



Informatica® B2B Data Exchange  
10.2.2

# Operator Guide

© Copyright Informatica LLC 1993, 2022

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, the Informatica logo, Informatica Cloud, PowerCenter, PowerExchange, and Big Data Management are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

See patents at <https://www.informatica.com/legal/patents.html>.

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

#### NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2022-04-20

# Table of Contents

<b>Preface</b> .....	<b>8</b>
Informatica Resources. . . . .	8
Informatica Network. . . . .	8
Informatica Knowledge Base. . . . .	8
Informatica Documentation. . . . .	8
Informatica Product Availability Matrixes. . . . .	9
Informatica Velocity. . . . .	9
Informatica Marketplace. . . . .	9
Informatica Global Customer Support. . . . .	9
<b>Chapter 1: Document Processing</b> .....	<b>10</b>
Document Processing Overview. . . . .	10
Document Processing Stages. . . . .	10
Document Processing with PowerCenter. . . . .	11
Document Processing Customization with Profiles. . . . .	12
Document Tracking with Events. . . . .	12
Partner and Profile Setup Prerequisites. . . . .	13
<b>Chapter 2: Operation Console</b> .....	<b>15</b>
Operation Console Overview. . . . .	15
Connection and Login Guidelines. . . . .	15
Navigating Object Lists. . . . .	16
Sorting Object Lists. . . . .	16
Searching Object Lists. . . . .	16
Performing a Basic Search. . . . .	18
Performing an Advanced Search. . . . .	18
<b>Chapter 3: Partners and Profiles</b> .....	<b>20</b>
Partners and Profiles Overview. . . . .	20
Categories. . . . .	21
Partners. . . . .	21
Setting Up a Partner. . . . .	21
Searching for Partners. . . . .	23
Editing a Partner. . . . .	24
Deleting a Partner. . . . .	24
Adding an Account to a Partner. . . . .	24
Partner Promotion. . . . .	25
Creating a Portal User. . . . .	30
Searching for a Portal User. . . . .	31
Editing a Portal User. . . . .	31

Deleting a Portal User. . . . .	31
Profiles. . . . .	31
Setting Up a Profile. . . . .	32
Searching for Profiles. . . . .	33
Editing a Profile. . . . .	34
Deleting a Profile. . . . .	35
Enabling or Disabling a Profile. . . . .	35
Running a Batch Profile. . . . .	35
Profile Usage in Endpoints. . . . .	35
Delayed Events . . . . .	36
<b>Chapter 4: On-Boarding Checklists. . . . .</b>	<b>48</b>
On-Boarding Checklists Overview. . . . .	48
Creating an On-boarding Checklist. . . . .	49
Editing an On-boarding Checklist. . . . .	50
Monitoring the Status of On-boarding Checklists. . . . .	53
On-boarding Checklist Charts. . . . .	55
<b>Chapter 5: Managed File Transfer Web Users. . . . .</b>	<b>59</b>
Managed File Transfer Web Users Overview. . . . .	59
MFT Web User Properties. . . . .	60
Creating an MFT Web User. . . . .	64
<b>Chapter 6: Managed File Transfer Connections. . . . .</b>	<b>65</b>
Managed File Transfer Connections Overview. . . . .	65
AS2 MFT Connection Properties. . . . .	66
FTP MFT Connection Properties. . . . .	68
FTPS MFT Connection Properties. . . . .	70
HTTP MFT Connection Properties. . . . .	73
HTTPS MFT Connection Properties. . . . .	75
Mailbox MFT Connection Properties. . . . .	76
MQ MFT Connection Properties. . . . .	77
SMTP MFT Connection Properties. . . . .	78
SFTP, SCP, or SSH MFT Connection Properties. . . . .	78
Creating an MFT Connection. . . . .	82
Testing an MFT Connection. . . . .	82
<b>Chapter 7: Endpoints. . . . .</b>	<b>83</b>
Endpoints Overview. . . . .	83
Endpoint Types. . . . .	84
Common Endpoint Properties. . . . .	86
File Receive Endpoint Properties. . . . .	87
File Send Endpoint Properties. . . . .	89

JMS Receive Endpoint Properties. . . . .	89
JMS Send Endpoint Properties. . . . .	90
MFT Hosted Receive Endpoint Properties. . . . .	91
MFT Hosted Send Endpoint Properties. . . . .	94
MFT Remote Receive Endpoint Properties. . . . .	95
MFT Remote Send Endpoint Properties. . . . .	100
Configuration Variables in Endpoints. . . . .	104
Adding an Informatica Managed File Transfer Hosted Receive Endpoint. . . . .	105
Adding an Informatica Managed File Transfer Hosted Send Endpoint. . . . .	105
Adding an Informatica Managed File Transfer Remote Receive Endpoint. . . . .	106
Adding an Informatica Managed File Transfer Remote Send Endpoint. . . . .	107
Adding Local Endpoints. . . . .	108
Editing and Deleting Endpoints. . . . .	108
Processing Files with Informatica Intelligent Cloud Services Mappings. . . . .	109
Input File Parameters. . . . .	110
Formatting Options for Flat File Sources. . . . .	110
Processing Files with a Mass Ingestion Task. . . . .	111
Adding Local Endpoints. . . . .	111
Endpoint Error Events. . . . .	112
<b>Chapter 8: Events. . . . .</b>	<b>113</b>
Events Overview. . . . .	113
Event Actions. . . . .	114
Managing Events on the Event List Page. . . . .	114
Basic Event Search Properties. . . . .	115
Performing a Basic Search for Events. . . . .	115
Advanced Event Search Properties. . . . .	115
Performing an Advanced Search for Events. . . . .	116
Message Processing Event Types and Statuses. . . . .	117
Informatica Managed File Transfer Logs. . . . .	118
Archived Events. . . . .	118
Viewing Archived Events in the Operation Console. . . . .	118
<b>Chapter 9: Event Monitors. . . . .</b>	<b>119</b>
Event Monitors Overview. . . . .	119
Creating an Event Monitor. . . . .	119
Viewing Monitored Events. . . . .	124
<b>Chapter 10: Reconciliations. . . . .</b>	<b>125</b>
Reconciliations Overview. . . . .	125
Reconciliation Monitors. . . . .	125
Creating a Reconciliation Monitor. . . . .	126
Updating a Reconciliation. . . . .	129

Reconciliation Problems. . . . .	132
Monitoring and Resolving Timed-out Reconciliations. . . . .	133
<b>Chapter 11: Event Resubmission. . . . .</b>	<b>134</b>
Event Resubmission Overview. . . . .	134
Reprocessing an Event. . . . .	134
Resending an Event. . . . .	136
<b>Chapter 12: Audit and Authorization. . . . .</b>	<b>137</b>
Audit and Authorization Overview. . . . .	137
Audit Events. . . . .	137
Audit Record Properties. . . . .	138
Viewing Audit Records. . . . .	139
Legacy Audit Trail Events. . . . .	139
Legacy Audit Event Properties. . . . .	140
Viewing Legacy Audit Events. . . . .	140
Authorization. . . . .	140
Operator Action Properties. . . . .	141
Authorization Rules and Guidelines. . . . .	142
Approving or Rejecting Actions. . . . .	143
<b>Chapter 13: Advanced Exception Handling. . . . .</b>	<b>144</b>
Advanced Exception Handling Overview. . . . .	144
Advanced Exception Handling Example. . . . .	145
Advanced Exception Handling Issue Attributes. . . . .	145
Regular Exception Issue. . . . .	145
NOT Exception Issue. . . . .	146
Batch Exception Issues. . . . .	147
Reconciliation Exception Issue. . . . .	147
Creating an Advanced Exception Handling Issue. . . . .	148
Displaying Exception Handling Issue Details. . . . .	148
Reopening an Exception Issue. . . . .	148
<b>Chapter 14: Dashboard and Reports. . . . .</b>	<b>150</b>
Dashboard and Reports Overview. . . . .	150
Dashboard Filters. . . . .	151
Dashboard Panels. . . . .	151
Average Processing Time Panel. . . . .	153
Error Events by Account Panel. . . . .	155
Error Events by Account - All Errors Panel. . . . .	156
Error Events by Account - Unresolved Errors Panel. . . . .	157
Error Events by Event Status Panel. . . . .	158
Error Events by Event Status - All Errors Panel. . . . .	159

Error Events by Event Status - Unresolved Errors Panel. . . . .	160
Error Events by Event Type Panel. . . . .	161
Error Events by Event Type - All Errors Panel. . . . .	162
Error Events by Event Type - Unresolved Errors Panel. . . . .	163
Error Events by Partner Panel. . . . .	164
Error Events by Partner - All Errors Panel. . . . .	165
Error Events by Partner - Unresolved Errors Panel. . . . .	166
Error Events Distribution Panel. . . . .	168
Error Rate Panel. . . . .	169
Events by Account Panel. . . . .	170
Events by Event Status Panel. . . . .	170
Events by Event Type Panel. . . . .	172
Events by Partner Panel. . . . .	173
Events Distribution Panel. . . . .	173
SLA Violations Panel. . . . .	175
Tasks Panel. . . . .	177
Dashboard Panel CSV File Structure. . . . .	178
Managing the Dashboard. . . . .	179
<b>Chapter 15: Service Level Agreement Management. . . . .</b>	<b>180</b>
Service Level Agreement Management Overview. . . . .	180
Service Level Agreement Rules. . . . .	180
Service Level Agreement Rule Properties. . . . .	181
Service Level Agreement Rule Examples. . . . .	182
Service Level Agreement Violations. . . . .	183
Managing Service Level Agreement Rules. . . . .	184
Viewing Service Level Agreement Violations. . . . .	184
Selecting SLA Rules for the Partners Portal. . . . .	185
<b>Chapter 16: Glossary. . . . .</b>	<b>186</b>
<b>Index. . . . .</b>	<b>189</b>

# Preface

The *B2B Data Exchange Operator Guide* provides information about the operational tasks available in the B2B Data Exchange Operation Console. It assumes that you have a working knowledge of the format and requirements of the messages processed in B2B Data Exchange. It also assumes that you are familiar with message processing requirements of the trading partners.

## Informatica Resources

### Informatica Network

Informatica Network hosts Informatica Global Customer Support, the Informatica Knowledge Base, and other product resources. To access Informatica Network, visit <https://network.informatica.com>.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- 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 search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit <https://kb.informatica.com>. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

### Informatica Documentation

To get the latest documentation for your product, browse the Informatica Knowledge Base at [https://kb.informatica.com/\\_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx](https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx).

If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).



## Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access PAMs at

<https://network.informatica.com/community/informatica-network/product-availability-matrixes>.

## Informatica Velocity

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

If you are an Informatica Network member, you can access 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](mailto:ips@informatica.com).

## Informatica Marketplace

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

## Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:

<http://www.informatica.com/us/services-and-training/support-services/global-support-centers>.

If you are an Informatica Network member, you can use Online Support at <http://network.informatica.com>.

# CHAPTER 1

## Document Processing

This chapter includes the following topics:

- [Document Processing Overview, 10](#)
- [Document Processing with PowerCenter, 11](#)
- [Document Processing Customization with Profiles, 12](#)
- [Document Tracking with Events, 12](#)
- [Partner and Profile Setup Prerequisites, 13](#)

### Document Processing Overview

B2B Data Exchange processes complex structured and unstructured documents, such as NACHA and EDI documents, SWIFT and HIPAA transactions, and so on. You can receive documents from partners for processing or process documents to send out to partners.

You can use the Operation Console to customize, manage, and monitor processing of similar types of documents for different partners. The Operation Console enables you to perform the operational and administrative tasks required to process the documents, such as setting up and managing partners, workflows, and profiles, and monitoring the events that are generated when the documents are processed.

The B2B Data Exchange developer can create PowerCenter workflows to process documents. These workflows typically include Data Exchange Transformations and Unstructured Data Transformations. In B2B Data Exchange, the administrator can create a workflow that represents the PowerCenter workflow. The Data Exchange Server uses profiles to determine the workflow and parameters to use to process documents for a partner.

### Document Processing Stages

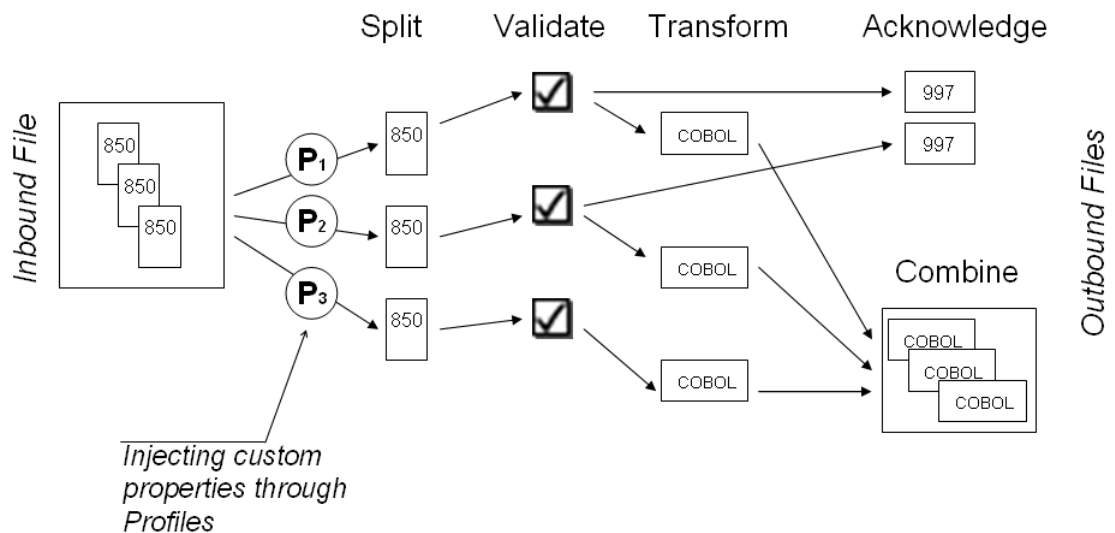
Although each enterprise can have specific rules and guidelines for managing partners and processing documents, document processing in B2B Data Exchange typically includes the following stages:

1. **Create partners that represent customers or applications.** For more information, see [“Partners” on page 21](#).
2. **Create accounts that represent customer departments or divisions.** For more information, see [“Adding an Account to a Partner” on page 24](#).
3. **Create profiles to associate a partner or an account with a workflow.** For more information, see [“Profiles” on page 31](#).

4. **Create endpoints for partners or accounts.** For more information, see [“Endpoints Overview” on page 83.](#)
5. **Test and enable the profiles that you created.** You can run the workflow that is associated with a profile in a test environment to process test documents.
6. **Review the events that are generated when you run the profiles.** For more information, see [“Managing Events on the Event List Page” on page 114.](#)
7. **If the profile requires delayed events, create delayed processing rules.** For more information, see [“Delayed Events ” on page 36.](#)
8. **Create on-boarding checklists to manage partner creation and maintenance.** For more information, see [“On-Boarding Checklists Overview” on page 48.](#)

## Document Processing with PowerCenter

The following diagram shows the transformation of EDI purchase order requests (X12 850) to COBOL format:



Processing the purchase order requests includes the following stages:

1. B2B Data Exchange receives the document file from the partner and routes the document to the PowerCenter workflow.
2. If the inbound file contains multiple X12 850 documents, the PowerCenter workflow splits the file to individual X12 850 documents.
3. The PowerCenter workflow runs a B2B data transformation to validate each document.
4. If required, the PowerCenter workflow generates an EDI Acknowledgement document (997) after the validation.
5. If no errors are encountered, the PowerCenter workflow runs a B2B data transformation that transforms the documents to COBOL format.
6. The PowerCenter workflow combines the individual COBOL documents into a single COBOL file.
7. The PowerCenter workflow returns the 997 files to B2B Data Exchange.
8. B2B Data Exchange delivers the 997 documents to the partner.

# Document Processing Customization with Profiles

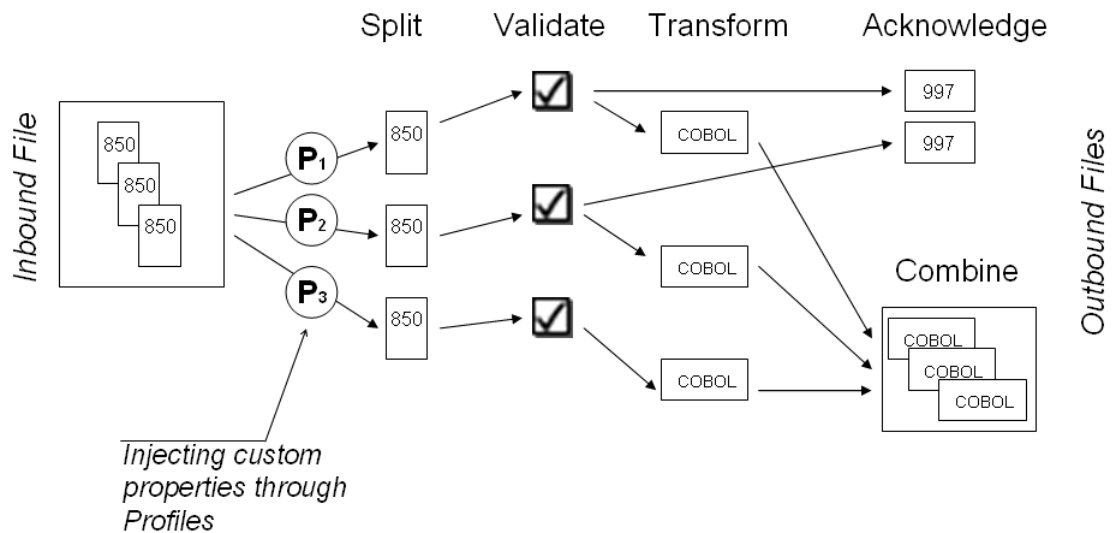
Normally, B2B Data Exchange receives documents from multiple partners for processing, and processes documents to send to multiple partners. Documents from different partners can require the same PowerCenter transformation but with customized handling needs. For example, not all customers that require transformation of EDI documents to COBOL files also require acknowledgment documents.

Profiles enable you to customize the transformation process according to parameters that define the transformation process.

You can use the following parameter types:

- **Validation parameters.** Data validation within the document. For example, the parameter can set the control sequence number or determine the version of an EDI document.
- **Enrichment parameters.** Values to add to the document. For example, the parameter can contain data for the EDI ISA control envelope when an EDI output is generated.
- **Control parameters.** Evaluate various conditions during the transformation. For example, the parameter can control how to generate an EDI acknowledgement or how to process documents in a test environment.

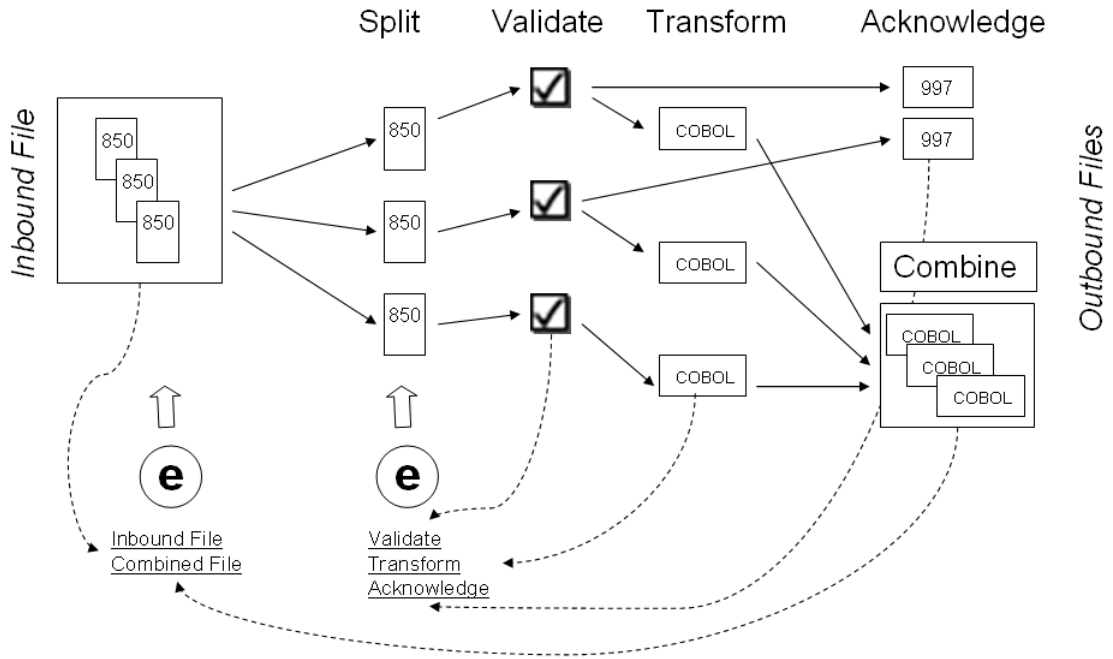
The following diagram shows how profiles customize the transformation process:



# Document Tracking with Events

The B2B Data Exchange developer sets up workflows to generate events at different stages of the document processing. These events help ensure that documents are processed correctly. While the documents are processed, the Data Exchange Server generates events that show the status of the documents in each processing stage. You can view and analyze the events in the Operation Console. You can also create event monitors that notify you of any problems that occurred while processing the documents.

The following diagram shows events that are generated during the document processing:



## Partner and Profile Setup Prerequisites

Before you can set up customers as partners in B2B Data Exchange, you need information about the organization and requirements. To process documents for partners, you also need information about the transformation objects that are involved with processing these documents.

The following table includes the information that you need to set up a profile:

Type	Description
Workflow Name	Name of the PowerCenter workflow to use when you process documents for each partner.
Processing Requirements	Specific requirements for running the profile. These can include acknowledgement requirements or whether a profile runs in test mode or production mode.
Event Hierarchy Documentation	Outline of the events that should be generated when the documents are processed. When you view these events, the event hierarchy documentation can help you interpret the events and determine how to resolve errors.
Delayed Processing Rules	Rules and conditions for delaying events. Delayed processing might be required if documents must be processed in groups, or when processing large documents may take a long time.

The following table includes the information that you need to set up a partner:

Type	Description
Customer Name	Name of the customer. This name is used as the partner name in B2B Data Exchange.
Departments	List of customer departments that need to send or receive documents. Each department name is used as an account name in B2B Data Exchange. <b>Note:</b> <ul style="list-style-type: none"><li>- A partner must include at least one account.</li><li>- You can define more than one account for a single partner.</li></ul>
Processing Requirements	Specific instructions or rules for processing documents. These can include requirements such as sending acknowledgements at specific time intervals.

## CHAPTER 2

# Operation Console

This chapter includes the following topics:

- [Operation Console Overview, 15](#)
- [Connection and Login Guidelines, 15](#)
- [Navigating Object Lists, 16](#)
- [Sorting Object Lists, 16](#)
- [Searching Object Lists, 16](#)

## Operation Console Overview

The Operation Console is a Web-based application to manage the document processing operation and to manage users and resources.

The Operation Console contains two areas:

Area	Description
Left pane	Navigator. Enables you to navigate between tasks that you can perform in the Operation Console.
Right pane	Current page. Main work area in which you perform the tasks that you select in the Navigator.

## Connection and Login Guidelines

When you connect to the Operation Console, follow these guidelines:

- The minimum screen resolution requirement is 1200 X 800.  
**Note:** If your browser is Microsoft Internet Explorer version 10 or version 11, do not use compatibility mode to view the Operation Console. Ensure that the setting is non-compatibility mode.
- You must have a user account to log in to the Operation Console. The role that is assigned to your user account determines the tasks that you can perform.
- You can access the Operation Console with one of the following URLs:

```
http://<HostName>:<HTTPS-PortNumber>/dx-console  
http://<HostName>:<PortNumber>/dx-console
```

- For security and resource allocation purposes, B2B Data Exchange ends the user session if there is no activity for 30 minutes.
- If you are unable to connect to the Operation Console, or if you see incorrect data after you connect, verify that the database settings in the following files are identical:

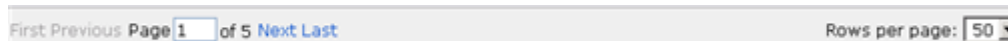
```
<DataExchangeInstallationDir>/conf/dx-configuration.properties
<DataExchangeInstallationDir>/tomcat/shared/classes/dx-configuration.properties
```

These files contain the PowerCenter repository connection settings.

## Navigating Object Lists

By default, the Operation Console displays a maximum of 15 objects in a page. You can change this number to display more or less objects in each page.

The options at the bottom of each page display the current page, the total number of pages, and enable you to move to the next or previous page.



1. To change the maximum number of rows that are displayed in each page, select the relevant value in the **Rows per page** field.
2. If the list contains more objects than the number you specified, click **Next** to navigate to the remaining objects.
3. To return to the previous object list, click **Previous**.

## Sorting Object Lists

You can sort an object list to view objects according to ascending or descending order.

To sort a list of objects, click the title of the column by which you want to sort. When you sort a list of objects by a column, an arrow indicates whether the column is sorted in ascending or descending order.

## Searching Object Lists

Can search for objects in any list in the Operation Console. This functionality enables you to filter object lists and view only the objects that match the search criteria. You can perform a basic search, in which you specify a simple text string to search. You can also perform an advanced search, in which you search multiple object properties.

### Note:

- This functionality is not available while you add or edit an object.
- Searching for an ID property is numeric and therefore requires an exact match. All other fields enable a partial string search.



The following table shows the properties that you can search for the different objects:

<b>Object</b>	<b>Basic Search Properties</b>	<b>Advanced Search Properties</b>
Application	Name	No advanced search
Audit Trail Event	<ul style="list-style-type: none"> <li>- Event ID</li> <li>- Subject</li> <li>- Event Status</li> </ul>	No advanced search
Category	Name	No advanced search
Endpoint	Name	No advanced search
Event	<ul style="list-style-type: none"> <li>- Event ID</li> <li>- Event Type</li> <li>- Event Status</li> <li>- Partner Name</li> <li>- Account Name</li> <li>- Account Number</li> <li>- Profile Name</li> </ul>	<ul style="list-style-type: none"> <li>- Reconciliation Status</li> <li>- Reconciliation Type</li> <li>- Parent Event ID</li> <li>- Event Status Description</li> <li>- Document Receipt Date</li> <li>- Show Child Events</li> <li>- Event Attributes</li> </ul>
Event Monitor	<ul style="list-style-type: none"> <li>- Name</li> <li>- Categories</li> </ul>	<ul style="list-style-type: none"> <li>- Partner Name</li> <li>- Workflow Name</li> <li>- Event Type</li> <li>- Include/Exclude All Partners</li> <li>- Include/Exclude All Workflows</li> </ul>
On-Boarding Checklist	Name	<ul style="list-style-type: none"> <li>- Partner Name</li> <li>- Workflow Name</li> <li>- State</li> <li>- Deadline</li> <li>- Start Date</li> <li>- Due Date</li> <li>- End Date</li> </ul>
Partner	<ul style="list-style-type: none"> <li>- Partner ID</li> <li>- Partner Name</li> </ul>	Partner Categories
Profile	<ul style="list-style-type: none"> <li>- Profile ID</li> <li>- Profile Name</li> <li>- Partner Name</li> <li>- Workflow Name</li> </ul>	<ul style="list-style-type: none"> <li>- Account Name</li> <li>- Profile Categories</li> </ul>
User	<ul style="list-style-type: none"> <li>- User ID</li> <li>- User Name</li> <li>- User Role</li> </ul>	User Group

Object	Basic Search Properties	Advanced Search Properties
User Event	<ul style="list-style-type: none"> <li>- Event ID</li> <li>- Partner Name</li> <li>- Profile Name</li> <li>- Event Type</li> <li>- Event Status</li> <li>- Event Status Comments</li> <li>- Event Attribute</li> <li>- Event Parent ID</li> <li>- Account Name</li> <li>- Account Number</li> <li>- Reconciliation Status</li> <li>- Description</li> <li>- Receipt Date</li> </ul>	<ul style="list-style-type: none"> <li>- Subject</li> <li>- Generation Date</li> <li>- Show Parent Events</li> </ul>
Workflow	<ul style="list-style-type: none"> <li>- Workflow ID</li> <li>- Workflow Name</li> </ul>	Application Name

## Performing a Basic Search

When you perform a basic search, you specify a simple text string to search in predefined properties of the specific object type. You cannot select the properties in which to search.

1. If the page is in Advanced Search mode, click **Basic Search**.
2. In the Find field, enter a text string and click **Go**.

The Operation Console displays objects whose properties contain the text string that you specified.

**Note:** The search properties that are included in the basic search may not be displayed in the columns of the search results. For example, when you perform a basic search for events, the Operation Console searches in the Account Number property, even though the Account Number column is not displayed in Event List page or the Event Details page.

3. To clear the Find field and display all objects in the page, click **Reset**.
4. To display the last search results, click **Reload**.

## Performing an Advanced Search

When you perform an advanced search, you select which properties of the specific object type to search, and specify text strings to search in each property.

1. If the page is in Basic Search mode, click **Advanced Search**.
2. Define the search criteria for the properties in which you want to search.

**Note:**

- For text fields, you can enter partial strings as the search criteria.
- Searching for an ID property is numeric and therefore requires an exact match.
- For list fields, press **SHIFT** to select multiple values.

3. To find objects that match any of the properties for which you defined search criteria, select the **OR** operator.

To find objects with properties that contain all of the specified text strings and selections, select the AND operator.

4. To find objects that match all of the properties for which you defined search criteria, select the **AND** operator.
5. Click **Go**.  
The Operation Console displays the list of objects that match the search criteria.
6. To clear the Find field and display all objects in the page, click **Reset**.
7. To display the last search results, click **Reload**.

## CHAPTER 3

# Partners and Profiles

This chapter includes the following topics:

- [Partners and Profiles Overview, 20](#)
- [Categories, 21](#)
- [Partners, 21](#)
- [Profiles, 31](#)

## Partners and Profiles Overview

A partner represents an external or internal entity that sends documents to be processed or receives processed documents from B2B Data Exchange. A partner can be an organization such as a vendor or a customer, or an internal system such as an accounting application or an ERP system.

Each partner contains one or more accounts. In a customer organization, an account can be a division, a department, or a subsidiary. In an internal system, an account can be a customer ID or a vendor code.

A workflow represents the transformation logic required to process documents for a partner. The B2B Data Exchange developer creates a PowerCenter workflow to process the documents and a workflow in the B2B Data Exchange Operation Console to represent the PowerCenter workflow.

Profiles enable you to associate a workflow with a partner or an account. A profile defines how to process a document for a partner or an account. You can add parameters to the profile that customize the selected workflow for a partner. When you run a workflow that is associated with a profile, the PowerCenter workflow processes the documents for the partner that is defined in the profile.

You can restrict access to partners, accounts, and profiles with categories. Categories are classifications that can represent regional division or departments in the organization. When you assign categories to objects, you also restrict access to related objects, such as events, endpoints, and SLA rules. The B2B Data Exchange administrator assigns categories to user groups to determine which users can access the objects.

# Categories

A category controls access to partners, accounts, and profiles. You assign categories to the objects to determine the users that can view or modify the objects.

By default, accounts inherit categories from the partner and profiles inherit categories from the account. You can choose to manage individual account or profile categories. Inherited categories for accounts and profiles appear in read-only mode.

When you assign categories to objects, you also restrict access to the following related objects:

- Endpoints. Inherit categories from the account.
- Events. Inherit categories from the account.
- Monitors. Inherit categories from the partner.
- SLA rules. Inherit categories from the account.

When you add an account to a partner, B2B Data Exchange sets the account categories according to the category management mode. For example, if you apply partner categories to the accounts, new accounts inherit the partner categories. If you add or remove categories from the partner, B2B Data Exchange applies the change to all accounts for that partner.

If you change the category management mode to inherit from the partner or account, all existing categories for the profile or account are overridden. If you change the category management mode to manage individual account categories, you must save the partner before you can assign categories to individual accounts.

The B2B Data Exchange administrator creates categories and grants permissions for the categories to user groups. Objects without categories are accessible by all B2B Data Exchange users. Objects with categories are accessible only by users with permissions to one or more categories.

# Partners

Partners are the entities that send documents to B2B Data Exchange for processing and receive the processed documents in return. A partner can be an organization like a vendor or customer. Internal systems, like accounting systems and ERP systems, can also be defined as partners.

B2B Data Exchange provides the following functions for working with partners:

- Setting up a partner
- Searching for partners
- Editing a partner
- Deleting a partner
- Adding an account to a partner
- Promoting partners

## Setting Up a Partner

Setting up a partner explains how to add a partner to the B2B Data Exchange repository.

1. In the Navigator, click Partner Management > Partners.
2. Click New Partner to create a partner, or click a Copy icon to copy an existing partner.

On all Operation Console screens, fields marked with an asterisk (\*) are mandatory.

3. On the Create Partner page, enter a name for the partner.  
The partner name can be up to 60 characters and can include spaces and special characters.
4. In the Description field, enter any relevant information or a description of the partner.  
You can enter up to 255 characters in the Description field.
5. To flag this partner as ready for promotion, click the Ready to be promoted checkbox.
6. To manage contact information for this partner, click Contacts.
7. To add a contact, click Add Contact. The Contact Information form opens.
8. Complete the form according to the following table, and click Save. You can edit an existing contact.

Property	Description
Name	Name of the contact person. The contact name can contain up to 60 characters.
Description	Description of the contact person. The description can be up to 255 characters.
Title	Title of the contact person. The title can contain up to 255 characters.
Address	Address of the contact person. The address can contain up to 255 characters.
Mobile	Mobile phone number of the contact. Can be up to 20 characters.
Business Phone	Business telephone number of the contact person. The telephone number can contain up to 20 characters.
Fax	Fax number of the contact person. Fax number can be up to 20 characters.
Email	Email address of the contact person. The email address can contain up to 255 characters.

9. To update additional information about this partner, click Additional Information and edit the contents of the form. Click Save.  
The content of the additional information form is dynamic and is controlled by the Administrator.
10. To assign categories to the partner, click Categories.
11. On the Categories tab, choose whether to apply partner categories to all accounts or to manage categories for individual accounts.
12. Select categories in the Available Partners Categories to associate with the partner and click the right arrow to move them to the Selected Partner Categories column.  
Use the Shift key to select multiple categories.
13. Click Save.
14. To add an account to the partner, click Accounts > Add Account.  
The Create Account form opens.  
**Note:** A partner must have at least one account.

## Searching for Partners

You can search for partners by name and other properties.

1. In the Navigator, click Partner Management > Partners. The Partners screen appears showing all partners in descending order of Partner Id.
2. To search for a specific partner by name, enter your search string in the Find field and click Go.
3. To search for partners by Partner Promotion status, Partner Categories, or Custom Attributes, click Advanced Search.

4. To search by Partner Id or Partner Name, enter your search string in the appropriate field and click Go.
5. To search for partners by Partner Promotion status, select a value from the list. The default value is All.
6. You can search for partners using up to three custom partner or account attributes in one search. To search by custom attributes, click the Browse button (...).

The Custom Attributes Search Criteria window appears.

7. On the Customs Attribute Search Criteria screen, select a Partner/Account, then an Attribute, then an Operator. Type in the search value of the attribute. Repeat for up to three custom attributes. Click OK. The Partners Screen reappears.
8. On the Partners screen, choose an operation for the search – either Or (default) or And . This operator applies to all search criteria on the screen, including Custom Attributes.

9. The Operation Console displays a list of partners matching your search criteria. To edit, copy or delete a partner, click on the appropriate icon at the right side of the screen.
10. To display all the events sent to or received from a specific partner in the Partners screen, click the Events link in the desired partner's row. The Operation Console shows the events for the selected partner in the Event List screen.

## Editing a Partner

To edit a partner, click Partner Management > Partners and click Edit for the partner to edit. Modify the properties and click Save.

## Deleting a Partner

To delete a partner, click **Partner Management > Partners** and click the **Delete** icon for the partner you want to remove. Confirm the deletion. If the partner has portal users, confirm that you want to delete the portal users.

## Adding an Account to a Partner

You can add several accounts to a partner. Each account can have separate categories and additional information. Each account can send and receive documents.

1. In the Navigator, click Partner Management > Partners.
2. Click New Partner to create a partner, or click Edit for an existing partner.
3. Click Accounts > New Account.
4. In the General tab, enter the account number and name.

The combination of account number and account name must be unique within a partner. The account number can be up to 60 characters. The account name can be up to 60 characters and can contain spaces and special characters.
5. To configure additional information for the account, click Additional Information and fill in the form.

For more information about customizing the partner and account information, see the *B2B Data Exchange Administrator Guide*.
6. To assign the account to categories, click Categories.
7. From the Available Account Categories column, select the categories to assign to the account and click the right arrow to move them to the Selected Account Categories column.
8. Click Save.
9. Repeat steps 3 through 8 to add more accounts to a partner.
10. On the Create Partner or Update Partner page, click Save to save the list of accounts added to the partner.

## Account Uniqueness

The `dx.system.account.uniqueness` system property indicates whether an account is unique within the scope of the partner or within the scope of B2B Data Exchange.

If the `dx.system.account.uniqueness` system property is set to PARTNER, the account is unique within the scope of the partner. You can assign the same account number to multiple partners. If you do, the B2B Data Exchange Server determines the profile based on the application, partner, and account number.



If the `dx.system.account.uniqueness` system property is set to `SYSTEM`, the account is unique within the scope of B2B Data Exchange and you cannot use the same account number more than once. If the `dx.system.account.uniqueness` system property is set to `SYSTEM`, the B2B Data Exchange Server determines the profile based on the application and account number.

## Default Outbound Endpoint for Account

If an account has several outbound endpoints associated with it, you can specify a default outbound endpoint for the account.

You can edit the account settings and select a Default Outbound Endpoint. B2B Data Exchange uses the default endpoint to route outgoing files.

## Partner Promotion

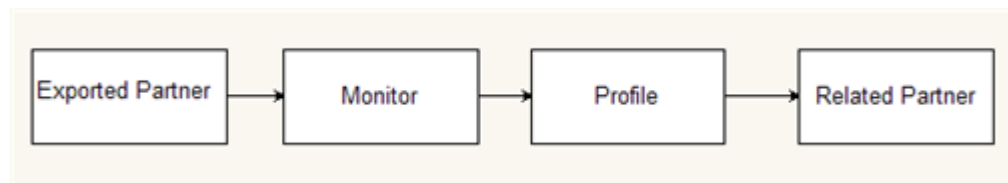
Partner promotion enables you to export one or more partners and their related entities from one environment to another. For example, you can promote partners from development to test or from test to production. Partner promotion consists of exporting partners from the source environment and importing them into the target environment.

After you create and test a partner and its associated entities in the test environment you can flag it as "Ready to be promoted" on the Update Partner screen. You can later search for all the partners that you marked and export them all at once.

The partner export process creates a file of partners to be exported as well as partners and entities associated with the partners. The following associated entities are exported with the partners:

- Accounts
- Profiles
- Endpoints
- Monitors
- Workflows

The export file contains partners that are related to the exported partners. A related partner is a partner that is connected to an exported partner through a monitor that executes a profile that refers to the related partner. The following figure illustrates the connection between an exported partner and a related partner:



In addition to associated entities and related partners, the export process transparently exports some additional entities that are required by the imported partners to function properly. These entities are:

- Applications
- Event attributes
- Categories
- Partner and Account custom attributes
- Schedules
- Calendars

- Event Statuses
- Event Types

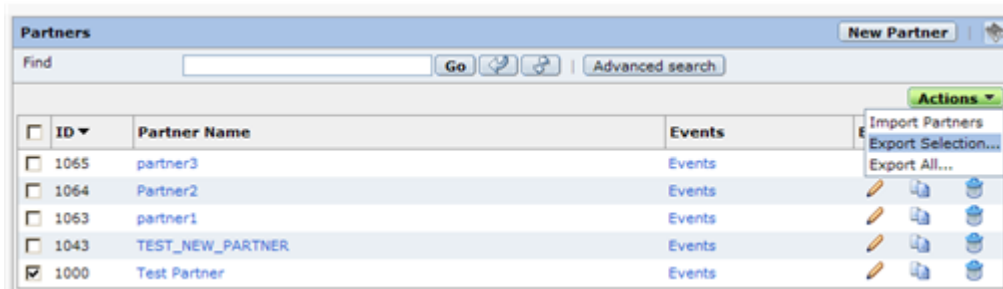
When importing a partner file, the import process may discover that a conflict exists between an entity in the import file one with the same identity in the target environment. B2B Data Exchange provides you with several choices to deal with conflicts:

- Import and replace – the entity from the file is imported and replaces the entity in the target environment.
- Don't import – the entity from the import file is skipped.
- Abort the import – the import process is aborted.

## Exporting Partners

Create a file of the partners that you want to export.

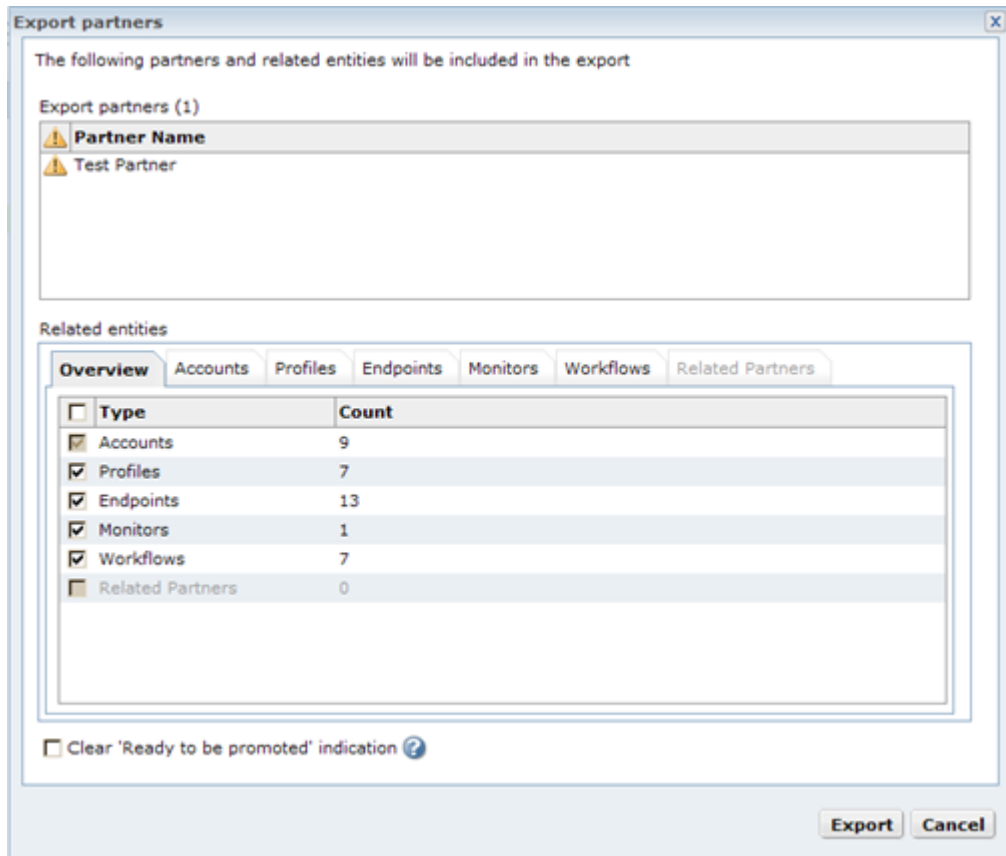
1. In the Navigator, click Partner Management > Partners.
2. Choose one of the following options to select the partners for promotion:
  - Perform a basic or advanced search and select some partners from the results of the search.
  - Using the advanced search you can find the partners marked as Ready to be Promoted. To do this, select "Ready to be Promoted" from the list in the Partner Promotion field.
3. In the Partners page, select an action from the list.



Choose one of the following actions:

- **Export selection.** This action exports only those partners that you selected.
- **Export all.** This action exports all the partners appearing in all pages of the displayed list.

