



# **TIBCO BusinessConnect™ Container Edition – Services Plug-in**

## **User Guide**

Version 1.5.0 | October 2024

# Contents

---

<b>Contents</b>	<b>2</b>
<b>Introduction</b>	<b>6</b>
Protocol Features	6
Support for Public Transports	7
Support for Operations	7
XML Validation	7
Support for Multiple Attachments	7
Duplicate Message Detection	8
Other Supported Features	8
<b>Tutorial</b>	<b>9</b>
Tutorial Steps	9
Importing the Tutorial	10
Configuring the Initiator BusinessConnect Container Edition	11
Configuring the Responder BusinessConnect Container Edition	14
Configuring Private Processes	17
Running the Tutorial	20
<b>BusinessConnect Container Edition – Services Plug-in URIs</b>	<b>27</b>
Exchanging URIs	27
Email Transport	28
File Transport	28
FTP Transport	29
HTTP/S Transport	29
URI for the HTTP Transport	29
URI for the HTTPS Transport	30
Populating URIs	30

<b>Managing BusinessConnect Container Edition – Services Plug-in Operations</b>	<b>31</b>
BusinessConnect Container Edition – Services Plug-in Operations	31
Notify Operation	31
Synchronous Request Response Operation	32
Asynchronous Request Response Operation	34
Schema Validation in BusinessConnect Container Edition – Services Plug-in	35
Caching of Schemas	35
Duplicate Message Detection	36
Outbound Duplicate Detection Criteria	36
Inbound Duplicate Detection Criteria	37
Configuring BusinessConnect Container Edition – Services Plug-in Operations	37
Adding a New Category	37
Adding a New Version	38
Adding a New Operation	38
<b>Setting Up Trading Hosts and Partners</b>	<b>44</b>
Configuring BusinessConnect Container Edition – Services Plug-in for a Host	44
Assigning Default Host	45
Configuring BusinessConnect Container Edition – Services Plug-in for a Partner	46
General Tab	46
Transport Tab	47
<b>Configuring Business Agreements</b>	<b>49</b>
Adding a New Business Agreement	49
Configuring Agreement Protocol Binding for BusinessConnect Container Edition – Services Plug-in	50
Operations Tab	50
Document Exchange Tab	51
Transports Tab	53
Override Configuration Tab	55
<b>Private Messages</b>	<b>58</b>

About Private Messages .....	58
Initiator Messages .....	59
Initiator Outbound Request—Private Process to BusinessConnect .....	59
Initiator Inbound Response—BusinessConnect to Private Process .....	61
Responder Messages .....	65
Responder Inbound Request—BusinessConnect to Private Process .....	65
Responder Outbound Response—Private Process to BusinessConnect .....	68
Responder Acknowledgment—Private Process to BusinessConnect .....	70
General Messages .....	71
Error Messages .....	71
Multiple Attachments .....	72
Resending Services Plug-in Private Process Messages .....	74
<b>Viewing Logs .....</b>	<b>75</b>
Transactions Screen .....	75
Customizing Transactions Screen .....	76
Sort Transactions .....	77
Search for Transactions .....	78
Using Search .....	78
Transaction Details .....	79
Resend Transactions .....	79
Resending Transactions .....	81
Viewing Resend History .....	82
<b>File Pollers .....</b>	<b>84</b>
Outbound File Pollers for BusinessConnect Container Edition – Services Plug-in .....	84
URI Format for Outbound File Pollers .....	84
Inbound File Pollers for BusinessConnect Container Edition – Services Plug-in .....	85
<b>Copying Large Files to NFS (Sharing) .....</b>	<b>87</b>
<b>TIBCO Documentation and Support Services .....</b>	<b>89</b>

<b>Legal and Third-Party Notices .....</b>	<b>91</b>
--	-----------

# Introduction

---

TIBCO BusinessConnect™ Container Edition – Services Plug-in is an easy-to-use data transfer protocol that can be used to exchange data securely over the Internet.

Trading partners managed by TIBCO BusinessConnect™ Container Edition can quickly and efficiently be configured to exchange documents securely with the BusinessConnect™ Container Edition host using this plug-in, without the overhead of interpreting the document contents.

