loader uses this time as the starting point the next time it loads the events. Default is `01/01/2005 00:00:00.00` **Note:** Do not modify the variable after the workflow runs. You can modify the variable before the first run.
Workflow menu > **Edit** > **Variables tab**	$$WF_Number_Of_Retry_Attempts	Number of times that the event loader attempts to load the events to the operational data store. If the event loader cannot complete successfully after the defined number of attempts, the workflow fails and creates a B2B Data Exchange error event. Default is `3`.

How to Access	Property	Description
Workflow menu > Edit > Variables tab	$$WF_Wait_Before_Next_Load_Minutes	Number of minutes to wait before the event loader loads the event to the operational data store. Default is `15`.
WAIT_BEFORE_RETRY task > Edit > Timer tab	Start_After	Number of minutes to wait before a retry attempt in case of an error in the workflow. Default is 1.

Service Level Agreement Violation Detector

If you define service level agreement (SLA) rules in the Operation Console, the SLA violation detector searches operational data store for violations of SLA rules. The operational data store event loader starts the SLA violation detector at the end of each event load process.

If the SLA violation detector finds violations, it stores the violation information in proprietary SLA tables in the operational data store. B2B Data Exchange displays information from the tables in the SLA Violations panel of the Dashboard. The violation information remains in the operational data store even if you modify or delete the SLA rule from the Operation Console.

The SLA violations detector reports violations either as soon as they occur or at the end of the time frame that you define in the SLA rule. For more information about SLA rules, see the *B2B Data Exchange Operator Guide*.

Dashboard and Reports Management Rules and Guidelines

When you work with the Dashboard and the operational data store, consider the following rules and guidelines:

- The Dashboard and Reports component supports only Oracle databases.
- By default, the session timeout for the Dashboard is 30 minutes. To ensure consistency with the Operation Console, if you change the session timeout for the Operation Console, change the value of the Dashboard session timeout property in the following file: `<DXInstallationDir>/tomcat/dx-dashboard/WEB_INF/web.xml`.

INDEX

private keys *(continued)*
    management 84
privileges
    administrator 47
    analyst 48
    developer 49
    operator 50

R

repository
    management 77
repository utility
    command syntax 94
    description 94
REST API 123
resume all endpoints 126
resume_all_dx_endpoints 126
runendpoint 108

S

schedule
    deleting 58
    editing 57
    paginations 55
    searching 57
    sorting 55
schedules utility 92
security
    overview 14
    secret token 15
    server shutdown 14
    server startup 14
    transformations 15
server statua 123
server utility
    description 119
    UNIX command syntax 120
    Windows command syntax 120
services utility
    command syntax 118
    description 118
system properties
    advanced exception handling 75
    dashboard and reports 128

system properties *(continued)*
    definition 66
    endpoints 68
    event monitors 70
    general 67, 72
    Informatica Intelligent Cloud Services 71
    managing 76
    PowerCenter 74

T

Toggle server 123

U

user
    definition 43
user account
    deleting 43
user authentication
    configuring 43
user authentication mode
    configuring 44, 45
    definition 42
user group
    definition 46
    managing 52
    privileges 47
users
    account properties 42
    policies 41
utilities
    console 118
    JMS Broker 121
    overview 117
    server 119
    services 118

W

workflow
    batch 55
workflows
    description 16