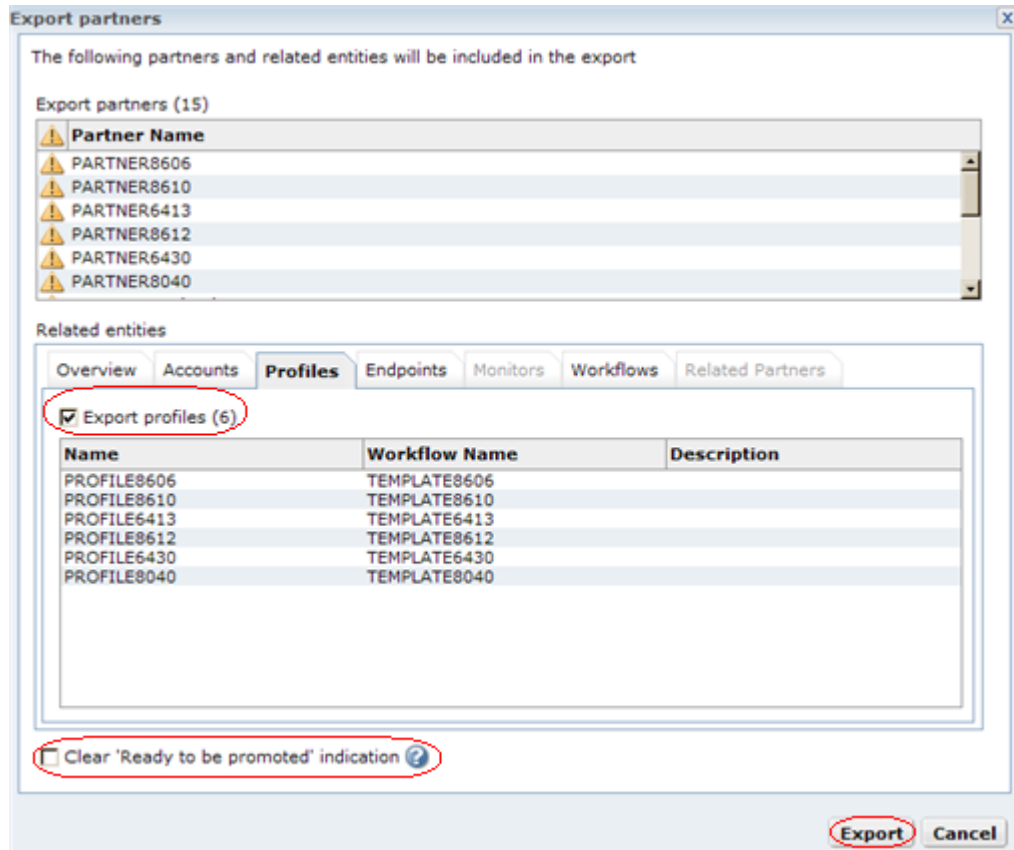
4. The Operation Console displays the Export partners page:



The top half of the page displays the partners to be exported. A warning symbol appearing to the left of a partner name indicates that this partner is not marked as 'Ready to be promoted'. This notice is informational only.

The bottom half of the page shows all the related entities that are associated with the partners to be exported.

5. To prevent the export of a related entity, for example profiles, uncheck the Export profiles checkbox in the Profiles tab or the Overview tab of the Export partners page. You cannot prevent the export of accounts.



6. To clear the 'Ready to be promoted' indications that may be set for some of the exported partners, click the "Clear 'Ready to be promoted' indication" checkbox. By default, these indications are not cleared.
7. To export the partners, click Export.  
If the export succeeds, the Operation Console displays a message indicating that the promotion export file was created successfully.
8. Click Download to download the promotion export file.  
The file download window opens.
9. Click Save to save the file.
10. When the download is complete, the Download Complete window opens. Click Close.

**Note:** You are limited to exporting a total of 500 accounts in one file. If you exceed this limit, the Operation Console displays an error message. There are two workarounds:

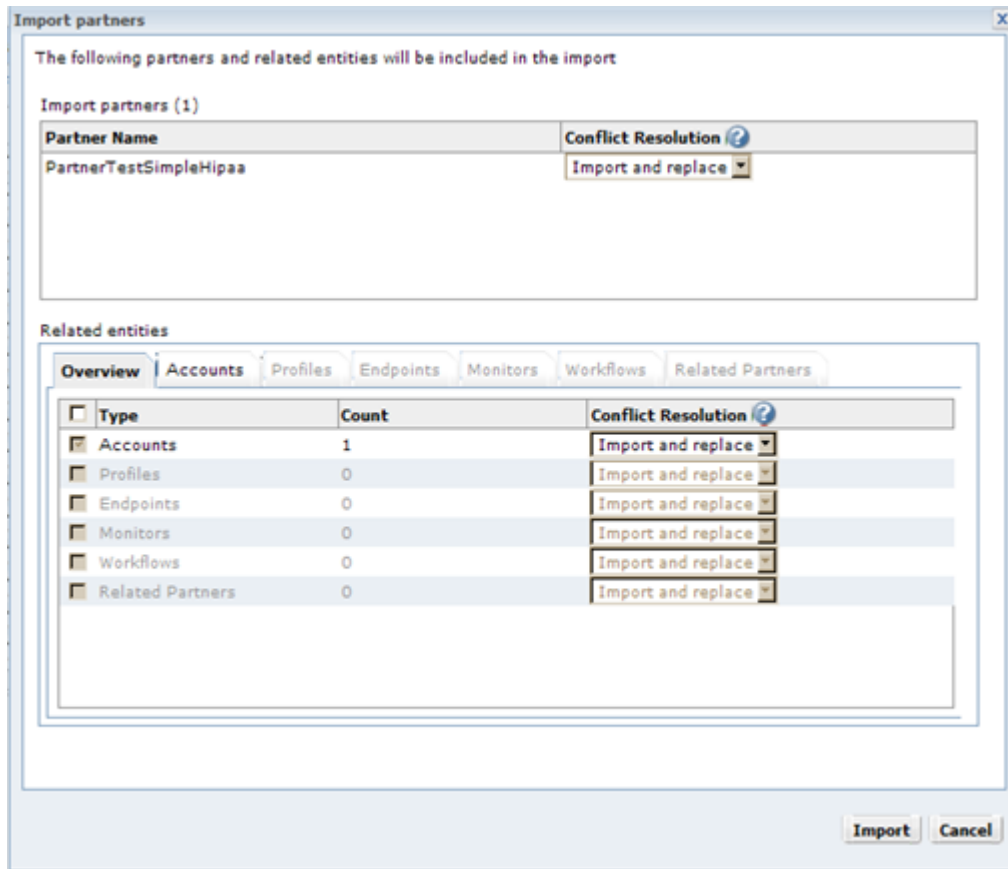
- Reduce the number of partners in the file until there are fewer than 500 accounts.
- Ask your system administrator to export the partners using the partner import/export command line utility. The limit on the number of accounts does not apply to this utility.

If you export objects that include MFT endpoints, perform an export operation in both the B2B Data Exchange operation console and the Managed File Transfer administrative console. PowerCenter entities, such as mappings, workflows, and Data Transformation services, are not exported with partners and have to be exported/imported separately.

## Importing Partners

Use the Import action on the Partners page to import a partner file into a new environment.

1. Browse to the environment where you want to import the partners. Click OK.
2. In the Navigator, click Partners > Partners.
3. Click Actions > Import Partners.  
The Import Partner page appears.
4. Browse to the promotion export file and click Open > Upload. The Import partners page appears.



5. The conflict Resolution column of the Overview tab lists all the conflicts. To resolve a conflict, choose one of the following actions:
  - Import and replace. Replace existing entities with imported entities.
  - Don't import. Do not import existing entities.
  - Abort. Cancel the import process.
6. The Related Entities section of the Partners page displays a list of related entities that were exported with the partners and, by default, will be imported. To prevent the import of a related entity, click a related entity tab and uncheck the Import checkbox.
7. Click Import.  
The Import Partner Results page displays, showing what entities that the import process created.

Consider the following rules and guidelines when you import partners:

- You might encounter difficulties when importing a partner file that was created by the command line import/export utility previous versions of B2B Data Exchange. If so, export the partners again using the current and re-import the file.
- The import process is limited to handling files with a maximum of 500 accounts. If your file exceeds this limit, the Operation Console displays an error message directing you to reduce the number of accounts in the file. To import a file with more than 500 accounts, ask your System Administrator to import it for you using the import/export command line utility.
- MFT endpoints are imported in disabled status. MFT endpoint information is stored in the B2B Data Exchange repository and in the B2B Managed File Transfer repository. If you import objects that include MFT endpoints, perform an export operation in both the B2B Data Exchange operation console and B2B Managed File Transfer administrative console. Make sure to import the objects first to MFT and then to Data Exchange. For more information about importing and exporting MFT endpoints, see the *B2B Managed File Transfer User Guide*.
- Non-MFT endpoints are imported as-is, depending on the endpoints' enable/disable status during import.
- PowerCenter entities, such as mappings, workflows, and Data Transformation services, are not included in the exported partners file. You have to be export and import them separately.
- If you import partners from B2B Data Exchange 9.5.0 or earlier, account categories are not imported and the accounts inherit categories from the partner after the import process.

## Creating a Portal User

Create portal users so that partners can access the Partners Portal. You can create one or more Partners Portal users for any partner.

1. In the **Navigator**, click **Partner Management > Portal Users**.

2. To create a new user, click **New Portal User**.

On all Operation Console screens, fields marked with an asterisk (\*) are mandatory.

3. On the **Create Portal User** page, enter an email as the User ID for the partner.

**Note:** The email must be unique, is not case sensitive, and cannot be changed later.

4. Enter a name for the portal user.

The user name can be up to 255 characters and can include spaces and special characters.

5. In the **Partner** field, select an existing partner.

6. To add the portal user to a user group, in the User Groups tab, select a user group from the **Available User Groups** panel and transfer the group to the **Selected User Groups** panel.

When you assign the portal user to a user group, the portal user obtains all the privileges associated with the user group. You can select more than one user group. If you do not assign a user group, the portal user can only view the Dashboard in the Partners Portal.

7. To add the user and invite the user to access the portal, click **Save and Send Invitation**.

The message is sent and an invitation message appears with the date and time that the message was sent. It may take a few minutes for the invitation to arrive to the portal user.

8. In the invitation message, click **OK**.

9. To save the changes and to add the portal user to the list, click **Save**.

The user appears in the **Portal Users** list.

10. To cancel any changes since the last save, click **Cancel**.

## Searching for a Portal User

You can search for partners by name and other properties.

1. In the Navigator, click **Partner Management > Portal Users**. The Portal Users screen appears showing all portal users in descending order of User ID.
2. To search for a specific portal user by name, user ID, or partner name, enter your search string in the **Find** field and click **Go**.
3. The Operation Console displays a list of portal users matching your search criteria. To edit or delete a portal user, click the appropriate icon at the right side of the screen.

## Editing a Portal User

To edit a portal user, click **Partner Management > Portal Users** and click **Edit** for the portal user to edit. Modify the properties and click **Save**.

## Deleting a Portal User

To delete a portal user, click **Partner Management > Portal Users** and click the **Delete** icon for the portal user you want to remove. Confirm the deletion.

# Profiles

A profile associates a workflow to a partner or account. It also defines the properties that customize that workflow to process documents for the associated partner or account.

When you set up a profile, use the following rules and guidelines to associate a workflow with a partner or account:

- To process different types of documents for a partner or account, you can associate multiple workflows with a partner or account.
- To process similar documents for different partners or accounts, you can associate a workflow with multiple partners or accounts. You can also associate a workflow with multiple accounts of the same partner.
- Each profile must have a unique combination of application, workflow, partner, and account.
- You cannot associate a partner or account with more than one workflow of the same application.
- You cannot associate a workflow with a partner and an account of that partner. For example, PartnerOne has AccountOne and AccountTwo. If you create a profile to associate WorkflowOne with AccountOne, you can create another profile to associate WorkflowOne with AccountTwo. If you create a profile to associate WorkflowOne with PartnerOne, you cannot create a profile to associate WorkflowOne with AccountOne or AccountTwo.

You can set up a profile in the following ways:

- **Create a profile.** You can create a profile to associate a workflow with a partner or an account.

- **Copy a profile.** When you copy a profile, the new profile contains the same description, workflow, status, categories, and workflow parameters. You must associate the workflow with a different partner or account. If you plan to use the same workflow, description, and categories for a new profile, copying a profile can be a quicker way to create a profile.

The Workflow Parameters tab of the Profile page displays the list of parameters associated with a selected workflow. A developer sets up the workflow parameters when the creating a PowerCenter workflow. You can use these attributes to specify additional event information at run time.

Usually, an administrator sets up the event attributes on the Operation Console. Contact the B2B Data Exchange administrator for information about the event attribute requirements for a profile.

## Setting Up a Profile

1. In the **Navigator**, click **Partner Management > Profiles**.
2. Click **New Profile**.  
The **Create Profile** page appears.
3. Enter a name for the profile, which can contain up to 60 characters.
4. In the **Description** field, enter any relevant information or a description of the profile. The description can be up to 255 characters.
5. To select a partner, click the **Browse** button and select a partner from the list. Click **OK**.
6. Select an account from the list and click **OK**.
7. Select a workflow from the list. Click **OK**.
8. Select a schedule from the list.  
Add schedules to batch workflows that do not contain a file trigger. A schedule is necessary to activate the workflow.
9. Select a status from the list.
  - **Enabled.** Run the workflow that is associated with the profile immediately after the profile is created.
  - **Disabled.** Do not run the workflow immediately.

**Note:** You cannot run the workflow for a disabled profile.
10. Click the **Workflow Parameters** tab and enter the values for the workflow parameters.  
If you selected an Informatica Cloud workflow, the workflow is associated with an Informatica Intelligent Cloud Services (Data Integration) mapping.  
If you installed the Partners Portal component, the Portal Parameters tab displays the list of workflow parameters that the Message Profile wizard shows in the Partners Portal and that the partner can edit. You can create default settings for these parameters.  
**Note:** The name of the Portal Parameters tab is configurable, and the tab might have another name.
11. Click the **Event Attributes** tab.  
The **Event Attributes** tab displays the list of attributes associated with events created when the workflow associated with this profile runs. You can use the attributes to specify additional event information at run time.  
Usually, an administrator sets up the event attributes on the Operation Console. Contact the B2B Data Exchange administrator for information about the event attribute requirements for a profile.
12. Enter the values for the event attributes. The values you enter will be used as default values, but might be overridden by the workflow when processing a specific message.
13. To enter delayed processing information, click the **Delayed Processing** tab.



14. To select whether Portal users can change message profile settings, click the **Portal** tab. To allow changes, select **Allow portal users to edit message profile**. To prevent Portal users from changing their message profiles, select **Do not allow Portal users to edit the profile**.
15. To assign categories to the profile, click the **Categories** tab.
16. On the **Categories** tab, choose whether to inherit categories from the account or to manage categories for the profile.
17. From the **Available Profile Categories** column, select a category to associate with the profile and click the right arrow to move it to the **Selected Profile Categories** column.
18. Click **Save**.

## Profile ID

The profile ID uniquely identifies a profile. When you create a profile, the B2B Data Exchange Server generates and sets the profile ID. When you import a profile into another instance of B2B Data Exchange, the B2B Data Exchange Server of the new instance generates a new profile ID for the imported profile. The imported profile ID can differ from the original profile ID.

You can use the profile ID variable, \$profileId, to represent a profile in the file pattern in the endpoint setup. The value of the variable can vary from one system to another for profiles with the same name. Each B2B Data Exchange instance can generate a different profileId for the same profile name.

For example, when you move a profile from a development environment of B2B Data Exchange to a production environment, the production instance generates a profile ID. For this reason, if you develop and test workflows in a development environment and then move them to a production environment, use the \$profileName variable instead of the \$profileId to associate between a partner and workflow.

## Application, Partner, and Account Number

The administrator sets up the application name when creating an application. When the developer creates a workflow, the administrator or the developer can associate it with an application. When you add an account to a partner, you set the account name and number. The application name and account number do not change when you export and then import them into another instance of B2B Data Exchange.

When you create a profile, you must associate it with a workflow, partner, and account. The workflow determines the application associated with the profile.

## Searching for Profiles

Perform a basic or advanced search for profiles based on certain search criteria.

1. In the Navigator, click **Partner Management > Profiles**.  
The **Profiles** page displays all profiles sorted by profile Id in descending order.
2. To perform a basic search, enter one of the following properties in the **Find** field:

Property	Description
Profile Name	Name or part of the name of the profile.
Profile Id	Unique identifier for the profile. Exact match only.
Partner Name	Name or part of the name of the related partner.

Property	Description
Workflow Name	Name or part of the name of the related workflow.

- To search for profiles based on additional search criteria, click **Advanced Search** and enter one or more of the following properties:

Property	Description
Profile Name	Name or part of the name of the profile.
Profile Id	Unique identifier for the profile. Exact match only.
Partner Name	Name or part of the name of the related partner.
Account Number	Number of the related account. Exact match only.
Workflow Name	Name or part of the name of the related workflow.
Profile Categories	Categories for the profile. You can select multiple categories.
Operation	Logical operator for the search. Choose one of the following options: <ul style="list-style-type: none"> <li>• And. Searches for profiles that match all of the search criteria.</li> <li>• Or. Searches for profiles that match any of the search criteria.</li> </ul>

- Click **Search**.  
The **Profiles** page displays the search results.

## Editing a Profile

You can customize the workflow associated with a partner or an account.

- Click **Partner Management > Profiles**.
- Click the name of the profile that you want to edit.

The Update Profile page opens.

**Note:** If a portal user or operator is editing a message profile or has submitted changes for approval, you cannot edit the message profile. The message profile parameters appear in read-only mode. You can unlock a locked message profile by reverting changes that are in progress, or by approving or rejecting a change request from a portal user.

- Select one of the following tabs:
  - General
  - Workflow Parameters
  - Event Attributes
  - Delayed Processing
  - Categories
- Edit the property values, and then click **Save**.

## Deleting a Profile

To delete a profile, click **Partner Management > Profiles**. Select the check boxes next to the profiles that you want to delete and click **Actions > Delete**. Confirm the deletion.

## Enabling or Disabling a Profile

When you create a profile, set the profile status. If you set the status to Enabled, the Data Exchange Server runs the workflow associated with the profile when you save the profile. The workflow runs continuously until you disable the profile.

To temporarily stop running the workflow associated with profile, set the status of the profile to Disabled. To start running the workflow again, set the status of the profile to Enabled.

To enable or disable a profile:

1. In the Navigator, click **Partner Management > Profiles**.
2. Click the name of the profile you want to disable.
3. On the Update Profile page, click the **General** tab.
4. Set the profile status:
  - **Enabled**. Start running the associated workflow.
  - **Disabled**. Stop the associated workflow from running.
5. Click **Save**.

## Running a Batch Profile

A batch profile associates a batch workflow with a partner. A batch workflow represents a PowerCenter batch workflow.

You can run them manually from the Profiles screen.

To run a batch profile manually:

1. Click **Partner Management > Profiles**.  
The Profiles page appears.
2. Select the check box next to the batch profile that you want to run and click **Actions > Run**.



<input type="checkbox"/>	Profile ID	Partner	Account	Profile Name	Template	Status	Last Modified	Events	Delays All
<input type="checkbox"/>	1000	Hartford Medical	11	Hartford Cardiac Associates	TEST_SIMPLE		12 June 2010	Events	<input type="checkbox"/>
<input type="checkbox"/>	1020	Clarion Assoc.	test1	Clarion Health Marketing	Users details		12 June 2010	Events	<input type="checkbox"/>

## Profile Usage in Endpoints

The Data Exchange Server identifies the profile that defines the association between a partner and a workflow based on the information that you provided when you created an endpoint.

When creating an endpoint, you can explicitly define the profile to be used for each file name pattern expected to be received at that endpoint. If no explicit profile is defined for a file pattern, the Data Exchange Server uses an implicit routing procedure and identifies the required profile based on the application, partner, and account number.

For more more information about endpoints, see the [“Endpoints Overview” on page 83](#).

## Delayed Events

It is sometimes necessary to delay events before they are submitted to PowerCenter. Delayed event processing may be required, for example, to process all transactions of the same type at once, or to hold certain transactions until the night when server resources are available.

The conditions for delaying event processing are defined for a profile. All messages meeting a delay rule are delayed until released by the rule, by a workflow, or by the operator.

You can choose between the following delay rules:

- **Timing rules.** A timing rule defines when delayed event release is evaluated.
- **Delay Rules.** Delay rules define what events to delay, and what conditions trigger their release.
- **Release rules.** Release rules define how delayed events are released to PowerCenter.

In order to delay all events sent to a specific profile, without regard for delay rules, use the Delay All Events flag on the Delayed Processing tab. Setting this flag to On delays all events arriving at the profile and suspends release rules. You can manually release delayed events by using the Release delayed events action in the Profiles screen or the Release action in the Event Search Results screen. The workflow can also release events using the DX\_Release\_Delayed\_Events transformation. When the Delay all Events flag is Off, delayed events are either released immediately, or delayed, according to the defined delay rules. When Delay all Events is turned Off, all events that arrived while the flag was On, and were thus delayed, are immediately released.

## Delayed Events Example

Sometimes it is necessary to delay events that arrive until the evening and to synchronize them with a summary document. This use case illustrates some of the B2B Data Exchange delayed processing rules functionality.

Assume that you need to delay all the events of type "Claim" that arrive during the day and process them after 10:00 PM. The events are released by the arrival of a Claims Summary message. When released, the events are released in groups of ten events.

To implement this scenario, do the following steps:

1. On the Schedule screen, define a schedule whose start time is 10:00 PM and recurs daily.
2. On the Profile screen, create a new profile for processing Claim events, and delay rules, as explained below.
3. On the Profile > Delayed Processing tab, add a Timing Rule using the Scheduling Rule option. Select Daily at 10:00 PM as the scheduling policy for this rule. Specify that if mandatory rules are not met within two hours, wait for the next processing window.
4. On the Profile > Delayed Processing tab, add a Delay Rule, using the Specific Event Rule option. Use EventType as the attribute name, and Claims summary as its value. Make the rule mandatory. This rule delays all Claims until an event occurs that has an event attribute EventType with value Claims summary.
5. On the Profile > Delayed Processing tab, create an additional rule, a Release Rule, using the Max. Volume Rule. Specify Process events in groups of 10. Make the rule mandatory.

Using these delay rules, B2B Data Exchange delays all incoming events that are routed to the Claims profile. Starting at 10:00 PM, B2B Data Exchange evaluates the delay rules once every minute for two hours. If a

Claims Summary message arrives, the delayed Claims are released in groups of ten. Any remaining claims are held over until the next business day.

## Timing Rules

Timing rules define when delayed events are released.

The timing rules are:

- **Schedule rule.** A schedule rule defines a processing window whose starting time is set by a pre-defined schedule and whose length is operator-configurable. At the scheduled time, B2B Data Exchange evaluates the delay rules.
- **Timeout rule.** A timeout rule defines the maximum time an event sent to this profile can be delayed. This time is defined by the operator. At the end of the timeout, B2B Data Exchange evaluates the delay rules defined for this profile.

Both timing rules let the operator decide how to handle delayed events that cannot be released according to the release rules. Either save them until the next processing window, or discard them.

The operator can define one timing rule per profile.

## Delay Rules

Delay rules define which events should be delayed and what conditions trigger their release. Multiple delay rules are allowed.

The following delay rules are available:

- **Number of events rule.** This rule specifies the minimum number of events that need to be delayed in order to release them for processing.
- **Specific event rule.** This rule states that B2B Data Exchange should delay all events until a specific event arrives which meets a condition set in the rule. An example of such a special event is one with an attribute set to a specific value, for example, an event whose EndOfDay attribute is True.
- **Combination rule.** There are several variations of the definition of the combination rule.  
The first one is to delay all events until a threshold number of events has been delayed, for example, delay 900 events. This rule is similar to the Number of Events rule.  
The second variation of the combination rule is to delay all events until the accumulated total of an event attribute reaches an operator configurable value - for example, total price equals a threshold value.  
The third variation of the combination rule is optional, and can be combined with one of the first two variations. This rule allows the operator to define which events are accumulated. Events are identified by an event attribute that holds a specific value, for example, delay 100 events whose PartnerCode attribute is 147, or delay all events whose PartnerCode attribute is 147, until their Total price equals 10,000.
- **By-event rule.** This rule is used to re-group events. The rule groups events by an operator-selected event attribute. The size of the groups can be specified by another event attribute.

## Release Rules

Release rules determine how to release delayed events.

There are multiple types of release rules:

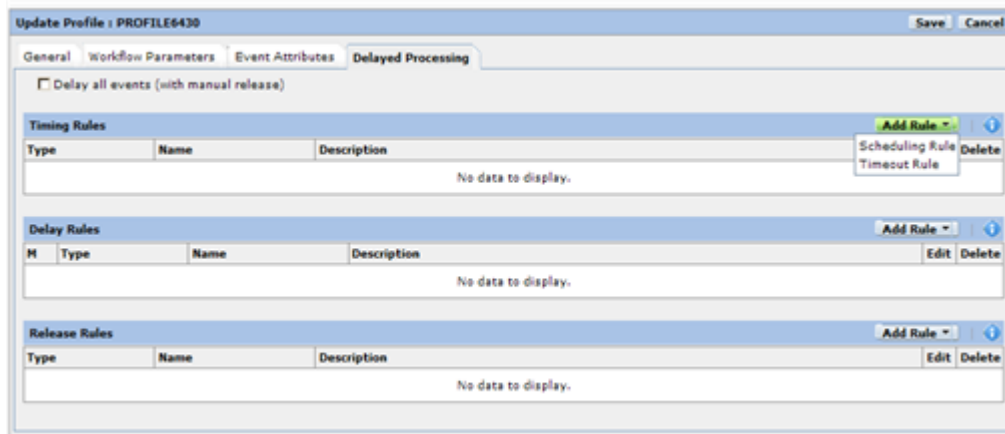
- **Release as One Rule.** This rule specifies how to release the delayed events and which parameters B2B Data Exchange passes to the PowerCenter workflow. You can select from the following options:
  - Concatenate all delayed event documents in a single file. The file has one new root event, and the list of delayed event documents is separated by a rule-provided separator.
  - Prepare a list of input files and pass it by reference to a PowerCenter batch workflow that expects an indirect set of sources. Specify which event attribute contains the source file name. You can also pass the original Event ID for each delayed event to the PowerCenter workflow.
- **Note:** If you do not specify a Release as One Rule, B2B Data Exchange releases each event one by one.
- **Maximum Volume Rule.** This rule specifies that the events are released in groups, and specifies the maximum number of events for each group.
- **Order By Rule.** This rule lets you specify the order to use when releasing delayed events. Specify an event attribute that determines the order in which the events are released. The order of events can be either ascending or descending. You can choose the data format for comparing the event attribute values: string, number, or date. For example, release events by creation date/time, starting with the earliest event.

The operator can define multiple release rules, provided that there is just one of each type.

## Setting Up Delayed Processing Rules

To configure delayed processing rules for a profile:

1. On the Navigator, click Partner Management > Profiles.  
The Profiles page appears.
2. Click the Edit icon of the relevant profile.  
The Update Profile page appears.
3. Click Delayed Processing.  
The Delayed Processing page appears. Use this page to define the delay rules relevant to this profile.
4. Timing rules define time-related processing rules. You can define one timing rule for each profile. To define a timing rule, click the Timing Rules Add button and select the rule.  
The Add list opens.



5. A scheduling rule defines a processing period. A schedule in the system defines the start time and the rule defines the length of scheduled time. When the processing period commences, B2B Data Exchange evaluates the scheduling rules every minute. When rule conditions are met, B2B Data Exchange releases the delayed events.

To configure a scheduling rule, select Scheduling Rule from the list.

The New Scheduling Rule page appears.

6. Enter the following fields in the page:

Field	Description
Rule name	The name of the rule.
Select schedule	Select a schedule from the list of defined schedules. The property indicates the starting point of the processing window. For more information about creating schedules, see <i>B2B Data Exchange Administrator Guide</i> .
If mandatory rules are not met within	Number + time units (minutes, days, hours), for example, which delay rules are checked at frequent intervals.
Wait for the next processing window	Hold delayed events for the next processing window.
Discard delayed events	Discard delayed events.
Generate error event	Generate an error event if mandatory rules are not met within the processing period.

Click Save.

7. A timeout rule defines the maximum time that events sent to this profile can be delayed.  
To configure a timeout rule, select Timeout Rule from the list of rules.

The New Timeout Rule page appears.

8. Enter the following fields in the page:

Field	Description
Rule name	The name of the rule.
Do not delay events for more than	Number and time units (minutes, days, hours), for example, 2 hours. This property indicates the maximum delay time.
Change to manual release mode	Event release is manual. Automatic event release is disabled. Manual (operator) release is possible by clicking the Release icon on the Profile page, or selecting the Release action on the Event List page.
Discard delayed events	Discard delayed events.
Generate error event	Generate an error event if mandatory rules are not met with the processing period.

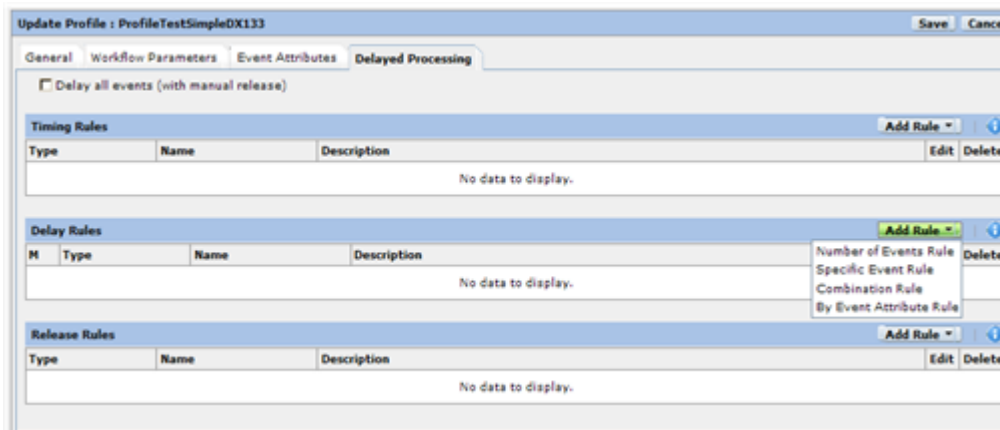
Click Save.

9. Delay rules define how events are delayed and what conditions trigger their release. Multiple delay rules can be defined for a single profile.

To set up a delay rule, click the Delay Rules > Add Rule button.



The list of rules opens.



- The Number of Events Rule defines the minimum number of events that need to be received and delayed before they can be released.

To configure a Number of Events rule, select Number of Events rule from the rules list.

The New Number of Events page appears.



- Fill in the fields in the page as follows:

Field	Description
Rule name	The name of the rule.
Process events after receiving at least N events	The minimum number of events to be delayed before release.
This rule is mandatory	If mandatory, the conditions of the rule must be met in order to release the delayed events.

Click Save.

- A Specific Event rule delays events according to an event attribute.

To configure a Specific Event rule, select Specific Event Rule from the list of rules.

The New Specific Event Rule page appears.

The screenshot shows a dialog box titled "New Specific-Event Rule". It contains the following elements:

- A text input field labeled "\* Rule name".
- A dropdown menu labeled "\* Process events after receiving at least one event where" with "Select Attribute Name" selected.
- The word "is" followed by a text input field.
- A checked checkbox labeled "This rule is mandatory".
- "Save" and "Cancel" buttons at the bottom right.

- Fill in the fields on the page as follows:

Field	Description
Rule name	The name of the rule.
Process events after receiving at least one event where	Select an event attribute from the list.
Is (equal to)	A value for the selected event attribute that will cause delayed events to be released.
This rule is mandatory	If mandatory, the conditions of the rule must be met in order to release the delayed events.

Click Save.

- A combination rule is an advanced rule that offers delayed event release according to a number of conditions.

To configure a combination rule, select Combination Rule from the list of rules.

The New Combination Rule page appears.

The screenshot shows a dialog box titled "New Combination Rule". It has a close button (X) in the top right corner. The main area contains the following elements:

- \*Rule name: [Text input field]
- \*Release events when:
  - Number of delayed events reaches [Text input field]
  - Accumulated [Select Attribute Name dropdown] reaches [Text input field with value 1]
- For events where [Select Attribute Name dropdown] is [Text input field]
- This rule is mandatory

At the bottom right, there are two buttons: "Save" and "Cancel".

Field	Description
Rule name	The name of the rule.
Number of delayed events reaches <value>.	The number of delayed events that must accumulate before they can be released for processing.
Accumulated <Event Attribute > is <value>.	Delay events when the accumulated value of <Event Attribute> reaches <value>.
For events where <Event Attribute> is <value>	The number of delayed events or the accumulated value is calculated for events having <Event Attribute> = <value>.
This rule is mandatory	If mandatory, the conditions of the rule must be met in order to release the delayed events.

15. Select whether to release events according to the number of events delayed or according to the cumulative total value of some event attribute of the delayed events. For example, you can release events when five have arrived, or when the total payment amount of all delayed events reaches \$4,500.

Fill in the fields in the page as follows:

- To release events according to the number of delayed events: Select Number of delayed events and enter the threshold value into the Reaches field.
- To release events based on the accumulated value of some event attribute: Select Accumulated, select an event attribute from the list, and enter the threshold value into the Is field. For example, select the event attribute Payment Amount from the list and enter 4500 into the Is field.
- To restrict the number of events or the accumulated value of events based on an event attribute, check "For events where", select an event attribute from the list and fill in the attribute value, for example, "For events where document type" is <invoice>.
- Check "This rule is mandatory" to make the rule mandatory.

- Click Save.

16. A By Event Attribute rule is used to re-group events based on a specific event attribute. To configure a By Event Attribute rule, select By Event Rule from the list of rules. The New By Event Attribute Rule page appears.

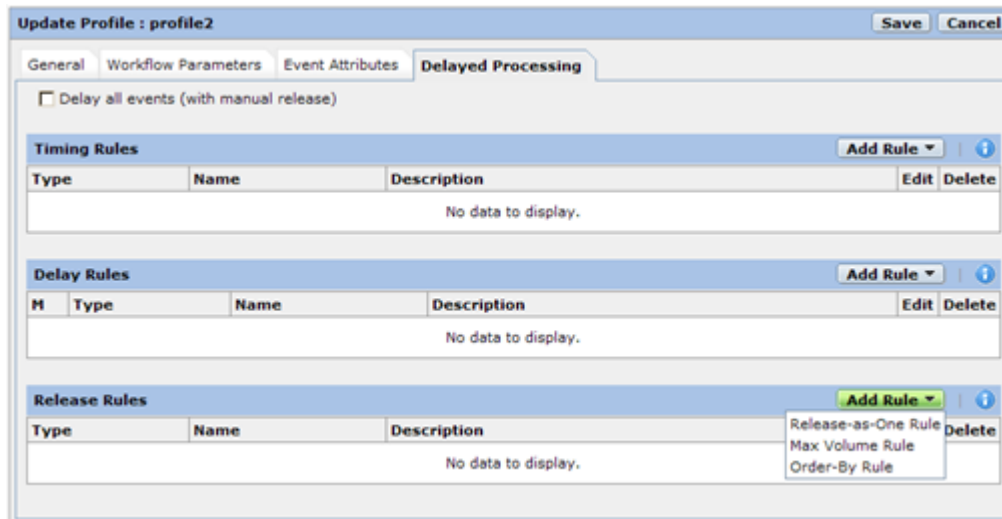
17. Fill in the fields in the page as follows:

Field	Description
Rule name	The name of the rule.
Group events by	Select an event attribute from the list. The events will be grouped by the selected event attribute.
Determine group size using	Select an event attribute from the list. The numerical value of this attribute is the group size.
This rule is mandatory	If mandatory, the conditions of the rule must be met in order to release the delayed events.

Click Save.

18. Release rules define the conditions for delayed event release. To define a release rule, click the Release Rules Add Rule button and select a rule from the list.

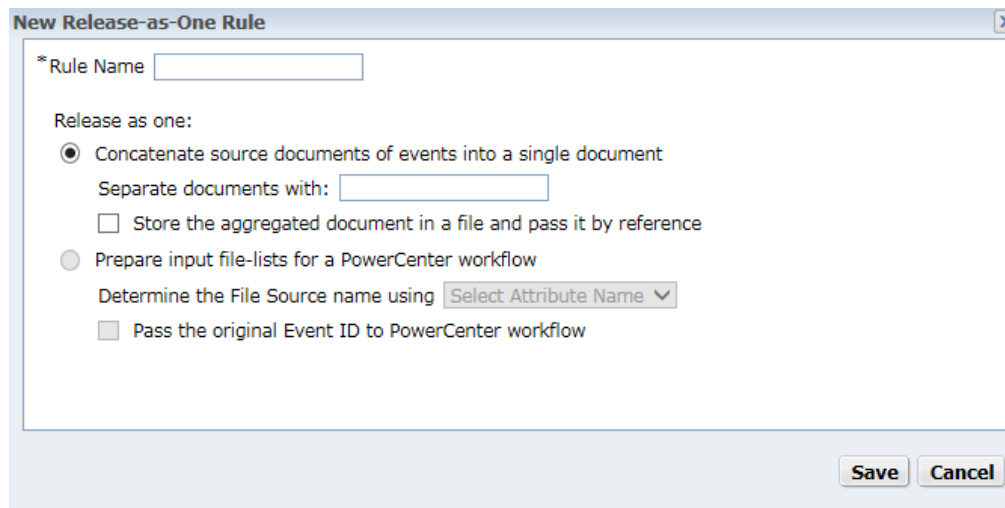
The list of rules opens.



- The Release-As-One-Rule page appears. This rule combines all the delayed events for the profile into one single event and releases it for processing.

To define a Release as One rule, select Release-As-One Rule from the new rules list.

The Release-As-One Rule page appears.



- Fill in the fields in the Release as One Rule page, as follows:

Field	Description
Rule name	The name of the rule.
Concatenate events documents ...	Select to combine input documents of all delayed events into one document.
Separate documents with	Enter a string for separating aggregated documents one from another.

Field	Description
Store the aggregated document ...	Send the aggregated message to the workflow as a file pointer. Use this option if the aggregated message is expected to be very large and you don't want to submit it through the queue.
Prepare input files lists for a PowerCenter workflow	As an alternative to concatenating source documents into a single file, you can choose to prepare a list of input files and pass it by reference (using the file source name that you select) to a PowerCenter batch workflow that expects an indirect set of sources.
Determine the file source name using	Select an event attribute name from the list. This attribute holds the file source name.
Pass the original Event ID to PowerCenter workflow	Add a second column to the list of input files with the original Event ID for each source file.

Click Save.

21. A Max Volume rule determines the maximum number of events to release in one batch.

To create a maximum volume rule, select Max Volume from the list of rules.

The New Max Volume Rule page appears.

The screenshot shows a dialog box titled "New Max Volume Rule". Inside the dialog, there are two input fields. The first is labeled "\* Rule name" and is empty. The second is labeled "\* Process events in groups of" followed by a text box containing the number "1" and the word "events". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

22. Fill in the fields in the page as follows:

Field	Description
Rule name	The name of the rule.
Process events in groups of	Fill in a numerical group size.

Click Save.

23. An order by rule defines how to order the released events.

To define an order by rule, select Order-By Rule from the list of rules.

The New Order-By Rule page appears:

24. Fill in the fields in the page as follows:

Field	Description
Rule name	The name of the rule.
Order events by	Select an event attribute name from the list. The released events are ordered by the selected event attribute.
Order	Select ascending or descending order.
Compare as	Chose the data format of the selected event attribute for sorting the released events: string, date, or numeric.

Click Save.

25. To delay all events and release them manually, select the Delay-All-Events (with manual release) checkbox from the top of the Update Profile page.

The operator can release events manually:

- In the Navigator, click Partner Management > Profiles. Select a profile and click Actions > Release Delayed Events.
- In the Navigator, click Events > All Events > Advanced Search. Select the events to be released. Click Actions > Release.

## CHAPTER 4

# On-Boarding Checklists

This chapter includes the following topics:

- [On-Boarding Checklists Overview, 48](#)
- [Creating an On-boarding Checklist, 49](#)
- [Editing an On-boarding Checklist, 50](#)
- [Monitoring the Status of On-boarding Checklists, 53](#)
- [On-boarding Checklist Charts, 55](#)

## On-Boarding Checklists Overview

Partner on-boarding is the organizational process that transforms a new trading agreement into a working connection for a new partner, allowing him to send and receive messages using B2B Data Exchange.

The on-boarding process often involves multiple roles within the organization, each of which is responsible to perform one or more tasks to implement the trading agreement. Some of these tasks are performed in the B2B Data Exchange environment, while other tasks are carried out in external systems, like CRM and Accounting.

On-boarding a partner is implemented by using an on-boarding checklist, which contains all the tasks that must be accomplished to complete the on-boarding process. An on-boarding checklist might refer to some B2B Data Exchange tasks, like creating a partner and its accounts, or to tasks which are outside of the B2B Data Exchange environment, like opening a partner account in the accounting system. It is the responsibility of the operator to enter starting and ending times of each task in the process checklist, and to monitor the progress of each and every task.

The responsibilities for creating an on-boarding checklist are divided between the administrator and the operator.

- **On-boarding checklist templates.** Created by the administrator. Different checklist templates represent different on-boarding processes. Each checklist template defines the tasks that the B2B Data Exchange operator must do to successfully complete the on-boarding process.
- **An on-boarding checklist.** Created by the operator, based on an on-boarding checklist template. Choose the most appropriate template for the specific process and partner.

The on-boarding checklist enables the operator to meet two responsibilities:

- **Implementing partner on-boarding.** Implementing partner on-board consists of carrying out the operator tasks which appear in the checklist. An operator can report on the beginning and completion of every task, as well as flag any tasks which are experiencing delays or other difficulties.



- **Monitoring the progress of the on-boarding process.** Progress monitoring assures that the on-boarding process is carried out smoothly and on-time. B2B Data Exchange provides a variety of tracking capabilities to monitor progress.

## Creating an On-boarding Checklist

On-boarding checklists contain all the tasks that must be accomplished to complete the on-boarding process.

1. In the Navigator, click **Partner Management > On-boarding > New Checklist**.

The Create New Checklist page appears.

2. Enter details in the following fields:

Field	Description
Name	Required. The name of the new checklist.
Template	Required. The on-boarding template for this checklist. The Task List is populated only after selecting a template.
Partner	The partner being on-boarded. When on-boarding a new partner, you can create the checklist before creating the partner and then create the partner as a part of the checklist. After creating the partner, enter the partner details in this field. When on-boarding an existing partner, enter the partner details when creating the checklist.
Due Date	The deadline for completing the checklist. Click the <b>Browse</b> button to open the calendar and select a date.
Description	Text description of the checklist.
Task List	The name and description of every task in the selected checklist template.

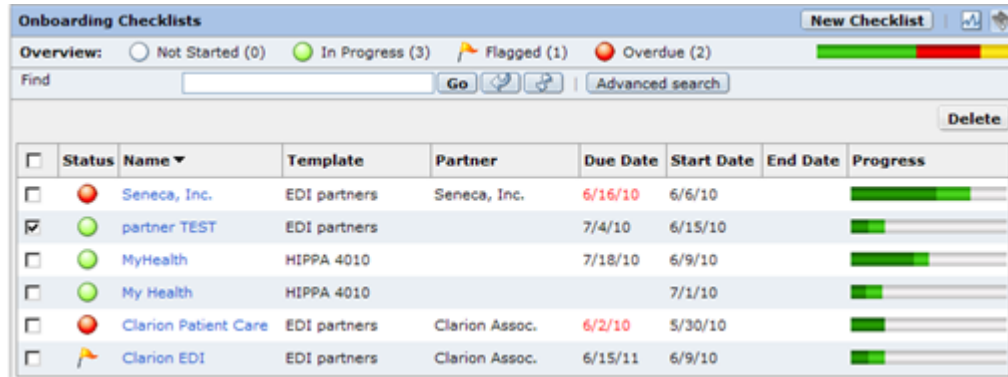
3. Click **Save**.