You can track each document sent or received from a trading partner using the Request or Response operation type in BusinessConnect™ Container Edition – Services Plug-in. This function can be independent of the transport mechanism, and it correlates the corresponding response document with the trading partner. The back-office applications focus on the processing of the document contents sent or received from BusinessConnect Container Edition, which ensures that the response document is properly logged with the corresponding request document and delivered or received to or from the trading partner on time.

## Protocol Features

BusinessConnect Container Edition – Services Plug-in contains the following features. Each feature is discussed in the following sections:

- [Support for Public Transports](#)
- [Support for Operations](#)
- [XML Validation](#)
- [Support for Multiple Attachments](#)
- [Duplicate Message Detection](#)
- [Other Supported Features](#)

## Support for Public Transports

The basic transport connectivity includes File, Email, HTTP/S, FTP/S, and SSHFTP transports. These transports follow industry transport protocol standards such as AS1, AS2, SMTP, POP, S/MIME, SSH, and SSL to provide document security by encryption and document authenticity by digital signature.

## Support for Operations

BusinessConnect Container Edition – Services Plug-in supports the following operations:

- [Notify Operation](#)

Notify operation is a one-way operation. It can send a document to the trading partner and receive the acknowledgment. It cannot receive a response from the trading partner.

- [Synchronous Request Response Operation](#)

Synchronous Request Response operation sends the document to the trading partner and waits until it receives the response. It suspends any further processing for that request.

- [Asynchronous Request Response Operation](#)

Asynchronous Request Response operation sends the document to the trading partner and waits for the response, but it allows further processing irrespective of when it receives a response from the partner.

## XML Validation

BusinessConnect Container Edition – Services Plug-in supports XSD and DTD schema validation.

## Support for Multiple Attachments

BusinessConnect Container Edition – Services Plug-in supports multiple attachments. Private process can send these attachments in a sequence. For more information about the structure of each attachment, see [Multiple Attachments](#).

## Duplicate Message Detection

BusinessConnect Container Edition – Services Plug-in supports verification of both incoming and outgoing public messages for duplicates.

## Other Supported Features

- Electronic signing and message encryption or decryption.
- Audit logging, including the user `transactionID` in the audit log.
- Exchange of notices with trading partners.
- XML, plain text, and binary data blobs.



# Tutorial

---

This tutorial is designed for beginners who want to configure BusinessConnect Container Edition – Services Plug-in for the Asynchronous Request Response Operation.

This tutorial gives an example of an Asynchronous Request Response Operation on:

- How to create a private process on the Initiator and the Responder machine
- How to create and process an Asynchronous Request Response operation

In this tutorial, the following two machines are required:

- The Initiator machine: **Buyer**
- The Responder machine: **Seller**

For an overview of the operation, see [Asynchronous Request Response Operation](#).

## Tutorial Steps

### Before you begin

Install the following software packages on both the Initiator and the Responder machines:

1. TIBCO BusinessConnect™ Container Edition, for the procedure to install see *TIBCO BusinessConnect™ Container Edition Installation and Deployment*.
2. TIBCO BusinessConnect™ Container Edition – Services Plug-in, for the procedure to install see *TIBCO BusinessConnect™ Container Edition – Services Plug-in Installation*.

This tutorial requires that you perform the following steps:

Step no.	Step	Note
1	<a href="#">Importing the Tutorial</a>	Perform this step on both the Initiator and the Responder machines.

Step no.	Step	Note
2	<a href="#">Configuring the Initiator BusinessConnect Container Edition</a>	Perform this step only on the Initiator machine.
3	<a href="#">Configuring Private Processes</a>	Perform this step on both the Initiator and the Responder machines.
4	<a href="#">Running the Tutorial</a>	Perform this step on both the Initiator and the Responder machines.

## Importing the Tutorial

Perform the following steps to import the tutorial on both the machines (Initiator and Responder):

### Procedure

1. On the B2B Administration tile > **Operations Editor**, click **EZComm**.
2. Click the **Import** icon.
3. On the **Import Operations Data** dialog, click **Upload File**.
4. Upload the following file for TIBCO Business Studio™: EZComm\_HOME/samples/interfaces/ezcommtutorial\_for\_bw6-operations\_ V2.csx.  
Enter a password if it is necessary.
5. Click **Import**.

After the operations are imported, continue to configure the machines.

### What to do next

[Configuring the Initiator BusinessConnect Container Edition](#).

# Configuring the Initiator BusinessConnect Container Edition

In this tutorial, the host's machine name is **Buyer**, and the partner's machine name is **Seller**.

Perform the steps described in the following sections to configure the Initiator BusinessConnect Container Edition machine:

**i Note:** The following sections contain only the steps necessary for this tutorial.

- [Configuring the Initiator Default Host](#)
- [Configuring the Initiator Partner](#)
- [Configuring the Initiator Business Agreement](#)

## Configuring the Initiator Default Host

Perform the following steps to configure the initiator default host:

### Procedure

1. On the Partner Management tile, click **Hosts**.
2. On the Hosts page, click **Create Host** in the upper-right corner of the page.
3. Enter Buyer in the **Host Name** field; then click **Proceed**.

**i Note:** For this tutorial, you do not need to edit additional settings to configure the protocol.

4. Select the **Make this as Default Host** checkbox to set **Buyer** as the default host.
5. Click **Done**.

### Result

A host **Buyer** is created and set as the default host.

## What to do next

### Configuring the Initiator Partner

## Configuring the Initiator Partner

Perform the following steps to configure the initiator partner:

### Procedure

1. On the Partner Management tile, click **Partners**.
2. On the Partners page, click **Create Partner** in the upper-right corner of the page.
3. Enter Seller in the **Partner Name** field and click **Proceed**.
4. On the **Protocols** tab, select the **EZComm** checkbox to enable the EZComm protocol for the Initial Partner.
5. Add a transport for the Initial Partner:
  - a. After you enable the EZComm protocol, click **Edit Configurations**.
  - b. On the EZComm Configurations page, **Transport** tab, click **Add Outbound Transport**.
  - c. On the **Add Transport** dialog, select or enter data as explained in the following table:

Field	Description
<b>Transport Name</b>	Enter the name for the transport.
<b>Transport Type</b>	Select the transport type from the <b>Transport Type</b> list. For this tutorial, select <b>HTTP</b> .
<b>URL</b>	Enter the URL of the company: http://<host_address>:<gs_port>/dmz/EZComm.
<b>Use HTTP Basic Authentication</b>	(Optional) Select the <b>Use HTTP Basic Authentication</b> checkbox.

Field	Description
User name	No entry is required for this tutorial.
Password	No entry is required for this tutorial.
Retry Count	Use the default value: 3
Retry Interval	Use the default value: 60
Socket Timeout (seconds)	Use the default value: 300

d. Click **Add**.

6. Click **Save**; then click **Done** to complete the configuration process.

## Result

For the Initiator Partner **Seller**:

- Enabled the EZComm protocol
- Added the **HTTP** transport

## What to do next

[Configuring the Initiator Business Agreement](#)

# Configuring the Initiator Business Agreement

Perform the following steps to configure the initiator business agreement:


## Before you begin

Configure both the trading partners.

## Procedure

1. On the Partner Management tile, click **Business Agreements**.
2. On the Business Agreements page, click **Create Agreement** in the upper-right corner

of the page.

3. Select **Buyer** from the list in the **Host** field.
4. Select **Seller** from the list in the **Partner** field.
5. Click **Proceed**.
6. Enable the **Active**  toggle on the **Validity** tab to validate the agreement.

**i** **Note:** The **Active**  toggle is enabled by default.

## Result

Created a valid business agreement between host **Buyer** and partner **Seller**.

## What to do next

[Configuring the Responder BusinessConnect Container Edition](#)

# Configuring the Responder BusinessConnect Container Edition

This section describes about configuring the Responder BusinessConnect Container Edition on another machine, where your previous host is the partner, and the previous partner is now the host.

Perform the steps described in the following sections to configure the Responder BusinessConnect Container Edition machine:

**i** **Note:** The following sections contain only the steps necessary for this tutorial.

- [Configuring the Responder Default Host](#)
- [Configuring the Responder Partner](#)
- [Configuring the Responder Business Agreement](#)

## Configuring the Responder Default Host

Perform the following steps to configure the default responder host:

### Procedure

1. On the Partner Management tile, click **Hosts**.
2. On the Hosts page, click **Create Host** in the upper-right corner of the page.
3. Enter **Seller** in the **Host Name** field and click **Proceed**.

**i Note:** For this tutorial, you do not need to edit additional settings to configure the protocol.

4. Select the **Make this as Default Host** checkbox to set the **Seller** as default host.
5. Click **Done**.

### Result

A host **Seller** is created and set as the default host.