# Editing an On-boarding Checklist

You can view details and update task progress for on-boarding checklists.

1. In the Navigator, click **Partner Management > On-boarding**.

The On-boarding Checklists page appears.



The screenshot shows the 'Onboarding Checklists' interface. At the top, there is an 'Overview' section with status indicators: Not Started (0), In Progress (3), Flagged (1), and Overdue (2). Below this is a search bar with a 'Go' button and an 'Advanced search' link. A 'Delete' button is located in the top right corner of the table area. The table itself has the following columns: Status, Name, Template, Partner, Due Date, Start Date, End Date, and Progress. The data rows are as follows:

<input type="checkbox"/>	Status	Name	Template	Partner	Due Date	Start Date	End Date	Progress
<input type="checkbox"/>	Overdue	Seneca, Inc.	EDI partners	Seneca, Inc.	6/16/10	6/6/10		Dark Green
<input checked="" type="checkbox"/>	In Progress	partner TEST	EDI partners		7/4/10	6/15/10		Light Green
<input type="checkbox"/>	In Progress	MyHealth	HIPPA 4010		7/18/10	6/9/10		Dark Green
<input type="checkbox"/>	In Progress	My Health	HIPPA 4010			7/1/10		Light Green
<input type="checkbox"/>	Overdue	Clarion Patient Care	EDI partners	Clarion Assoc.	6/2/10	5/30/10		Dark Green
<input type="checkbox"/>	Flagged	Clarion EDI	EDI partners	Clarion Assoc.	6/15/11	6/9/10		Light Green

The On-boarding Checklists page is divided into two parts.

The upper part is called the Overview. It shows the number of incomplete checklists according to the checklist status:

- **Not started.** A checklist for which no task started.
- **In progress.** A checklist that started but not was not completed.
- **Flagged.** A checklist with a flagged task.
- **Overdue.** An In Progress checklist whose due date is past.

The status bar to the right of the checklist status shows the number of active tasks by status:

- **Green.** In Progress.
- **Red.** Overdue.
- **Yellow.** Flagged.

The lower part of the page displays information about the checklists that are in progress. Note the progress bar at the right of each checklist. Dark green bars show the number of completed tasks, light green indicates the number of in-progress tasks, and grey indicates the number of tasks that have not started. The progress bar has a fixed length, regardless of how many tasks are in the checklist. The length each colored bar is proportional to the ratio between the different categories of task progress.

If a task is overdue, the due date is displayed in red.

2. To search for on-boarding checklists, Click **Advanced Search**.

The advanced search window appears.

You can use the following parameters to search inside on-boarding checklists:

Parameter	Description
Checklist Name	Name of the checklist.
Partner Name	Name of the partner.
Template Name	Name of the on-boarding checklist template.
Status	Status of the checklists.
Deadline	A specific number of days before or after the checklist due date.
Operator	Logical operators to include in the search: - OR. Search for any of the fields that contain values. - AND. Search for all of the fields that contain values.
Start Date	A range of dates during which the checklist started. Click <b>Browse</b> to open the calendar tool. Click <b>X</b> to delete the date.
Due Date	A range of dates during which the checklist is due to be completed. Click <b>Browse</b> to open the calendar tool. Click <b>X</b> to delete the date.
End Date	A range of dates during which the checklist was completed. Click <b>Browse</b> to open the calendar tool. Click <b>X</b> to delete the date.

- Click the name of the checklist that you want to edit.

The selected checklist appears and displays the tasks and task statuses.

The screenshot shows a window titled "MyHealth" with a "Save" and "Cancel" button in the top right. The main area contains a form with the following fields:

- Name: MyHealth
- Partner: [Empty]
- Template: HIPPA 4010
- Status:  In Progress
- Due Date: 07/18/2010
- Start Date: 06/09/2010 19:05
- End Date: [Empty]
- Description: [Empty]

Below the form is a list of tasks:

Task Name	Action	Status
▶ <input checked="" type="radio"/> Fill in HIPPA excel details	Custom action	Completed in 4 Days
▶ <input checked="" type="radio"/> Create partner	Create Partner	Completed in 1 Minutes
▶ <input checked="" type="radio"/> Create HIPPA 837 profile	Create Profile	Completed in 3 Minutes
▶ <input type="radio"/> Create HIPPA 835 profile	Create Profile	Elapsed 18 Days
▶ <input type="radio"/> Get sample messages	Custom action	Not Started
▶ <input type="radio"/> Create endpoints	Create Endpoint	Not Started
▶ <input type="radio"/> Create monitor	Create Monitor	Not Started
▶ <input type="radio"/> Test 835	Custom action	Not Started
▶ <input checked="" type="radio"/> Test 837	Custom action	Completed in 1 Seconds
▶ <input type="radio"/> move to production	Custom action	Not Started

- To edit the details of a task, click the arrowhead icon of the task you want to edit.

The details of the chosen task appear:

The screenshot shows the detailed view for the task "Fill in HIPPA excel details". It includes the following fields:

- Task Name:  Fill in HIPPA excel details
- Action: Custom action
- Status: Completed in 4 Days
- Start Time: 06/09/2010 19:05
- End Time: 06/14/2010 14:54
- Flag task:
- Comments: [Empty]

The following table describes the properties of a task

Field	Description
Circle Icon	Read-only. The status of the task: <ul style="list-style-type: none"> <li>- Empty circle. Task has not yet started. Start Time is blank.</li> <li>- Green circle. Task is in progress. Start Time has a value. End Time is blank.</li> <li>- Check mark. Task is complete. End Time has a value.</li> </ul>
Task Name	Read-only. Taken from the checklist template.
Task Action	If the task is to perform a B2B Data Exchange operation, like Create Partner, click the link to open the appropriate B2B Data Exchange Operation Console page. When you close this page, you are returned to the checklist page. If the task is a custom task, the task Action is read-only.
Task description	Read-only.
Task Status	Read-only.
Start Time	Date and time the task was started.
End Time	Date and time the task was completed.

Field	Description
Flag Task	Select to flag (mark) this task for special attention. To explain the reason for the flag, use the Description field.
Description	Task description.

- To indicate that the handling of this task has begun, and to set the Start Time to the current date and time, click Start task.
- To indicate that the task is complete, expand the task and click End Task.

When you click Start or End Task, the Undo button appears. Start and End times are used for statistical analysis of the status of all tasks. Report start and end times on time.

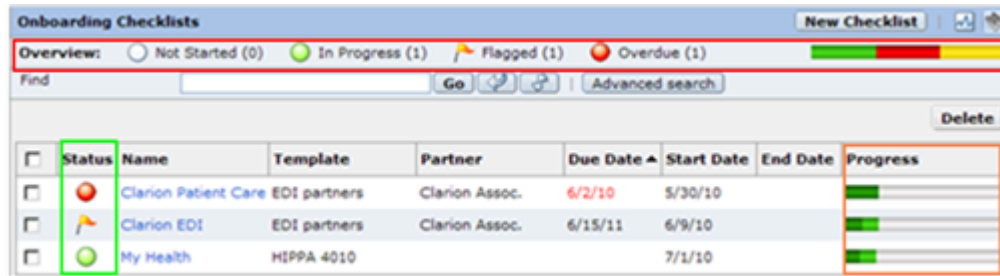
- To flag a task, select Flag task.
- To edit the Description field. type in the text box.
- Click Save.

## Monitoring the Status of On-boarding Checklists

The On-boarding Checklists screen (Partner Management > Onboarding), that shows the in-process checklists, displays the following status information:

- Overview (top of the screen)
- Checklist Status (left side of the screen)

- Checklist Progress (right side of the screen)



The Overview area contains the following status fields:

Field	Description
Not started	The number of checklists that were created but processing has not yet started.
In process	The number of checklists have started but are not yet complete.
Flagged	The number of checklists that are flagged.
Overdue	The number of checklists that are overdue (current date > due date).
Progress bar	Red = overdue. Yellow = flagged. Green = in process. The length of the bars indicate the ratio between the overdue, flagged and in progress checklists.

The checklist status column contains three icons showing the status of the checklists:

Icon	Description
Flag	Flagged
Green Circle	In process
Red Circle	Overdue
White circle	Not started

**Note:** If a task is overdue, the due date is displayed in red.

The Progress column shows the proportion of checklists by status. The light green bar indicates the number of tasks that are in progress, the dark green bar the number of completed tasks, and the grey bar the number of tasks not yet started.

# On-boarding Checklist Charts

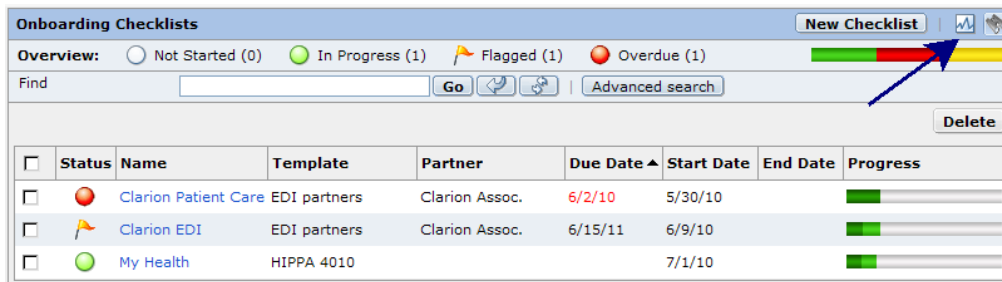
The on-boarding checklist charting capability improves the visibility of the on-boarding process in the organization. This visibility is required for two purposes:

- **Operational purposes.** To answer partner queries about on-boarding status and to identify those processes which require managerial attention.
- **Productivity improvements.** Identify tasks that create bottlenecks and delay process completion.

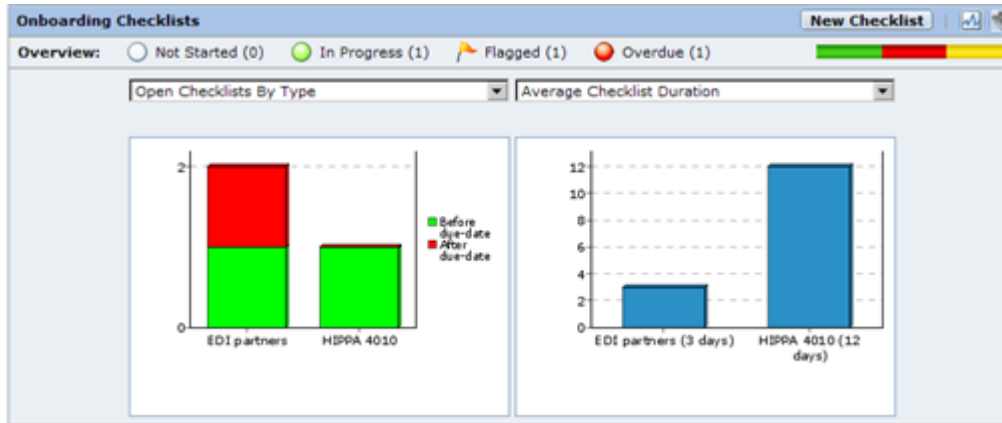
The on-boarding charts include operational and analytical charts.

- **Operational charts.** Open Checklists by Partner and Open Checklists by Type.
- **Analytical charts.** Average Checklist/Task Duration and Top 10 Checklists/Tasks Duration.

To displays the charts, click the chart icon in the upper right-hand corner of the screen.



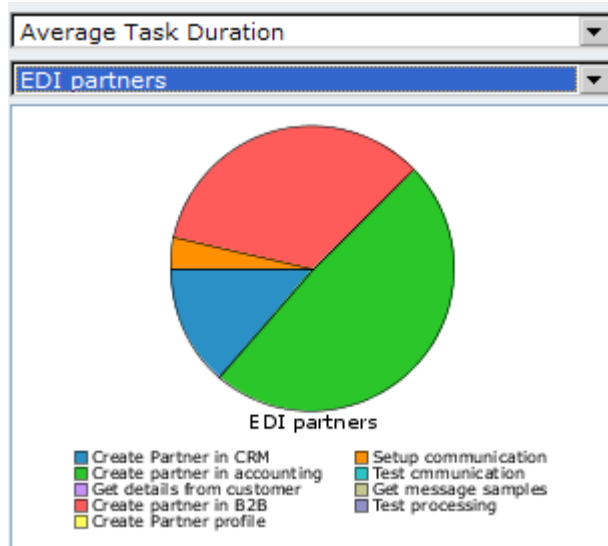
The chart windows appear:



By default, the left window displays the Open Checklists by Type chart and the right window displays the Average Checklist Duration chart. You can view other charts by selecting from the chart list in each window. The two lists of charts are identical, allowing you to display different charts side-by-side.

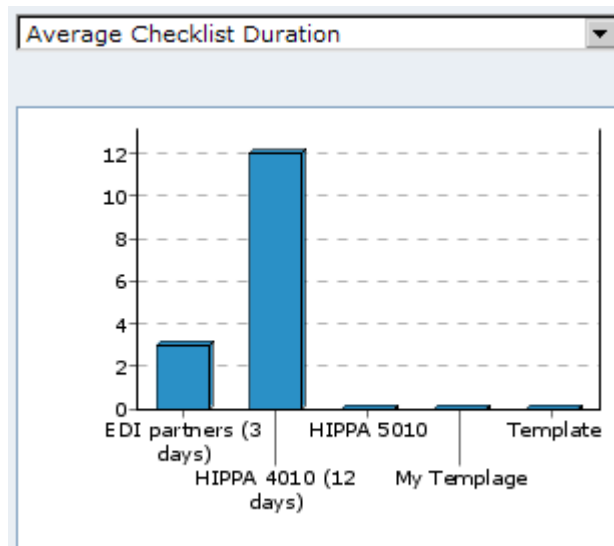
The available charts are described below. Some charts require a parameter to open them.

### Average Task Duration



This chart shows average elapsed time per task for all completed checklists of a certain checklist template. In this example, the template is EDI partners. The checklist enables you to identify the tasks that take the longest time to complete.

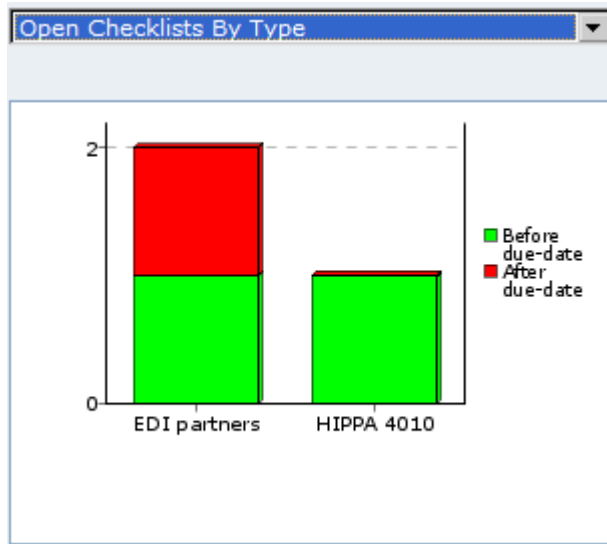
### Average Checklist Duration



This chart shows the average time (in days), by checklist template, required to complete a checklist. This chart displays only completed checklists, not open ones.

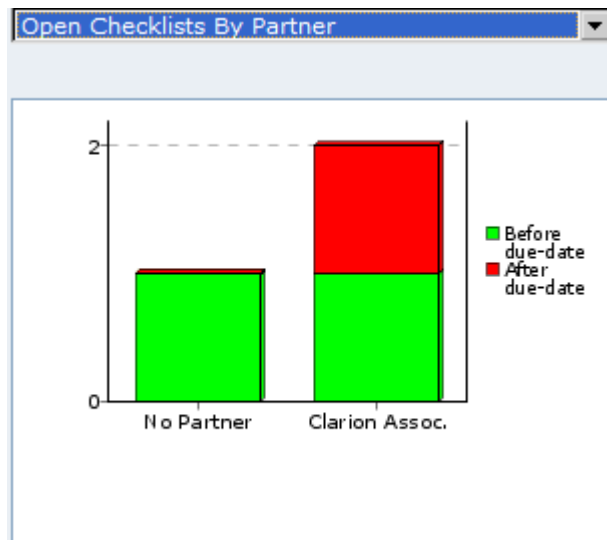


### Open Checklists by Type



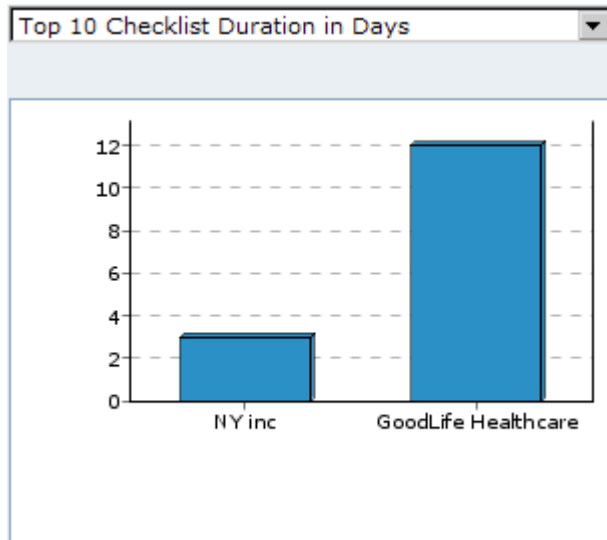
This chart shows the number of open checklists by type (template). The green bar shows the number of open checklists before their due-dates. The red bar shows the number of overdue checklists.

### Open Checklists by Partner



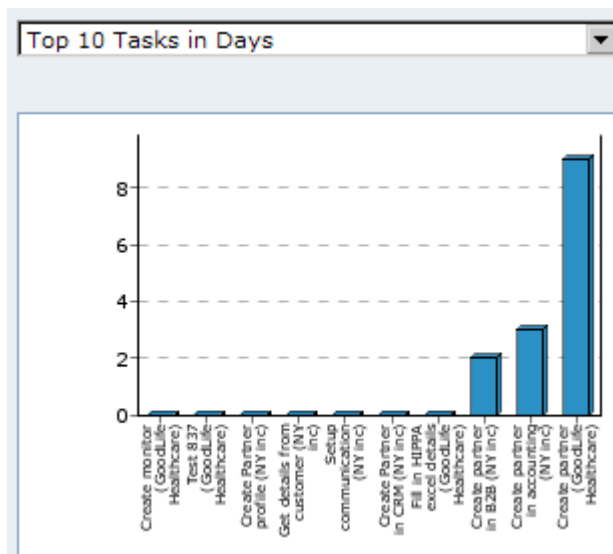
This chart shows the number of open checklists by partner. The green bar indicates the number of checklists before their due date. The red bar shows the number of overdue checklists.

### Top 10 Checklist Duration in Days



This chart displays the ten completed checklists that took the longest time (in days) to complete. The names on the x-axis, in the example NY inc. and Goodlife Healthcare, are checklist names.

### Top 10 Tasks in Days



This chart shows the ten tasks, from all completed checklists, that took the longest time to complete. The labels on the x-axis are the names of the tasks and their templates.

Click the chart icon to close the chart window.

## CHAPTER 5

# Managed File Transfer Web Users

This chapter includes the following topics:

- [Managed File Transfer Web Users Overview, 59](#)
- [MFT Web User Properties, 60](#)
- [Creating an MFT Web User, 64](#)

## Managed File Transfer Web Users Overview

MFT Web Users comprise the accounts that can access Informatica Managed File Transfer hosted servers to exchange files using standard protocols.

You create an MFT Hosted Endpoint to use Informatica Managed File Transfer to receive files from the partner to a mailbox hosted on an organization server, or send files from the hosted mailbox to the partner. Before you create an MFT Hosted endpoint, create an MFT Web User. You must assign an MFT Web User to the MFT Hosted endpoint.

**Note:** An MFT Web User can only be associated with one endpoint.

### RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Hosted Receive Endpoint” on page 105](#)
- [“Adding an Informatica Managed File Transfer Hosted Send Endpoint” on page 105](#)

# MFT Web User Properties

Create an MFT Web User so that partners can access Informatica Managed File Transfer hosted servers to exchange files. When you define an MFT Web User, specify the user authentication properties and contact details.

The following table describes the properties in the **Basic** tab:

Property	Description
Username	Name of the MFT Web User.
Status	Status of the MFT Web User. The MFT Web User can be enabled or disabled.
First Name	The MFT Web User first name.
Last Name	The MFT Web User last name.
Email Address	The primary email address of the MFT Web User. An email address should be specified if the MFT Web User receives email communication for account creation, password reset, forgot password or they have access to Secure Mail.
Description	The description is optional information pertaining to the MFT Web User. This field is limited to 512 characters.
Organization	The company or organization which the MFT Web User belongs to.

The following table describes the properties in the **Authentication** tab:

Property	Description
Login Method	Specify which technique should be used to authenticate the MFT Web User. Valid methods are Active Directory (AD), LDAP, LDAP Managed Server, and Native.
Password Generation	Passwords for MFT Web User accounts can be generated automatically based on the MFT Web User Password Policy. Otherwise the MFT Web User Manager creating the account can manually specify a password. If specifying the password, you are alerted if the password does not meet the MFT Web User Password Policy. The maximum password length is 20 characters.
Authentication Type	<p>The Authentication Type can be specified per service. For example, an MFT Web User can be forced to use a Password and Certificate when authenticating to FTPS but only require a Password for HTTPS. If a certificate is used for authentication, the Client Authentication setting on the SSL tab of the specific service must be set to Optional or Required.</p> <p>If certificate authentication is specified and the certificate being used is either self-signed or signed by an untrusted Certificate Authority (CA), then the certificate will need to be imported into the Default Trusted Certificates Key Store. Importing the certificate instructs Informatica Managed File Transfer to trust this source. If the certificate being used is already signed by a trusted authority (for example, Verisign, GoDaddy, Equifax, etc.) the certificate does not need to be imported since the trust is inherited.</p> <p>The following options are available:</p> <p><b>HTTPS</b></p> <ul style="list-style-type: none"> <li>- Password - MFT Web Users login using their standard MFT Web User name and password.</li> <li>- Certificate - MFT Web Users are authenticated by a certificate which must be in the Informatica Managed File Transfer Default Trusted Key Store and on the MFT Web User's local computer. This method does not require the MFT Web User to specify a user name or password any time they use Informatica Managed File Transfer. If Certificate is selected, type the unique SHA1 Fingerprint for the MFT Web User's certificate in the box. Each MFT Web User must have a unique SHA1 Fingerprint.</li> <li>- Either - If a matching certificate is found during the connection, the MFT Web User will automatically authenticate. However if a match is not found, the MFT Web User can still login to the Informatica Managed File Transfer server with a user name and password. If Either is selected, type the unique SHA1 Fingerprint for the MFT Web User's certificate in the box.</li> </ul> <p><b>AS2</b></p> <ul style="list-style-type: none"> <li>- Password - MFT Web Users login using their standard MFT Web User name and password.</li> <li>- Certificate - MFT Web Users are authenticated by a certificate which must be in the Informatica Managed File Transfer Default Trusted Key Store and on the MFT Web User's local computer. This method does not require the MFT Web User to specify a user name or password any time they use Informatica Managed File Transfer. If Certificate is selected, type the unique SHA1 Fingerprint for the MFT Web User's certificate in the box.</li> <li>- Either - If a matching certificate is found during the connection, the MFT Web User will automatically authenticate. However if a match is not found, the MFT Web User can still login to the Informatica Managed File Transfer server with a user name and password. If Either is selected, type a SHA1 Fingerprint for the MFT Web User's certificate in the box.</li> <li>- Password and Certificate - MFT Web Users are authenticated by their standard MFT Web User name and password along with a shared certificate that is both on the Informatica Managed File Transfer server and the MFT Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.</li> </ul> <p><b>FTPS (Explicit SSL)</b></p> <ul style="list-style-type: none"> <li>- Password - MFT Web Users login using their standard MFT Web User name and password.</li> <li>- Certificate - MFT Web Users are authenticated by a certificate which must be in the Informatica Managed File Transfer Default Trusted Key Store and on the MFT Web User's local computer. This method does not require the MFT Web User to specify a password any time they use Informatica Managed File Transfer. If Certificate is selected, type the certificate's SHA1 Fingerprint in the box.</li> </ul>

Property	Description
	<ul style="list-style-type: none"> <li>- Either - If a matching certificate is found during the connection, the MFT Web User will automatically authenticate. However if a match is not found, the MFT Web User can still login to the Informatica Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.</li> <li>- Password and Certificate - MFT Web Users are authenticated by their standard MFT Web User name and password along with shared certificate that is both on the Informatica Managed File Transfer server and the MFT Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.</li> </ul> <p><b>FTPS (Implicit SSL)</b></p> <ul style="list-style-type: none"> <li>- Password - MFT Web Users login using their standard MFT Web User name and password.</li> <li>- Certificate - MFT Web Users are authenticated by a certificate which must be in the Informatica Managed File Transfer Default Trusted Key Store and on the MFT Web User's local computer. This method does not require the MFT Web User to specify a password any time they use Informatica Managed File Transfer. If Certificate is selected, type the certificate's SHA1 Fingerprint in the box.</li> <li>- Either - If a matching certificate is found during the connection, the MFT Web User will automatically authenticate. However if a match is not found, the MFT Web User can still login to the Informatica Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.</li> <li>- Password and Certificate - MFT Web Users are authenticated by their standard MFT Web User name and password along with shared certificate that is both on the Informatica Managed File Transfer server and the MFT Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.</li> </ul> <p><b>SFTP</b></p> <ul style="list-style-type: none"> <li>- Password - MFT Web Users login using their standard MFT Web User name and password.</li> <li>- Public Key - MFT Web Users use a public key on the server to encrypt a session key that produces a secure login.</li> <li>- Either - If a matching public key is found during the connection, the MFT Web User will automatically pass authentication. However if a key match is not found, the MFT Web User can still login to the Informatica Managed File Transfer server with a user name and password.</li> <li>- Password and Public Key - MFT Web Users must login using their MFT Web User name and password along with a public key.</li> </ul>

The following table describes the properties in the **AS2** tab:

Property	Description
AS2 ID	The AS2 ID of the MFT Web User. The AS2 ID is case sensitive and can be 1 to 128 ASCII printable characters in length.
Signature Certificate Alias	This is the alias of the public certificate used by this MFT Web User to sign their messages. If the certificate is signed by a certificate authority (for example, Verisign), this field can be left blank since the certificate chain already exists in the Default Trusted Certificates Key Store. If a specific certificate is to be used by the Web User for signing messages or they use a self-signed certificate, then that certificate should be imported into the Default Trusted Certificates Key Store. For more information, see the <i>Informatica Managed File Transfer Guide</i> .
Default Upload Folder	The location where AS2 messages are saved when received (uploaded). The default location is the default home directory for the MFT Web User, which is the <code>[installdirectory]/userdata/webdocs/[webuser]</code> folder, where <code>[installdirectory]</code> is the installation directory of Managed File Transfer and <code>[webuser]</code> is the account name of the Web User.

Property	Description
When File Exists	The action that Informatica Managed File Transfer performs when a file with the same name already exists in the default upload folder.
Require Encryption	This option indicates whether or not messages sent by this MFT Web User must be encrypted.
Require Signature	A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this MFT Web User will be rejected.
Require Authentication	Require username/password or certificate authentication for messages uploads. If authentication is not required, Informatica Managed File Transfer will use the AS2 ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.
Asynchronous MDN Approval	If a return receipt is requested by the MFT Web User, select if the MDN will be sent automatically during the MFT Web User session or manually after the message is processed. A manual receipt can only be sent if a message is received successfully. If an error occurs during transmission, an asynchronous receipt is sent automatically.

The following table describes the properties in the **SSH Keys** tab:

Property	Description
Name	The name identifies the SSH key. The maximum length of the name is 64 characters.
Algorithm	The algorithm to use when generating the key. Valid values are RSA and DSA. It is generally recommended to use RSA.
Key Size	The length (in bits) of the key. Valid values are 512, 1024, 2048 or 4096 bits. Large key sizes will provide strong protection, but will slow the performance of encryption/decryption processes.
Fingerprint	This is the password that protects the private key portion of the SSH Key Pair and should be recorded in a safe place.
Public Key Format	The format in which to store the public key. Valid values are OpenSSH or SecureShell. It is generally recommended to use OpenSSH unless your trading partner dictates otherwise. <b>Note:</b> Private Keys and passphrases should be kept confidential and should NOT be shared with trading partners.
Comments	A description to store with the key. This typically should contain the name of your organization (for example, "ABC Company SSH Key"), which will allow others to quickly identify the key.
Created By	The name of the user that created the SSH key.
Created On	The date that the user created the SSH key.

# Creating an MFT Web User

Before you create an MFT Hosted endpoint, you create an MFT Web User.

1. In the Navigator, click **Partner Management > MFT Web Users**.
2. To add an MFT Web User, click **New MFT Web User**.
3. On the **Basic** tab, define the user name, status, description, organization, and contact details.
4. On the **Authentication** tab, define the login method, password generation, and authentication type and method.
5. For an AS2 connection type, on the **AS2** tab, specify AS2 ID, signature certificate alias, default upload folder, encryption, signatures, authentication requirement, and asynchronous MDN approval.
6. For an SSH connection type, on the **SSH Keys** tab, to add an SSH key click **Add SSH Key**. Select an SSH key from the list and click **Select**.
7. Click **Save**.

The **MFT Web Users** page displays the MFT Web User.

## RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Hosted Receive Endpoint” on page 105](#)
- [“Adding an Informatica Managed File Transfer Hosted Send Endpoint” on page 105](#)



## CHAPTER 6

# Managed File Transfer Connections

This chapter includes the following topics:

- [Managed File Transfer Connections Overview, 65](#)
- [AS2 MFT Connection Properties, 66](#)
- [FTP MFT Connection Properties, 68](#)
- [FTPS MFT Connection Properties, 70](#)
- [HTTP MFT Connection Properties, 73](#)
- [HTTPS MFT Connection Properties, 75](#)
- [Mailbox MFT Connection Properties, 76](#)
- [MQ MFT Connection Properties, 77](#)
- [SMTP MFT Connection Properties, 78](#)
- [SFTP, SCP, or SSH MFT Connection Properties, 78](#)
- [Creating an MFT Connection, 82](#)
- [Testing an MFT Connection, 82](#)

## Managed File Transfer Connections Overview

MFT Connections define the names and connection properties of the remote partner servers, and other data sources, that Informatica Managed File Transfer can interact with.

You create an MFT Remote Send Endpoint to use Informatica Managed File Transfer to receive files from the organization to a remote partner server. You create an MFT Remote Receive Endpoint for the organization to receive files from a remote partner server.

Before you create an MFT Remote Send or MFT Remote Receive endpoint, you create an MFT Connection. The MFT Connection defines how Informatica Managed File Transfer communicates with the remote partner server. The defined MFT Connections can be used with Informatica Managed File Transfer Remote endpoints by choosing the MFT Connection names from the project variables drop-down lists.

### RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Remote Receive Endpoint” on page 106](#)
- [“Adding an Informatica Managed File Transfer Remote Send Endpoint” on page 107](#)

# AS2 MFT Connection Properties

Create an AS2 MFT Connection to define communications using the AS2 protocol for an MFT Remote endpoint. The AS2 MFT Connection specifies the settings used when messages are sent using the AS2 1.2 specification. AS2 is a standard originally created to securely transfer EDI documents, but it can also be used to transmit virtually any file type. The messages are structured using the standard S/MIME format and are sent over HTTP(S) connections.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
URL	This is the URL of the server that receives the messages. The URL syntax must be a valid server and location where [hostname] can be an IP Address or a Domain name and [portnumber] is the port on which the AS2 Server listens.
AS2 From ID	The AS2 From ID is the name or ID used by the sender (most commonly you are the sender). The ID is arbitrary, but if the receiving server filters by this ID, the ID's must match. The AS2 From ID is case sensitive, can be 1 to 128 ASCII printable characters in length, and may not contain whitespaces.
AS2 To ID	The AS2 To ID is the name or ID used by the recipient. The ID is arbitrary. The AS2 To ID is case sensitive, can be 1 to 128 ASCII printable characters in length, and may not contain whitespaces.

The following table describes the properties in the **Message** tab:

Property	Description
Encrypt Messages	Encrypting the message itself during transmission within the encrypted tunnel is optional, but highly recommended. The default value if left blank is No.
Encryption Algorithm	The Encryption Algorithm is the algorithm used to encrypt the message. The default encryption algorithm is AES128.
Encryption Certificate Alias	The Encryption Certificate Alias is the certificate alias to use in the Default Trusted Certificate Key store.
Sign Messages	Signing the message with a digital signature to further identify yourself is optional, but highly recommended.
Signature Algorithm	The signature algorithm used to sign the messages can be SHA1, SHA224, SHA256, SHA384, SHA512, or MD5. The default is SHA1.
Signature Certificate Alias	This is the private key alias used to sign the message. The private key is located in the Default Private Key store.
Compress Messages	Messages can be compressed to reduce bandwidth using the zlib format. The default is No.

Property	Description
Receipt Certificate Alias	<p>The Receipt Certificate Alias is optional when the receipt signature contains an embedded certificate. In this scenario, Managed File Transfer will ensure that the embedded certificate is also located in the Default Trusted Certificate Key Store. To enhance security, a Receipt Certificate Alias can be specified which verifies the certificate that signed the receipt is a specific certificate in the key store.</p> <p>If the receipt signature does not contain an embedded certificate, then the Receipt Certificate Alias must be specified in order to verify and trust the signature. Typically, the same certificate that is used to encrypt the outbound message can be used to verify the receipt signature.</p>
Receipt Transfer Encoding	Define the encoding of a receipt. This is useful when the receipt does not include the transfer encoding.

The following table describes the properties in the **Connection** tab:

Property	Description
User	The user name (login name) to use for connecting to the AS2 server. This is only required if the AS2 server needs the AS2 client to authenticate using either the BASIC or DIGEST authentication schemes.
Password	The password to use for connecting to the AS2 server. This is only required if the AS2 server needs the AS2 client to authenticate using either the BASIC or DIGEST authentication schemes. After entering the password, you can optionally click the Encrypt button, which will encrypt the password when it is stored in Managed File Transfer's database. Note: If you do not wish to store the password for the AS2 server resource, the password can be supplied when executing a Project.
Is Password Encrypted	Indicates whether or not the password is encrypted. You should choose Yes if you clicked the Encrypt button for the Password.
Connection Timeout	The maximum amount of time, in seconds, to wait when trying to establish a connection to the AS2 server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, the default value is 60 seconds.
Read Timeout	The maximum amount of time, in seconds, to wait for a (read) response from the AS2 server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value is 0 (zero).
Connection Retry Attempts	The number of times the AS2 Resource will attempt to connect if a connection cannot be established on the first attempt.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. If left blank, the retry interval is 0 (zero) seconds.
Follow Redirects	Specify whether or not to follow redirects. The default value is yes.
Enable Cookies	Specify whether or not to enable cookies. The default value is yes.
User Agent	The user agent is the value used in the message header to indicate what application created or sent the message. The default value is Managed File Transfer/\${currentProductVersion}.
Use Chunked Encoding	Indicates if the length of the request will be pre-calculated or sent in chunks. Pre-calculating the content length may slow performance when sending large files, but not all AS2 servers support chunked encoding. The default setting is No.

Property	Description
Client Certificate Alias	A particular key within the default key store can be used for client authentication by indicating the key alias. The specified key will be used when required by the AS2 server.
SSL Context Protocol	Specify the protocol to use when creating the SSLContext. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (SSL) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support SSLv3.

The following table describes the properties in the **Proxy** tab:

Property	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.
Host	The host name (or IP address) of the proxy server on your network.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use to connect to the proxy server.
Password	The password to use to connect to the proxy server.

## FTP MFT Connection Properties

Create an FTP MFT Connection to define communications using the FTP protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to standard FTP servers to exchange files. When defining an FTP MFT Connection, indicate the FTP connection properties such as the host name or IP address, user and password.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.

Property	Description
User	The user name to use for connecting to the server.
Password	The password to use for connecting to the server.

The following table describes the properties in the **Connection** tab:

Property	Description
Use passive mode	<p>Indicates whether or not the MFT Connection will use <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode. If neither value is selected, then the default mode of <b>Active</b> will be used.</p> <p>In Active mode, the server will attempt to connect back to a port on the Managed File Transfer client in order to perform the data transfer. The challenge with Active mode is that your firewall may block the server from trying to open a port back into your network.</p> <p>In Passive mode, the server does not need to connect back to a port on the Managed File Transfer client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the server, you may want to change the mode to Passive by selecting Yes for this option.</p>
Data Connection Start Port	The starting port number to use for the data connection. This should be used when Active mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
Data Connection End Port	The ending port number to use for the data connection. This should be used when Active mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.
Connection Retry Attempts	The number of times to retry the FTP connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.
Connection Retry Interval	<p>The number of seconds to wait between each connection retry attempt.</p> <p><b>Note:</b> For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.</p>
Initial Remote Directory	The initial directory to start in after connecting to the server. If left blank, then the initial directory will be the home directory assigned to the user on the server.
Control Encoding	If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support more international characters.
Throttle Bandwidth	Limit the inbound and outbound bandwidth used for file transfers.

The following table describes the properties in the **Directory Listing** tab:

Property	Description
List Parser	The list parser to use for the server connection. If the field is left blank, Managed File Transfer will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used. If you experience problems listing directories, select a different list parser.
Date Format	This field is used if the date returned by the server is different than the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values.

The following table describes the properties in the **Proxy** tab:

Property	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
Host	The host name or IP address of the proxy server. <b>Note:</b> If the Proxy Type or Host fields are blank, a direct connection to the target host is implied.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use for connecting to the proxy server.
Password	The password to use for connecting to the proxy server.

## FTPS MFT Connection Properties

Create an FTPS MFT Connection to define communications using the FTPS protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to FTPS (FTP over SSL) servers for secure file exchange. When you define an FTPS MFT Connection, you need to indicate the FTPS connection properties

such as the host name or IP address, user and password. Optionally you can specify the certificates to use for authentication.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.
User	The user name to use for connecting to the server.
Password	The password to use for connecting to the server.

The following table describes the properties in the **Connection** tab:

Property	Description
Use passive mode	Indicates whether or not the MFT Connection will use <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode. If you do not select either value, the default <b>Active</b> is applied.  In Active mode, the server will attempt to connect back to a port on the Managed File Transfer client in order perform the data transfer. The challenge with Active mode is that your firewall might block the server from trying to open a port back into your network.  In Passive mode, the server does not need to connect back to a port on the Managed File Transfer client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the server, you might want to change the mode to Passive by selecting Yes for this option.
Data Connection Start Port	The starting port number to use for the data connection. This should be used when Active mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
Data Connection End Port	The ending port number to use for the data connection. This should be used when Active mode is specified and there is a limited range of open ports on your firewall allowed for data connections.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.
Connection Retry Attempts	The number of times to retry the FTPS connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.
Initial Remote Directory	The initial directory to start in after connecting to the server. If left blank, then the initial directory will be the home directory assigned to the user on the server.

Property	Description
Control Encoding	If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support more international characters.
Throttle Bandwidth	Limit the inbound and outbound bandwidth used for file transfers.
The server is considered trusted and validation will not be attempted using digital certificates.	If enabled, Managed File Transfer uses the default certificate that is defined in the Managed File Transfer default key store.
Client Certificate Alias	Select a Managed File Transfer client certificate using the client certificate alias. A particular key within the Managed File Transfer default key store can be used for client authentication by indicating the key alias. The specified key will be used when required by the FTPS server.

The following table describes the properties in the **Directory Listing** tab:

Property	Description
List Parser	The list parser to use for the server connection. If the field is blank, Managed File Transfer will try to use the MLSD parser. If the server does not support the MLSD parser, the UNIX parser is used. If you experience problems listing directories, select a different list parser.
Date Format	Use this field if the server returns a date that is different from the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values.

The following table describes the properties in the **Proxy** tab:

Property	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers might support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
Host	The host name or IP address of the proxy server. <b>Note:</b> If the Proxy Type or Host fields are blank, a direct connection to the target host is implied.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.



Property	Description
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use for connecting to the proxy server.
Password	The password to use for connecting to the proxy server.

The following table describes the properties in the **SSL** tab:

Property	Description
Connection Type	Indicates if the connection type is Implicit SSL or Explicit SSL. The preferred connection type is the more modern Explicit SSL standard, however some trading partners might still require Implicit SSL. If this field is left blank, then the default connection type of Explicit SSL will be used.
Security Protocol	Indicates whether SSL or TLS should be used for Explicit SSL connections. TLS is the latest security protocol standard, however many trading partners still use the SSL protocol for Explicit SSL connections. If this field is left blank, then the default security protocol of SSL will be used.
Clear Command Channel	Indicates whether or not to use a clear command channel (CCC) for the FTPS connection. Specify <b>No</b> to keep the command channel encrypted. Specify <b>Yes</b> to not encrypt the control command channel (however, the actual data transfers will remain encrypted). If neither value is selected, then the default value of <b>No</b> will be used. <b>Note:</b> SSL connections require a Clear Command Channel (CCC) when connecting from behind a NAT firewall.
Data Channel Protection Level	The data channel protection level indicates if the data channel is encrypted. Select <b>Private</b> to keep the data channel encrypted. If the FTPS server does not support an encrypted data channel, select <b>Clear</b> to leave the data channel unencrypted. The default setting is Private.
Send SSL Close Notify	After the command channel is closed, most servers automatically close the SSL/TLS connection, however some servers do not understand the "close_notify" command. Select <b>No</b> to keep Informatica Managed File Transfer from sending the "close_notify" command. The default value is <b>Yes</b> .
SSL Context Protocol	Specify the protocol to use when creating the SSLContext. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (TLS) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support TLS 1.0.

## HTTP MFT Connection Properties

Create an HTTP MFT Connection to define communications using the HTTP protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to HTTP servers for exchanging files. When

defining an HTTP MFT Connection, indicate the HTTP connection properties such as the host name or IP address, and optionally the user, password and proxy information.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Host	The host name or IP address of the server.

The following table describes the properties in the **Connection** tab:

Property	Description
Port	The port number to use for connecting to the server. If left blank, the default port number is 80.
User	The user name (login name) to use for connecting to the HTTP server. This is only needed if the HTTP server requires that the client be authenticated using either the BASIC or DIGEST authentication schemes.
Password	The password to use for connecting to the HTTP server. This is only needed if the HTTP server requires that the client be authenticated using either the BASIC or DIGEST authentication schemes.
Connection Timeout	The maximum amount of time, in seconds, to wait when trying to establish a connection to the HTTP server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.
Read Timeout	The maximum amount of time, in seconds, to wait for a (read) response from the HTTP server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

The following table describes the properties in the **Proxy** tab:

Property	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.
Host	The host name (or IP address) of the proxy server on your network. This is only needed if your system uses a proxy server to make HTTP connections.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number of the proxy server on your network. This is only needed if your network uses a proxy server to make HTTP connections.
User	The user name (login name) to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP connections.
Password	The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP connections.

# HTTPS MFT Connection Properties

Create an HTTPS MFT Connection to define communications using the HTTPS protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to HTTPS servers to securely exchange files over encrypted SSL connections. When you define an HTTPS MFT Connection, indicate the HTTPS connection properties such as the host name or IP address, and optionally the SSL certificates, user, password and proxy information.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Host	The host name or IP address of the server.

The following table describes the properties in the **Proxy** tab:

Property	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.
Host	The host name (or IP address) of the proxy server on your network. This is only needed if your system uses a proxy server to make HTTP connections.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number of the proxy server on your network. This is only needed if your network uses a proxy server to make HTTP connections.
User	The user name (login name) to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP connections.
Password	The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP connections.