### What to do next

[Configuring the Responder Partner](#)

## Configuring the Responder Partner

Perform the following steps to configure the responder partner:

### Procedure

1. On the Partner Management tile, click **Partners**.
2. On the Partners page, click **Create Partner** in the upper-right corner of the page.
3. Enter **Buyer** in the **Partner Name** field and click **Proceed**.
4. On the **Protocol** tab, select the **EZComm** checkbox to enable the EZComm protocol for the Responder Partner.
5. Add a transport for the Responder Partner:

- a. After you enable the EZComm protocol, click **Edit Configurations**.
- b. On the EZComm Configurations page, click **Add Outbound Transport**.
- c. On the **Add Transport** dialog, enter data as explained in the following table.

Field	Description
<b>Transport Name</b>	Enter the name for the transport.
<b>Transport Type</b>	Select the transport type from the <b>Transport Type</b> list. For this tutorial, select <b>HTTP</b> .
<b>URL</b>	Enter the URL of the company: http://<host_address>:<gs_port>/dmz/EZComm.
<b>Use HTTP Basic Authentication</b>	Select the <b>Use HTTP Basic Authentication</b> checkbox
<b>User name</b>	No entry is required for this tutorial.
<b>Password</b>	No entry is required for this tutorial.
<b>Retry Count</b>	Use the default value: 3.
<b>Retry Interval</b>	Use the default value: 60.
<b>Socket Timeout</b> (seconds)	Use the default value: 300.

- d. Click **Add**.

6. Click **Save**; then click **Done** to complete the configuration process.

## Result

For the Responder Partner **Buyer**:

- Enabled the EZComm protocol
- Added the **HTTP** transport



## What to do next

[Configuring the Responder Business Agreement](#)


# Configuring the Responder Business Agreement

Perform the following steps to configure the responder business agreement:

## Before you begin

Configure both the trading partners before configuring a business agreement.

## Procedure

1. On the Partner Management tile, click **Business Agreements**.
2. On the Business Agreements page, click **Create Agreement** in the upper-right corner of the page.
3. Select **Seller** from the list in the **Host** field.
4. Select **Buyer** from the list in the **Partner** field.
5. Click **Proceed**.
6. Enable the **Active**  toggle on the **Validity** tab to validate the agreement.

**i** **Note:** The **Active**  toggle is enabled by default.

## Result

Created a valid business agreement between host **Seller** and partner **Buyer**.

## What to do next

[Configuring Private Processes](#)

# Configuring Private Processes

This section describes how to configure the private processes on the Initiator and Responder machines.

# Configuring Private Processes in TIBCO Business Studio

## Before you begin

Install TIBCO ActiveMatrix BusinessWorks™ Plug-in for BusinessConnect™ in TIBCO Business Studio.

**i Note:** For more information about installing BusinessConnect Palette or ActiveMatrix BusinessWorks™ Plug-in in for BusinessConnect, see *TIBCO BusinessConnect™ Palette Installation* or *TIBCO ActiveMatrix BusinessWorks™ Plug-in for BusinessConnect™ Installation*.

Perform the steps described in the following sections to configure the private process in TIBCO Business Studio:

- [Task A: Opening the BusinessWorks Project](#)
- [Task B: Configuring Connections to Initiator BusinessConnect](#)
- [Task C: Configuring Connections to Responder BusinessConnect](#)

## Task A: Opening the BusinessWorks Project

Perform the following steps to open the TIBCO ActiveMatrix BusinessWorks™ project in TIBCO Business Studio:

### Procedure

1. Start TIBCO Business Studio.
2. Click **File > Import**.
3. On the Import page, expand the **General** folder and select the **Existing Studio Projects into Workspace** item. Click **Next**.
4. Click **Browse** next to the **Select archive file** field and navigate to the `ezcomm_for_bw6.zip` file. Click **Finish**.

**i Note:** The sample project is in the `bcce-ezcomm-<version>/samples/tutorial` directory.

## What to do next

Perform the following steps after importing the sample project:

1. Expand **Module Descriptors** in the Project Explorer view.
2. Double-click **Module Properties**.

## Result

The **Module Properties** editor is displayed according to your configurations.

# Task B: Configuring Connections to Initiator BusinessConnect

Perform the following steps to configure connections to BusinessConnect on the Initiator machine:

## Procedure

1. In the Project Explorer view, go to **Resources > ezcomm\_demo > INITIATOR.bcResource**.
2. On the **Server Access** tab, select or enter the following information:

Field	Description
<b>JDBC Driver Type</b>	Select the JDBC driver that you want to use to communicate with the BusinessConnect configuration store from the <b>JDBC Driver Type</b> list.
<b>JDBC Driver</b>	Select the JDBC driver to use with the database.
<b>JDBC URL</b>	Enter the URL for the configuration store.
<b>DB User</b>	Provide a valid username for the database.
<b>DB Password</b>	Enter the password associated with the database username.

3. Click **Apply**.
4. Click **Update from Configuration Store** on the **Configuration** tab.
5. Select **EZComm** from the **Protocol Name** list.

**i** **Note:** If you select the **Select Operations** checkbox, you could select any of the configured or imported operations. For this tutorial, select all operations and click **OK**.

6. Click **Import Selected Business Protocol**.
7. Click **Save**.

### What to do next

[Task C: Configuring Connections to Responder BusinessConnect](#)

## Task C: Configuring Connections to Responder BusinessConnect

On the Responder machine, perform all the steps described in [Task B: Configuring Connections to Initiator BusinessConnect](#) by replacing all instances of Initiator with Responder.

### What to do next

[Running the Tutorial](#)

## Running the Tutorial

To see the complete tutorial for Asynchronous Request Response Operation, run it on both the machines **Buyer** and **Seller**.

**i** **Note:** You can also run the Synchronous Request Response and Notify transactions using the processes in this tutorial.

## Running the Tutorial on the Seller Machine

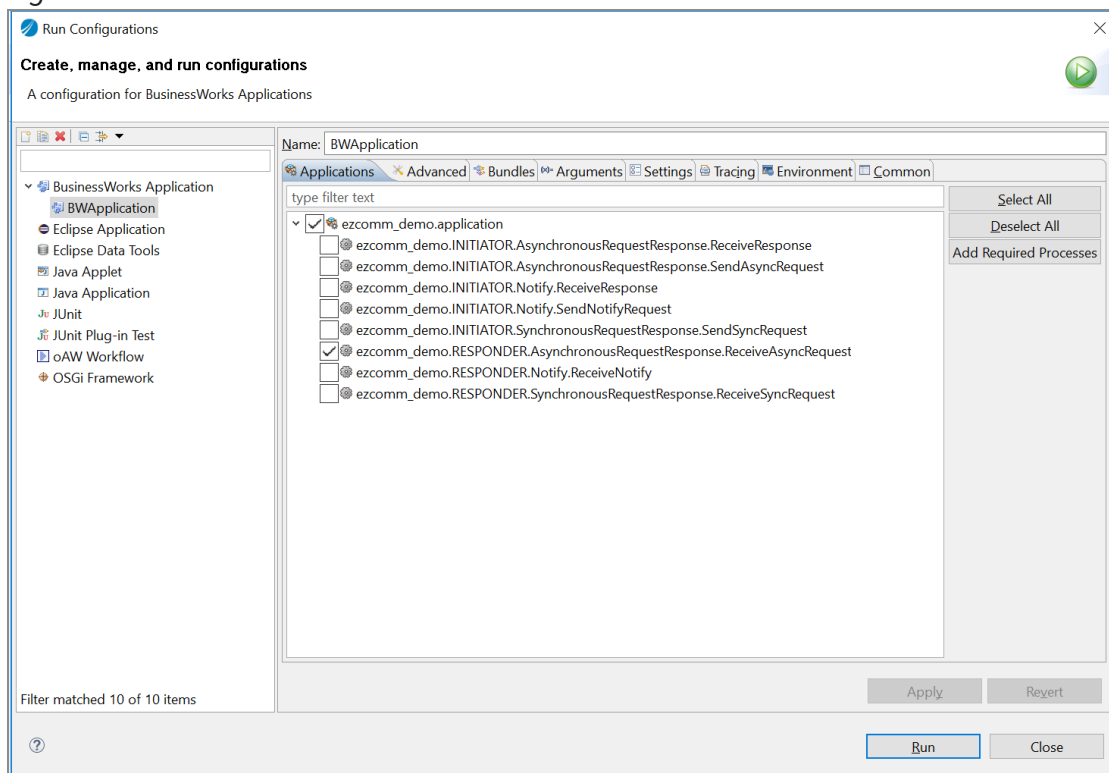
Perform the following steps to run the tutorial on the seller machine:

### Procedure

1. In TIBCO Business Studio, expand the **RESPONDER** folder.
2. Click **Asynchronous Request Response > Receive Async Request**.
3. Go to **Read File > Input Tab > ReadActivityInput** and verify that the path given in the **fileName** field is valid.
4. Click **Run Configurations**.
5. Click **Start testing viewed process**.