The following table describes the properties in the **Connection** tab:

Property	Description
Port	The port number to use for connecting to the server. If left blank, the default port number is 80.
User	The user name (login name) to use for connecting to the HTTP server. This is only needed if the HTTP server requires that the client be authenticated using either the BASIC or DIGEST authentication schemes.
Password	The password to use for connecting to the HTTP server. This is only needed if the HTTP server requires that the client be authenticated using either the BASIC or DIGEST authentication schemes.

Property	Description
Connection Timeout	The maximum amount of time, in seconds, to wait when trying to establish a connection to the HTTP server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.
Read Timeout	The maximum amount of time, in seconds, to wait for a (read) response from the HTTP server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.
SSL Context Protocol	Specify the protocol to use when creating the SSLContext. The value depends on the security providers you have installed in the Java Runtime Environment. In most cases, the default value SSL is fine. However, on some IBM JRE implementations the default value does not work if the server to which you connect to does not support SSLv3. Select whether the server is considered trusted so that validation will not be attempted using digital certificates. By default, this option is enabled.
The server is considered trusted and validation will not be attempted using digital certificates.	If enabled, Managed File Transfer uses the default certificate that is defined in the Managed File Transfer default key store.
Client Certificate Alias	A particular key within the default key store can be used for client authentication by indicating the key alias. The specified key will be used when required by the HTTPS server.

## Mailbox MFT Connection Properties

Create a Mailbox MFT Connection to define communications using a mailbox for an MFT Remote endpoint. Informatica Managed File Transfer can connect to mail box servers to retrieve email messages. Both POP-3 and IMAP mail box server types are supported. This is especially useful for processing incoming email attachments. When defining a Mailbox MFT Connection for an Informatica MFT endpoint, you need to indicate the connection properties such as the host name or IP address, user and password.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Server Type	Indicates if the mail box server type is POP-3 or IMAP. If this field is left blank, then the default server type of POP-3 will be used.
Host	The host name or IP address of the server.
User	The user name to use for connecting to the mailbox server.
Password	The password to use for connecting to the mailbox server.

The following table describes the properties in the **Connection** tab:

Property	Description
Port	The port number to use for connecting to the server. If left blank, the default port number is 25.
Connection Type	The connection type to use when communicating with the SMTP Server. The following options are available: <ul style="list-style-type: none"> <li>- Normal - The connection is not encrypted.</li> <li>- Explicit SSL - After initial authentication with the SMTP server, the connection is encrypted with SSL.</li> <li>- Implicit SSL - The entire connection and transmission is encrypted using SSL.</li> </ul>
Timeout	The number of seconds to wait when attempting to connect to the mail box server. A timeout error will occur if the connection cannot be established in the specified amount of time. If this field is left blank, the default timeout value of 300 seconds will be used.

## MQ MFT Connection Properties

Create an MQ MFT Connection to define communications using the MQ protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to enterprise messaging systems using JMS (Java Message Service) to send and receive messages from queues and topics.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Connection Type	The connection type for the MQ server. The MQ server can use the JMS Standard (Java Message Service) or a connection type specific to the MQ Provider. When connecting to Websphere MQ, SonicMQ or ActiveMQ use the MQ Provider Specific type and use JNDI (JMS Standard) for others.
URL	The connection string to an MQ Provider Specific server uses the following syntax: <code>providerCode:[transportProtocol:]//host[:port][?key1=value1&amp;key2=value2]</code> . The connection string to a JNDI (JMS Standard) server is supplied by the MQ server administrator.
JNDI Initial Context Factory	The JNDI (Java Name and Directory Interface) context factory is the fully qualified name of the class used to look up the JMS connection factory object. For example, the class might be <code>com.sun.jndi.fscontext.RefFSContextFactory</code> or <code>com.sun.jndi.ldap.LdapCtxFactory</code> . This is required when the connection type is set to use the JMS Standard.
JNDI Name	The name of the JMS connection factory object to use. This is required when the connection type uses the JMS Standard.
JNDI Properties	The optional JNDI properties are specified using <code>key=value</code> pairs. Each pair is defined on a separate line.

Property	Description
User	The user name to use for connecting to the server.
Password	The password to use for connecting to the server.

## SMTP MFT Connection Properties

Create an SMTP MFT Connection to define communications using the SMTP protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to SMTP mail servers to send email messages. This is especially useful for distributing files as email attachments. When you define an SMTP MFT Connection, indicate the SMTP connection properties such as the host name or IP address, and optionally the user and password.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Host	The host name or IP address of the server.

The following table describes the properties in the **Connection** tab:

Property	Description
Port	The port number to use for connecting to the server. If left blank, the default port number is 25.
User	The user name to use for connecting to the server.
Password	The password to use for connecting to the server.
Connection Type	The connection type to use when communicating with the SMTP Server. The following options are available: <ul style="list-style-type: none"> <li>- Normal - The connection is not encrypted.</li> <li>- Explicit SSL - After initial authentication with the SMTP server, the connection is encrypted with SSL.</li> <li>- Implicit SSL - The entire connection and transmission is encrypted using SSL.</li> </ul>

## SFTP, SCP, or SSH MFT Connection Properties

Create an SSH (SFTP, SCP, or SSH) MFT Connection to define communications using the SFTP, SCP, or SSH protocol for an MFT Remote endpoint. Informatica Managed File Transfer can connect to SSH Servers to perform SFTP (SSH File Transfer Protocol) file transfers, SCP (Secure Copy) file transfers and to run SSH

remote commands. When defining an SSH MFT Connection, you must indicate the connection properties such as the host name or IP address and user. You can specify a password, SSH private key or both for authentication.

The following table describes the properties in the **Basic** tab:

Property	Description
Name	Name of the MFT Connection.
Description	Provide a description for the MFT Connection.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.
User	The user name to use for connecting to the server.
Password	The password to use for connecting to the server.

The following table describes the properties in the **Connection** tab:

Property	Description
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.
Connection Retry Attempts	The number of times to retry the connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.
Initial Remote Directory	The initial directory to start in after connecting to the server. If left blank, then the initial directory will be the home directory assigned to the user on the server.
Throttle Bandwidth	Limit the inbound and outbound bandwidth used for file transfers.

The following table describes the properties in the **Proxy** tab:

Property	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
Host	The host name or IP address of the proxy server. <b>Note:</b> If the Proxy Type or Host fields are blank, a direct connection to the target host is implied.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use for connecting to the proxy server.
Password	The password to use for connecting to the proxy server.

The following table describes the properties in the **SSH Keys** tab:

Property	Description
Host Key	The fingerprint of the server's public key, which will be used to authenticate the server. If a fingerprint is not specified, then the server will be treated as trusted.
Private Key Alias	The private key used to authenticate the server, which is located in the SSH Key Manager.
Private Key File Password	The password to use for accessing the Private Key File. After entering the password, you can optionally click the Encrypt button, which will encrypt the password when it is stored in Managed File Transfer's database. A private key password is only required if using SSH private key authentication or both password and SSH private key authentication.



On the Algorithms tab, specify the authentication options and algorithms to use for this SFTP, SCP, or SSH connection. The following table describes the properties in the **Algorithms** tab:

Property	Description
Authentication	Specify the authentication option to use for this connection. The following options are available: <ul style="list-style-type: none"> <li>- gssapi-with-mic</li> <li>- publickey</li> <li>- password</li> <li>- keyboard-interactive</li> </ul>
Cipher	Specify the cipher option to use for this connection. The following options are available: <ul style="list-style-type: none"> <li>- aes256-cbc</li> <li>- aes192-cbc</li> <li>- aes128-cbc</li> <li>- 3des-cbc</li> <li>- blowfish-cbc</li> <li>- twofish256-cbc</li> <li>- twofish-cbc</li> <li>- twofish192-cbc</li> <li>- twofish128-cbc</li> <li>- serpent256-cbc</li> <li>- serpent192-cbc</li> <li>- serpent128-cbc</li> <li>- arcfour</li> <li>- idea-cbc</li> <li>- cast128-cbc</li> <li>- des-cbc</li> <li>- arcfour128</li> <li>- arcfour256</li> <li>- aes128-ctr</li> <li>- aes192-ctr</li> <li>- aes256-ctr</li> <li>- 3des-ctr</li> <li>- blowfish-ctr</li> <li>- twofish128-ctr</li> <li>- twofish192-ctr</li> <li>- twofish256-ctr</li> <li>- serpent128-ctr</li> <li>- serpent192-ctr</li> <li>- serpent256-ctr</li> <li>- idea-ctr</li> <li>- cast128-ctr</li> </ul>
Mac	Specify the mac connection option to use for this connection. The following options are available: <ul style="list-style-type: none"> <li>- hmac-md5</li> <li>- hmac-sha1</li> <li>- hmac-sha2-256</li> <li>- hmac-sha1-96</li> <li>- hmac-md5-96</li> </ul>
Compression	Specify the mac connection option to use for this connection. The following options are available: <ul style="list-style-type: none"> <li>- none</li> <li>- zlib</li> <li>- zlib@openssh.com</li> </ul>

The options on the Algorithms tab allow customization of the supported algorithms for each SSH server resource. The entries in the left column are the available algorithms and the entries in the right column are the selected algorithms. By selecting one or more algorithms, only those will be used during the communication. If no algorithms are selected for a section, the defaults for that section will be used.

During the handshake process, the selected options are negotiated with the server, starting with the entry at the top of the list. The first cipher and mac and compression algorithms to match an algorithm supported by the server will be used for the connection. If your company prefers certain algorithms over others, use the arrow buttons to move that cipher to the Selected column and to set the order with the most preferred algorithm at the top. Press the CTRL key while clicking to select multiple entries.

## Creating an MFT Connection

Create an MFT Connection to define communications for an MFT Hosted endpoint using a specific protocol.

1. In the Navigator, click **Partner Management > MFT Connections**.
2. To add an MFT Connection, click **New MFT Connection**, and then select the relevant connection type by protocol.
3. On the **Basic** tab, define the connection name, description, host, port, user, and password, as relevant.
4. Depending on the connection type, on the **Connection** tab, define the connection parameters such as timeout, retry attempts, and control encoding.
5. Depending on the connection type, on the **Proxy** tab, specify the proxy parameters.
6. For an FTP or FTPS connection type, on the **Directory Listing** tab, define the parameters only if the list parser must be customized.
7. For an SSH connection type, on the **SSH Keys** tab, specify the SSH Key parameters. On the **Algorithms** tab, specify the communication authentication type and algorithms.
8. For an AS2 connection type, on the **Message** tab, specify encryption, signatures, and receipt certificate parameters.
9. Click **Save**.

The **MFT Connections** page displays the MFT Connection.

### RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Remote Receive Endpoint” on page 106](#)
- [“Adding an Informatica Managed File Transfer Remote Send Endpoint” on page 107](#)

## Testing an MFT Connection

After you create or edit an MFT Connection, you can test it to ensure that the settings are correct.

1. In the Navigator, click **Partner Management > MFT Connections**.
2. When you finish adding or editing an MFT Connection, click **Test**.  
The **Test Results** window displays the results of the connection test.

# CHAPTER 7

## Endpoints

This chapter includes the following topics:

- [Endpoints Overview, 83](#)
- [Endpoint Types, 84](#)
- [Configuration Variables in Endpoints, 104](#)
- [Adding an Informatica Managed File Transfer Hosted Receive Endpoint, 105](#)
- [Adding an Informatica Managed File Transfer Hosted Send Endpoint, 105](#)
- [Adding an Informatica Managed File Transfer Remote Receive Endpoint, 106](#)
- [Adding an Informatica Managed File Transfer Remote Send Endpoint, 107](#)
- [Adding Local Endpoints, 108](#)
- [Editing and Deleting Endpoints, 108](#)
- [Processing Files with Informatica Intelligent Cloud Services Mappings, 109](#)
- [Processing Files with a Mass Ingestion Task, 111](#)
- [Adding Local Endpoints, 111](#)
- [Endpoint Error Events, 112](#)

## Endpoints Overview

Endpoints are points of entry or exit for documents in B2B Data Exchange. Endpoints specify how and where B2B Data Exchange sends and receives documents for specific partners or accounts.

You create endpoints as a part of the on-boarding process for one or more partners or accounts. B2B Data Exchange uses the information in the endpoint when a workflow runs for the partner or the account.

When you create endpoints, you define common properties, such as endpoint type, description, and partner or account. In addition, you define unique properties for each endpoint type.

For some endpoints, you can use configuration variables when you specify file name patterns. The configuration variables can represent object name, such as partners, accounts, or profiles. For example, use (\$partnerId) to represent the partner ID for which to process documents to or from the endpoint.

You can use the Operation Console to configure protocol communication parameters and details for Informatica Managed File Transfer endpoints. Before you can do this, you must install the Informatica Managed File Transfer application and enable Single Sign On.

Create an MFT Remote Receive Endpoint to use Informatica Managed File Transfer to receive files from a partner hosted server to the organization. Create an MFT Remote Send Endpoint to use Informatica Managed File Transfer to send files from the organization to the server hosted by the partner.

**Note:** Before you create an MFT Remote Send or MFT Remote Receive endpoint, create an MFT Connection. The MFT Connection defines how Informatica Managed File Transfer communicates with the remote server.

Create an MFT Hosted Receive Endpoint to receive files uploaded by the web users associated with the partner, to the services hosted by Informatica Managed File Transfer. Create an MFT Hosted Send Endpoint to send files to web users associated with the partner.

**Note:** Before you create an MFT Hosted Send endpoint or MFT Hosted Receive endpoint, create an MFT Web User. The MFT Web User is an account that supports partner communication with the organization-hosted servers, defined in Informatica Managed File Transfer as Services. Managed File Transfer Services support FTP, FTPS, SFTP, HTTPS, and AS2 protocols.

## Endpoint Types

The endpoint type that you create depends on the communication method between B2B Data Exchange and the partner.

The following table describes the types of endpoints that you can define:

Endpoint Type	Description
File Receive	File system directory for incoming files from partners or accounts.
File Send	File system directory for outgoing files to partners or accounts.
JMS Receive	Incoming JMS messages.
JMS Send	Outgoing messages to any JMS queue.
Web Service Receive	Location for incoming files that are sent by the DX_Endpoint Web service. You cannot create Web Service Receive endpoints in the Operation Console. The B2B Data Exchange administrator manages Web Service Receive endpoints in the Web Service API.
Informatica MFT Hosted Receive	<p>The following protocols are supported for the services hosted in the Informatica Managed File Transfer:</p> <ul style="list-style-type: none"> <li>- FTP</li> <li>- FTPS</li> <li>- SFTP</li> <li>- HTTPS</li> <li>- AS2</li> </ul> <p><b>Note:</b> The endpoint is not directly associated with any protocol, but rather primarily stores information about the partner MFT Web User. The MFT Web User is an account that supports partner communication with the organization-hosted services.</p>

Endpoint Type	Description
Informatica MFT Hosted Send	<p>The following protocols are supported for the services hosted in the Informatica Managed File Transfer:</p> <ul style="list-style-type: none"> <li>- FTP</li> <li>- FTPS</li> <li>- SFTP</li> <li>- HTTPS</li> <li>- AS2</li> </ul> <p><b>Note:</b> The endpoint is not directly associated with any protocol, but rather primarily stores information about the partner MFT Web User. The MFT Web User is an account that supports partner communication with the organization-hosted services.</p>
Informatica MFT Remote Receive	<p>Mailbox on a server hosted in the partner DMZ that uses a specific protocol for incoming documents. The following protocols are available:</p> <ul style="list-style-type: none"> <li>- FTP</li> <li>- FTPS</li> <li>- SSH (SFT/SCP/SSH)</li> <li>- AS2</li> <li>- HTTP</li> <li>- HTTPS</li> <li>- SMTP</li> </ul> <p><b>Note:</b> The endpoint is not directly associated with any protocol, but obtains the protocol information from the Informatica Managed File Transfer project with which the endpoint is associated.</p>
Informatica MFT Remote Send	<p>Mailbox on a server hosted in the partner DMZ that uses a specific protocol for outgoing documents. The following protocols are available:</p> <ul style="list-style-type: none"> <li>- FTP</li> <li>- FTPS</li> <li>- SSH (SFT/SCP/SSH)</li> <li>- AS2</li> <li>- HTTP</li> <li>- HTTPS</li> <li>- SMTP</li> </ul> <p><b>Note:</b> The endpoint is not directly associated with any protocol, but obtains the protocol information from the Informatica Managed File Transfer project with which the endpoint is associated.</p>

## RELATED TOPICS:

- [“Adding Local Endpoints” on page 108](#)

## Common Endpoint Properties

When you add an endpoint, you define common properties for all endpoint types on the **General** tab of the **New Endpoint** page.

The following table describes the common endpoint properties:

Property	Description
Account	The account associated with the endpoint. You can either associate the endpoint with a specific account or leave the <b>Account</b> field empty to instruct B2B Data Exchange to process documents for all accounts to or from the endpoint.
Connectivity Guide	Add a connectivity guide that describes how the partner configures communications with the organization. If you choose to select and upload a file, it can then be viewed from the Partners Portal.
Description	Description of the endpoint.
Name	Name of the endpoint.
Partner	Partner to associate with the endpoint. You can either associate the endpoint with a specific partner or leave the <b>Partner</b> field empty to instruct B2B Data Exchange to process documents for all partners to or from the endpoint.
Status	Operational status of the endpoint. Default value is <b>Enabled</b> .
Type	Type of the endpoint.
Enable Portal File Exchange	Indicates whether files for this endpoint can be uploaded, downloaded, or deleted using the Partners Portal. Applies only to endpoint types File receive and File send.

## RELATED TOPICS:

- [“Adding Local Endpoints” on page 108](#)

# File Receive Endpoint Properties

In addition to the basic properties that you define on the **General** tab of the **New Endpoint** page, you also define unique properties for the File Receive endpoint type on the **File Receive Options** tab of the **New Endpoint** page.

The following table describes the File Receive endpoint **Receiving Options** properties:

Property	Description
Use endpoint root directory	<p>Specifies whether to store incoming documents in the root directory of the endpoint. The administrator defines the root directory path in the <code>dx.endpoint.file.prefix.path</code> system property.</p> <p>For example, if B2B Data Exchange stores all documents in <code>H:/comserver/partners_msg/</code>, the administrator can add this path to the system property and define a variable name for the path, such as <code>Partners_Root</code>. Use this name instead of the full root directory path, and add only a partner name, such as <code>&lt;Partners_Root&gt;&lt;MyPartner&gt;</code>.</p>
Incoming file path	<p>Path to the folder in which to store incoming files. You can include configuration variables in the incoming file path.</p>
Pass by reference	<p>Passes documents that B2B Data Exchange receives through this endpoint to PowerCenter by reference. When you pass documents by reference, PowerCenter stores the file path in the repository instead of the actual file.</p> <p>Pass large files by reference to improve performance and optimize storage.</p>
Add Pattern...	<p>List of all of the file patterns that the endpoint can receive. B2B Data Exchange picks up files that match one of these file patterns. You can select one or more of the following file pattern types:</p> <ul style="list-style-type: none"><li>- For Profile. Instructs B2B Data Exchange to use a specific profile when it processes documents with the specific file pattern. To process files with an Informatica Intelligent Cloud Services (Data Integration) mapping, select a profile associated with the relevant Informatica Cloud workflow.</li><li>- For Application. Instructs B2B Data Exchange to use a specific application when it processes documents with the specific file pattern.</li><li>- None. Instructs B2B Data Exchange to process all documents with the specific file pattern.</li></ul> <p>You must configure at least one file name pattern.</p>
File name pattern	<p>File pattern that B2B Data Exchange receives through the endpoint. You can use variables (<code>\$xxx</code>) and the asterisk (*) wildcard in the file name pattern.</p>
Regular expression	<p>Create a regular expression to identify the file name that B2B Data Exchange receives through the endpoint.</p>
Regular Expression Partial Match	<p>When you define a regular expression, B2B Data Exchange checks the file path and file name that follows the defined endpoint root directory and incoming file path for a match. If you use a regular expression that does not match the path or name structure, the files are not matched. For example, the endpoint file name is <code>text.in</code> and you do not check for a period as part of the regular expression. You entered <code>[a-z]+</code> instead of <code>[a-z]+\.</code>. The file is not matched. To check any part of the file path and file name for a match, select the <b>Regular Expression Partial Match</b> option.</p>

You can define the files that the endpoint can receive with a file name pattern, or a regular expression, or both. When you define a regular expression, B2B Data Exchange checks the file path and name after the defined endpoint root directory and incoming file path for a match. If you use a regular expression, the **Incoming file path** cannot include a configuration variable.

**Note:** The regular expression syntax is Java based. For more information about the regular expression syntax, see <http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html>.

If you use a regular expression and a file name pattern, B2B Data Exchange matches the elements in the regular expression to variables in the file name pattern. If the regular expression has more or less elements than the file name pattern, the endpoint files are processed according to the regular expression, but the file name pattern variables might not be matched to the regular expression elements.

The following table describes the File Receive endpoint **Backup** properties:

Property	Description
Enable backup	Saves a copy of each file that B2B Data Exchange receives through the endpoint. If you disable backup, B2B Data Exchange transfers the files from the endpoint to the target and then deletes the files.
Use endpoint root directory	Specifies whether to store the backup copies of the files in the root directory of the endpoint. The administrator defines the endpoint root directory in a system property. For example, if the root directory is <code>Z:\backup</code> , select <b>Use endpoint root directory</b> and enter the subdirectory path in the <b>Backup path</b> field. B2B Data Exchange stores the backup copies of the documents in <code>Z:\backup\&lt;subdirectory&gt;</code> .
Backup path	Path to the directory in which to save copies of the files.

The following table describes the File Receive endpoint **Store in HDFS** properties:

Property	Description
Store a copy in HDFS	Saves a copy of each file that B2B Data Exchange receives through the endpoint in a Hadoop file system (HDFS). <b>Note:</b> You cannot store files that B2B Data Exchange receives from directories with a file path that includes two back slashes ( <code>\</code> ), such as Windows network folders.
Use HDFS root directory	Stores the backup copies of the files in the root directory of the HDFS. The administrator defines the HDFS root directory in a system property. For example, if the root directory is <code>Z:\HDFS_storage</code> , select <b>Use HDFS root directory</b> and enter the subdirectory path in the <b>HDFS path</b> field. B2B Data Exchange stores the backup copies of the documents in the following location: <code>Z:\HDFS_storage\&lt;subdirectory&gt;</code> .
HDFS path	Path to the HDFS directory in which to save copies of the files.

The following table describes the File Receive endpoint **Advanced** properties:

Property	Description
Pick up file when size remains the same for <x> seconds	Pick up and process incoming files when the file size remains the same for a specific time interval. Select to help ensure that larger files are complete before B2B Data Exchange transfers them. Default value is 10.

## RELATED TOPICS:

- [“Adding Local Endpoints” on page 108](#)
- [“Configuration Variables in Endpoints” on page 104](#)



## File Send Endpoint Properties

In addition to the basic properties that you define on the **General** tab of the **New Endpoint** page, you also define unique properties for the File Send endpoint type on the **File Receive Options** tab of the **New Endpoint** page.

The following table describes the File Send endpoint properties:

Property	Description
Use endpoint root directory	Specifies whether to store outgoing documents in the root directory of the endpoint. The administrator defines the root directory path in the <code>dx.endpoint.file.prefix.path</code> system property.  For example, if B2B Data Exchange stores all documents in <code>H:/comserver/partners_msg/</code> , the administrator can add this path to the system property and define a variable name for the path, such as <code>Partners_Root</code> . Use this name instead of the full root directory path, and add only a partner name, such as <code>&lt;Partners_Root&gt;&lt;MyPartner&gt;</code> .
Outgoing file path	Path to the folder that contains outgoing files. You can include configuration variables in the outgoing file path.
File pattern	File pattern to which the outgoing file names must comply. You can use regular expressions and the asterisk (*) wildcard in the file name pattern.

### RELATED TOPICS:

- [“Adding Local Endpoints” on page 108](#)
- [“Configuration Variables in Endpoints” on page 104](#)

## JMS Receive Endpoint Properties

In addition to the basic properties that you define on the **General** tab of the **New Endpoint** page, you also define unique properties for the JMS Receive endpoint type on the **JMS Receive Options** tab of the **New Endpoint** page.

The following table describes the JMS Receive endpoint **JNDI** properties:

Property	Description
Use values from java.naming system properties	Uses the context factory and provider URL that are defined in the system properties.
Context factory	URL of the context factory with which to establish a JMS connection.
Provider URL	URL of the JNDI service provider.

The following table describes the JMS Receive endpoint **JMS** properties:

Property	Description
Connection factory	URL of the connection factory used to create a connection to the JMS.
Destination queue name	Destination queue name to use in the endpoint.

Property	Description
User name	User name for the JMS queue.
Password	Password for the JMS queue.

#### RELATED TOPICS:

- [“Adding Local Endpoints” on page 108](#)

## JMS Send Endpoint Properties

In addition to the basic properties that you define on the **General** tab of the **New Endpoint** page, you also define unique properties for the JMS Send endpoint type on the **JMS Send Options** tab of the **New Endpoint** page.

The following table describes the JMS Send endpoint **JNDI** properties:

Property	Description
Use values from java.naming system properties	Uses the context factory and provider URL defined in the system properties.
Context factory	URL of the context factory with which to establish a JMS connection.
Provider URL	URL for the JNDI service provider.

The following table describes the JMS Send endpoint **JMS** properties:

Property	Description
Connection factory	URL to the connection factory used to create a connection with the JMS.
Message type	Type of the message. You can send the following message types: <ul style="list-style-type: none"> <li>- Text</li> <li>- Bytes</li> </ul> Make sure that the message type matches the <b>Message Body Type</b> value in the DX_Return_Queue transformation in PowerCenter.
Destination queue name	Destination queue name to use in the endpoint.
User name	User name for the JMS queue.
Password	Password for the JMS queue.

## RELATED TOPICS:

- [“Adding Local Endpoints” on page 108](#)

## MFT Hosted Receive Endpoint Properties

Create an MFT Hosted Receive Endpoint to receive files uploaded by the web users associated with the partner, to the services hosted by the Informatica Managed File Transfer. Define properties for the MFT Hosted Receive endpoint type on the **Create New MFT Hosted Endpoint - Receive** page.

**Note:** Before you create an MFT Hosted Receive endpoint, create an MFT Web User for the endpoint.

The following table describes the **Basic** properties in the **Basic** tab:

Property	Description
Name	Name of the endpoint.
Endpoint Type	Specifies the type of endpoint, whether hosted or remote, send or receive.
Description	Provide a description for the endpoint.
Connectivity Guide	Add a connectivity guide that describes how the partner configures communications with the organization.
Partner	Partner to associate with the endpoint. You can either associate the endpoint with a specific partner or leave the Partner field empty to instruct B2B Data Exchange to process documents for all partners to or from the endpoint.
Account	The account associated with the endpoint.
Status	Operational status of the endpoint. Default value is Enabled.
Project	Optionally, select an Informatica Managed File Transfer project that defines additional file processing tasks. Informatica Managed File Transfer contains pre-configured projects that you can use out of the box, or you can create and use a customized project.  The following out of the box projects can be used: - DX_Hosted_PGP_Decrypt: Receive files using PGP encryption and decrypt the files. - DX_Hosted_Unzip: Receive and unzip the files.  After you select a project, the project variables are displayed. Define values for the project variables.  For general information about projects, see the <i>Informatica Managed File Transfer Guide</i> .

After you select a project, the project properties table displays variables that relate to the project.

If you select a pre-packaged DX\_Hosted\_PGP\_Decrypt project, define the following properties:

Property	Description
PGP_Key_RING	Mandatory. Select a pre-configured OpenPGP key ring.
PGP_Key_Passphrase	Specify the passphrase for decryptions using keyring.
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Hosted\_Unzip project, define the following properties:

Property	Description
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

The following table describes the **Receiving Options** properties in the **Processing** tab:

Property	Description
Pass by reference	<p>Passes documents that B2B Data Exchange receives through this endpoint to PowerCenter by reference. When you pass documents by reference, PowerCenter stores the file path in the repository instead of the actual file.</p> <p>Pass large files by reference to improve performance and optimize storage.</p>
Add Pattern...	<p>List of all of the file patterns that the endpoint can receive. B2B Data Exchange picks up files that match one of these file patterns. You can select one or more of the following file pattern types:</p> <ul style="list-style-type: none"> <li>- For Profile. Instructs B2B Data Exchange to use a specific profile when it processes documents with the specific file pattern.</li> <li>- For Application. Instructs B2B Data Exchange to use a specific application when it processes documents with the specific file pattern.</li> <li>- For MFT Project. Instructs B2B Data Exchange to process the file through the Project in Informatica Managed File Transfer. This option is enabled only when the endpoint is configured with a project.</li> <li>- None. Instructs B2B Data Exchange to processes all documents with the specific file pattern.</li> </ul> <p>You must configure at least one file name pattern.</p> <p><b>Note:</b> B2B Data Exchange picks up files that match the file name pattern after the following Informatica Managed File Transfer operations are completed:</p> <ul style="list-style-type: none"> <li>- For project or job runs, file matching and pick up is performed after archive tasks, decrypt operations, unzip operations, or untar operations.</li> <li>- For job tasks, file matching and pick up is performed after renaming files, or read/write operations.</li> <li>- For files tasks, file matching and pick up is performed after file upload, file download, file put operations, file get operations, AS2 transfer, MLLP transfer, or portal download.</li> </ul>
File name pattern	File pattern that B2B Data Exchange receives through the endpoint. You can use (\$xxx) variables in the file name pattern.
Regular expression	Create a regular expression to identify the file name that B2B Data Exchange receives through the endpoint.
Regular expression partial matched	If enabled, the regular expression is matched to any section of the file name and path that follows the defined endpoint root directory and incoming file path, so the match does not need to be exact. If cleared, the regular expression is treated as if the expression had the prefix ^ and postfix \$.

The following table describes the **Backup** properties in the **Processing** tab:

Property	Description
Enable backup	Saves a copy of each file that B2B Data Exchange receives through the endpoint. If you disable backup, B2B Data Exchange transfers the files from the endpoint to the target and then deletes the files.
Use endpoint root directory	Specifies whether to store the backup copies of the files in the root directory of the endpoint. The administrator defines the endpoint root directory in a system property. For example, if the root directory is Z:\backup, select <b>Use endpoint root directory</b> and enter the subdirectory path in the <b>Backup path</b> field. B2B Data Exchange stores the backup copies of the documents in Z:\backup\ <subdirectory&gt;.< td=""> </subdirectory&gt;.<>
Backup path	Path to the directory in which to save the backup copies of the files that B2B Data Exchange receives through the endpoint.

The following table describes the **Store in HDFS** properties in the **Processing** tab:

Property	Description
Store a copy in HDFS	Saves a copy of each incoming file that B2B Data Exchange receives through the endpoint in a Hadoop file system (HDFS). <b>Note:</b> You cannot store files that B2B Data Exchange receives from directories with a file path that includes two back slashes (\), such as Windows network folders.
Use HDFS root directory	Stores the backup copies of the incoming files in the root directory of the HDFS. The B2B Data Exchange administrator defines the HDFS root directory in a system property. For example, if the root directory is Z:\HDFS_storage, select <b>Use HDFS root directory</b> and enter the subdirectory path in the <b>HDFS path</b> field. B2B Data Exchange stores the backup copies of the documents in the following location: Z:\HDFS_storage\ <subdirectory&gt;.< td=""> </subdirectory&gt;.<>
HDFS path	Path to the HDFS directory in which to save copies of the incoming files.

The following table describes the **MFT Web User** properties in the **MFT Web Users** tab:

Property	Description
Add Web Users	Select from a list of all of the MFT Web Users that you can assign to the endpoint. You must add at least one MFT Web User. <b>Note:</b> you cannot associate a single MFT Web User to multiple hosted receive endpoints.
Username	The username of the MFT Web User.
First Name	The first name of the MFT Web User contact.
Last Name	The last name of the MFT Web User contact.
Email Address	The email address of the MFT Web User contact.
Status	Operational status of the MFT Web User. Default value is Enabled.
Organization	The organization associated with the MFT Web User.

## RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Hosted Receive Endpoint” on page 105](#)

## MFT Hosted Send Endpoint Properties

Create an MFT Hosted Send Endpoint to use Informatica Managed File Transfer to send files to the partner from an organization server. Define the properties for the MFT Hosted Send endpoint type on the **Create New MFT Hosted Endpoint - Send** page.

**Note:** Before you create an MFT Hosted Send endpoint, create an MFT Web User for the endpoint.

The following table describes the **Basic** properties in the **Basic** tab:

Property	Description
Name	Name of the endpoint.
Endpoint Type	Specifies the type of endpoint, whether hosted or remote, send or receive.
Description	Provide a description for the endpoint.
Connectivity Guide	Add a connectivity guide that describes how the partner configures communications with the organization.
Partner	Partner to associate with the endpoint. You can either associate the endpoint with a specific partner or leave the Partner field empty to instruct B2B Data Exchange to process documents for all partners to or from the endpoint.
Account	The account associated with the endpoint.
Status	Operational status of the endpoint. Default value is Enabled.

The following table describes the **Sending Options** properties:

Property	Description
Add Web Users	List of all of the MFT Web Users that you can assign to the endpoint. You must add an MFT Web User. You can only add a single MFT Web User. <b>Note:</b> You cannot add an MFT Web User that is associated with any other partner.
Username	The user name of the MFT Web User.
First Name	The first name of the MFT Web User contact.
Last Name	The last name of the MFT Web User contact.
Email Address	The email address of the MFT Web User contact.
Status	Operational status of the MFT Web User. Default value is Enabled.
Organization	The organization associated with the MFT Web User.
File name pattern	File pattern that defines the files the endpoint sends. You can use (\$xxx) variables in the file name pattern.

The following table describes the **Project** properties:

Property	Description
Project Name	<p>Optionally, select an Informatica Managed File Transfer project that defines additional file processing tasks. Informatica Managed File Transfer contains pre-configured projects that you can use out of the box, or you can create and use a customized project.</p> <p>The following out of the box projects can be used:</p> <ul style="list-style-type: none"> <li>- DX_Hosted_PGP_Encrypt: Encrypt the files with PGP encryption and then send the files.</li> <li>- DX_Hosted_Zip: Zip and then send the files.</li> </ul> <p>After you select a project, the project variables are displayed. Define values for the project variables.</p> <p>For general information about projects, see the <i>Informatica Managed File Transfer Guide</i>.</p>

After you select a project, the project properties table displays variables that relate to the project.

If you select a pre-packaged DX\_Hosted\_PGP\_Encrypt project, define the following properties:

Property	Description
PGP_Key_RING	Mandatory. Select a pre-configured OpenPGP key ring.
PublicKey_ID	Specify the ID of the key. The Key ID is used to identify which key to select.
Content_File_Suffix	Specifies an extension for the output file. Default value: <code>.txt</code>
Compressed_OutputFile_Suffix	Specifies an extension for the compressed output file. Default value: <code>.zip</code>
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Hosted\_Zip project, define the following properties:

Property	Description
Content_File_Suffix	Specifies an extension for the output file. Default value: <code>.txt</code>
Compressed_OutputFile_Suffix	Specifies an extension for the compressed output file. Default value: <code>.zip</code>
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

## RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Hosted Send Endpoint” on page 105](#)

## MFT Remote Receive Endpoint Properties

Create an MFT Remote Receive Endpoint to use Informatica Managed File Transfer to receive files from a service hosted on the partner server to the organization. Define the properties for the MFT Remote Receive endpoint type on the **Create New MFT Remote Endpoint - Receive** page.

**Note:** Before you create an MFT Remote Receive endpoint, create an MFT Connection for the endpoint.

The following table describes the MFT Remote Receive endpoint **Basic** properties in the **Basic** tab:

Property	Description
Name	Name of the endpoint.
Endpoint Type	Specifies the type of endpoint, whether hosted or remote, send or receive.
Description	Provide a description for the endpoint.
Connectivity Guide	Add a connectivity guide that describes how the partner configures communications with the organization.
Partner	Partner to associate with the endpoint. You can either associate the endpoint with a specific partner or leave the Partner field empty to instruct B2B Data Exchange to process documents for all partners to or from the endpoint.
Account	The account associated with the endpoint.
Status	Operational status of the endpoint. Default value is Enabled.

You must select a project in the **Project** properties in the **Basic** tab:

Property	Description
Project Name	<p>Select an Informatica Managed File Transfer project that defines communications between the partner and the organization. Informatica Managed File Transfer contains pre-configured projects that you can use out of the box, or you can create and use a customized project.</p> <p>The following out of the box projects can be used:</p> <ul style="list-style-type: none"> <li>- DX_Remote_FTP_Receive: Receive files using the FTP communications protocol.</li> <li>- DX_Remote_FTPS_Receive: Receive files using the FTPS communications protocol.</li> <li>- DX_Remote_HTTP_Get: Receive files using the HTTP communications protocol.</li> <li>- DX_Remote_HTTPS_Get: Receive files using the HTTPS communications protocol.</li> <li>- DX_Remote_SCP_Receive: Receive files using the SCP communications protocol.</li> <li>- DX_Remote_SFTP_Receive: Receive files using the SFTP communications protocol.</li> </ul> <p>For general information about projects, see the <i>Informatica Managed File Transfer Guide</i>.</p>

After you select a project, the project properties table displays variables that relate to the project.

If you select a pre-packaged DX\_Remote\_FTP\_Receive project, define the following properties:

Property	Description
Source_FTP_Connection	Mandatory. Select a pre-configured server connection from the list of available Managed File Transfer connections of the FTP type.
Source_Directory	Specify a directory from which files are downloaded. If no filters are defined, all files in this directory are downloaded. Default value: /.
RegEx_or_Wildcard	Specify whether to use a wild card filter or a regular expression filter to search for files to receive. Possible values are <b>Wildcard</b> or <b>RegEx</b> . Default value: <b>RegEx</b> .
File_Pattern_To_Download	Specify the file name pattern used to select the files that Informatica Managed File Transfer receives to the endpoint. Default value: <b>*.txt</b> .



Property	Description
Delete_From_Source_After_Download	Select whether or not to delete a file after it is downloaded. Default value: <b>true</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_FTPS\_Receive project, define the following properties:

Property	Description
Source_FTPS_Connection	Mandatory. Select a pre-configured connection from the list of the available Managed File Transfer connections of the FTPS type.
Source_Directory	Specify a directory from which files are downloaded. If no filters are defined, all files in this directory are downloaded. Default value: /.
RegEx_or_Wildcard	Specify whether to use a wild card filter or a regular expression filter to search for files to receive. Possible values are <b>Wildcard</b> or <b>RegEx</b> . Default value: <b>RegEx</b> .
File_Pattern_To_Download	Specify the file name pattern used to select the files that Informatica Managed File Transfer receives to the endpoint. Default value: <b>*.txt</b> .
Delete_From_Source_After_Download	Select whether or not to delete a file after it is downloaded. Default value: <b>true</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_HTTP\_Get project, define the following properties:

Property	Description
Source_HTTP_Connection	Mandatory. Select a pre-configured connection from the list of the available Managed File Transfer connections of the HTTP type.
Get_URI	Specify the URI with which to query the HTTP server.
Destination_File_Name	Specify the query destination file name. Default value: <b>destination.txt</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_HTTPS\_Get project, define the following properties:

Property	Description
Source_HTTPS_Connection	Mandatory. Select a pre-configured connection from the list of the available Managed File Transfer connections of the HTTPS type.
Get_URI	Specify the URI with which to query the HTTP server.
Destination_File_Name	Specify the query destination file name. Default value: <b>destination.txt</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_SCP\_Receive project, define the following properties:

Property	Description
Source_SCP_Connection	Mandatory. Select a pre-configured connection from the list of the available Managed File Transfer connections of the SCP type.
Source_Directory	Specify a directory from which files are downloaded. If no filters are defined, all files in this directory are downloaded. Default value: <b>/</b> .
File_Pattern_To_Download	Specify the file name pattern used to select the files that Informatica Managed File Transfer receives to the endpoint. Default value: <b>*.txt</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_SFTP\_Receive project, define the following properties:

Property	Description
Source_SFTP_Connection	Mandatory. Select a pre-configured connection from the list of the available Managed File Transfer connections of the SFTP type.
Source_Directory	Specify a directory from which files are downloaded. If no filters are defined, all files in this directory are downloaded. Default value: <b>/</b> .
Regex_or_Wildcard	Specify whether to use a wild card filter or a regular expression filter to search for files to receive. Possible values are <b>Wildcard</b> or <b>Regex</b> . Default value: <b>Regex</b> .
File_Pattern_To_Download	Specify the file name pattern used to select the files that Informatica Managed File Transfer receives to the endpoint. Default value: <b>*.txt</b> .
Delete_From_Source_After_Download	Select whether or not to delete a file after it is downloaded. Default value: <b>true</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

The following table describes the MFT Remote Receive endpoint **Receiving Options** properties in the **Processing** tab:

Property	Description
Pass by reference	<p>Passes documents that B2B Data Exchange receives through this endpoint to PowerCenter by reference. When you pass documents by reference, PowerCenter stores the file path in the repository instead of the actual file.</p> <p>Pass large files by reference to improve performance and optimize storage.</p>
Schedule	<p>Select one or more schedules for the endpoint. A schedule determines the pickup intervals for the endpoint. For example, you can choose to pick up each file when it arrives, or pick up files at specific time intervals regardless of the number of files.</p>
Add Pattern...	<p>List of all of the file patterns that the endpoint can receive. B2B Data Exchange picks up files that match one of these file patterns. You can select one or more of the following file pattern types:</p> <ul style="list-style-type: none"> <li>- For Profile. Instructs B2B Data Exchange to use a specific profile when it processes documents with the specific file pattern.</li> <li>- For Application. Instructs B2B Data Exchange to use a specific application when it processes documents with the specific file pattern.</li> <li>- None. Instructs B2B Data Exchange to processes all documents with the specific file pattern.</li> </ul> <p>You must configure at least one file name pattern.</p>
File name pattern	<p>File pattern that B2B Data Exchange receives through the endpoint. You can use (\$xxx) variables in the file name pattern.</p>

The following table describes the MFT Remote Receive endpoint **Backup** properties in the **Processing** tab:

Property	Description
Enable backup	<p>Saves a copy of each file that B2B Data Exchange receives through the endpoint. If you disable backup, B2B Data Exchange transfers the files from the endpoint to the target and then deletes the files.</p>
Use endpoint root directory	<p>Specifies whether to store the backup copies of the files in the root directory of the endpoint. The administrator defines the endpoint root directory in a system property.</p> <p>For example, if the root directory is Z:\backup, select <b>Use endpoint root directory</b> and enter the subdirectory path in the <b>Backup path</b> field. B2B Data Exchange stores the backup copies of the documents in Z:\backup\<subdirectory&gt;.< p=""> </subdirectory&gt;.<></p>
Backup path	<p>Path to the directory in which to save the backup copies of the files that B2B Data Exchange receives through the endpoint.</p>

The following table describes the MFT Remote Receive endpoint **Store in HDFS** properties in the **Processing** tab:

Property	Description
Store a copy in HDFS	Saves a copy of each incoming file that B2B Data Exchange receives through the endpoint in a Hadoop file system (HDFS). <b>Note:</b> You cannot store files that B2B Data Exchange receives from directories with a file path that includes two back slashes (\\), such as Windows network folders.
Use HDFS root directory	Stores the backup copies of the incoming files in the root directory of the HDFS. The B2B Data Exchange administrator defines the HDFS root directory in a system property.  For example, if the root directory is <code>Z:\HDFS_storage</code> , select <b>Use HDFS root directory</b> and enter the subdirectory path in the <b>HDFS path</b> field. B2B Data Exchange stores the backup copies of the documents in the following location: <code>Z:\HDFS_storage\&lt;subdirectory&gt;</code> .
HDFS path	Path to the HDFS directory in which to save copies of the incoming files.

#### RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Remote Receive Endpoint” on page 106](#)

## MFT Remote Send Endpoint Properties

Create an MFT Remote Send Endpoint to use Informatica Managed File Transfer to send files from the organization to the partner-hosted server. Define the properties for the MFT Remote Send endpoint type on the **Basic** tab of the **Create New MFT Remote Endpoint - Send** page.

**Note:** Before you create an MFT Remote Send endpoint, create an MFT Connection for the endpoint.

The following table describes the **Basic** properties in the **Basic** tab:

Property	Description
Name	Name of the endpoint.
Endpoint Type	Specifies the type of endpoint, whether hosted or remote, send or receive.
Description	Provide a description for the endpoint.
Connectivity Guide	Add a connectivity guide that describes how the partner configures communications with the organization.
Partner	Partner to associate with the endpoint. You can either associate the endpoint with a specific partner or leave the Partner field empty to instruct B2B Data Exchange to process documents for all partners to or from the endpoint.
Account	The account associated with the endpoint.
Status	Operational status of the endpoint. Default value is Enabled.

The following table describes the **Sending Options** properties:

Property	Description
File name pattern	File pattern of files that B2B Data Exchange sends through the endpoint. You can use (\$xxx) variables in the file name pattern. For more information, see <a href="#">"Configuration Variables in Endpoints" on page 104</a> .

You must select a project in the **Project** properties:

Property	Description
Project Name	<p>Select an Informatica Managed File Transfer project that defines communications between the partner and the organization. Informatica Managed File Transfer contains pre-configured projects that you can use out of the box, or you can create and use a customized project.</p> <p>The following out of the box projects can be used:</p> <ul style="list-style-type: none"> <li>- DX_Remote_MI_Send: Send files using the Data Integration mass ingestion task.</li> <li>- DX_Remote_AS2_Send: Send files using the AS2 communications protocol.</li> <li>- DX_Remote_FTP_Send: Send files using the FTP communications protocol.</li> <li>- DX_Remote_FTPS_Send: Send files using the FTPS communications protocol.</li> <li>- DX_Remote_HTTP_POST: Send files using the HTTP communications protocol.</li> <li>- DX_Remote_HTTPS_POST: Send files using the HTTPS communications protocol.</li> <li>- DX_Remote_SCP_Send: Send files using the SCP communications protocol.</li> <li>- DX_Remote_SFTP_Send: Send files using the SFTP communications protocol.</li> </ul> <p>For general information about projects, see the <i>Informatica Managed File Transfer Guide</i>.</p>

After you select a project, the project properties table displays variables that relate to the project.

If you select a pre-packaged DX\_Remote\_MI\_Send project, define the following properties:

Property	Description
MI_Source_Directory	Mandatory. Specify the server directory from which to send files that is specified in the mass ingestion task.
MI_Task_Name	Mandatory. Specify the name of the mass ingestion task.
MI_Project_Location	Mandatory. Specify the project folder location of the mass ingestion task.
Max_Time_Poll_MI	Optional. Specify the maximum polling time for the mass ingestion task in hours. Default: 1.

If you select a pre-packaged DX\_Remote\_AS2\_Send project, define the following properties:

Property	Description
Destination_AS2_Connection	Mandatory. Select a pre-configured server connection.
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.
DX_RequestReceipt	Optional. Specify whether or not to request a receipt from the server. Default value: <b>none</b> .

Property	Description
DX_Receipt_Destination	Optional. Specify if and where the receipt, if any, should be sent. Default value: <b>discard</b> .
DX_Receipt_Destination_File	Optional. Specify the location of the file to which the receipt should be saved. Default value: <b>discard</b> .
DX_Receipt_Destination_File_overwrite	Optional. Specify the action to take when the receipt file already exists. Default value: <b>rename</b> .
DX_Receipt_email	Specify the email address to which the receipt, if any, should be sent. Required if Receipt Destination is set to email.
DX_Receipt_URL	Specify the URL to which the receipt, if any, should be sent. Required if Receipt Destination is set to <b>url</b> .
DX_Content_Type	Specify the value to send in the Content-Type header field when making the request. Default value: <b>multipart/mixed</b> .

If you select a pre-packaged DX\_Remote\_FTP\_Send project, define the following properties:

Property	Description
Destination_FTP_Connection	Mandatory. Select a pre-configured server connection.
Destination_Directory	Optional. Specify a partner server directory to which to send files. Default value: <b>/</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_FTPS\_Send project, define the following properties:

Property	Description
Destination_FTPS_Connection	Mandatory. Select a pre-configured server connection.
Destination_Directory	Optional. Specify a partner server directory to which to send files. Default value: <b>/</b> .
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_HTTP\_POST project, define the following properties:

Property	Description
Destination_HTTP_Connection	Mandatory. Select a pre-configured server connection.
Destination_URI	Specify the URI to which files will be uploaded.

Property	Description
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_HTTPS\_POST project, define the following properties:

Property	Description
Destination_HTTPS_Connection	Mandatory. Select a pre-configured server connection.
Destination_URI	Specify the URI to which files will be uploaded.
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_SCP\_Send project, define the following properties:

Property	Description
Destination_SCP_Connection	Mandatory. Select a pre-configured server connection.
Destination_Directory	Optional. Specify a partner server directory to which to send files. Default value: /.
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

If you select a pre-packaged DX\_Remote\_SFTP\_Send project, define the following properties:

Property	Description
Destination_SFTP_Connection	Mandatory. Select a pre-configured server connection.
Destination_Directory	Optional. Specify a partner server directory to which to send files. Default value: /.
SMTP_Server	Specify the SMTP server that receives error notifications.
Email_For_Notification	Specify the email address that receives error notifications.

## RELATED TOPICS:

- [“Adding an Informatica Managed File Transfer Remote Send Endpoint” on page 107](#)

# Configuration Variables in Endpoints

You can use configuration variables to include object names in the value of endpoint properties, such as a file or directory path. B2B Data Exchange sets the values for these variables when you run a workflow for a profile through an endpoint.

For example, if you enter the `($accountNumber)_report.txt` file name pattern in a File Receive endpoint, when B2B Data Exchange receives a document that matches the file name pattern, such as `20534_report.txt`, it processes the document through the File Receive endpoint.

**Note:** If you associate an endpoint or a profile with a specific partner or account, B2B Data Exchange ignores the partner or account configuration variables.

The following table describes the variables you can use in the file or directory patterns:

Variable	Description
<code>(\$sequence)</code>	Sequential number generated by B2B Data Exchange.
<code>(\$application)</code>	Application name.
<code>(\$accountId)</code>	Unique identifier for the account. B2B Data Exchange generates the account ID when you create a account. <b>Note:</b> If you import the account into another instance of B2B Data Exchange, B2B Data Exchange generates another account ID.
<code>(\$accountNumber)</code>	Account number. If you use <code>(\$accountId)</code> and <code>(\$accountNumber)</code> , B2B Data Exchange ignores this variable.
<code>(\$partnerId)</code>	Unique identifier for the partner. B2B Data Exchange generates the partner ID when you create a partner. <b>Note:</b> If you import the partner into another instance of B2B Data Exchange, B2B Data Exchange generates another partner ID.
<code>(\$partnerName)</code>	Partner name. If you use <code>(\$partnerId)</code> and <code>(\$partnerName)</code> , B2B Data Exchange ignores this variable.
<code>(\$profileId)</code>	Unique identifier for the profile. B2B Data Exchange generates the profile ID when you create a profile. <b>Note:</b> If you import the profile into another instance of B2B Data Exchange, B2B Data Exchange generates another profile ID.
<code>(\$profileName)</code>	Profile name. If you use <code>(\$profileId)</code> and <code>(\$profileName)</code> , B2B Data Exchange ignores this variable.

## RELATED TOPICS:

- [“File Receive Endpoint Properties” on page 87](#)
- [“File Send Endpoint Properties” on page 89](#)



# Adding an Informatica Managed File Transfer Hosted Receive Endpoint

Create an MFT Hosted Receive Endpoint to use Informatica Managed File Transfer to receive files from the partner to an Informatica Managed File Transfer server hosted by the organization.

Before you create an MFT Hosted Receive endpoint, create an MFT Web User.

1. In the Navigator, click **Partner Management > Endpoints**.
2. To add an endpoint, click **New Endpoint**, and select **MFT Endpoint**.
3. To add an MFT Hosted Receive endpoint, select **MFT Hosted Receive** from the list.  
The **Create New MFT Hosted Endpoint - Receive** page appears.
4. On the **Basic** tab, define the endpoint name, partner, account, and status.
5. Optionally, select a project and specify values for the project variables.
6. On the **Processing** tab, define the **Receiving Options** properties. Select whether to pass documents by reference or to add a file name pattern.
7. Define the **Backup** properties. Select whether to enable backup, use the endpoint root directory for backup, and define a backup path.
8. Define the **Store in HDFS** properties. Select whether to store a copy of the file in HDFS, use the HDFS root directory for backup, and define an HDFS path.
9. On the **MFT Web Users** tab, select a Web User.  
**Note:** A Web User cannot be assigned to more than one endpoint.
10. Click **Save**.  
The **Endpoints** page displays the endpoint.

## RELATED TOPICS:

- [“MFT Hosted Receive Endpoint Properties” on page 91](#)
- [“Managed File Transfer Web Users Overview” on page 59](#)
- [“Creating an MFT Web User” on page 64](#)

# Adding an Informatica Managed File Transfer Hosted Send Endpoint

Create an MFT Hosted Send Endpoint to use Informatica Managed File Transfer to send files to the partner from an Informatica Managed File Transfer server hosted by the organization.

Before you create an MFT Hosted Send endpoint, create an MFT Web User.

1. In the Navigator, click **Partner Management > Endpoints**.
2. To add an endpoint, click **New Endpoint**, and select the **MFT Endpoint** endpoint type from the list.
3. To add an MFT Hosted Send endpoint, select **MFT Hosted Send** from the list.  
The **Create New MFT Hosted Endpoint - Send** page appears.

4. On the **Basic** tab, define the endpoint name, partner, account, and status.
5. Optionally, select a project and specify values for the project variables.
6. Select a Web User.  
**Note:** A Web User cannot be assigned to more than one endpoint.
7. Define the **Sending Options** properties. Select a file name pattern to specify the types of files the endpoint sends.
8. Select a Project.  
After you select a project, the **Project** properties table displays variables that relate to the project.
9. Define the properties in the **Project** properties table.
10. Click **Save**.  
The **Endpoints** page displays the endpoint.

#### RELATED TOPICS:

- [“MFT Hosted Send Endpoint Properties” on page 94](#)
- [“Managed File Transfer Web Users Overview” on page 59](#)
- [“Creating an MFT Web User” on page 64](#)

## Adding an Informatica Managed File Transfer Remote Receive Endpoint

Create an MFT Remote Receive Endpoint to use Informatica Managed File Transfer to receive files from the partner-hosted server to the organization.

Before you create an MFT Remote Receive endpoint, create an MFT Connection.

1. To add an endpoint, click **New Endpoint**, and select the **MFT Endpoint** endpoint type from the list.
2. To add an MFT Remote Receive endpoint, select **MFT Remote Receive** from the list.  
The **Create New MFT Remote Endpoint - Receive** page appears.
3. On the **Basic** tab, define the endpoint name, partner, account, and status.
4. Select a Project.  
After you select a project, the **Project** properties table displays variables that relate to the project.
5. On the **Processing** tab, define the **Receiving Options** properties. Select whether to pass documents by reference.
6. To add a schedule, select a schedule from the list and then click **Add Schedule**.
7. Specify the file name pattern used to select the files that the endpoint receives.  
You must configure at least one file name pattern.
8. Define the **Backup** properties. Select whether to enable backup, use the endpoint root directory for backup, and define a backup path.
9. Define the **Store in HDFS** properties. Select whether to store a copy of the file in HDFS, use the HDFS root directory for backup, and define an HDFS path.

10. Click **Save**.

The **Endpoints** page displays the endpoint.

#### RELATED TOPICS:

- [“MFT Remote Receive Endpoint Properties” on page 95](#)
- [“Managed File Transfer Connections Overview” on page 65](#)
- [“Creating an MFT Connection” on page 82](#)

## Adding an Informatica Managed File Transfer Remote Send Endpoint

Create an MFT Remote Send Endpoint to use Informatica Managed File Transfer to send files from the organization to a partner-hosted server.

Before you create an MFT Remote Send create an MFT Connection.

1. In the Navigator, click **Partner Management > Endpoints**.
2. To add an endpoint, click **New Endpoint**, and select the **MFT Endpoint** endpoint type from the list.
3. To add an MFT Remote Send endpoint, select **MFT Remote Send** from the list.  
The **Create New MFT Remote Endpoint - Send** page appears.
4. On the **Basic** tab, define the endpoint name, partner, account, and status.
5. Define the **Sending Options** properties. Specify a file name pattern used to identify which files to send from the endpoint.
6. Select a Project.  
After you select a project, the **Project** properties table displays variables that relate to the project.
7. Define the properties in the **Project** properties table.
8. Click **Save**.

The **Endpoints** page displays the endpoint.

#### RELATED TOPICS:

- [“MFT Remote Send Endpoint Properties” on page 100](#)
- [“Managed File Transfer Connections Overview” on page 65](#)
- [“Creating an MFT Connection” on page 82](#)

# Adding Local Endpoints

You can add a local (non-Informatica Managed File Transfer) endpoint to specify how and where documents are stored for processing by B2B Data Exchange.

1. In the Navigator, click **Partner Management > Endpoints**.  
The **Endpoints** page appears.
2. To add an endpoint, click **New Endpoint**, and select a local endpoint type from the list.  
The **New Endpoint** page appears.
3. In the **General** tab, enter values for the general endpoint properties.
4. Click the **Options** tab for the endpoint type that you want to define, and enter values for the unique endpoint properties.
5. Click **Save**.  
The **Endpoints** page displays the endpoint.

## RELATED TOPICS:

- [“Endpoint Types” on page 84](#)
- [“Common Endpoint Properties” on page 86](#)
- [“File Receive Endpoint Properties” on page 87](#)
- [“File Send Endpoint Properties” on page 89](#)
- [“JMS Receive Endpoint Properties” on page 89](#)
- [“JMS Send Endpoint Properties” on page 90](#)

# Editing and Deleting Endpoints

You can modify endpoint properties or delete an endpoint that you no longer use.

1. In the Navigator, click **Partner Management > Endpoints**.  
The **Endpoints** page appears.
2. Choose to edit or delete an endpoint.
  - To edit an endpoint, click the **Edit** icon next to the endpoint that you want to edit, and modify the properties of the endpoint.
  - To delete an endpoint, click the **Delete** icon next to the endpoint that you want to remove.

# Processing Files with Informatica Intelligent Cloud Services Mappings

You can use a Cloud Data Integration mapping to transfer enterprise data assets in a flat file format from on-premises to cloud ecosystems. You can create inbound endpoints to transfer files processed with a Cloud Data Integration mapping over Informatica Cloud.

## Before you use Cloud Data Integration

Before you use Cloud Data Integration to create and run mappings, ensure that you have an active Informatica Intelligent Cloud Services account, have defined user roles through the Administrator, and have a relevant license. Ensure that you install the Secure Agent on the same machine as B2B Data Exchange. For more information, see the *Informatica Intelligent Cloud Services Administrator Guide*.

## Configure the B2B Data Exchange system properties

Configure the following system properties in B2B Data Exchange:

- dx.iics.url
- dx.iics.username
- dx.iics.password
- dx.iics.runtime.environment
- dx.iics.max.poll.time.minutes
- dx.iics.object.prefix

For more information, see the *B2B Data Exchange Administrator Guide*.

## Create a mapping in Cloud Data Integration

Create a mapping with a flat file source transformation, Expression transformations, any additional transformations whose functionality you wish to use, and a target transformation.

You must parametrize the source transformation connection and source type. For example, for the source transformation connection, create `_Src_Connection_Param`, and for the source type, create `_Src_Type_Param`.

You must create an Expression transformation with a parameter for the input file path, and you can also define parameters for the flat file source formatting. For more information, see [“Input File Parameters” on page 110](#) and [“Formatting Options for Flat File Sources” on page 110](#).

For more information about transformations, see the *Informatica Intelligent Cloud Services Transformations Guide*.

## Create a workflow in B2B Data Exchange

Create a workflow with an `Informatica Cloud workflow` flow type, and select the Cloud Data Integration mapping for the workflow.

For more information, see the *B2B Data Exchange Developer Guide*.

## Create a profile

Create a profile and associate it with the Informatica Cloud workflow. The mapping parameters that you created in the Expression transformations are displayed as workflow parameters. You can configure the mapping input file parameter and flat file formatting parameters as part of the workflow parameters associated with the profile.

### Create an endpoint

Create an inbound endpoint such as a File Receive endpoint. As part of the file pattern configuration, select the profile associated with the Informatica Cloud workflow.

## Input File Parameters

Most Cloud Data Integration transformations require the file path of an input file to be passed from the Source transformation to the transformation. The integrated Cloud Data Integration mapping must use a flat file source connection and a source object that are parameterized to support integration with B2B Data Exchange, so we cannot obtain the input file path directly from the source connection.

To enable the Cloud Data Integration mapping to obtain the input file path, you create an Expression transformation parameter for the input file parameter, and use the Expression transformation to pass the input file path to the downstream transformation in the mapping.

Create an expression parameter named `Prop_DxInputFilePath` of type `output field` in the Expression transformation.

B2B Data Exchange automatically populates the value for this parameter during runtime. The parameter is read-only and hidden in the B2B Data Exchange Operations Console by default as the value for this parameter is passed automatically during runtime.

## Formatting Options for Flat File Sources

You can format flat file source connections for Cloud Data Integration mappings using Expression transformation parameters.

When you create a flat file source, note that B2B Data Exchange supports only the **Delimited** formatting option. B2B Data Exchange does not support the **Fixed Width** option.

The flat file formatting parameters are created with predefined names. These parameter values are later defined in B2B Data Exchange using workflow parameters and passed back to Cloud Data Integration.

You can create the following expression parameters:

- `Prop_SrcFormattingOpt_Delimiter`. Define a delimiter. Accepts text values as follows:
  - Comma resolves to `,` which is the default setting.
  - Semicolon resolves to `;`
  - Colon resolves to `:`
  - Tab resolves to `\T`
  - Any other value is passed directly as text.
- `Prop_SrcFormattingOpt_TextQualifier`. Define a text qualifier. Accepts text values as follows:
  - Double Quote resolves to `\"` which is the default setting.
  - None resolves to `none`
  - Single Quote resolves to `'`
  - Any other value is considered an error. The default value is passed instead.
- `Prop_SrcFormattingOpt_FirstDataRow`. Identify the first data row.
- `Prop_SrcFormattingOpt_ImportRow`. Import the header from a row.
- `Prop_SrcFormattingOpt_EscapeChar`. Defines an escape character.

For more information about Expression transformations, see *Informatica Intelligent Cloud Services Transformations Guide*.

# Processing Files with a Mass Ingestion Task

You can use a mass ingestion task to transfer enterprise data assets in a flat file format from on-premises to cloud ecosystems such as Amazon S3 data stores and Amazon Redshift data warehouses in the cloud using FTP, SFTP, and FTPS standard protocols. You can create an MFT Remote Send endpoint to enable file transfer with a Cloud Data Integration mass ingestion task over Informatica Cloud.

## Import the custom task and project into Informatica Managed File Transfer

Before you can use the custom Informatica Managed File Transfer task and project to run the Data Integration mass ingestion task, import the relevant task and project. For more information, see the *Informatica Managed File Transfer Installation and Configuration Guide*.

## Before you use Cloud Data Integration

Before you can use Cloud Data Integration to create and run tasks, ensure that you have an active Informatica Intelligent Cloud Services account, have defined user roles through the Administrator, and have a relevant license. Ensure that you install the Secure Agent on the same machine as B2B Data Exchange. For more information, see the *Informatica Intelligent Cloud Services Administrator Guide*.

## Configure the B2B Data Exchange system parameters

Configure the following system properties:

- dx.iics.url
- dx.iics.username
- dx.iics.password
- dx.iics.runtime.environment
- dx.iics.max.poll.time.minutes
- dx.iics.object.prefix

After you configure the properties, restart B2B Data Exchange. For more information, see the *B2B Data Exchange Administrator Guide*.

## Create a mass ingestion task in Data Integration

Create a mass ingestion task with valid source and target transformations. For more information, see the *Informatica Intelligent Cloud Services Deploy Guide*.

## Create an MFT Remote Send endpoint in B2B Data Exchange

1. Create an MFT Remote Send endpoint.
2. Select the DX\_Remote\_MI\_Send project for the endpoint.
3. Enter values for the project parameters.

# Adding Local Endpoints

You can add a local (non-Informatica Managed File Transfer) endpoint to specify how and where documents are stored for processing by B2B Data Exchange.

1. In the Navigator, click **Partner Management > Endpoints**.  
The **Endpoints** page appears.
2. To add an endpoint, click **New Endpoint**, and select a local endpoint type from the list.

The **New Endpoint** page appears.

3. In the **General** tab, enter values for the general endpoint properties.
4. Click the **Options** tab for the endpoint type that you want to define, and enter values for the unique endpoint properties.
5. Click **Save**.

The **Endpoints** page displays the endpoint.

#### RELATED TOPICS:

- [“Endpoint Types” on page 84](#)
- [“Common Endpoint Properties” on page 86](#)
- [“File Receive Endpoint Properties” on page 87](#)
- [“File Send Endpoint Properties” on page 89](#)
- [“JMS Receive Endpoint Properties” on page 89](#)
- [“JMS Send Endpoint Properties” on page 90](#)

## Endpoint Error Events

For each error that occurs when B2B Data Exchange processes a file through an endpoint, B2B Data Exchange generates an event with an **Error** status and adds a log entry. For each subsequent error for the same document, B2B Data Exchange updates the status of the existing event and adds another log entry.

After you resolve an endpoint error, you can change the event status from **Error** to a different value. Changing the event status helps you differentiate between multiple errors that occur within the same document.



# CHAPTER 8

## Events

This chapter includes the following topics:

- [Events Overview, 113](#)
- [Event Actions, 114](#)
- [Basic Event Search Properties, 115](#)
- [Advanced Event Search Properties, 115](#)
- [Message Processing Event Types and Statuses, 117](#)
- [Informatica Managed File Transfer Logs, 118](#)
- [Archived Events, 118](#)

## Events Overview

An event is a representation of a document at a particular stage of processing. The B2B Data Exchange server generates events as it processes documents, and it changes the status of the events as they go through the transformation process.

When the B2B Data Exchange server receives a file that contains documents to process, it generates an event associated with the file. This initial event is a file-level event. It is the root event for the file and is the parent event for all other events that the B2B Data Exchange server generates during the course of processing the documents in the file. The workflow that processes the document can generate child events of the file-level event during document processing.

You monitor and perform actions on events in the Operation Console. You can view all events on the Event List page. You can perform a basic or advanced search for events, and drill down to a specific event to view event details.

You can view parent events and child events for system events, user events, and monitor events. To track a set of events, you can create an event monitor and set up the rules for the events to be included in the monitor. You can create multiple event monitors to track events for different profiles or to track different types of events. You can configure the monitor to notify you of changes to the events that you track.

You can view all events that the B2B Data Exchange server generated since the last archive. To keep the volume of events displayed in the Operation Console at a manageable level, archive the events regularly. If you archive events with the B2B Data Exchange accelerator for Informatica Data Archive from the B2B Data Exchange repository to the history database, you can view the archived events in the Operation Console.

# Event Actions

You can perform actions on events from the **Event List** page based on the event status, state, or other requirements in your organization.

The following table describes actions that you can perform on events:

Action	Description
Reprocess	Reprocesses the documents of the selected event.
Resend	Resends the target documents of the selected event.
Change event status	Changes the status of the selected events in the Change Event Status pop-up window.
Release	Releases the selected delayed events.
Discard	Discards all of the selected events. The status of the selected events is changed to Discarded, but the events are not deleted.
Export event list to a CSV file	Creates a .csv file that contains all of the events in the event list. You can then convert the file to Excel format.

## Managing Events on the Event List Page

In the **Event List** page, you can view a list of events, an overview summary of events, and event details. You can also drill to parent and child events and perform actions on events.

1. In the Navigator, click **Events > Event List**.
2. To display events that were created within a specific time range, select a value from the **Time frame** list.
3. To change the default time frame, select a new value and click **Set as default time frame**.

**Note:** On Windows operating systems, the default time frame applies to the current browser for the current Windows account. If you use multiple browsers for the same Windows account, you need to define a default time frame for each browser.

4. To view a summary of all of the events that were created within the time frame according to the event type and status, click **Overview**.

The overview displays the total number of events for each event type and status. Each total number contains a link that you can click to display the list of events for that event type or status.

5. To view details for a specific event, click the event ID for the event that you want to view.

The **Details** section displays information about the event.

6. To drill to parent or child events for which you have viewing privileges, click the **Drill Up** or **Drill Down** icon next to the event that you want to view.

The **Details** section displays information about the child or parent event.

7. To perform an action on one or more events, select the events and click **Actions**.

The **Actions** list displays the actions that you can perform on the selected events.

# Basic Event Search Properties

You can perform a basic search for events based on the event type or status. You can also filter the search results according to a specific time frame.

The following table describes basic event properties for which you can perform a basic search:

Property	Description
Event ID	Unique identifier for the event.
Partner Name	Name of the related partner.
Account	Name or identifier of the related account.
Event Type	Type of the event.
Event Status	Status of the event. This list contains two properties: <ul style="list-style-type: none"><li>- State. Indicates whether the event is still processing or reached a final status.</li><li>- Status. Current progress of the event, regardless of whether the event finished processing.</li></ul>

## Performing a Basic Search for Events

You can perform a basic search for events. The search results appear in a list or in an overview summary according to the event type and status. You cannot perform a basic search in child events.

1. In the Navigator, click **Events > Event List**.
2. If the Advanced Search pane appears, click **Basic search**.
3. In the **Find** field, enter the search string.
4. To search in the subject field, select **Include subject field**.  
**Note:** If you select this check box, the search may be slower.
5. Click **Go** to start the search.

The Event List page displays the list of events that match the search criteria.

# Advanced Event Search Properties

In addition to the basic search criteria, you can perform an advanced search for specific event properties.

The following table describes event properties for which you can perform an advanced search:

Property	Description
Account	Account associated with the event.
Aggregated Status	The aggregated status of all child events.
Comment	Comment associated with the event.

Property	Description
Event Attributes	Attributes of the event. Click <b>Browse</b> and select up to 3 attributes and operators in the <b>Event Attributes Search Criteria</b> window.
Event ID	ID of the event.
Event Status	Status of the event.
Event Type	The type of event.
Operation	Select whether all search properties apply together or whether any of them may apply to the search.
Parent Event ID	Unique identifier of the parent events for any events that match the search criteria.
Partner	Partner associated with the event.
Profile	Name of the related profile.
Reconciliation Status	Status of associated reconciliations.
Reconciliation Type	Type of associated reconciliations.
Subject	Subject associated with the event.
Show child events	Indicates whether to perform the search in child events. Cleared by default.
Time frame	Time frame in which the event occurred.

## Performing an Advanced Search for Events

In addition to the basic search criteria, you can perform an advanced search for specific event properties. You can also search for parent and child events.

1. In the Navigator, click **Events > Event List**.
2. If the Advanced Search pane is hidden, click **Advanced search**.
3. Select a search operator:
  - **And**. Search for all of the fields that contain values.
  - **Or**. Search for any of the fields that contain values.
4. To search in child events, select the **Show child events** check box.
5. Enter values in the event properties that you want to search and click **Go**.

The **Event List** page displays the search results. If you selected to show child or parent events, the **Drill Up** or **Drill Down** columns display links to parent or child events for which you have viewing privileges, and the event ID appears when you hover the mouse over the icon for the event that you want to view.

# Message Processing Event Types and Statuses

B2B Data Exchange provides a set of default B2B Data Exchange event types and event statuses for message processing events.

## Default Event Types

When B2B Data Exchange processes messages, it assigns the following event types to message processing events:

- Custom Event. Indicates a predefined custom event.
- File Level Event. Indicates an 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. Indicates an event associated with groups included in a document.
- Segment Level Event. Indicates an event associated with segments included in a document.
- System Event. Indicates an event generated by the B2B Data Exchange server for system notifications.
- Transaction Level Event. Indicates an event associated with transactions included in a document.

## Default Event Statuses

For message processing events, B2B Data Exchange assigns the following event statuses:

- Complete. Assigned when the event completes processing. Child events might, however, still be processing. Message reconciliation can be completed later.
- 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.
- Error. Assigned when the event processing produces an error.
- Critical. Assigned when the event processing produces a critical error.
- Reprocessed. Assigned when the event is processed again.
- Warning. Can be assigned when the event processing produces specific problematic states.
- New. This event type is not currently used.
- Rejected. Assigned when the message was rejected.
- Transferring. Assigned while the message is transferred from B2B Data Exchange to an outbound endpoint. After the transfer is finished, B2B Data Exchange changes the event type to Complete or Error depending on the result.
- 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.

## Aggregated Statuses

An Aggregated status indicates the overall state of message processing. When an event has child events, for example when a file contains several transactions, the aggregated status indicates the status of all the child events. B2B Data Exchange assigns the following aggregated statuses:

- Delayed: Assigned if message processing is delayed due to processing rules, or if message processing waits for a processing rule to release the message, or if message processing waits to be manually released.
- Error: Assigned when the event processing produces an error.
- Final: Assigned when the event processing finalizes.

- In Process: Assigned while the event is processing.

## Informatica Managed File Transfer Logs

Informatica Managed File Transfer logs are integrated with the B2B Data Exchange Event Log.

For endpoints associated with an Informatica Managed File Transfer project, the Event Logs panel displays the file send jobs and receive jobs with a link to related Managed File Transfer jobs. To view the Managed File Transfer job details, click the link and the job details are displayed in a separate tab.

For Informatica Managed File Transfer hosted endpoints, the event details also provide access to service jobs that log the files that MFT Web Users upload to the organization-hosted server.

## Archived Events

You can view archived events in the Operation Console for short-term archiving that the B2B Data Exchange performs with Informatica Data Archive to the history database.

Use the **Archived Events** page of the Operation Console to access the archived events and view events for which you have viewing privileges. You can perform an advanced search for events. The advanced search properties are similar to the advanced search properties for other event pages.

You can view detailed information about the events, such as the creation time, status, and type. You can also export the archived events list to a CSV file. The archived events appear in read-only mode. You cannot modify the event details, status, or state.

You cannot view archived events from the file archive in the Operation Console. To view archived events in the file archive, use Informatica Data Archive.

## Viewing Archived Events in the Operation Console

Use the **Archived Events** page in the Operation Console to view events that the B2B Data Exchange administrator archives to the history database with Informatica Data Archive. You can view only events for which you have viewing privileges that the B2B Data Exchange assigned to you.

1. In the Navigator, click **Events > Archived Events**.  
The **Archived Events** page displays the time frame from which you can select to view archived events. By default, the page does not display any events.
2. To display archived events, enter values in the search fields and click **Go**.  
**Note:** If you only enter a time frame in the search, the results may take longer to appear.
3. To view event details, click the event ID for the event that you want to view.  
The **Details** section displays information for the selected event.
4. To export the archived events list to a CSV file, click **Actions > Export to CSV** and select a location in which to save the file.

## CHAPTER 9

# Event Monitors

This chapter includes the following topics:

- [Event Monitors Overview, 119](#)
- [Creating an Event Monitor, 119](#)
- [Viewing Monitored Events, 124](#)

## Event Monitors Overview

You can create an event monitor to track a set of events. You can configure an event monitor to notify you when an event is generated or the status of an event changes. Use event monitors to get notification on events that may need attention, such as events with error status.

Event monitors run continuously to capture changes to events. You can run an event monitor manually or configure it to run on a schedule. You cannot run a monitor that is disabled.

Event monitors can be set up to deliver captured events to the Advanced Exception Handling module. To do this, choose the Deliver event and create issue option on the Event Monitor screen. For more information on Advanced Exception Handling, see [Chapter 13, “Advanced Exception Handling” on page 144](#).

You can view event monitors that are configured to send you notification. You must have the Monitors Full Access privilege to view monitors that you create. If you do not have the Monitors Full Access privilege and you create a monitor that you do not configure to send you notification, you cannot view the monitor or the events in the monitor.

## Creating an Event Monitor

Event monitors track events based on the event type and status. You can also define different monitors to track events generated for specific workflows, partners, and accounts.

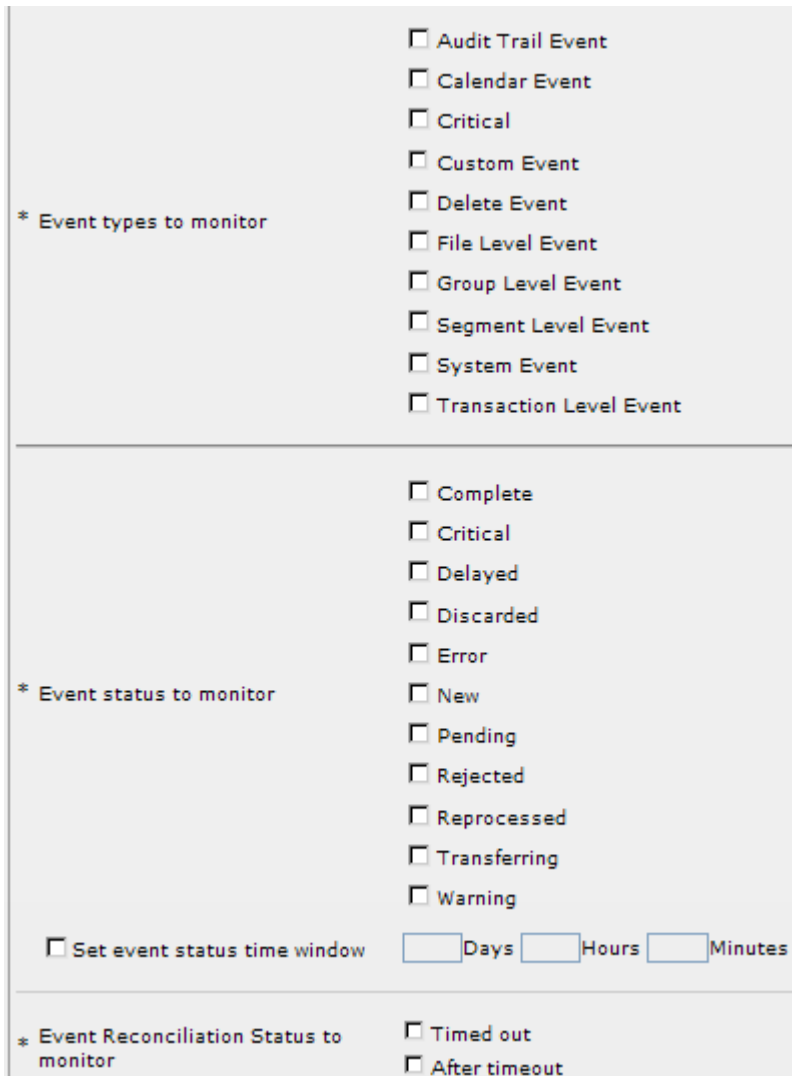
1. In the Navigator, click **Event Monitors > Monitors**.
2. Click **New Monitor**.

The Create Monitor page appears.



The screenshot shows a 'Create monitor' dialog box. At the top right are 'Save' and 'Cancel' buttons. Below the title bar, there is a '\* Name' field with the text 'Monty' and a 'Monitor Categories' field with a browse button (...). The 'Events' section is highlighted in blue.

3. Enter a name for the event monitor.
4. To select categories to monitor, click **Browse**.
5. Select the event type or status to monitor.



The screenshot shows two sections of the 'Create Monitor' page. The first section, '\* Event types to monitor', has a list of event types with checkboxes: Audit Trail Event, Calendar Event, Critical, Custom Event, Delete Event, File Level Event, Group Level Event, Segment Level Event, System Event, and Transaction Level Event. The second section, '\* Event status to monitor', has a list of event statuses with checkboxes: Complete, Critical, Delayed, Discarded, Error, New, Pending, Rejected, Reprocessed, Transferring, and Warning. Below this list is a checkbox for 'Set event status time window' followed by three input fields for 'Days', 'Hours', and 'Minutes'. The third section, '\* Event Reconciliation Status to monitor', has a list of reconciliation statuses with checkboxes: Timed out and After timeout.

**Note:** You can monitor only event type and status or reconciliation status, but not both. If you want to define a reconciliation monitor, follow the steps in [“Creating a Reconciliation Monitor” on page 126](#).

6. If you monitor event status, select **Set event status time window** to define the amount of time that an event must remain in specific status before the monitor reports this event. For example, if you set the time window to 2 days and 15 hours, the monitor reports the event only after the event remains in the specific status for 2 days and 15 hours.



7. To monitor events associated with a specific partner, select the radio button next to the **Partner** field, click **Browse**, and select a partner from the list.

The screenshot shows a configuration panel titled "Partners, accounts, and workflows". It contains three sections, each with a radio button and a text input field with a "Browse" button:

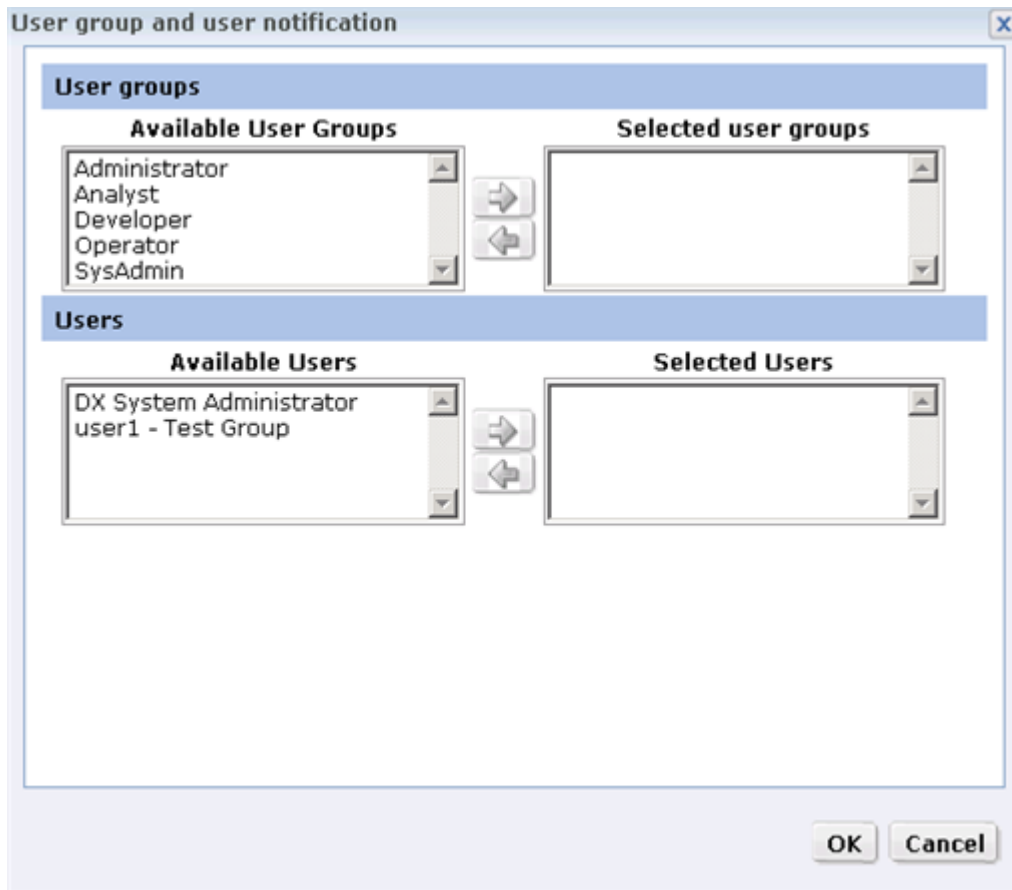
- Partner:** Radio button selected next to "All partners".
- Accounts:** Radio button selected next to "All accounts". The text input field contains "(none)".
- Workflows:** Radio button selected next to "All workflows".

8. To monitor events associated with one or more accounts for the selected partner, select an account from the list. Use the **Shift** key to select multiple accounts.
9. To monitor events associated with a specific workflow, click the radio button next to the **Workflow** list, click **Browse**, and select one or more workflows from the list.
10. To be notified when events that match the monitor criteria do not occur, select **Report if event does NOT occur**.

The screenshot shows a configuration panel titled "Notification". It contains the following options:

- Exception:** A checkbox labeled "Report if event does NOT occur" is currently unchecked.
- Users and User Groups:** A text input field.
- Action after notification:** A list of radio button options:
  - Deliver event only
  - Deliver event and send email
  - Deliver event and run workflow [text input field]
  - Deliver event and run profile (none) [text input field]
  - Deliver event and create issue
- Batch notification

- To specify the user accounts and user groups to notify, click **Users and User Groups** and select from the lists.



**Note:** You can choose multiple users and multiple user groups. When you select a user group, all the users in that group are notified.

- Select the action that the Data Exchange Server should take when the monitor reports events that match the monitor criteria:

Action After Notification	Description
Deliver event only	Add the event to the list of events in the event monitor and display the event in the console.
Deliver event and send email	Add the event to the list of events in the event monitor and send an email to the selected users.
Deliver event and run workflow	Add the event to the list of events in the event monitor and run a workflow. Click the <b>Select Workflow</b> button to select the workflow to run after the delivery.
Deliver event and run profile	Add the event to the list of events in the event monitor and run a workflow associated with a profile. Click the <b>Select Profile</b> button to select a partner, account, and profile. After delivery, the Data Exchange Server runs the workflow associated with the selected profile.

Action After Notification	Description
Deliver event and create issue	Add the event to the list of events in the event monitor and create an advanced exception handling issue.
Batch notification	Select to send a single email that contains a list of all events that the monitor found. Otherwise, each event is sent in a separate email. <b>Note:</b> The maximum number of events that can be sent in a single email is 200. If more than 200 events are found, the notifications are sent in multiple emails.

**Note:** To send email notifications, you must configure a mail server for B2B Data Exchange. For more information, see the *B2B Data Exchange Installation and Configuration Guide*. The user account to which you send email notifications must have valid email addresses.

13. Select the priority level for email notifications from the **Select Priority** list.

A screenshot of a web form showing a dropdown menu labeled 'Select Priority'. The menu is open, displaying three options: 'High', 'Medium', and 'Low'. The 'Select Priority' text is visible at the top of the dropdown.

14. To change the status of the events that the monitor reports, select **Change event status** and select a status from the **Target event status** list.

A screenshot of a configuration interface showing the 'Actions' section. The 'Change event status' checkbox is checked. Below it, the 'Target event status' dropdown menu is set to 'Rejected'.

15. To suspend monitor activity on holidays, select the name of the calendar that contains the relevant holidays from the **Holiday Calendar** list.

A screenshot of a web form showing a dropdown menu labeled 'Holiday Calendar'. The menu is open, displaying the option '(none)'.

16. Select the frequency at which the monitor runs:

Frequency	Description
Disabled	Do not run the monitor according to a schedule. When a monitor is disabled, you cannot run the monitor.
Custom	Run the monitor in a specific time interval in hours and minutes.
Daily	Run the monitor at a specific time every day.

Frequency	Description
Weekly	Run the monitor at a specific hour once a week. If a scheduled run occurs on a holiday, select the action that the Data Exchange Server performs: <ul style="list-style-type: none"> <li>- <b>Skip run.</b> Do not run the monitor during the holiday week. The Data Exchange Server runs the monitor the following week.</li> <li>- <b>Run before holiday.</b> Run the monitor one day before the day of the scheduled run.</li> <li>- <b>Run after holiday.</b> Run the monitor one day after the day of the scheduled run.</li> </ul>
Monthly	Run the monitor at a specific hour once a month. . When a scheduled run falls on a holiday, select the action that the Data Exchange Server performs: <ul style="list-style-type: none"> <li>- <b>Skip run.</b> Do not run the monitor during the holiday month. The Data Exchange Server runs the monitor the following week.</li> <li>- <b>Run before holiday.</b> Run the monitor one day before the day of the scheduled run.</li> <li>- <b>Run after holiday.</b> Run the monitor one day after the day of the scheduled run.</li> </ul>

17. Click **Save**.

## Viewing Monitored Events

You can view events that the monitor found in the following lists:

- **User events.** List of events found by monitors that are configured to send you notifications. If you create a monitor that does not send you notification, the events for that monitor are not included in the user events list. The user events list can display events from multiple event monitors.
- **Events for a monitor.** List of events that match the monitor criteria. This list includes the total number of events found by a specific monitor and the number of events that you did not view.