The Select Process to Load page is displayed.

*Figure 1: Select Process to Load*



6. Select the **Receive Async Request(current)** checkbox.

#### 7. Click **Load Selected**.

After the request is received from the **Buyer** machine, this process receives the RESPONDER.REQUEST message and then sends the RESPONDER.RESPONSE message to BusinessConnect Container Edition.

## Running the Tutorial on the Buyer Machine

Perform the following steps to run the tutorial on the buyer machine:

### Procedure

1. In TIBCO Business Studio, click **INITIATOR > Asynchronous Request Response**.
2. Click **Send ASync Request process**.
3. Click **SendRequest activity**.
4. Enter Buyer in the **fromTP** field and Seller in the **toTP** field on the **Input** tab.

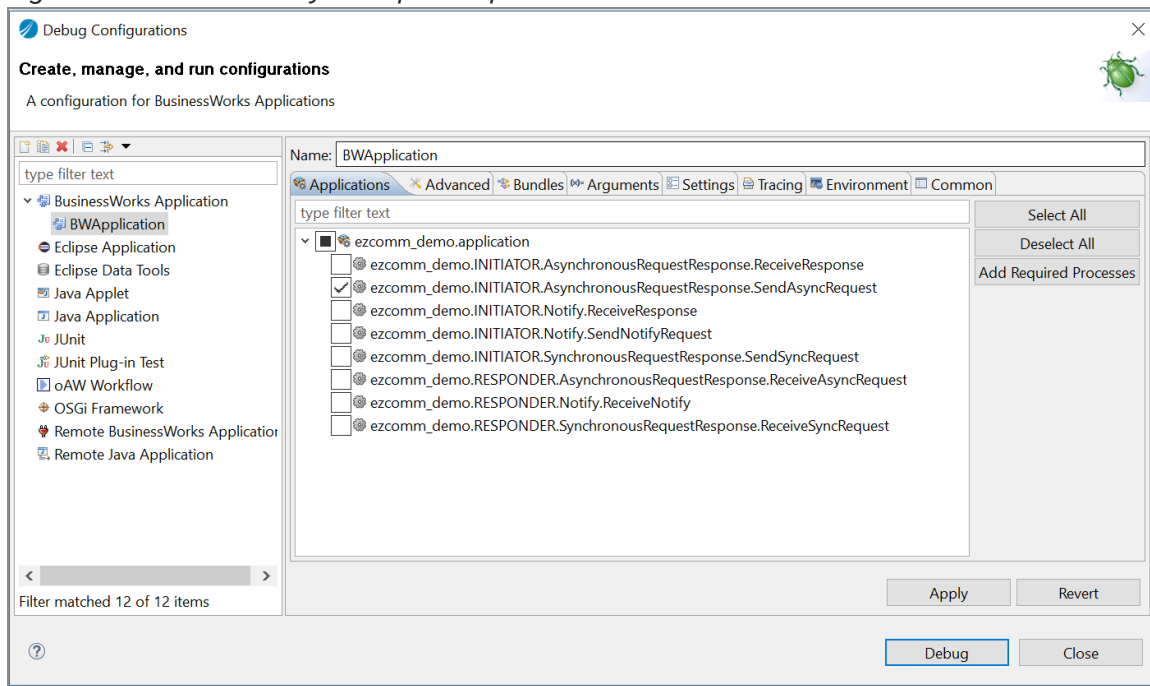
Figure 2: SendRequest (Input)

The screenshot displays the configuration for the **SendRequest** activity. The top diagram shows a sequence of activities: **Timer**, **ReadFile**, **ParseXml**, and **SendRequest**. The bottom pane, titled **SendRequest (SendRequest)**, has the **Input** tab selected. It shows two main sections: **Data Source** and **XPath Expression**.