When you view monitored events, you can see the same type of information as when you view all events. You can perform basic and advanced search. You can also drill into parent and child events.

1. In the Navigator, click **Event Monitors > User Events**.

**Note:** The User Events node displays the number of events you did not view in square brackets.

2. To view the details of an event, click the event ID.

The Operation Console displays the Event Details section below the list of events.

3. To drill into a parent event or a child event, click the **Drill Up** or **Drill Down** icon.

# CHAPTER 10

## Reconciliations

This chapter includes the following topics:

- [Reconciliations Overview, 125](#)
- [Creating a Reconciliation Monitor, 126](#)
- [Updating a Reconciliation, 129](#)
- [Reconciliation Problems, 132](#)

### Reconciliations Overview

Reconciliation is the process of correlating an event with another event.

An example of reconciliation is when you send a document file to a partner containing transactions such as payments or orders that require acknowledgment. When you send the file to the partner, the Data Exchange Server initiates a reconciliation. When you receive the acknowledgment from the partner, the Data Exchange Server completes the reconciliation. The Data Exchange Server uses a correlation ID to identify each transaction and to reconcile the initial event with the acknowledgement.

When the Data Exchange Server initiates a reconciliation for an event, it sets a limit to the amount of time that the reconciliation can take to complete. The reconciliation status of an event indicates whether the Data Exchange Server completed the reconciliation within the time limit.

### Reconciliation Monitors

The Data Exchange Server requires a reconciliation monitor to track events and update the status of the reconciliations. The schedule you set for the reconciliation monitor determines how often the Data Exchange Server updates the status of the reconciliations. If you do not create reconciliation monitors, the Data Exchange Server does not update the reconciliation status of any event.

When a reconciliation monitor runs, the Data Exchange Server updates the status of the reconciliations for the events within the scope of the monitor. If you create multiple reconciliation monitors with the same scope and the monitors run at different times, the monitors find the reconciliations at different stages. When the first monitor runs and finds an event that falls within the scope of the monitor, it can change the status of the event. If the status changes, the other monitors do not find the same event because the new reconciliation status does not fall within the scope of the monitor.

For example, you create reconciliation monitor A to track reconciliations for account 100 with status Reconciled after timeout and schedule it to run at 8:00 a.m. every day. You also create reconciliation monitor B to track reconciliations for account 100 with status Reconciled after timeout and schedule it to run at 10:00 a.m. every day. When monitor A runs, the Data Exchange Server finds one event for account 100 with the

status Reconciled after timeout. It changes the status to Reconciliation complete. When monitor B runs, the Data Exchange Server does not find any event for account 100 with status Reconciled after timeout.

You can configure the reconciliation monitor to notify you of the events that fall within the scope of the reconciliation monitor. You can use the reconciliation monitor to determine whether the reconciliations are completed in a timely manner. If a large number of reconciliations do not complete within the timeout limit, you might need to raise the timeout limit or modify the document reconciliation process.

## Creating a Reconciliation Monitor

You can monitor reconciliation status in the same way you monitor event type and status.

1. In the Navigator, click **Event Monitors > Monitors**.
2. Click **New Monitor**.
3. The Create Monitor page appears.

The screenshot shows a form with two main input areas. The first is labeled '\* Name' and contains an empty text box. Below it is a section for 'Monitor Categories' with an information icon (i) and a dropdown menu that is currently empty, followed by a three-dot menu icon.

4. Enter a name for the reconciliation monitor.
5. Select the reconciliation status to monitor.

The screenshot shows a section titled '\* Event Reconciliation Status to monitor'. It contains two radio button options: 'Timed out' and 'After timeout'. Both radio buttons are currently unselected.

You can create the following types of reconciliation monitors:

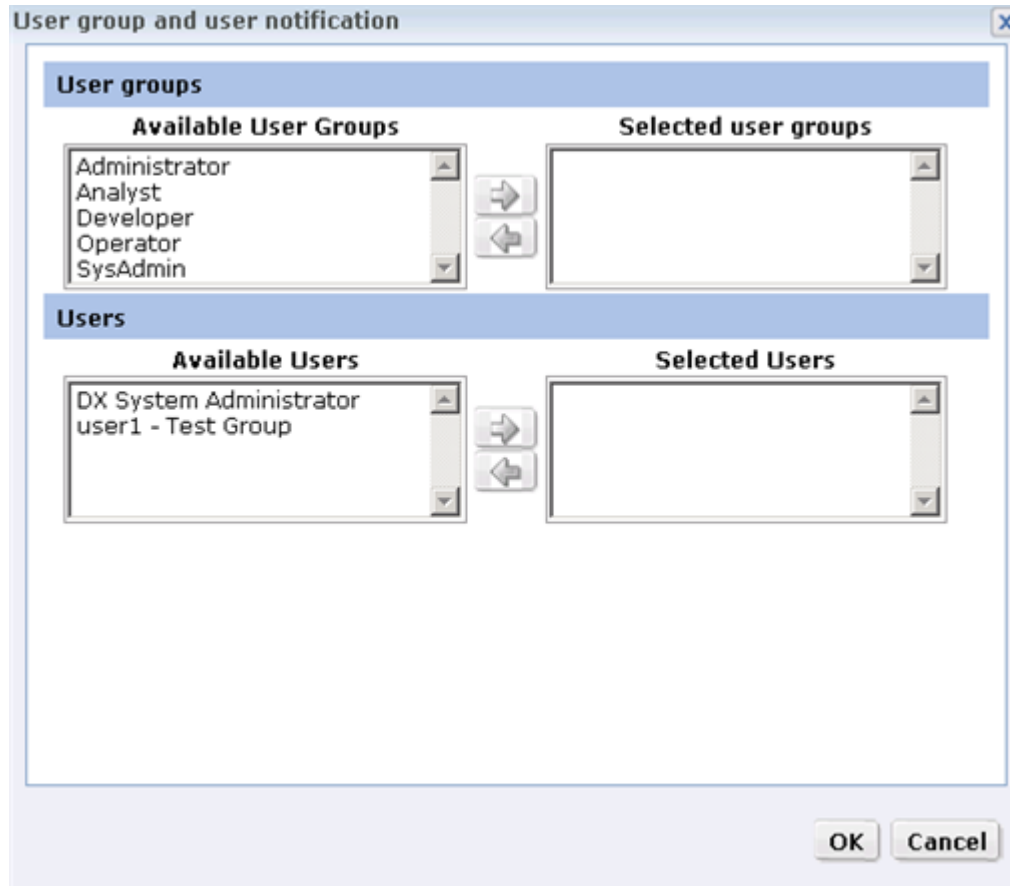
Monitor	Description
Timed out	Change the reconciliation status of the specified events to <b>Timed out</b> if no acknowledgment was received for the event within the time limit.
After timeout	Change the reconciliation status of the specified events to <b>After timeout</b> if an acknowledgement was received for the event after the time limit.

**Note:** You can monitor only event type and status or reconciliation status, but not both. If you want to define an event monitor, follow the steps in [“Creating an Event Monitor” on page 119](#).

6. To monitor event reconciliations associated with a specific partner, select the radio button next to the **Partner** field, click **Browse**, and select a partner from the list.

The screenshot shows a section titled 'Partners, accounts, and workflows'. It contains three radio button options: 'All partners', 'All accounts', and 'All workflows'. The 'All partners' radio button is selected. Below each radio button is a text box with a 'Browse' button. The 'All accounts' text box currently contains '(none)'. The 'All workflows' text box is empty.

7. To monitor event reconciliations associated with one or more accounts for the selected partner, select an account from the list. Use the `Shift` key to select multiple accounts.
8. To monitor event reconciliations associated with a specific workflow, click the radio button next to the **Workflow** list, click **Browse**, and select one or more workflows from the list.
9. To specify the user accounts and user groups to notify, click **Users and User Groups** and select from the lists.



**Note:** You can choose multiple users and multiple user groups. When you select a user group, all the users in that group are notified.

10. Select the action that the Data Exchange Server should take when the monitor reports events that match the monitor criteria:

Action After Notification	Description
Deliver event only	Add the event to the list of events in the event monitor and display the event in the console.
Deliver event and send email	Add the event to the list of events in the event monitor and send an email to the selected users.
Deliver event and run workflow	Add the event to the list of events in the event monitor and run a workflow. Click the <b>Select Workflow</b> button to select the workflow to run after the delivery.

Action After Notification	Description
Deliver event and run profile	Add the event to the list of events in the event monitor and run a workflow associated with a profile. Click the <b>Select Profile</b> button to select a partner, account, and profile. After delivery, the Data Exchange Server runs the workflow associated with the selected profile.
Deliver event and create issue	Add the event to the list of events in the event monitor and create an advanced exception handling issue.
Batch notification	Select to send a single email that contains a list of all events that the monitor found. Otherwise, each event is sent in a separate email. <b>Note:</b> The maximum number of events that can be sent in a single email is 200. If more than 200 events are found, the notifications are sent in multiple emails.

**Note:** To send email notifications, you must configure a mail server for B2B Data Exchange. For more information, see the *B2B Data Exchange Installation and Configuration Guide*. The user account to which you send email notifications must have valid email addresses.

- Select the priority level for email notifications from the **Select Priority** list.

- To change the status of the events that the monitor reports, select **Change event status** and select a status from the **Target event status** list.

- To suspend monitor activity on holidays, select the name of the calendar that contains the relevant holidays from the **Holiday Calendar** list.

- Select the frequency at which the monitor runs:

Frequency	Description
Disabled	Do not run the monitor according to a schedule. When a monitor is disabled, you cannot run the monitor.
Custom	Run the monitor in a specific time interval in hours and minutes.
Daily	Run the monitor at a specific time every day.



Frequency	Description
Weekly	Run the monitor at a specific hour once a week. If a scheduled run occurs on a holiday, select the action that the Data Exchange Server performs: <ul style="list-style-type: none"> <li>- <b>Skip run.</b> Do not run the monitor during the holiday week. The Data Exchange Server runs the monitor the following week.</li> <li>- <b>Run before holiday.</b> Run the monitor one day before the day of the scheduled run.</li> <li>- <b>Run after holiday.</b> Run the monitor one day after the day of the scheduled run.</li> </ul>
Monthly	Run the monitor at a specific hour once a month. . When a scheduled run falls on a holiday, select the action that the Data Exchange Server performs: <ul style="list-style-type: none"> <li>- <b>Skip run.</b> Do not run the monitor during the holiday month. The Data Exchange Server runs the monitor the following week.</li> <li>- <b>Run before holiday.</b> Run the monitor one day before the day of the scheduled run.</li> <li>- <b>Run after holiday.</b> Run the monitor one day after the day of the scheduled run.</li> </ul>

15. Click **Save**.

## Updating a Reconciliation

When you view a list of events, user events, or events for a specific monitor, you can view and change the reconciliation status of the event.

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

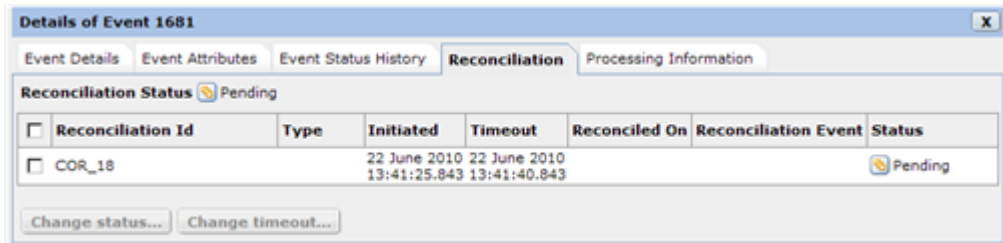
The Event List page appears.

Drill Up	Drill Down	Event Id	Partner	Account	Profile	Start Time	Event type	Event status	Reconciliation
<input type="checkbox"/>		2493	PartnerTestSimpleDX133	AccountTestSimpleDX133	ProfileTestSimpleDX133 (1202)	14 May 2011 03:24	File Level Event	Complete	
<input type="checkbox"/>		2485	PARTNER8040	ACCOUNT804001		14 May 2011 03:11	File Level Event	Complete	
<input type="checkbox"/>		2484	PARTNER8040	ACCOUNT804001	PROFILE8040 (1201)	14 May 2011 03:11	File Level Event	Pending	
<input type="checkbox"/>		2475	PARTNER6430	ACCOUNT643001	PROFILE6430 (1200)	14 May 2011 03:11	File Level Event	Pending	
<input type="checkbox"/>		2466	PARTNER8612	ACCOUNT861201		14 May 2011 03:10	System Event	Error	
<input type="checkbox"/>		2465	PARTNER8612	ACCOUNT861201	PROFILE8612 (1199)	14 May 2011 03:10	File Level Event	Pending	
<input type="checkbox"/>		2456	PARTNER6413	ACCOUNT641301	PROFILE6413 (1198)	14 May 2011 03:10	Transaction Level Event	Pending	
<input type="checkbox"/>		2455	PARTNER6413	ACCOUNT641301	PROFILE6413 (1198)	14 May 2011 03:10	Segment Level Event	Complete	
<input type="checkbox"/>		2446	PARTNER8610	ACCOUNT861001	PROFILE8610 (1197)	14 May 2011 03:09	Segment Level Event	Complete	
<input type="checkbox"/>		2437	PARTNER8606	ACCOUNT860601	PROFILE8606 (1196)	14 May 2011 03:09	File Level Event	Complete	
<input type="checkbox"/>						14 May	System	Error	

2. Click the event ID of an event with an entry in the **Reconciliation Status** column.

The Details page appears.

- Click the **Reconciliation** tab.

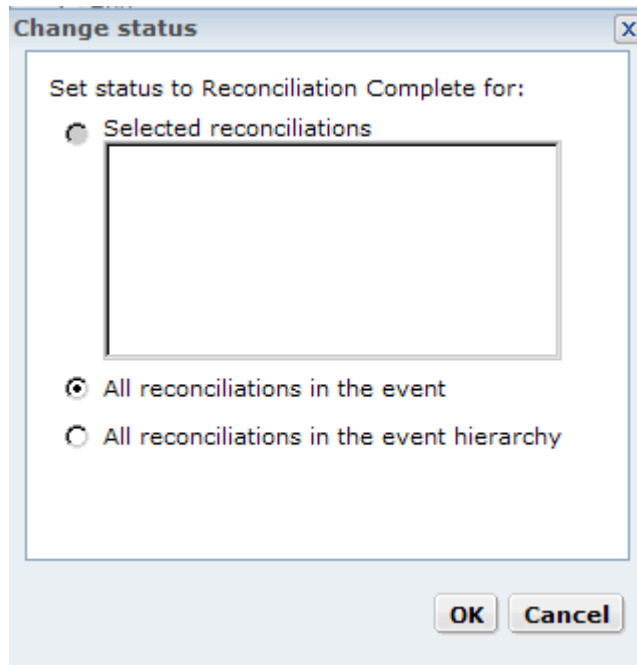


The following table describes the event reconciliation properties:

Property	Description
Reconciliation Status	Status of the reconciliation process.
Reconciliation ID	Identifier of the reconciliation request.
Type	Type of the reconciliation.
Initiated	Date and time on which the reconciliation request was submitted.
Timeout	Date and time on which the reconciliation must be completed.
Reconciled on	Date and time on which the reconciliation was completed.
Reconciliation Event	Identifier of the event that was created when the reconciliation completed successfully.
Status	Status of the event.

To change the reconciliation status of an event, select the check box next to the reconciliation ID and click **Change Status**.

The Change Status window appears.



**Note:** You can select multiple reconciliations.

4. Set the reconciliation status to **Reconciliation Complete** for one of the following options:

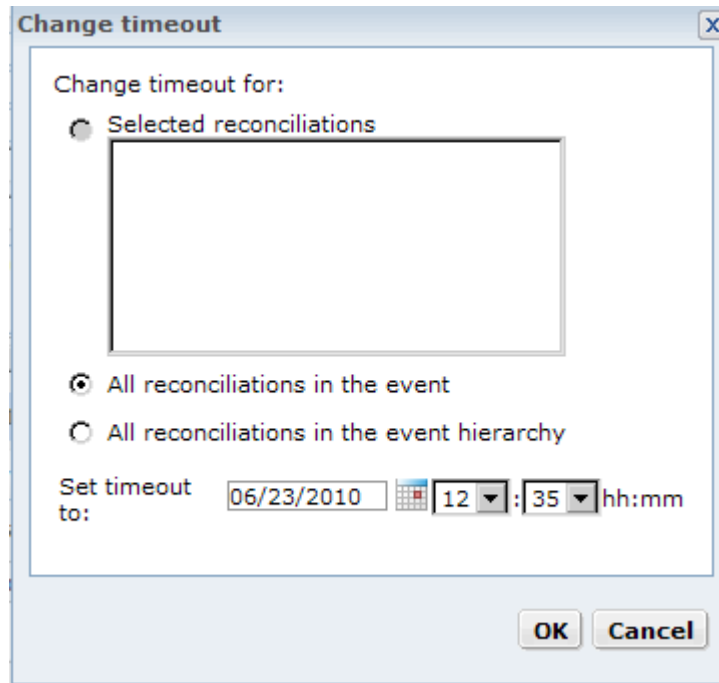
Option	Description
Selected reconciliations	Set the status of the selected reconciliations.
All reconciliations in the event	Set the status of all of the reconciliations that are associated with the event. <b>Note:</b> This is equivalent to selecting all off the reconciliations in the Reconciliation tab.
All reconciliations in the event hierarchy	Set the status of all of the reconciliations for this event and all of the related events, including parent and child events.

5. Click **OK**.

The Reconciliation Status displays the new status.

6. To change the timeout deadline for a reconciliation, select the check box next to the reconciliation ID and click **Change Timeout**.

The Change Timeout window appears.



**Note:** You can select multiple reconciliations.

7. Set the reconciliation timeout for one of the following options:

Option	Description
Selected reconciliations	Set the timeout of the selected reconciliations.
All reconciliations in the event	Set the timeout of all of the reconciliations that are associated with the event. <b>Note:</b> This is equivalent to selecting all off the reconciliations in the Reconciliation tab.
All reconciliations in the event hierarchy	Set the timeout of all of the reconciliations for this event and all of the related events, including parent and child events.

8. Click the calendar icon and select the new timeout date. Click **Apply** to close the calendar tool.
9. Set the new timeout hour and minute and click **OK**.

The Timeout column displays the new date and time for the selected reconciliations.

## Reconciliation Problems

A reconciliation status of Timed-out or Reconciled after timeout can indicate a problem that might require operator intervention.

## Monitoring and Resolving Timed-out Reconciliations

When the Data Exchange Server cannot reconcile events, you need to review the reconciliation process with the partner to determine the problem. You might need to modify the process to ensure that you receive the acknowledgments you require. If reconciliations time out because the partner sends acknowledgments too late, you might need to modify your agreement with the partner and adjust the time limit.

To monitor and resolve reconciliations that have timed out, complete the following steps:

1. Create a reconciliation monitor to track events with a reconciliation status of Timed-out.  
The Data Exchange Server uses the monitor to track and set the status of events that have reached the reconciliation time limit but have not completed the reconciliation.  
  
You can also configure the reconciliation monitor to notify you when the monitor finds events where the reconciliations have timed out.
2. View the events with the reconciliation status Timed-out.  
If you configure the monitor to send email notification, you can view the events indicated in the email you receive.
3. For each event with a reconciliation status of Timed-out, analyze and resolve the problem.  
Determine why an acknowledgment was not processed within the time limit. Call the partner to verify the process or check any automated systems that are set to provide acknowledgments.
4. If the partner will send an acknowledgment at a later date, update the time limit for the acknowledgment.  
View the event details and change the time out for the reconciliation to allow for additional time for the acknowledgment. You can change the time out for one event or for all related events.
5. If you resolve the problem manually and you do not expect to receive an acknowledgment at a later date, set the reconciliation status to Reconciliation complete.  
  
For example, the partner sends the acknowledgment by fax and there is no need to process an acknowledgment in B2B Data Exchange. You can manually set the reconciliation status to Reconciliation complete.  
  
View the event details and change the status of the reconciliation. You can change the status for one event or for all related events.

# CHAPTER 11

## Event Resubmission

This chapter includes the following topics:

- [Event Resubmission Overview, 134](#)
- [Reprocessing an Event, 134](#)
- [Resending an Event, 136](#)

### Event Resubmission Overview

You may occasionally need to reprocess an event. For example, if an event reaches an error status or remains pending or transferring in case of a system failure, you may want to resubmit the event to PowerCenter.

B2B Data Exchange supports the following resubmission types:

- **Reprocessing.** Running the workflow that processes the event again.
- **Resending.** Sending the target documents of an event to an endpoint again.

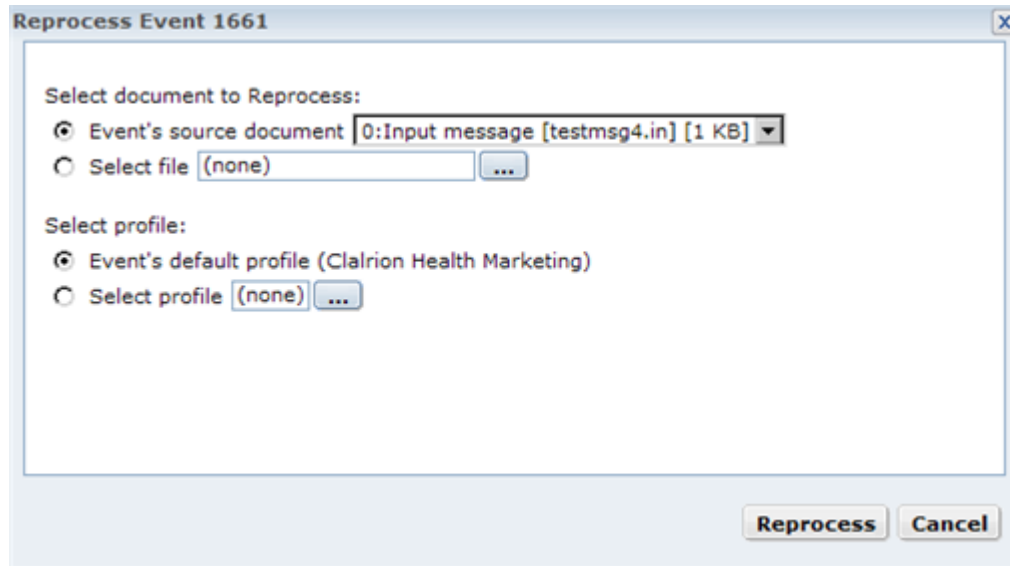
**Note:** If you use a real-time PowerCenter workflow to process the event, verify that the workflow is running before you resubmit the event.

### Reprocessing an Event

You can send events to PowerCenter for reprocessing, for example, if the event processing resulted in an error. If you reprocess a parent event, only the parent event is submitted to PowerCenter, but the status of all of the child events is changed to Reprocessed.

1. In the Navigator, click one of the following options:
  - **Events > All Events**
  - **Event Monitors > User Events**
2. Select the check box next to the event that you want to reprocess, and click **Actions > Reprocess**.

If you selected one event, the Reprocess Event window appears. If you selected multiple events, this window does not appear. Instead, B2B Data Exchange reprocesses the events according to the default values in the Reprocess Event window.



3. Select the source document of the event:

Option	Description
Event source document	Default. Original document that was attached to the event.
External file	External file to attach to the event for reprocessing. Select this option if you want to edit one of the original documents before reprocessing the event. <b>Note:</b> If the source of the event is <b>pass by reference</b> or if the event type is <b>File Set</b> , this option is not available. You can only reprocess the event with one of the original source documents.

4. Select the profile for the event:

Option	Description
Default event profile	Default. Original profile used to process the event.
Select profile	Different profile to use when processing the event.

5. Click **Reprocess**.

B2B Data Exchange checks that the selected events can be reprocessed, makes a copy of the original events, and submits the events to PowerCenter. It then changes the original event to read-only, sets the event status to **Reprocessed**, and attaches a log file to the event.

**Note:** To prevent an event from being reprocessible, the developer can set the dxProhibitReprocess event attribute to **True**.

# Resending an Event

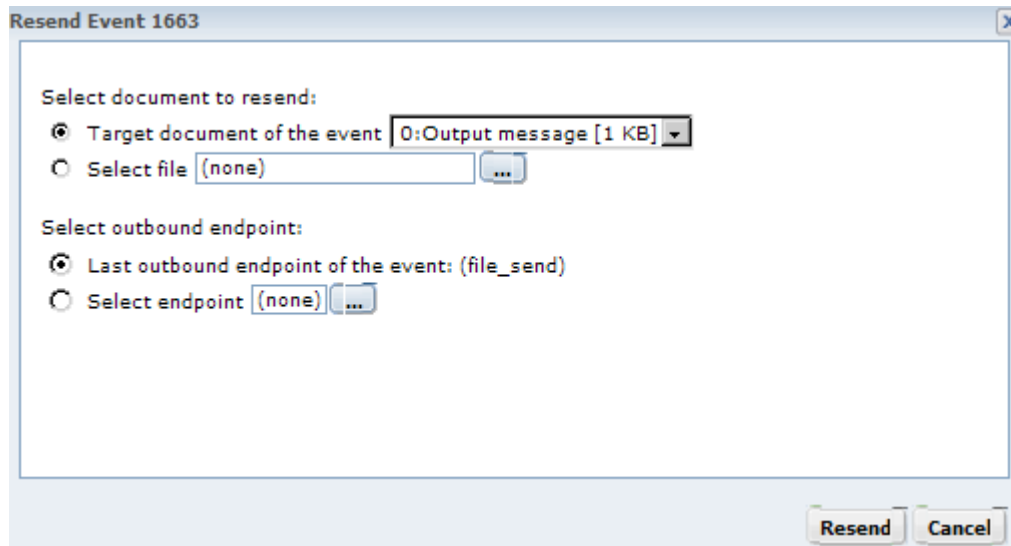
You can resend a copy of the event along with the target documents of the event to an endpoint.

1. In the Navigator, click one of the following options:

- **Events > All Events**
- **Event Monitors > User Events**

2. Select the check box next to the event that you want to resend, and click **Actions > Resend**.

If you selected one event, the Resend Event window appears. If you selected multiple events, this window does not appear. Instead, B2B Data Exchange resends the events according to the default values in the Resend Event window.



3. Select the target document of the event:

Option	Description
Event target document	Default. Original document that was attached to the event.
External file	External file to attach to the event. Select this option if you want to edit one of the original documents before reprocessing the event. <b>Note:</b> If the source of the event is <b>pass by reference</b> or if the event type is <b>File Set</b> , this option is not available. You can only resend the event with the original target document.

4. Select the endpoint to which to send the event:

Option	Description
Last outbound endpoint	Default. The endpoint to which the event was originally sent.
Select endpoint	Different endpoint to send the event.

5. Click **Resend**.



## CHAPTER 12

# Audit and Authorization

This chapter includes the following topics:

- [Audit and Authorization Overview, 137](#)
- [Audit Events, 137](#)
- [Legacy Audit Trail Events, 139](#)
- [Authorization, 140](#)

## Audit and Authorization Overview

When operators perform certain actions within the Operation Console, the organization may need to track or authorize these operator actions to accommodate business or legal needs.

B2B Data Exchange creates an audit trail to track actions that operators perform on objects in the Operation Console or the command line utilities, such as creating or editing a partner or an account. Operators with audit trail viewing privileges can view the audit records that correspond to the actions in the Operation Console and monitor object changes or troubleshoot issues with the objects on which the operators performed the actions.

Specific objects or specific actions that operators perform in the Operation Console may directly impact the business flow in the organization, and therefore may require approval before B2B Data Exchange completes the action. Similarly, when Portal users change message profile or endpoint settings in the Partners Portal, these changes require approval.

In such cases, operators with authorization privileges can review and approve or reject the actions. For example, operators that are responsible for specific partners might need to approve edits to the partners that other operators in the team perform, or updates made in the Partners Portal. Actions that B2B Data Exchange receives from the command line utilities or an API do not require approval.

## Audit Events

Operators with audit event viewing privileges can view and analyze current audit records. You can view audit records only for object types for which you already have viewing privileges.

B2B Data Exchange generates audit records for the following object types:

- Account

- Endpoint
- Monitor
- Partner
- Profile
- Portal User
- User
- User group

**Note:** When you modify a Managed File Transfer endpoint, B2B Data Exchange does not generate an audit record for mailbox or host changes.

## Audit Record Properties

Audit records include information about actions that operators performed in the Operation Console and in the command line utilities. Each audit event displays the operator action and the object on which the operator performed the action. The information appears in read-only mode.

The following table describes the general audit record properties:

Property	Description
Object Type	Type of the object on which the operator performed the action, such as partner or account.
Object Name	Name of the object on which the operator performed the action.
Action Date	Date in which the operator performed the action. If the action required approval, the audit trail displays the audit record after the operator approved the action with the date of approval.
User Name	Name of the operator that performed the action.
Action Type	Type of the action, such as <b>Create</b> or <b>Delete</b> .

When you drill down to individual audit record details, you can view the current and new value for the fields in the object.

The following table describes additional audit record properties that appear when you view individual audit record details:

Property	Description
Type	Object area in which the operator performed the action, such as <b>Details</b> .
Field Name	Name of the field on which the operator performed the action.
Current Value	Value of the field before the operator action. This property is not available if the operator created an object.
New Value	Value of the field after the operator performed the action.

## Viewing Audit Records

You view the audit trail to track and analyze actions the operators perform in the Operation Console and the command line utilities.

1. In the Navigator, click **Audit and Authorization > Audit Event**.  
The **Audit Event** page displays audit records that B2B Data Exchange generates.
2. To view the details of an audit record, click the **Details** icon for the record that you want to view.  
The **Action Details** section displays the operator action details.

## Legacy Audit Trail Events

In earlier versions B2B Data Exchange tracked operator changes with audit trail events. If you upgrade from earlier versions and do not archive or delete the audit trail events, you can view and analyze legacy audit events from earlier versions.

You can view legacy audit events for the following object types:

- Account
- Partner
- Profile
- Monitor
- Endpoint
- User
- User group
- Workflow
- Application
- Calendar
- System property
- Category
- Schedule
- On-boarding Checklist

## Legacy Audit Event Properties

Legacy audit events provide information about actions that operators performed in the Operation Console and in the command line utilities from earlier B2B Data Exchange versions. The information appears in read-only mode.

The following table describes the legacy audit event properties:

Property	Description
Event ID	Unique identifier for the event. Click the event ID to display additional information about the event, such as event details, event attributes, and event status history.
Subject	Textual description of the action, such as <b>create partner</b> .
Start Time	Date and time in which the operator performed the action.
Event Status	Status of the event. Events that reach a final status, such as <b>Complete</b> or <b>Error</b> , appear.

## Viewing Legacy Audit Events

You view legacy audit events to track and analyze actions the operators performed in the Operation Console and the command line utilities from earlier B2B Data Exchange versions.

1. In the Navigator, click **Audit and Authorization > Legacy Audit Events**.  
The **Legacy Audit Events** page displays audit events that earlier B2B Data Exchange versions generated.
2. To view the details of a legacy audit event, click the event ID of the event that you want to view.  
The **Event Details** section displays the operator action details.
3. To return to the **Legacy Audit Events** page, click **Back**.

## Authorization

If the organization requires approval of operator actions to specific objects in the Operation Console, operators with authorization privileges can review and approve or reject the actions. Operator actions on an object may require approval by one or two operators with authorization privileges.

Portal user actions in the Partners Portal to objects that require approval must be approved by operators with authorization privileges. Operators can review, approve, revert, or reject the portal user actions. Portal user actions require approval by just one operator.

When an operator or portal user performs an action that requires approval, the action appears as an approval request in the **Authorization** page. Operators with authorization privileges review the request and approve or reject the request as needed. If the action requires approval by two operators, the request remains pending until the second operator approves the request. If an operator or portal user 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.

The B2B Data Exchange administrator defines the authorization levels for each object type and assigns authorization privileges to specific operators based on the organization needs.

The following object types might require approval for **create**, **edit** or **delete** actions:

- Partner
- Account
- Profile

## Operator Action Properties

In the **Authorization** page, you can review and either approve or reject actions that operators or Portal users perform on objects that require approval. Each action contains information about the object type and the nature of the action that the operator or Portal users performed in the Operation Console or Partners Portal.

**Note:** You can access the **Authorization** page only if you have authorization privileges. The B2B Data Exchange administrator assigns authorization privileges according to the organization needs.

The following table describes the operator action properties:

Property	Description
Action Date	Date in which the operator performed the action. If actions on the object type require approval, the date of approval is displayed.
Action Type	Type of the action: <ul style="list-style-type: none"><li>- create</li><li>- edit</li><li>- delete</li></ul>
Object Name	Name of the object on which the operator performed the action.
Object Type	Type of the object on which the operator performed the create, edit, or delete action.
User Name	Name of the operator or portal user that performed the action.

When you drill down to individual action details, you can view the current and new value for the fields in the object.

The following table describes additional action properties that appear when you view individual action details:

Property	Description
Comment	Information about the approval or rejection of the action.
Current Value	Value of the field before the operator action. This property is not available if the operator created an object.
Field Name	Name of the field on which the operator performed the action.
First Level Approval	Name of the first operator that approved the action.
New Value	Value of the field after the operator performed the action.

Property	Description
Second Level Approval	Name of the second operator that approved the action. This property does not appear for actions that require approval by one operator or for portal user actions that require approval.
Type	Object area in which the operator performed the action, such as <b>Details</b> .

You can filter the list in the **Authorization** page based on the action status.

The following table describes the operator action statuses:

Status	Description
All	Actions with any status.
Approved	Actions that one or two operators with authorization privileges previously approved.
In Progress	Actions related to the message profile status that are in progress in the Partners Portal.
Invalid	Actions that B2B Data Exchange cancelled due to a more recent action that operators performed on the object with external tools, such as the command line utilities or the Web Services API. Actions can also be cancelled due to other operations such as an operator requesting to delete an account for which a profile change was submitted for approval.
Pending	Actions that require either approval by one operator or the first of approval by two operators with authorization privileges.
Rejected	Actions that operators with authorization privileges previously rejected.

## Authorization Rules and Guidelines

Consider the following rules and guidelines when you manage authorization for operator actions:

- Portal user actions must be approved by operators with authorization privileges. Portal user actions require approval by just one operator.
- 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.
- B2B Data Exchange does not send notifications for new pending operator actions. Operators can review pending actions in the **Authorization** page or in the **Dashboard** page.
- If the B2B Data Exchange administrator defined that actions that operators perform on a partner do not require approval but actions that operators perform on the accounts of the partner require approval, when you create a partner with accounts B2B Data Exchange creates the partner and submits the request to create the accounts for approval. You can view or edit the accounts only after the approval of an operator with authorization privileges.
- Only manual operator actions can require approval. If B2B Data Exchange receives an action on the object from the command line utilities or an API, B2B Data Exchange automatically accepts the action.
- If an operator performs an action with an external API on an object that already contains a pending action before the pending action is approved, B2B Data Exchange prevents the approval of the pending action by cancelling the action request when an operator attempts to approve the action. This ensures that approval of the original action does not override more recent actions.

- 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.

## Approving or Rejecting Actions

If you have authorization privileges, you can review actions performed on objects in the Operation Console and approve or reject the actions.

You can only access the Authorization page if the B2B Data Exchange administrator assigned authorization privileges to you.

1. In the Navigator, click **Audit and Authorization > Authorization**.

The Authorization page displays the list of actions that require approval, filtered by status.

2. To view the details for an action, click the **Details** icon for the action that you want to view.

The **Action Details** section displays the current and new value of the object and the authorization history.

3. To search for an action on a certain object name or with a certain user name, enter a test string in the **Find** box and click **Search**.

4. Choose to approve or reject the action:

- To approve the action, click the **Approve** icon next to the action that you want to approve. You can add a comment to describe any conditions related to the approval process.
- To reject the action, click the **Reject** icon next to the action that you want to reject and add a comment to the action.

**Note:** For portal authorization requests, the comment you add is displayed as a notification in the Partners Portal.

## CHAPTER 13

# Advanced Exception Handling

This chapter includes the following topics:

- [Advanced Exception Handling Overview, 144](#)
- [Advanced Exception Handling Example, 145](#)
- [Advanced Exception Handling Issue Attributes, 145](#)
- [Creating an Advanced Exception Handling Issue, 148](#)
- [Displaying Exception Handling Issue Details, 148](#)
- [Reopening an Exception Issue, 148](#)

## Advanced Exception Handling Overview

The Advanced Exception Handling option allows you to track exception events that arise in the course of normal B2B Data Exchange operations. You start by defining a monitor to trap an exception event and configure it to open an exception handling issue. Use the exception handling issue to interact with other parties in your organization to investigate and resolve the exception.

Advanced Exception Handling, an add-in that requires a separate license, provides complete functionality to support the process of issue resolution.

The following terms are important to understanding the functionality of the Advanced Exception Handling option:

- **Event.** An event is created when a document is received by B2B Data Exchange. Document status information is updated throughout the processing of the document.
- **Exception event.** An event that is defined in an event monitor. The monitor can be configured to create an exception handling issue when it traps an exception event.
- **Exception handling issue.** An exception handling issue is created by the Advanced Exception Handling module when an event monitor traps an event exception. The issue is updated with status information as its resolution workflow progresses. When the user updates the status of the event issue to Completed, the system updates the status of the exception event to Completed.
- **Regular event exception.** A regular event exception is a single B2B event that meets the conditions defined in an event monitor, for example, an error event for partner P.
- **NOT event exception.** A NOT event exception is a condition that meets the NOT condition defined in an event monitor. An example of a NOT event exception is not receiving any input from partner P in the last 24 hours.



- **Batch event exception.** A batch event exception represents the occurrence of one or more exception events over a period of time, for example, the receipt of one or more empty messages from Partner P over the course of a day.
- **Reconciliation event exception.** A reconciliation event exception is a reconciliation event that meets the conditions defined in an event monitor.

## Advanced Exception Handling Example

The following example illustrates the handling of an error event for Partner P.

First, define an event monitor to trap events from Partner P whose event status is Error. Configure the monitor Action after Notification as Deliver Event and Create Issue. Using the Advanced Exception Handling option, you can have the system notify you by email when it creates an exception handling issue.

The initial status of an issue is Created. After you review the details of the issue, you decide to contact the partner and ask that the message be re-sent. At this point you can display the issue, add a comment to document the actions you took, and change the status to In Progress.

When you see that the replacement message has been received and completed, you can display the issue again and change its status to Closed. The system changes the attached event status to Complete.

## Advanced Exception Handling Issue Attributes

An exception handling issue is created from an exception event that it traps. This section explains what the attributes of an exception handling issue are and how to review them.

### Regular Exception Issue

When you configure an event monitor to create a regular exception handling issue, it creates a regular exception issue when an event occurs. This type of issue contains the following attributes:

Attribute	Description	Source of the Attribute
Project	Name of the project used for exception issue handling.	System default or event attribute.
Issue Type	Event. (Default.)	System default or event attribute.
Issue ID	Unique identifier of the issue.	System-generated.
Priority	Relative priority of the issue: - <b>H.</b> Blocker. - <b>M.</b> Critical. - <b>L.</b> Major.	Monitor priority.
Reporter	User who reported the issue.	System default.

Attribute	Description	Source of the Attribute
Monitor	Created by DX monitor <monitor name>.	Monitor.
Summary	Event <event ID>: <Event Subject>	Event.
Partner	Name of the partner associated with the event.	Event.
Account Number	Number of the account associated with the event.	Event.
Account Name	Name of the account associated with the event.	Event.
Description	For each source, log, or target document in the source event, the following information is displayed: <document type>:<document description> <HTTP link to the document>	Event.
Attached Event	Link to the source event in the event repository.	System property in the attached event.
Attached Event ID	Unique identifier of the source event.	All of the following: - Event. - System property.
Assignee	User to whom the issue is assigned.	One of the following: - Event value. - System default.
Custom Properties	Unique properties defined for this system.	One of the following: - Event attributes - System properties.

**Note:** When the monitor creates exception issues:

- If any event attributes are empty, the monitor uses profile attributes.
- If both event attributes and profile attributes are empty, the monitor uses system properties.

## NOT Exception Issue

A monitor creates a NOT exception issue when the user selected the "Report If Event Does NOT Happen" option. An example of a NOT exception issue might be when no input is received from a specific partner during a 24-hour period.

The attributes of a NOT exception issue are:

Issue Attribute	Description	DX Source of the Attribute
Project	Name of the tracking project.	System property.
Issue Type	Event.	System property.
Issue ID	Unique issue ID.	Advanced Exception Handling module (sequential number).

Issue Attribute	Description	DX Source of the Attribute
Priority	Relative priority of this issue.	The priority set in the event monitor: H=Critical, M=Major, L=Minor.
Reporter	Person who reported the issue.	System Property.
First line of description	If the event monitor has a name, "Created by DX monitor [monitor name]."	Monitor.
Summary	Name of the DX NOT monitor.	Monitor.
Partner	Partner name as defined in the monitor.	NOT event (created by the monitor).
Account number	Account numbers defined in the monitor.	NOT event (created by the monitor).
Custom properties	Unique properties defined for this system.	System properties.
Assignee	Person to whom the issue is assigned.	System property.

## Batch Exception Issues

A batch exception issue is created when you create an event monitor and select the **Batch notification** option. A batch exception issue contains one or more events that occurred within the time period defined in the monitor schedule.

The following types of batch exception issues are available:

- Regular Batch Exception Issue.
- NOT Batch Exception Issue.

The attributes of a batch tracking issue are similar to the attributes of a NOT batch exception issue. Both issue types do not include attached events and no partner or account information, because they normally refer to multiple events, partners, or accounts.

## Reconciliation Exception Issue

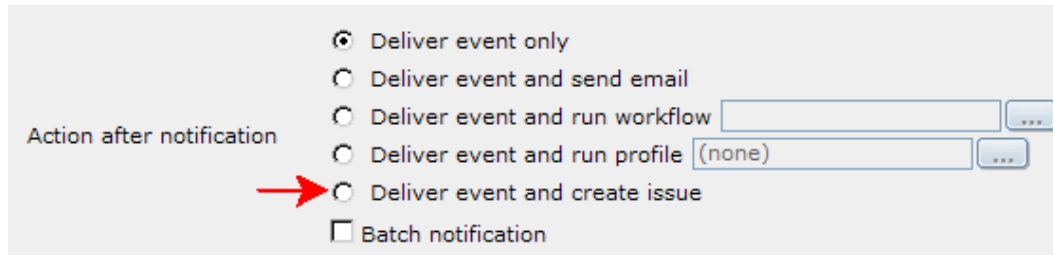
A reconciliation issue tracks a reconciliation event. The details of a reconciliation event are identical to the those of a regular event, with the following changes:

Issue Attribute	Description	DX Source of the Attribute
Additional Description (after line 1)	For each reconciliation: "Reconciliation [ID] of type [type] in status [status]. Initiation time:[initiated], timeout: [timeout], and Reconciled on [reconTime]."	Reconciliation event.

# Creating an Advanced Exception Handling Issue

You can configure an event monitor to create advanced exception handling issues for specific events. For more information on creating an event monitor, see [“Event Monitors Overview” on page 119](#).

To configure an event monitor to create an exception handling issue, follow the steps in [“Creating an Event Monitor” on page 119](#), and select the **Deliver event and create issue** option in the **Action after notification** section.



# Displaying Exception Handling Issue Details

You can display the details of exception handling issues for event monitors that you configured to create advanced exception handling issues.

To display details of an exception handling issue, go to the event details screen and click the issue link that is displayed together with the logging information.

To display an exception handling issue using the Monitor screen:

1. In the Navigator, click **Monitors > Event Monitors**.  
The Event Monitors page appears.
2. Select a monitor that contains advanced exception handling issues.  
The Events for Monitor page appears.
3. Click the event ID of the event you want to display.  
The Event Details page appears.
4. Scroll down to the Event Log section and click the **Issue <issue ID> was created by event monitor create issue on error** log entry.

The log entry displays the status, assignee, and description of the issue. You can also view the source message, the attached event, any logging documents, and other related information.

**Note:** Do not clone the issue, change the type of the issue, change the project of the issue, or delete an issue. If you do, the issue and the related event will not synchronize correctly.

# Reopening an Exception Issue

B2B Data Exchange can reopen an existing exception issue, for example, if multiple monitors report the same associated event. In this case, B2B Data Exchange does not open a duplicate issue. Instead, it reopens the existing issue.

When an issue is reopened, the issue attributes are updated according to the latest status of the event, the issue status is set to **Reopened**, and an appropriate comment is added to the issue.

## CHAPTER 14

# Dashboard and Reports

This chapter includes the following topics:

- [Dashboard and Reports Overview, 150](#)
- [Dashboard Filters, 151](#)
- [Dashboard Panels, 151](#)
- [Dashboard Panel CSV File Structure, 178](#)
- [Managing the Dashboard, 179](#)

## Dashboard and Reports Overview

The Dashboard is a collection of panels that display personalized visual reports about information that B2B Data Exchange processes. Each report appears in a panel that you view in the **Dashboard** page of the Operation Console.

Use the Dashboard to view summary information about B2B Data Exchange events and document processing, such as the number of events for certain partners or the error rate for specific event accounts. You can drill down to each report to view event details or manage daily tasks that require further investigation. You can focus on areas of interest and analyze statistical information about the processed data. In some panels you can export the report to a comma-separated-values (CSV) file for further analysis.

Most of the reports in the Dashboard are based on key performance indicators (KPIs) that B2B Data Exchange retrieves from the operational data store. The operational data store is a repository that contains aggregated information solely for reporting purposes. Each panel displays a different KPI, and you can apply global filters for all of the panels in all of the tabs.

Data that appears in the charts is filtered by global Dashboard filters, for example, by a time frame or by a partner. The data is then filtered by permissions. You can view data pertaining to applications to which you have access. All charts are visible to users with dashboard privileges.

By default, the Dashboard displays the Error Rate panel, the Tasks panel, the Error Events by Partner panel, the Events Distribution panel, and the Average Processing Time panel. In addition to the event panels, use the Tasks panel to view a link to unresolved error events and a link to the operator actions that are pending approval. The unresolved error panels and the Tasks panel retrieve information from the main B2B Data Exchange repository. You apply a separate time frame filter for panels that retrieve unresolved error event information.

The Dashboard page contains tabs in which to display the panels. You can personalize the Dashboard with additional tabs and add different panels to each tab as needed. The B2B Data Exchange developer can create additional Dashboard panels based on the organization needs. You can view the Dashboard only if the B2B

Data Exchange administrator installed and configured it. You can only view information for which you have assigned privileges.

If you delete an object with information that the Dashboard displays in a panel and then create an object with the same name, the operational data store event loader fails. For example, you delete a partner and create a partner with the same name. Do not delete objects with information that the Dashboard uses.

## Dashboard Filters

You can apply filters for each tab in the Dashboard. The filters apply to all of the panels all of the tab except for the time frame filter for unresolved error reports, which you apply separately.

The following table describes the Dashboard filters:

Filter	Description
Time Frame	Time period during which to display event information in the panels. You can choose one of the following options: <ul style="list-style-type: none"><li>- Last 24 hours</li><li>- Last 48 hours</li><li>- Last 72 hours</li><li>- Last 7 days</li><li>- Last 30 days</li><li>- All</li><li>- Custom</li></ul> If you select <b>Custom</b> , you can select a custom time frame in the <b>Custom Time Frame</b> dialog box.
Partner	Related partner for the events.
Account	Related account for the events. You must select a partner before you select an account.
Event Type	Type of the event.
Event Status	Status of the event.
Customize	Time period during which to display unresolved event information in the panels. You can click the link to choose a time frame in hours.

## Dashboard Panels

The Dashboard tabs contain panels in which you can view different reports based on information that B2B Data Exchange collects about different KPIs. You can personalize each tab by adding or removing panels

from the Dashboard catalog. The B2B Data Exchange developer can create custom Dashboard panels based on the organization needs.

The following table describes the Dashboard panels:

Panel	Description
Average Processing Time	Visual indication of the distribution of event processing time during the selected time frame. Appears by default.
Error Events by Account	Ten or 20 accounts with the highest number of error events or unresolved error events created during the selected time frame.
Error Events by Account - All Errors	Ten or 20 accounts with the highest number of error events created during the selected time frame.
Error Events by Account - Unresolved Errors	Ten or 20 accounts with the highest number of unresolved error events created during the selected time frame.
Error Events by Event Status	Ten or 20 event statuses with the highest number of error events or unresolved error events created during the selected time frame.
Error Events by Event Status - All Errors	Ten or 20 event statuses with the highest number of error events created during the selected time frame.
Error Events by Event Status - Unresolved Errors	Ten or 20 event statuses with the highest number of unresolved error events created during the selected time frame.
Error Events by Event Type	Ten or 20 event types with the highest number of error events or unresolved error events created during the selected time frame.
Error Events by Event Type - All Errors	Ten or 20 event types with the highest number of error events created during the selected time frame.
Error Events by Event Type - Unresolved Errors	Ten or 20 event types with the highest number of unresolved error events created during the selected time frame.
Error Events by Partner	Ten or 20 partners with the highest number of error events or unresolved error events created during the selected time frame. Appears by default.
Error Events by Partner - All Errors	Ten or 20 partners with the highest number of error events created during the selected time frame.
Error Events by Partner - Unresolved Errors	Ten or 20 partners with the highest number of unresolved error events created during the selected time frame.
Error Events Distribution	Number of error events created per hour or per day during the selected time frame.
Error Rate	Ratio of error events to the total events during the selected time frame in an intuitive and graphical format. Appears by default.
Events by Account	Ten or 20 accounts with the highest number of events created during the selected time frame.



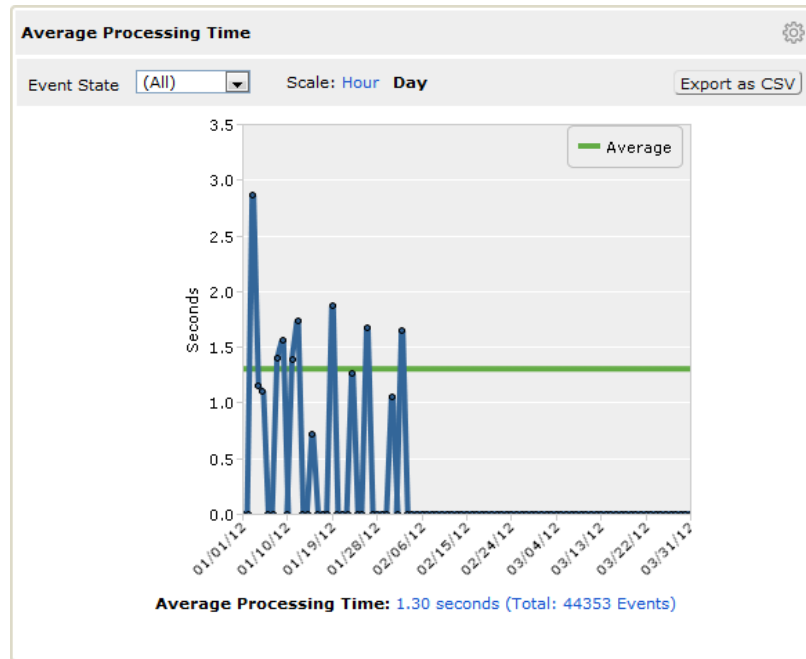
Panel	Description
Events by Event Status	Ten or 20 event statuses with the highest number of events created during the selected time frame.
Events by Event Type	Ten or 20 event types with the highest number of events created during the selected time frame.
Events by Partner	Ten or 20 partners with the highest number of events created during the selected time frame.
Events Distribution	Total number of events created per hour or per day during the selected time frame. Appears by default.
SLA Violations	Service level agreement (SLA) violations. The panel contains the following areas: <ul style="list-style-type: none"> <li>- Violations by SLA Rule. A breakdown of the top 10 violations according to the SLA rules.</li> <li>- Violations by KPI. A breakdown of the top 10 violations according to the type of event information, such as the number of events or the error rate.</li> <li>- Violations. List view of the first 50 violations. You can filter the list according to the SLA rule or the KPI. You can click a violation in the list to view the related events in the <b>Event List</b> page.</li> </ul> Appears by default on the <b>SLA</b> tab.
Tasks	Links to the number of unresolved error events and operator actions that are pending approval. Appears by default.

## Average Processing Time Panel

The Average Processing Time panel provides a visual indication of the average time that it took for B2B Data Exchange to process events during the selected time frame. Use the panel to identify deviations or other issues that might require further attention. You can click any point on the graph to display the events in the **Event List** page.

The Dashboard calculates the average processing time for time intervals during which B2B Data Exchange processed events.

The following image illustrates the Average Processing Time panel:



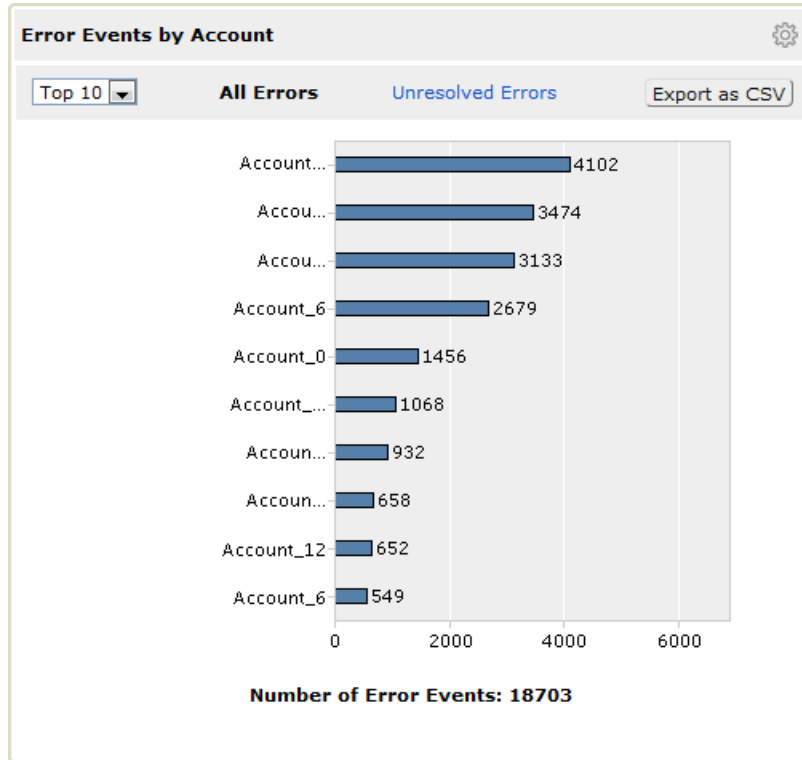
The following table describes the Average Processing Time panel elements:

Element	Description
Event State	State of the events to display in the panel. You can choose one of the following options: <ul style="list-style-type: none"> <li>- <b>All</b>. Displays all event states on the graph.</li> <li>- <b>Error</b>. Displays error event states on the graph.</li> <li>- <b>Non-Error</b>. Displays non-error event states on the graph.</li> </ul>
Scale	Time frame intervals. You can choose one of the following options: <ul style="list-style-type: none"> <li>- <b>Hour</b>. Displays the average processing time of events at hourly intervals as point on the graph.</li> <li>- <b>Day</b>. Displays the average processing time of events at daily intervals as point on the graph.</li> </ul> If you select a time frame filter longer than 7 days, you can only view events on a day scale.
Seconds	Average number of seconds from when B2B Data Exchange generated the events until the events finished processing during the selected time frame. Appears on the Y-axis of the panel.
Time Distribution	Date or time intervals during which B2B Data Exchange generated events. Appears on the X-axis of the panel.
Average Line	Average processing time for the entire time frame.
Average Processing Time	Average processing time for events that B2B Data Exchange generated each day or hour and the total number of events for the selected time frame. You can click the link to display the events in the <b>Event List</b> page.
Export as CSV	Saves the data in the panel as a CSV file.

## Error Events by Account Panel

The Error Events by Account panel displays the 10 or 20 accounts with the highest number of error events and unresolved error events created during the selected time frame. Use the panel to analyze account activity or identify potential bottlenecks. You can click each bar on the graph to display the error events or unresolved error events for the account in the **Event List** page.

The following image illustrates the Error Events by Account panel:



The following table describes the Error Events by Account panel elements:

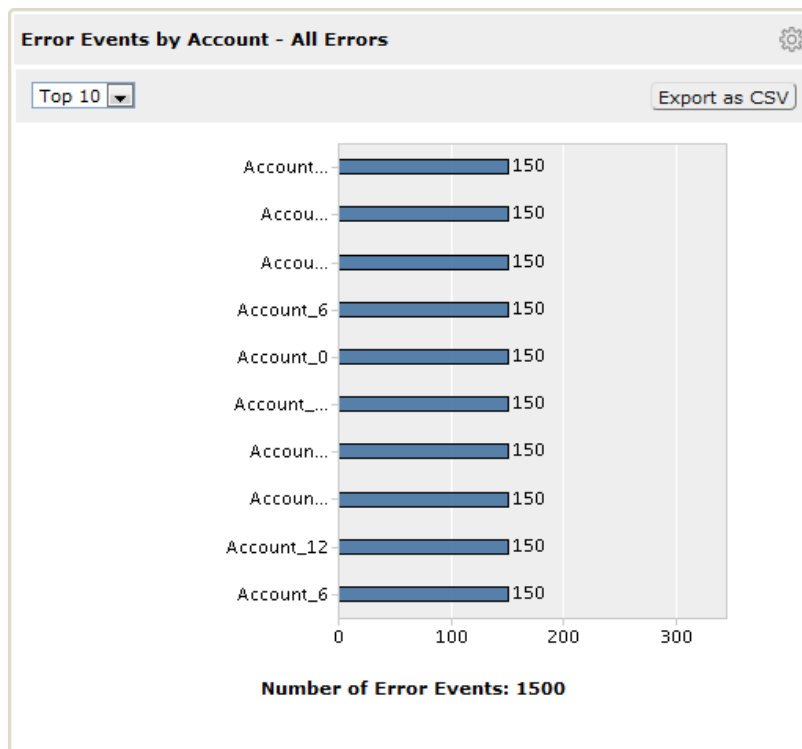
Element	Description
Top 10 / Top 20	Number of accounts for which to display the number of error events or unresolved error events for the selected time frame.
All Errors	Displays all events that reached an error state for the accounts during the selected time frame.
Unresolved Errors	Displays current error events for the accounts. The events appear based on the time frame that you select in the unresolved error events filter.
Account Name	Names of the accounts with the highest number of error events or unresolved error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of error events or unresolved error events for the accounts during the selected time frame. Appears on the X-axis of the panel.

Element	Description
Number of Events	Total number of error events or unresolved error events for the accounts during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Account - All Errors Panel

The Error Events by Account - All Errors panel displays the 10 or 20 accounts with the highest number of error events created during the selected time frame. Use the panel to analyze account activity or identify potential bottlenecks. You can click each bar on the graph to display the error events for the account in the **Event List** page.

The following image illustrates the Error Events by Account - All Errors panel:



The following table describes the Error Events by Account - All Errors panel elements:

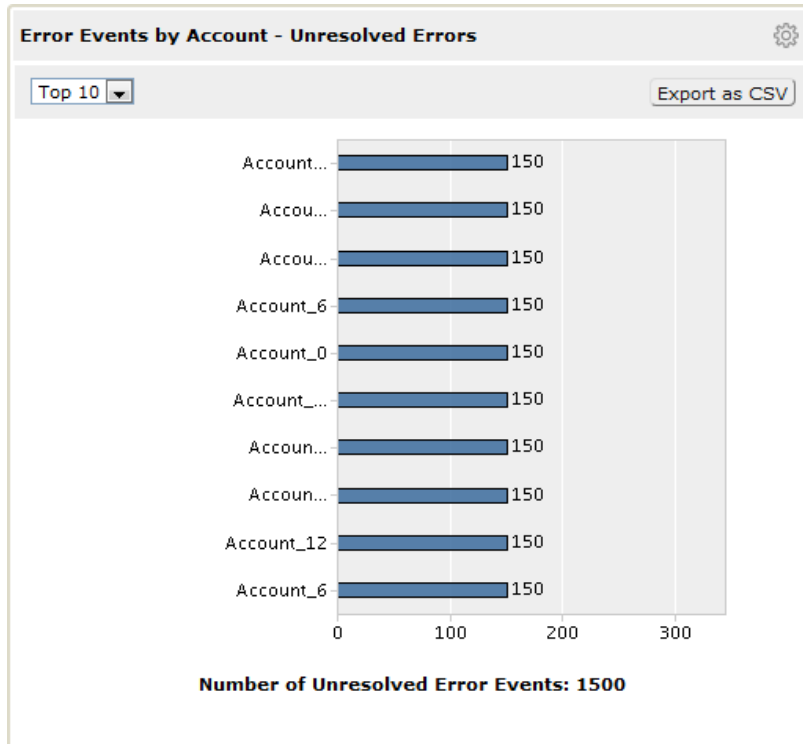
Element	Description
Top 10 / Top 20	Number of accounts for which to display the number of error events for the selected time frame.
Account Name	Names of the accounts with the highest number of error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of error events for the accounts during the selected time frame. Appears on the X-axis of the panel.

Element	Description
Number of Events	Total number of error events for accounts during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Account - Unresolved Errors Panel

The Error Events by Account - Unresolved Errors panel displays the 10 or 20 accounts with the highest number of unresolved error events created during the selected time frame. Use the panel to analyze account activity or identify potential bottlenecks. You can click each bar on the graph to display the unresolved error events for the account in the **Event List** page.

The following image illustrates the Error Events by Account - Unresolved Errors panel:



The following table describes the Error Events by Account - Unresolved Errors panel elements:

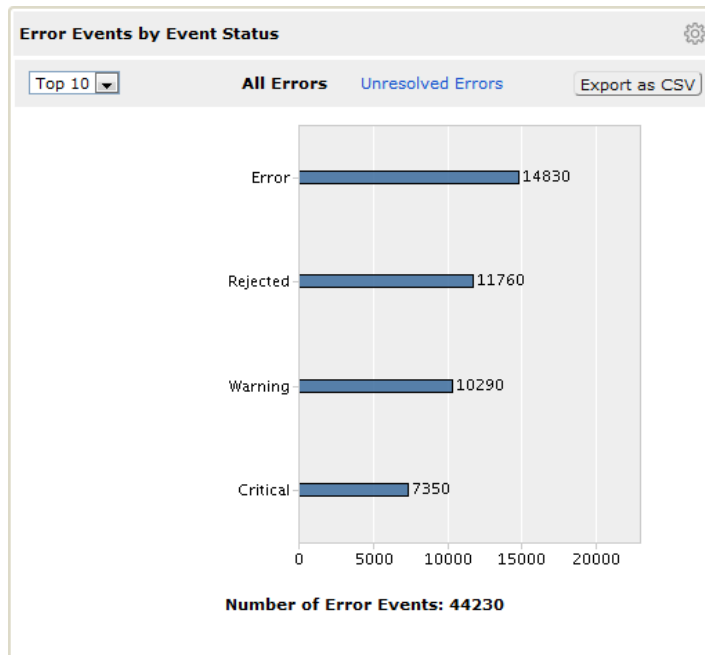
Element	Description
Top 10 / Top 20	Number of accounts for which to display the number of unresolved error events for the selected time frame.
Account Name	Names of the accounts with the highest number of unresolved error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of unresolved error events for the accounts during the selected time frame. Appears on the X-axis of the panel.

Element	Description
Number of Events	Total number of unresolved error events for accounts during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Event Status Panel

The Error Events by Event Status panel displays the 10 or 20 event statuses with the highest number of error events and unresolved error events created during the selected time frame. Use the panel to identify potential bottlenecks or other issues that might require further attention. You can click each bar on the graph to display the error events or unresolved error events for the event status in the **Event List** page.

The following image illustrates the Error Events by Event Status panel:



The following table describes the Error Events by Event Status panel elements:

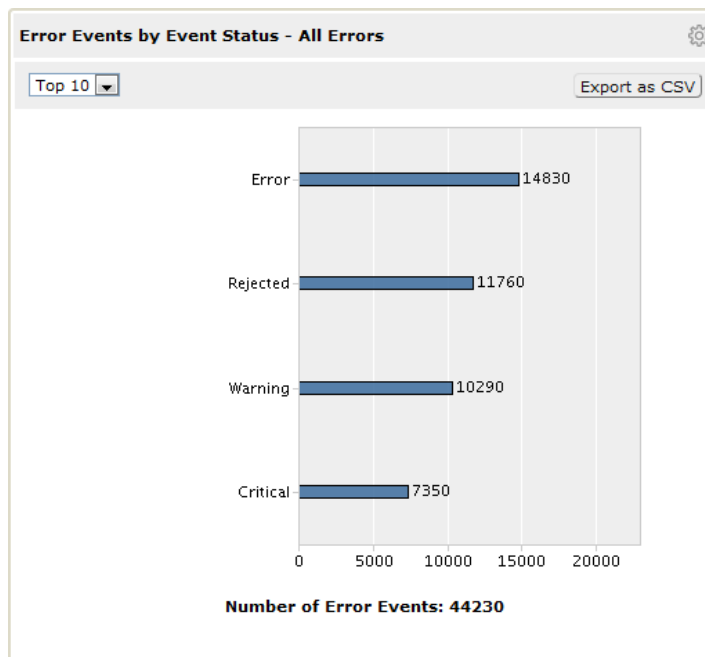
Element	Description
Top 10 / Top 20	Number of event statuses for which to display the number of error events or unresolved error events for the selected time frame.
All Errors	Displays all events that reached an error state for the event statuses during the selected time frame.
Unresolved Errors	Displays current error events for the event statuses. The events appear based on the time frame that you select in the unresolved error events filter.
Event Status	Names of the event statuses with the highest number of error events or unresolved error events for the selected time frame. Appears on the Y-axis of the panel.

Element	Description
Events	Number of error events or unresolved error events for the event statuses during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of error events or unresolved error events for the event statuses during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Event Status - All Errors Panel

The Error Events by Event Status - All Errors panel displays the 10 or 20 event statuses with the highest number of error events created during the selected time frame. Use the panel to identify potential bottlenecks or other issues that might require further attention. You can click each bar on the graph to display the error events for the event status in the **Event List** page.

The following image illustrates the Error Events by Event Status - All Errors panel:



The following table describes the Error Events by Event Status - All Errors panel elements:

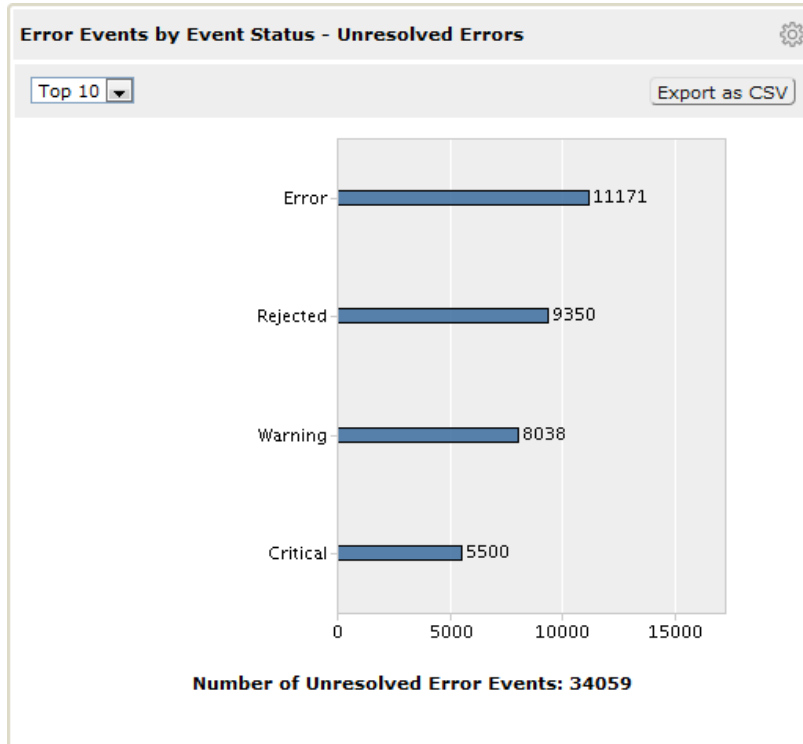
Element	Description
Top 10 / Top 20	Number of event statuses for which to display the number of error events for the selected time frame.
Event Status	Names of the event statuses with the highest number of error events for the selected time frame. Appears on the Y-axis of the panel.

Element	Description
Events	Number of error events for the event statuses during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of error events for the event statuses during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Event Status - Unresolved Errors Panel

The Error Events by Event Status - Unresolved Errors panel displays the 10 or 20 event statuses with the highest number of unresolved error events created during the selected time frame. Use the panel to identify potential bottlenecks or other issues that might require further attention. You can click each bar on the graph to display the unresolved error events for the event status in the **Event List** page.

The following image illustrates the Error Events by Event Status - Unresolved Errors panel:



The following table describes the Error Events by Event Status - Unresolved Errors panel elements:

Element	Description
Top 10 / Top 20	Number of event statuses for which to display the number of unresolved error events for the selected time frame.
Event Status	Names of the event statuses with the highest number of unresolved error events for the selected time frame. Appears on the Y-axis of the panel.

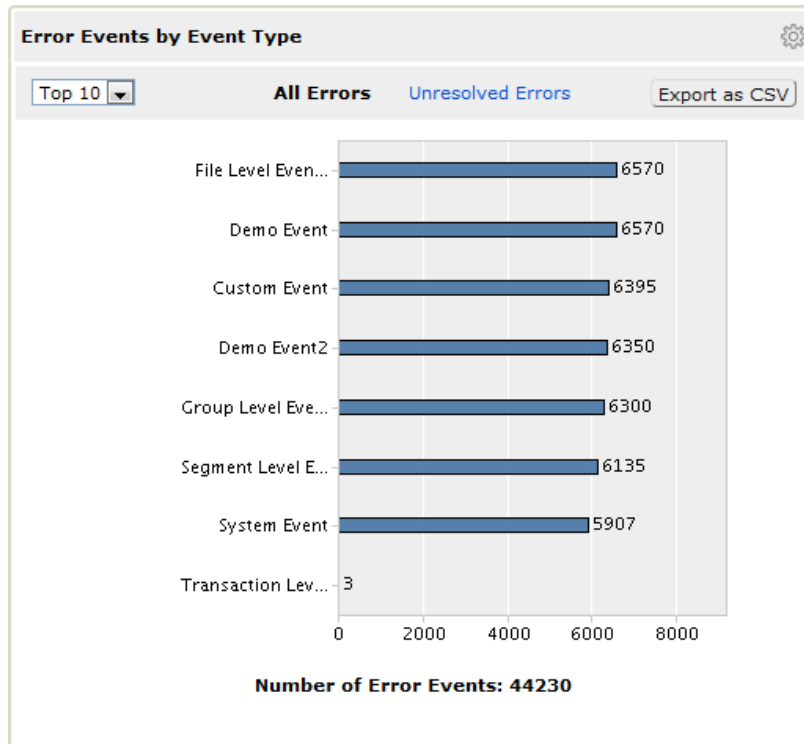


Element	Description
Events	Number of unresolved error events for the event statuses during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of unresolved error events for the event statuses during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Event Type Panel

The Error Events by Event Type panel displays the 10 or 20 event types with the highest number of error events and unresolved error events created during the selected time frame. Use the panel to identify potential bottlenecks or other issues that might require further attention. You can click each bar on the graph to display the error events or unresolved error events for the event type in the **Event List** page.

The following image illustrates the Error Events by Event Type panel:



The following table describes the Error Events by Event Type panel elements:

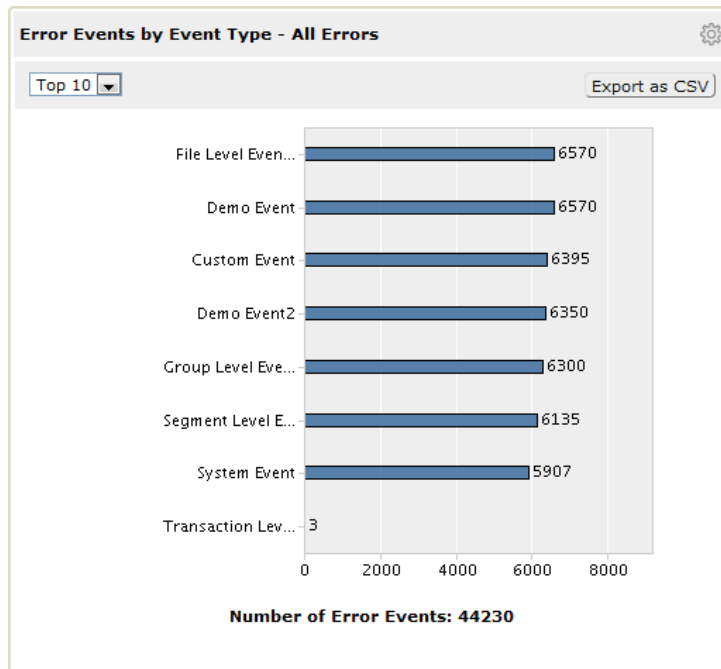
Element	Description
Top 10 / Top 20	Number of event types for which to display the number of error events or unresolved error events for the selected time frame.
All Errors	Displays all events that reached an error state for the event types during the selected time frame.

Element	Description
Unresolved Errors	Displays current error events for the event types. The events appear based on the time frame that you select in the unresolved error events filter.
Event Type	Names of the event types with the highest number of error events or unresolved error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of error events or unresolved error events for the event types during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of error events or unresolved error events for the event types during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Event Type - All Errors Panel

The Error Events by Event Type - All Errors panel displays the 10 or 20 event types with the highest number of error events created during the selected time frame. Use the panel to identify potential bottlenecks or other issues that might require further attention. You can click each bar on the graph to display the error events for the event type in the **Event List** page.

The following image illustrates the Error Events by Event Type - All Errors panel:



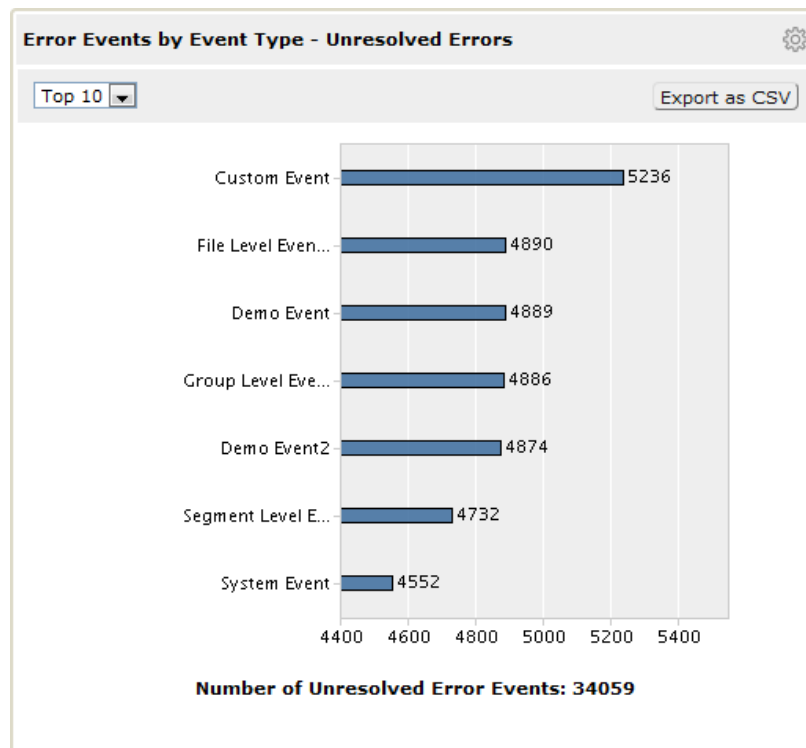
The following table describes the Error Events by Event Type - All Errors panel elements:

Element	Description
Top 10 / Top 20	Number of event types for which to display the number of error events for the selected time frame.
Event Type	Names of the event types with the highest number of error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of error events for the event types during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of error events for the event types during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Event Type - Unresolved Errors Panel

The Error Events by Event Type - Unresolved Errors panel displays the 10 or 20 event types with the highest number of unresolved error events created during the selected time frame. Use the panel to identify potential bottlenecks or other issues that might require further attention. You can click each bar on the graph to display the unresolved error events for the event type in the **Event List** page.

The following image illustrates the Error Events by Event Type - Unresolved Errors panel:



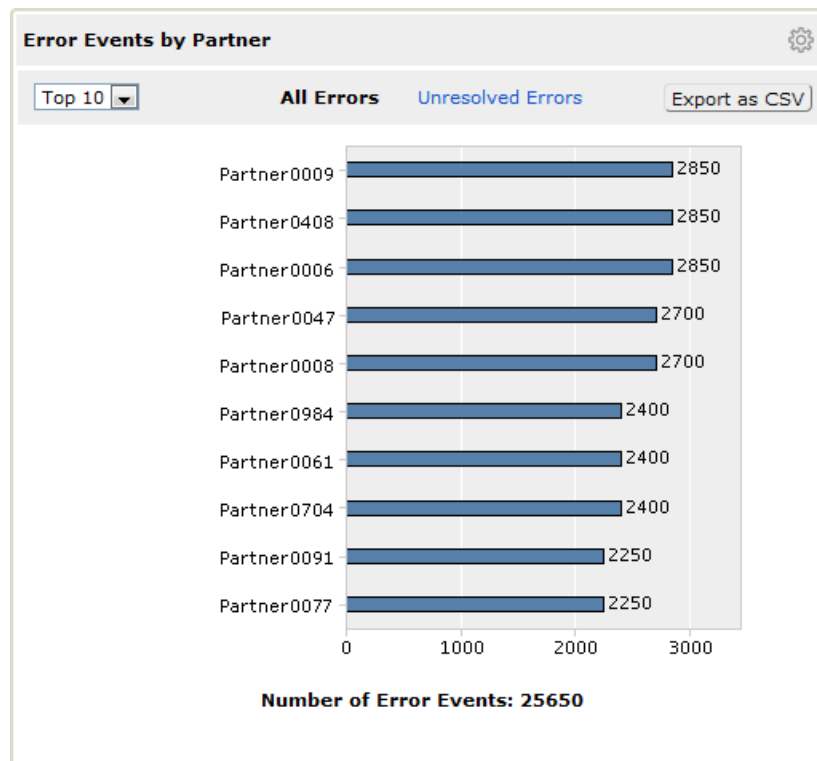
The following table describes the Error Events by Event Type - Unresolved Errors panel elements:

Element	Description
Top 10 / Top 20	Number of event types for which to display the number of unresolved error events for the selected time frame.
Event Type	Names of the event types with the highest number of unresolved error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of unresolved error events for the event types during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of unresolved error events for the event types during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Partner Panel

The Error Events by Partner panel displays the 10 or 20 partners with the highest number of error events and unresolved error events created during the selected time frame. Use the panel to analyze partner activity or identify potential bottlenecks. You can click each bar on the graph to display the error events or unresolved error events for the partner in the **Event List** page.

The following image illustrates the Error Events by Partner panel:



The following table describes the Error Events by Partner panel elements:

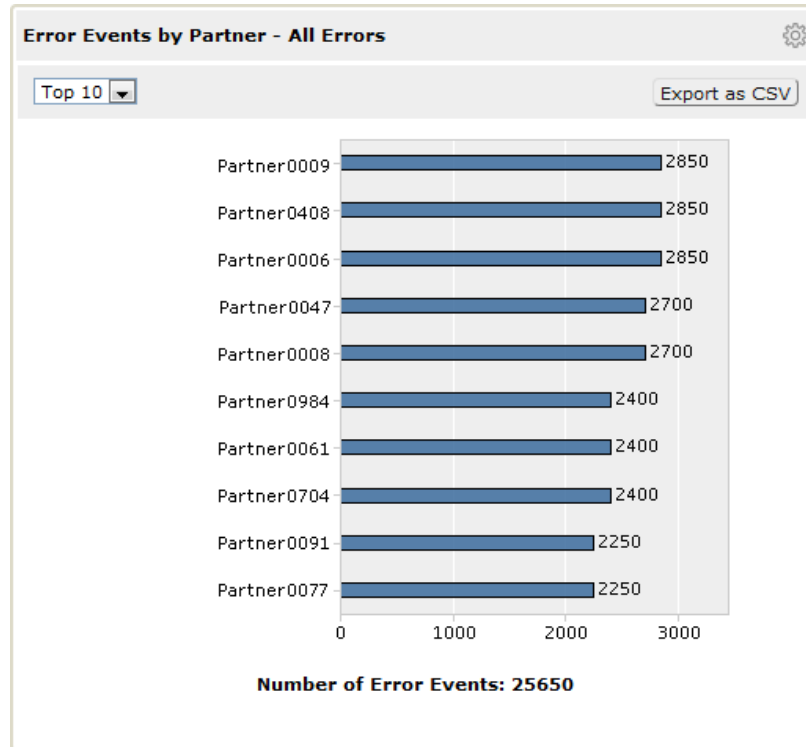
Element	Description
Top 10 / Top 20	Number of partners for which to display the number of error events or unresolved error events for the selected time frame.
All Errors	Displays all events that reached an error state for the accounts during the selected time frame.
Unresolved Errors	Displays current error events for the accounts. The events appear based on the time frame that you select in the unresolved error events filter.
Partner Name	Names of the partners with the highest number of error events or unresolved error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of error events or unresolved error events for the partners during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of error events or unresolved error events for the partners during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Partner - All Errors Panel

The Error Events by Partner - All Errors panel displays the 10 or 20 partners with the highest number of error events created during the selected time frame. Use the panel to analyze partner activity or identify potential

bottlenecks. You can click each bar on the graph to display the error events for the partner in the **Event List** page.

The following image illustrates the Error Events by Partner - All Errors panel:



The following table describes the Error Events by Partner - All Errors panel elements:

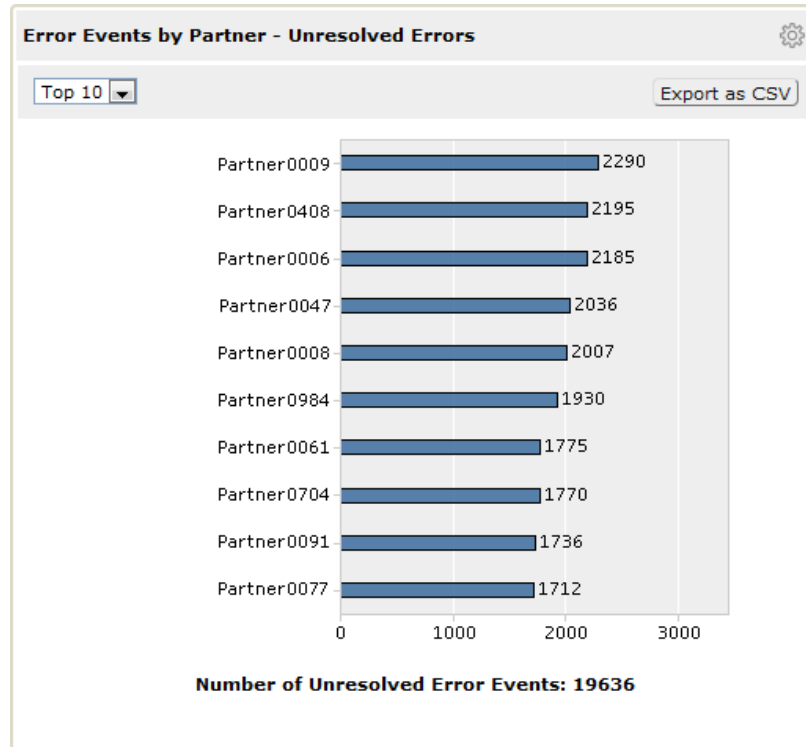
Element	Description
Top 10 / Top 20	Number of partners for which to display the number of error events for the selected time frame.
Partner Name	Names of the partners with the highest number of error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of error events for the partners during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of error events for the partners for the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events by Partner - Unresolved Errors Panel

The Error Events by Partner - Unresolved Errors panel displays the 10 or 20 partners with the highest number of unresolved error events created during the selected time frame. Use the panel to analyze partner activity or

identify potential bottlenecks. You can click each bar on the graph to display the unresolved error events for the partner in the **Event List** page.

The following image illustrates the Error Events by Partner - Unresolved Errors panel:



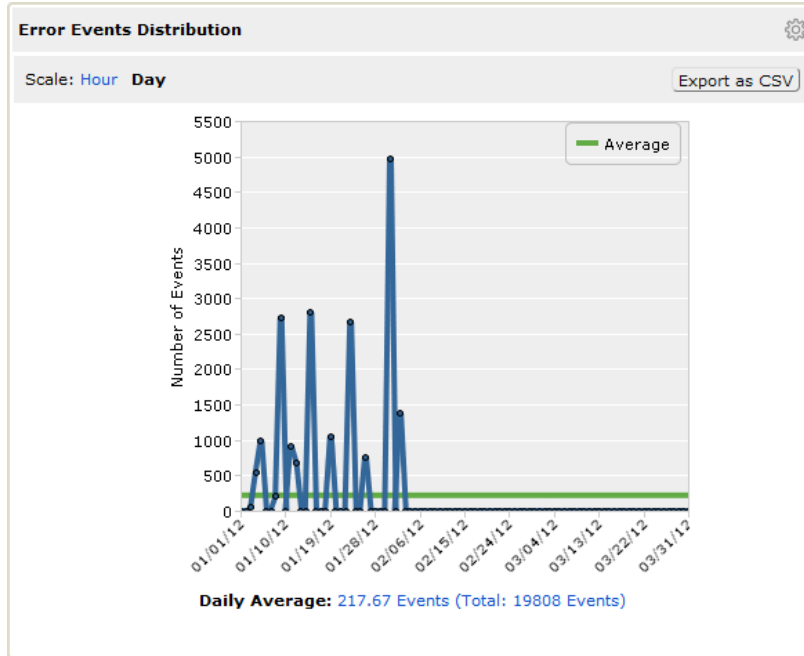
The following table describes the Error Events by Partner - Unresolved Errors panel elements:

Element	Description
Top 10 / Top 20	Number of partners for which to display the number of unresolved error events for the selected time frame.
Partner Name	Names of the partners with the highest number of unresolved error events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of unresolved error events for the partners during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of unresolved error events for the partners during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Error Events Distribution Panel

The Error Events Distribution panel displays the number of error events created per hour or per day during the selected time frame. Use the panel to identify error event creation peaks, and identify time periods that might require further attention. The panel displays all error events that reached a final state.

The following image illustrates the Error Events Distribution panel:



The following table describes the Error Events Distribution panel elements:

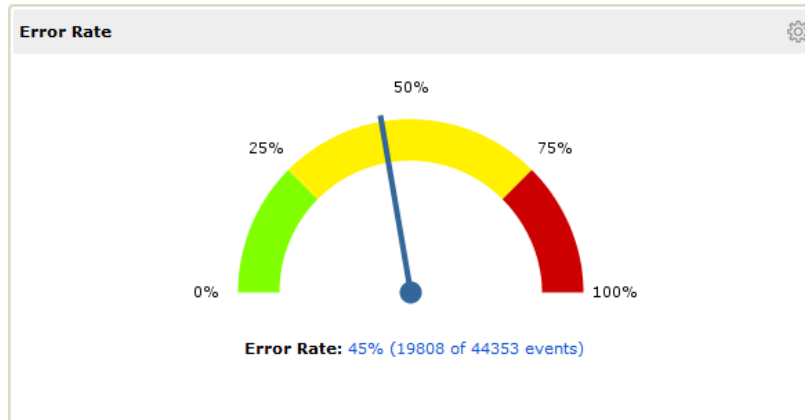
Element	Description
Scale	Time frame intervals. You can choose one of the following options: <ul style="list-style-type: none"> <li>- <b>Hour</b>. Displays the number of error events at hourly intervals as point on the graph.</li> <li>- <b>Day</b>. Displays the number of error events at daily intervals as point on the graph.</li> </ul> If you select a time frame filter longer than 7 days, you can only view error event distribution on a day scale.
Number of Events	Number of error events that B2B Data Exchange generated during the selected time frame. Appears on the Y-axis of the panel.
Time Distribution	Date or time intervals during which B2B Data Exchange generated error events. Appears on the X-axis of the panel.
Average Line	Average number of error events that B2B Data Exchange generated each day or hour and the total number of events for the selected time frame.
Daily/Hourly Average	Overall error event average and the total number of events for the selected time frame. You can click the link to display the error events in the <b>Event List</b> page.
Export as CSV	Saves the data in the panel as a CSV file.



## Error Rate Panel

The Error Rate panel displays the ratio of error events to the total events during the selected time frame in an intuitive and graphical format. The B2B Data Exchange administrator determines the percentage of error events to display in each zone.

The following image illustrates the Error Rate panel:



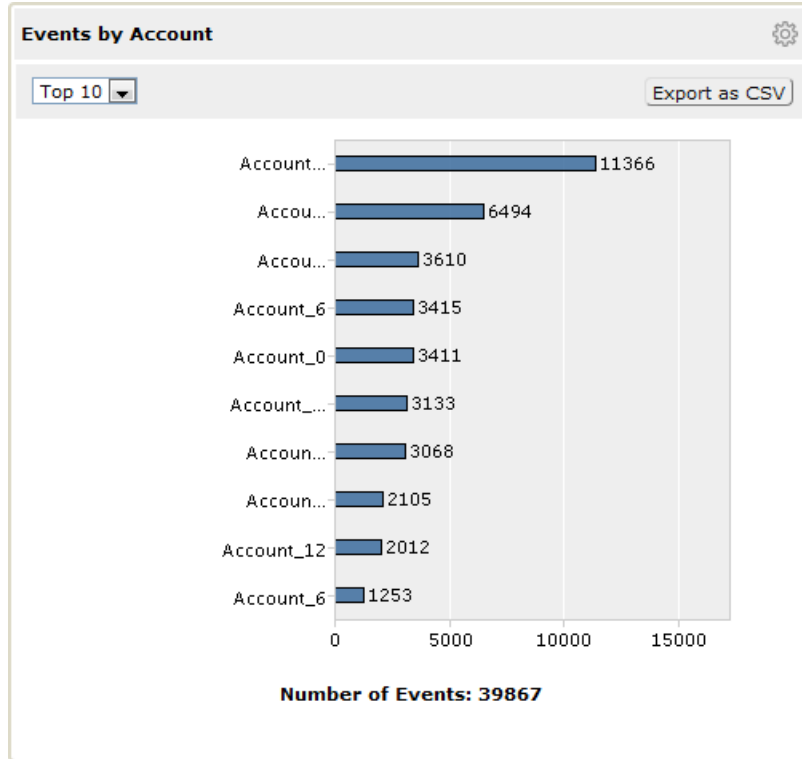
The following table describes the Error Rate panel elements:

Element	Description
Green Zone	Low percentage of error events for the selected time frame.
Yellow Zone	Medium percentage of error for during the selected time frame.
Red Zone	High percentage of error events for the selected time frame.
Dial Indicator	Visual indication of the error events percentage for the selected time frame.
Error Rate	Actual percentage and number of error events and the total number of events for the selected time frame. You can click the link to display the error events in the <b>Event List</b> page.

## Events by Account Panel

The Events by Account panel displays the 10 or 20 accounts with the highest number of events created during the selected time frame. Use the panel to analyze account activity or identify deviations. You can click each bar on the graph to display the events for the account in the **Event List** page.

The following image illustrates the Events by Account panel:



The following table describes the Events by Account panel elements:

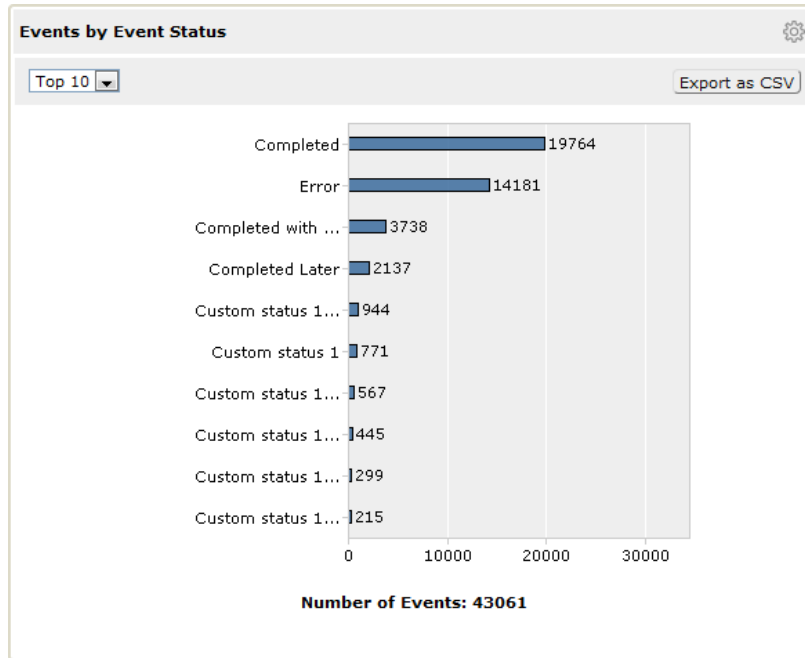
Element	Description
Top 10 / Top 20	Number of accounts for which to display the number of events for the selected time frame.
Account Name	Names of the accounts with the highest number of events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of events for the accounts during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of events for the accounts during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Events by Event Status Panel

The Events by Event Status panel displays the 10 or 20 event statuses with the highest number of events created during the selected time frame. Use the panel to identify deviations or other issues that might require

further attention. You can click each bar on the graph to display the events for the event status in the **Event List** page.

The following image illustrates the Events by Event Status panel:



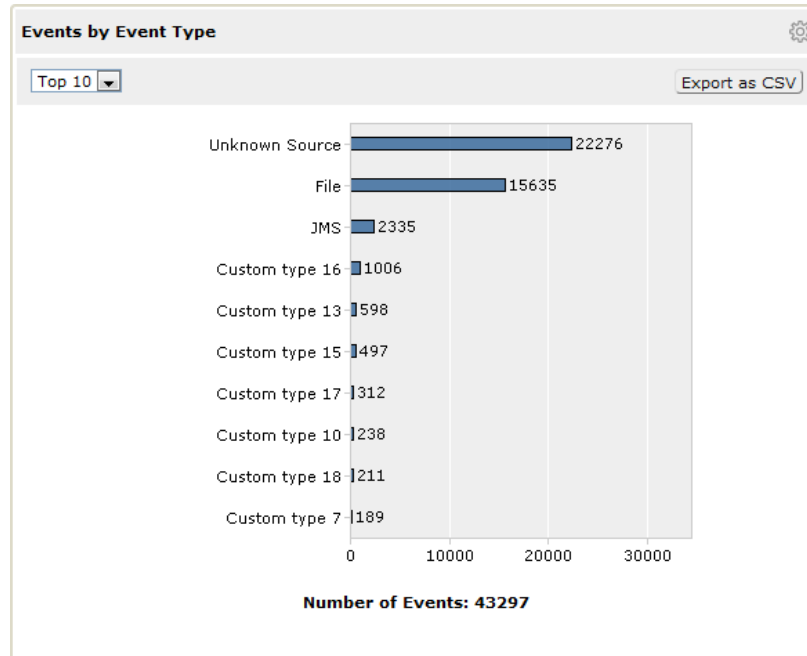
The following table describes the Events by Event Status panel elements:

Element	Description
Top 10 / Top 20	Number of event status for which to display the number of events for the selected time frame.
Event Status	Event statuses with the highest number of events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of events for the event status during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of events for the event statuses during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Events by Event Type Panel

The Events by Event Type panel displays the 10 or 20 event types with the highest number of events created during the selected time frame. Use the panel to identify deviations or other issues that might require further attention. You can click each bar on the graph to display the events for the event type in the **Event List** page.

The following image illustrates the Events by Event Type panel:



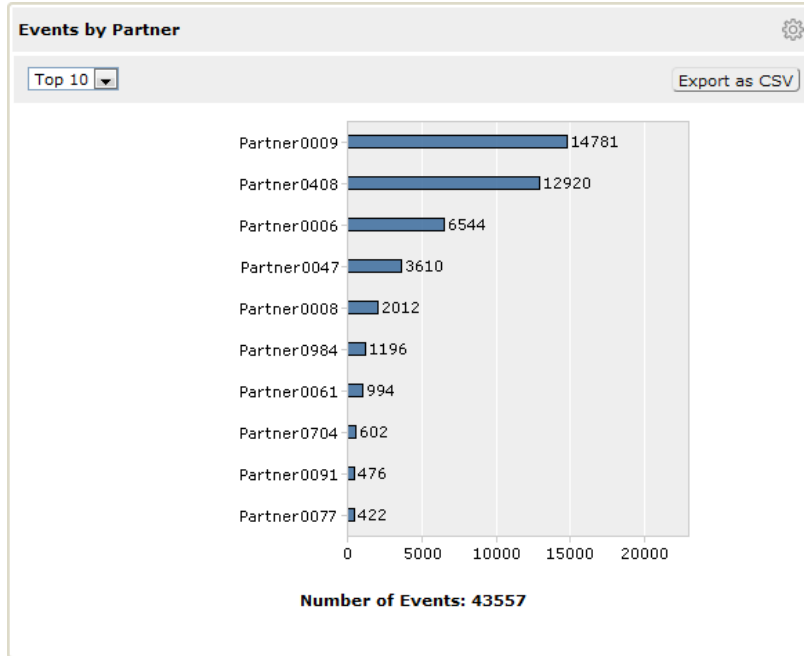
The following table describes the Events by Event Type panel elements:

Element	Description
Top 10 / Top 20	Number of event types for which to display the number of events for the selected time frame.
Event Type	Event types with the highest number of events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of events for the event type during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of events for the event types during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Events by Partner Panel

The Events by Partner panel displays the 10 or 20 partners with the highest number of events created during the selected time frame. Use the panel to analyze partner activity or identify deviations. You can click each bar on the graph to display the events for the partner in the **Event List** page.

The following image illustrates the Events by Partner panel:



The following table describes the Events by Partner panel elements:

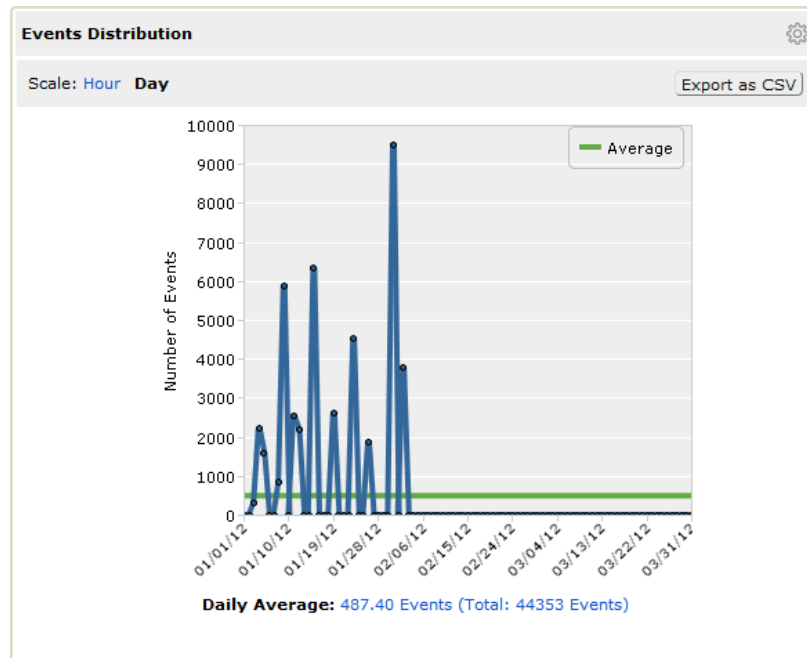
Element	Description
Top 10 / Top 20	Number of partners for which to display the number of events for the selected time frame.
Partner Name	Names of the partners with the highest number of events for the selected time frame. Appears on the Y-axis of the panel.
Events	Number of events for the partners during the selected time frame. Appears on the X-axis of the panel.
Number of Events	Total number of events for the partners during the selected time frame.
Export to CSV	Saves the data in the panel as a CSV file.

## Events Distribution Panel

The Events Distribution panel displays the total number of events created per hour or per day during the selected time frame. Use the panel to identify event creation peaks and valleys, and identify time periods that might require further attention.

The panel displays all event types and statuses that reached a final state. You can click any point on the graph to display the events in the **Event List** page.

The following image illustrates the Events Distribution panel:



The following table describes the Events Distribution panel elements:

Element	Description
Scale	Time frame intervals. You can choose one of the following options: - <b>Hour</b> . Displays the number of events at hourly intervals as point on the graph. - <b>Day</b> . Displays the number of events at daily intervals as point on the graph. If you select a time frame filter longer than 7 days, you can only view event distribution on a day scale.
Number of Events	Number of events that B2B Data Exchange generated during the selected time frame. Appears on the Y-axis of the panel.
Time Distribution	Date or time intervals during which B2B Data Exchange generated events. Appears on the X-axis of the panel.
Average Line	Average number of events that B2B Data Exchange generated each day or hour and the total number of events for the selected time frame.
Daily/Hourly Average	Overall event average and the total number of events for the selected time frame. You can click the link to display the events in the <b>Event List</b> page.
Export as CSV	Saves the data in the panel as a CSV file.

## SLA Violations Panel

The **SLA Violations** panel displays information about service level agreement (SLA) violations. Use the panel to identify deviations from the SLA requirements in your organization that require further attention. You manage SLA rules on the **SLA Rules** page of the Operation Console.

By default, the **SLA Violations** panel appears on the **SLA** tab of the Dashboard. You can apply global Dashboard filters to the panel. The panel displays violations for events that reached a final state.

The panel contains the following areas:

- Violations by SLA Rule diagram
- Violations by KPI diagram
- Violations list

You can view violations for events even if you do not have viewing permissions for the related partners. However, you cannot view the events for those partners in the Event List page when you click the violation in the list.

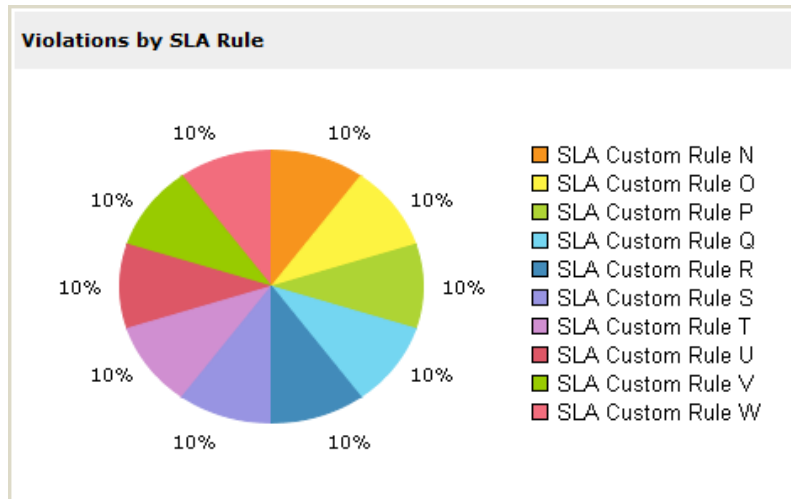
### RELATED TOPICS:

- [“Viewing Service Level Agreement Violations” on page 184](#)

### Violations by SLA Rule Area

The **Violations by SLA Rule** area displays visual and textual violation information according to the defined SLA rule.

The following image illustrates the **Violations by SLA Rule** area:

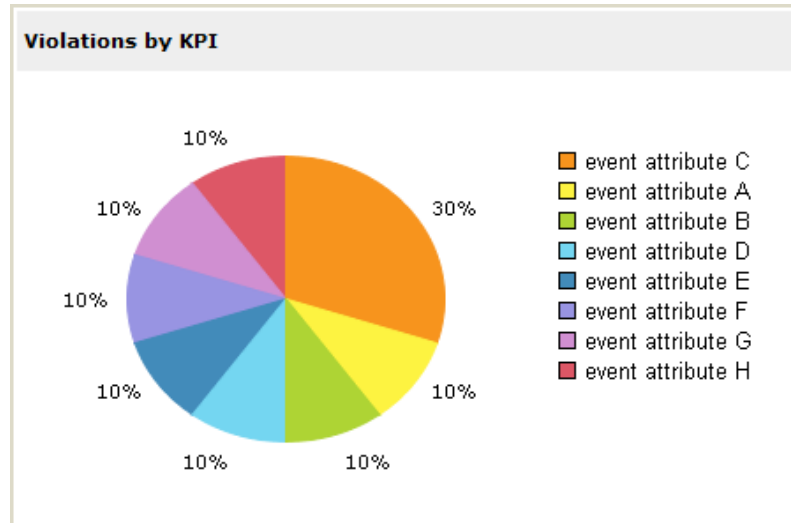


The area contains a pie chart and a legend that show a breakdown of violations for the top 10 rules. You can click any segment in the diagram to filter the violations in the Violations list. You can hover over any segment to view the number of violations for that rule.

## Violations by KPI Area

The **Violations by KPI** area displays visual and textual violation information according to the key performance indicator of the SLA rule.

The following image illustrates the **Violations by KPI** area:



The area contains a pie chart and a legend that show a breakdown of violations for the top 10 indicators. You can click any segment in the diagram to filter the violations in the Violations list. You can hover over any segment to view the number of violations for that indicator.

## Violations List

The **Violations** list displays detailed information about the first 50 violations according to the segment that you select from the diagrams.

By default, the **Violations** list displays violations sorted by the date and time that the violation was reported. You can click any column header to sort the visible violations in the list and hover over a violation to display the rule details.

The following table describes the **Violations** list columns:

Column	Description
Partner	Related partner for the violation.
Account	Related account for the violation.
KPI	Type of information that the rule uses, such as the number of events or the error rate percentage.
SLA Rule	Name of the rule.
Event Type	Type of the event.



Column	Description
Value	Actual value for the violation. For example, if you define a rule that event processing must not exceed 30 seconds and the actual processing time is 45 seconds, the Value column shows the total processing time as 45 seconds and the difference from the maximum processing time as 15 seconds. For SLA rules that you view at the end of the calculation level period, the column shows the total value for the violation. For example, if you define a rule that the number of errors in a day must not exceed 50 errors and the total number of errors for the day is 65, the Value column shows the total number of errors for all events that occurred during the time frame.
Detected	Date and time that the violation was reported.
Last Modified	Date and time that the violation was modified. The value of this property reflects the latest reported violation for that rule or KPI for the calculation level period.

## Tasks Panel

The Tasks panel displays the number of unresolved error events with a link to the **Events** page. It also displays the number of pending operator action requests with a link to the **Authorization** page. The panel displays a quick overview in a list of daily tasks.

The following table describes the Tasks panel elements:

Element	Description
Error events that occurred during the last <number of hours>.	Link to the <b>Events</b> page that displays the list of unresolved error events that occurred during the selected time frame.
Operator actions pending approval.	Link to the <b>Authorization</b> page that displays the list of pending operator actions. This link appears only if you have authorization privileges.

# Dashboard Panel CSV File Structure

You can export certain Dashboard panels to a comma-separated-value (CSV) file. The file contains all data in the panel in a single column, separated by semicolons. The file does not contain subtotals or formatting information.

The following table describes the CSV elements for the events or unresolved events panels:

Element	Description
<object>_ID	Identifier for the related object in B2B Data Exchange. You can view the following objects: <ul style="list-style-type: none"><li>- Partner</li><li>- Account</li><li>- Event Type</li><li>- Event Status</li></ul>
<object>_NAME	Name of the related object. You can view the following objects: <ul style="list-style-type: none"><li>- Partner</li><li>- Account</li><li>- Event Type</li><li>- Event Status</li></ul>
SUM_COUNT	Number of events that B2B Data Exchange generated for each object during the selected time frame.

The following table describes the CSV elements for the events or error events distribution panels:

Element	Description
ROW_NR	Numeric identifier for the time interval during which B2B Data Exchange processed the events.
DAY / TIMESLICE	Start date and time of the time intervals during which B2B Data Exchange processed events. The DAY column appears for panels that you view in a day scale. The TIMESLICE column appears for panels that you view in an hour scale.
TOTAL_COUNT	Total number of events that B2B Data Exchange processed during each time interval.

The following table describes the CSV elements for the average processing time panels:

Element	Description
ROW_NR	Numeric identifier for the time interval during which B2B Data Exchange processed the events.
DAY / TIMESLICE	Start date and time of the time intervals during which B2B Data Exchange processed events. The DAY column appears for panels that you view in a day scale. The TIMESLICE column appears for panels that you view in an hour scale.
TOTAL_COUNT	Total number of events that B2B Data Exchange processed during the each time interval.
TOTAL_TIME	Overall processing time for all of the events that B2B Data Exchange processed during each time interval.

# Managing the Dashboard

You use the Dashboard in the Operation Console to view and analyze events that B2B Data Exchange generates during a defined time frame. You personalize your view of the Dashboard and add or remove panels and tabs as needed. If you require more screen space to view the Dashboard, you can collapse the Navigator.

You can only view the Dashboard if the B2B Data Exchange administrator installed and configured it and if you have dashboard privileges.

1. In the Navigator, select **Dashboard**.

The B2B Data Exchange administrator can set the Dashboard to open by default when you log in to the Operation Console.

2. To add a tab to the Dashboard, perform the following steps:
  - a. Click the Add Tab icon, choose the panels that you want to add in the **Add Panels** window, and then click **Done**.
  - b. Click the Settings icon in the tab, choose **Change Layout**, choose the number of panel columns in the **Tab Layout** dialog box, and then click **Done**.
  - c. Click the Settings icon in the tab, choose **Rename Tab**, and then enter a name for the tab.
3. To further personalize the appearance of the Dashboard, use one or more of the following options:

- To add panels to a tab, click the Settings icon in the tab, choose the panels that you want to add in the **Add Panels** window, and then click **Done**.

**Note:** You can add only one instance of each panel to a single tab. All instances of a report display identical data. For example, if you change the local report filter on one tab, all instances of the same report in all tabs filter the data accordingly.

- To change the layout of a tab, click the Settings icon in the tab, choose **Change Layout**, choose the number of panel columns in the **Tab Layout** dialog box, and then click **Done**.
  - To rename a tab, click the Settings icon in the tab, choose **Rename Tab**, and then enter the new name.
  - To remove a tab, click the Settings icon in the tab and then choose **Remove Tab**.
  - To rename a panel in the tab, click the Settings icon in the panel, choose **Rename**, and then enter the new name. The panel retains its original name in the Dashboard catalog.
  - To remove a panel from the tab, click the Settings icon in the panel and then choose **Remove**. The panel remains available in the Dashboard catalog.
  - To restore the default Dashboard and remove any additional panels or tabs that you added, click **Restore Default Dashboard**.
4. In the **Filter** pane, define the filters that you want to use and click **Apply Filters**.

**Note:** The filters apply to all panels except for the time frame filter for the unresolved error event panels and the Tasks pane.
  5. To change the time frame filter in unresolved errors event panels and the Tasks pane, click **Customize...** below the **Filter** pane and define the time frame that you want to view.
  6. Navigate to the panel that you want to view and set the display preferences as needed.
  7. To export data from a specific panel to a CSV file, click **Export to CSV** in the specific panel and save the file.

## CHAPTER 15

# Service Level Agreement Management

This chapter includes the following topics:

- [Service Level Agreement Management Overview, 180](#)
- [Service Level Agreement Rules, 180](#)
- [Service Level Agreement Violations, 183](#)
- [Managing Service Level Agreement Rules, 184](#)
- [Viewing Service Level Agreement Violations, 184](#)
- [Selecting SLA Rules for the Partners Portal, 185](#)

## Service Level Agreement Management Overview

A service level agreement (SLA) defines business requirements between an organization and customers or between different departments in an organization. SLA requirements apply to properties of transactions that B2B Data Exchange processes, such as event processing time or error rate.

You create rules to manage and track compliance with service level agreement requirements. The SLA violation detector searches the operational data store and reports violations based on key performance indicators that you select when you define the rule. Key performance indicators (KPIs) provide measurable information about events, such as average processing time or number of events.

You can use SLA tracking and management if the B2B Data Exchange administrator installed the Dashboard and Reports component.

## Service Level Agreement Rules

You create and manage service level agreement rules on the **SLA Rules** page of the Operation Console.

You can define a rule for all partners and accounts or for a specific partner and account. If you define a rule for a specific partner and account, the partner and account are excluded from global rules that report the same violation type.

If you modify a rule, the SLA violation detector reports violations only the next time it runs. If the SLA violation detector reported violations before you modified the rule, you can view violations for the previous rule and for the modified rule. If you delete a rule, you can still view previously detected violations.

## Service Level Agreement Rule Properties

When you create or modify a rule, you define properties to determine the type, time frame, and conditions of the violation. If you do not have editing privileges for the rule, the properties appear in read-only mode.

The **Create SLA Rule** page contains the **General** tab and the **Rule** tab.

### General Tab

The following table describes the properties in the **General** tab:

Property	Description
SLA rule name	Name of the rule.
Description	Optional. Textual description of the rule.
Show in Portal	Select whether to hide or display the SLA rule in the Partners Portal for the selected partner. If you select to display SLA rules, the three SLA rules with the greatest number of relevant events are displayed in the Partners Portal.
Partner and Account	Determines whether to apply the rule to all partners and accounts or to a specific partner and account. You can choose from the following options: <ul style="list-style-type: none"> <li>- All partners and accounts. Reports violations for all partners and accounts. The violations appear separately for each partner and account.</li> <li>- Selected partner and account. Reports violations for a single partner an account. You must select a partner before you select an account.</li> </ul>

### Rule Tab

The following table describes the properties in the **Rule** tab:

Property	Description
Event type	Type of the event for which to report violations. You can choose to report violations for all event types or for a specific event type. The event types appear according to the event types that you define on the <b>Event Types</b> page of the Operation Console.
KPI	Type of information about the event that you want to report. You can choose from the following default key performance indicators: <ul style="list-style-type: none"> <li>- Number of events</li> <li>- Error rate (percent)</li> <li>- Number of errors</li> <li>- Average processing time (seconds)</li> <li>- Event processing time (seconds)</li> </ul> If the B2B Data Exchange developer created custom key performance indicators from event attributes, the custom indicators appear below the default key performance indicators.

Property	Description
Calculation level	<p>Scope of the violation to report. You can choose from the following options:</p> <ul style="list-style-type: none"> <li>- Per single event. Reports violations as they occur in individual events. The SLA violation detector reports violations at the end of the next operational data store event load process according to the schedule that the B2B Data Exchange administrator defines.</li> <li>- Per day. Reports violations that occur during a single day. The B2B Data Exchange administrator sets the start of the daily calculation level period in a system property.</li> <li>- Per week. Reports violations that occur during a week. The B2B Data Exchange administrator sets the first day of the week in a system property.</li> <li>- Per month. Reports violations that occur during a calendar month.</li> </ul>
Function	<p>Type of calculation to perform on custom key performance indicators. You can choose from the following options:</p> <ul style="list-style-type: none"> <li>- Sum</li> <li>- Count</li> <li>- Average</li> <li>- Max</li> <li>- Min</li> </ul> <p>Not available for default key performance indicators. Not available if you define a rule for a single event.</p>
Condition	<p>Mathematical operator to apply to the key performance indicator. You can choose from the following options:</p> <ul style="list-style-type: none"> <li>- Is less than. Reports violations in which the actual value is less than the required value.</li> <li>- Is greater than. Reports violations in which the actual value is greater than the required value.</li> </ul>
Value	<p>Numeric value in digits or percent according to the selected key performance indicator. For example, to report violations for the number of events, enter the number of events.</p> <p>To report violations for error rate, enter the percentage of errors relative to the total errors. To report violations for event processing time or average processing time, enter a value greater than zero in seconds.</p>

## Service Level Agreement Rule Examples

You define rule properties according to the service level agreement requirements in your organization.

The following examples show rules that you can define according to the requirements.

### Maximum Number of Events Per Day

Your organization wants to monitor daily network traffic for B2B Data Exchange to ensure environment reliability. You create a rule to report a violation if the total number of events that B2B Data Exchange processes during a single day is greater than 1,000.

The following table describes the rule properties to define on the **Rule** tab of the **Create SLA Rule** page:

Property	Value
Event type	File level event
KPI	Number of events
Calculation level	Per day

Property	Value
Condition	Is greater than
Value	1000

### Error Rate Per Week

Your organization has a contractual obligation for a partner to maintain an error rate of less than 25 percent during each week. You create a rule to report a violation if the error rate for events that B2B Data Exchange processed for that partner during a week is greater than 25 percent.

The following table describes the rule properties to define on the **Rule** tab of the **Create SLA Rule** page:

Property	Value
Event type	File level event
KPI	Error rate (percent)
Calculation level	Per week
Condition	Is greater than
Value	25

## Service Level Agreement Violations

The SLA violation detector searches the operational data store for violations of service level agreements.

The operational data store event loader collects aggregated event information from the run-time B2B Data Exchange repository and loads the information to the operational data store. At the end of the event load process, the SLA violation detector searches the aggregated event information for violations based on the SLA rules that you defined.

The SLA violation detector reports violations for events that reached a final state. Violations for events that processed during multiple time frames appear only in the time frame on which the event processing started. For example, if the SLA violation detector finds a violation for an event that started processing on Sunday and reached a final state on Monday, you will see the violation when you select violations for Sunday but not for Monday.

The SLA violation detector reports most violation types at the end of the time frame. For example, if you define an SLA rule in which the error rate for a single day does not exceed 20%, the SLA violation detector searches the events for the violation only at the end of the day.

The SLA violation detector reports violations immediately when the value of the following default key performance indicators is greater than the value that you define in the rule:

- Number of events
- Number of errors
- Event processing time

For example, if you define an SLA rule in which the maximum number of events for a single partner and account must not exceed 50 events in a day, the SLA violation detector reports the violation as soon as it finds event number 51 for that partner and account and the event reached a final state.

The SLA violation detector reports violations for custom key performance indicators immediately when you define the following conditions in the rule:

- The key performance indicator count is greater than the rule value
- The maximum key performance indicator value is greater than the rule value
- The minimum key performance indicator value is less than the rule value
- The calculation level period for the rule is **Per Single Event**

For example, if you define a rule in which each purchase order that a partner sends must have a value of at least 5,000 dollars, the SLA violation detector reports the violation as soon as it finds a purchase order with a lower value and the event reached a final state.

## Managing Service Level Agreement Rules

Manage rules on the **SLA Rules** page of the Operation Console. Define rules to detect violations based on criteria such as the KPI, time frame, or related partner and account.

Make sure that the dashboard is installed and that the operational data store event loader is running.

1. In the Navigator, click **Partner Management > SLA Rules**.  
The **SLA Rules** page displays the list of active SLA rules.
2. Choose to create, edit, or delete a rule.

After the SLA violation detector reports violations, you view the violations in the **SLA Violations** panel of the Dashboard.

## Viewing Service Level Agreement Violations

You view violations of SLA rules in the **SLA Violations** panel of the Dashboard.

The panel displays violations according to the defined SLA rule or the KPI for the SLA rule. By default, the panel appears on the **SLA** tab of the Dashboard.



## RELATED TOPICS:

- [“SLA Violations Panel” on page 175](#)

# Selecting SLA Rules for the Partners Portal

Select whether to hide or display violations for an SLA rule in the Partners Portal for a selected partner. After you select which rules to display, the three SLA rules with the greatest number of violations are displayed in the Partners Portal Dashboard.

1. In the Navigator, click **Partner Management > SLA Rules**.  
The **SLA Rules** page displays the list of active SLA rules.
2. Choose to create or edit a rule.
3. In the General tab, fill in the rule name, description, partner, and account.
4. To hide the SLA rule violations from the Partners Portal Dashboard, deselect **Show in Portal**. To display the SLA rule violations in the Partners Portal Dashboard, select **Show in Portal**.
5. In the Rules tab, fill in the rule properties.
6. Click **Save**.  
If the Partners Portal is open, close and re-open the Partners Portal.

# CHAPTER 16

## Glossary

### **account**

A sub-entity of a partner. In a customer organization, an account can represent a unit such as a department or subsidiary. For an internal system, an account can be a unit such as a customer ID or a vendor code.

### **advanced exception handling issue**

An advanced exception handling entity used by an operator to record and monitor progress towards the resolution of an exceptional event that arises during the course of B2B Data Exchange operations. Advanced exception handling issues are defined in event monitors.

### **application**

A set of related workflows. If multiple workflows are required to complete the processing of a document, you can group the workflows into one application.

### **B2B Data Exchange repository**

A relational database table set that contains the metadata required to process documents in B2B Data Exchange. It also contains the events that B2B Data Exchange generates while it processes documents.

### **B2B Data Exchange server**

A service that manages document processing in B2B Data Exchange. The B2B Data Exchange server triggers batch workflows and sends and receives notifications from PowerCenter.

### **batch workflow**

A PowerCenter workflow that runs once and stops after completion. The workflow reads from a file, a database, or another source and writes to a target. 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.

### **child event**

An event within the hierarchy of another event that acts as a parent event. The child event is a subsidiary of the parent event.

### **custom B2B Data Exchange mapping**

A mapping that processes a data set. The mapping includes the data sources and targets, metadata folders, and connections to process the data.

A custom mapping uses a PowerCenter workflow, a Big Data Management mapping, or an Informatica Cloud task to process data. Workflows and tasks can perform complex transformations on the data.

A custom mapping that uses a PowerCenter workflow or a Big Data Management mapping can include parameters.

### **Data Transformation Engine**

The Data Transformation Engine transforms data from any format to any other format. It can transform unstructured documents, such as Microsoft Excel and Word, as well as industry-specific documents such as SWIFT for financial services and HIPAA for health care. When you include an Unstructured Data transformation in a PowerCenter WebSphere Process Server mapping to process Data Exchange documents, the Data Transformation Engine converts the documents from one structure to another.

### **delayed processing rules**

A set of rules that defines when an event must be delayed or released for processing. Delayed processing rules define the threshold that must be met for events to be released.

### **document**

An instance of data to be processed. A document is the content of a file received by B2B Data Exchange and passed to the flow engine for transformation.

### **document store**

File directory where B2B Data Exchange stores all documents associated with a document reference. The document store directory must be accessible to the B2B Data Exchange server, the Apache Tomcat server, and the PowerCenter Integration Service with the same file path.

### **endpoint**

The point of entry and exit of documents in B2B Data Exchange. The endpoint definition in the Data Exchange configuration file specifies how and where B2B Data Exchange receives documents from and sends documents to partners.

### **event**

An occurrence of a document at each stage of processing. The B2B Data Exchange server generates the event and updates the event status while it processes the document.

### **event monitor**

A view of a set of events filtered by rules that specify the type of events to be included in the view, actions to be done to the events, and notifications to be sent about the events. You can set the frequency in which the view is updated. The event monitor can be used to track document processing problems and to specify actions required.

### **flow engine**

The B2B Data Exchange component that executes the transformation logic to process a document. PowerCenter is the main flow engine used to process Data Exchange documents.

### **Informatica Cloud workflow**

The B2B Data Exchange object that represents the transformation logic used to process a document in Cloud Data Integration. The workflow is a Cloud Data Integration mapping.

**mass ingestion task**

A Cloud Data Integration mass ingestion task can transfer data in a flat file format from on-premises to cloud ecosystems such as Amazon S3 data stores and Amazon Redshift data warehouses in the cloud using FTP, SFTP, and FTPS standard protocols.

**Operation Console**

Web interface to manage partners, customize and monitor document processing, and administer user access in B2B Data Exchange. Use a web browser to access the Operation Console.

**parent event**

An event at the top level of a hierarchy of events. The parent event status changes after all child events change status.

**partner**

An external or internal entity that sends documents for processing or receives documents after processing in B2B Data Exchange. A partner can be an organization such as a vendor or customer or an internal system such as an accounting system or an ERP system.

**profile**

A profile associates a workflow with a partner or account and defines the properties that customize a workflow to process documents for a specific partner or account.

**real-time workflow**

A PowerCenter real-time workflow that runs continuously and reads input from the JMS queue. You can use these workflows to process documents from B2B Data Exchange.

**reconciliation**

Reconciliation is the process of correlating an event with another event. For example, you send a document file to a partner containing transactions such as payments or orders that require acknowledgement. When you send the file to the partner, you initiate a reconciliation. When you receive the acknowledgement from the partner, you complete the reconciliation. The Data Exchange Server uses a correlation ID to identify each transaction and to reconcile the event associated with sending the file with the event associated with receiving the file.

**root event**

An event that does not have a parent event. A root event can be a parent event. See also [event on page 187](#).

**workflow**

The B2B Data Exchange object that represents the transformation logic used to process a document. The workflow can be an Informatica Cloud workflow or a PowerCenter workflow.

# INDEX

## A

- accounts
  - definition [20](#)
- advanced
  - exception handling [144](#)
- advanced exception handling
  - example workflow [145](#)
- advanced search
  - objects in view [18](#)
- archived events
  - overview [118](#)
  - viewing [118](#)
- audit
  - legacy [139](#)
  - legacy event properties [140](#)
  - viewing legacy [140](#)
- audit trail
  - definition [137](#)
  - object types [137](#)
  - properties [138](#)
  - viewing [139](#)
- authorization
  - approving [143](#)
  - definition [137](#)
  - object types [140](#)
  - properties [141](#)
  - rejecting [143](#)
  - rules and guidelines [142](#)

## B

- B2B Data Exchange
  - definition [10](#)
- basic search
  - objects in view [18](#)

## C

- charts
  - on-boarding checklist [55](#)
- Cloud Data Integration mapping
  - formatting flat file options [110](#)
  - input file parameter [110](#)
  - integration with B2B Data Exchange [109](#)

## D

- Dashboard and reports
  - managing [179](#)
  - overview [150](#)
- delay rules
  - delayed event processing [37](#)

- delayed event processing
  - configuring [38](#)
  - delay rules [37](#)
  - release rules [37](#)
  - timing rules [37](#)
- delayed processing
  - events [36](#)
- delayed processing events
  - example [36](#)
- Document Processing
  - Overview [10](#)
- DX\_Hosted\_PGP\_Decrypt [91](#)
- DX\_Hosted\_PGP\_Encrypt [94](#)
- DX\_Hosted\_Unzip [91](#)
- DX\_Hosted\_Zip [94](#)
- DX\_Remote\_AS2\_Send [100](#)
- DX\_Remote\_FTP\_Receive [95](#)
- DX\_Remote\_FTP\_Send [100](#)
- DX\_Remote\_FTPS\_Receive [95](#)
- DX\_Remote\_FTPS\_Send [100](#)
- DX\_Remote\_HTTP\_Get [95](#)
- DX\_Remote\_HTTP\_POST [100](#)
- DX\_Remote\_HTTPS\_Get [95](#)
- DX\_Remote\_HTTPS\_POST [100](#)
- DX\_Remote\_ML\_Send [100](#)
- DX\_Remote\_SCP\_Receive [95](#)
- DX\_Remote\_SCP\_Send [100](#)
- DX\_Remote\_SFTP\_Receive [95](#)
- DX\_Remote\_SFTP\_Send [100](#)

## E

- endpoint
  - configuration variables [104](#)
  - creating [105–108, 111](#)
  - deleting [108](#)
  - editing [108](#)
  - errors [112](#)
  - File Receive [87](#)
  - File Send [89](#)
  - Informatica Managed File Transfer [91, 94, 95, 100](#)
  - JMS Receive [89](#)
  - JMS Send [90](#)
  - MFT hosted receive endpoint [91](#)
  - MFT hosted send endpoint [94](#)
  - MFT remote receive endpoint [95](#)
  - MFT remote send endpoint [100](#)
  - types [84](#)
- endpoint integration
  - Informatica Cloud workflow [109](#)
  - Informatica Intelligent Cloud Services mapping [109](#)
  - mass ingestion task [111](#)
- event
  - audit [139](#)
  - reprocessing [134](#)

- event (*continued*)
  - resending [136](#)
- event monitor
  - creation [119](#)
  - definition [119](#)
- event resubmission
  - definition [134](#)
- events
  - actions [114](#)
  - advanced search properties [115](#)
  - archived [118](#)
  - basic search properties [115](#)
  - delayed processing [36](#)
  - Informatica Managed File Transfer [118](#)
  - managing [114](#)
  - message processing [117](#)
  - overview [113](#)
  - searching for [115](#), [116](#)
  - types and statuses [117](#)
- events page
  - how to access [114](#)
  - how to search [115](#), [116](#)
- exception handling
  - advanced [144](#)
  - displaying issue details [148](#)

## F

- formatting options
  - flat file source [110](#)

## G

- glossary
  - of terms [186](#)

## I

- Informatica Cloud workflow [109](#)
- Informatica Managed File Transfer
  - jobs [118](#)
  - MFT Connection [65](#), [66](#), [68](#), [71](#), [74–79](#)
  - MFT Web User [60](#)
  - MFT Web Users [59](#)
- input files
  - parameterizing [110](#)

## M

- mass ingestion task
  - integration with B2B Data Exchange [111](#)
- message processing
  - event types and statuses [117](#)
- MFT Connection
  - description [65](#)
  - FTP properties [66](#), [68](#)
  - FTPS properties [71](#)
  - HTTP properties [74](#)
  - HTTPS properties [75](#)
  - Mailbox properties [76](#)
  - MQ properties [77](#)
  - SFTP, SCP, or SSH properties [79](#)
  - SMTP properties [78](#)

- MFT Web User
  - description [59](#)
  - properties [60](#)
- monitoring
  - on-boarding checklists [53](#)

## O

- on-boarding checklist
  - charts [55](#)
  - monitor [55](#)
- on-boarding checklists
  - monitoring [53](#)
- Operation Console
  - searching [16](#)
  - sorting objects [16](#)

## P

- Partner
  - Creating [21](#)
- partners
  - definition [20](#)
  - deleting [24](#)
  - editing [24](#)
- Partners Portal user
  - Creating [30](#)
- portal user
  - deleting [31](#)
- portal users
  - editing [31](#)
  - searching [31](#)
- prerequisites
  - Informatica Intelligent Cloud Services mapping [109](#)
  - mass ingestion task [111](#)
- profile
  - creating [32](#)
- profiles
  - creating [31](#)
  - definition [20](#)
  - rules and guidelines [31](#)
- progress
  - on-boarding checklist [55](#)

## R

- reconciliation monitor
  - creation [126](#)
  - definition [125](#)
- release rules
  - delayed event processing [37](#)
- resending
  - event [136](#)

## S

- search
  - advanced [18](#)
  - basic [18](#)
- SLA violations
  - by KPI [176](#)
  - by SLA rule [175](#)
  - list [176](#)

SLA Violations  
Dashboard panel [175](#)

**T**  
timing rules  
delayed event processing [37](#)