Data Source	Functions	Constants	XPath Expression
> \$processContext			SendRequest-input
\$BC_EXAMPLE_PATH			SendRequestInput
\$BC_HOME_DIR			BCInitiatorReques
\$BC_VERSION			fromTp?
\$Timer			toTp "Company1"
\$ReadFile			transactionID "101"
\$ParseXml			closure?
			attachment
			binaryRequest?
			as2-subject?

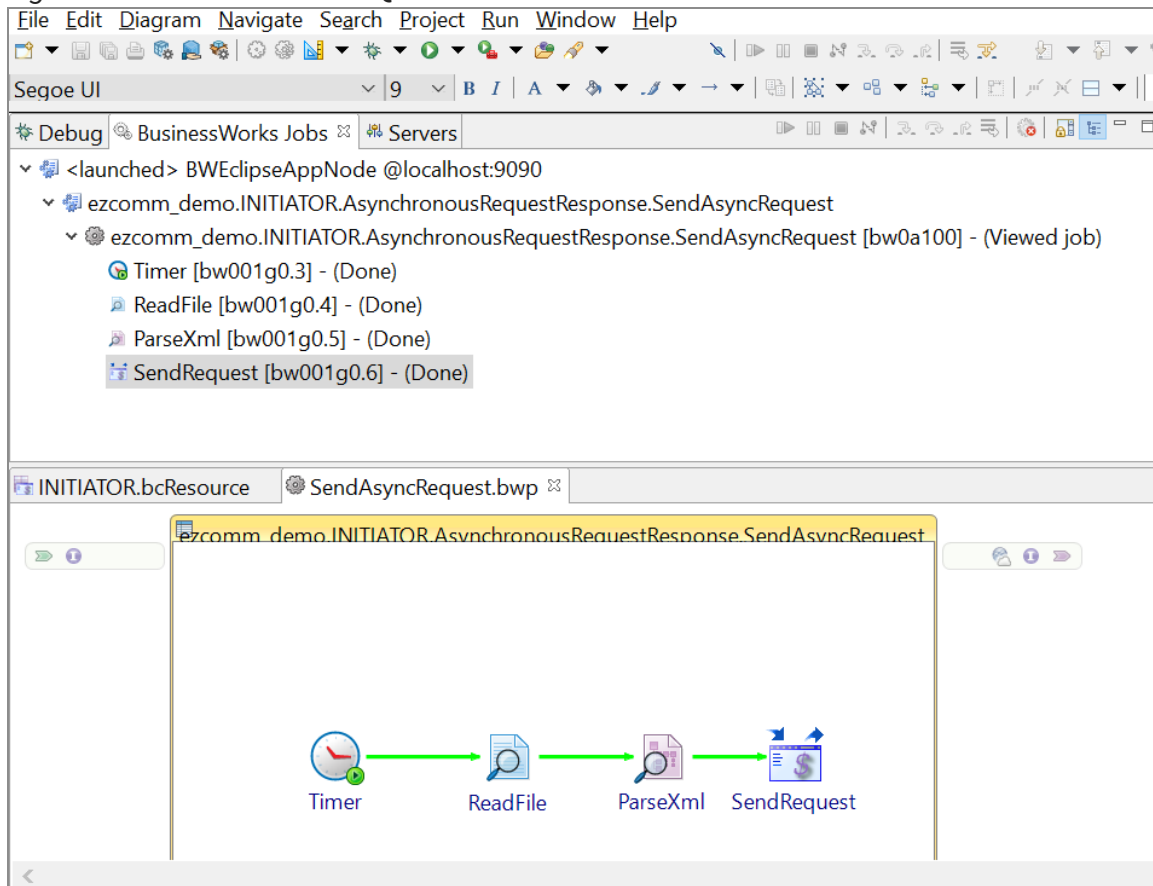
5. Go to **Read File > Input Tab > ReadActivityInput** and verify that the path given in the **fileName** field is valid.
6. Click **Apply** and **Save**.
7. Click **Run Configurations**.
8. Select two processes:
  - a. INITIATOR/Asynchronous Request Response/Send Async Request
  - b. INITIATOR/Asynchronous Request Response/Receive Response processes
9. Click **Load selected**.

Figure 3: Select SendAsyncRequest Operation



It sends an INITIATOR.REQUEST to the INITIATOR BusinessConnect Container Edition. At the same time, the Receive Response activity receives the INITIATOR.RESPONSE message.



*Figure 4: Send INITIATOR.REQUEST and Receive INITIATOR.RESPONSE*

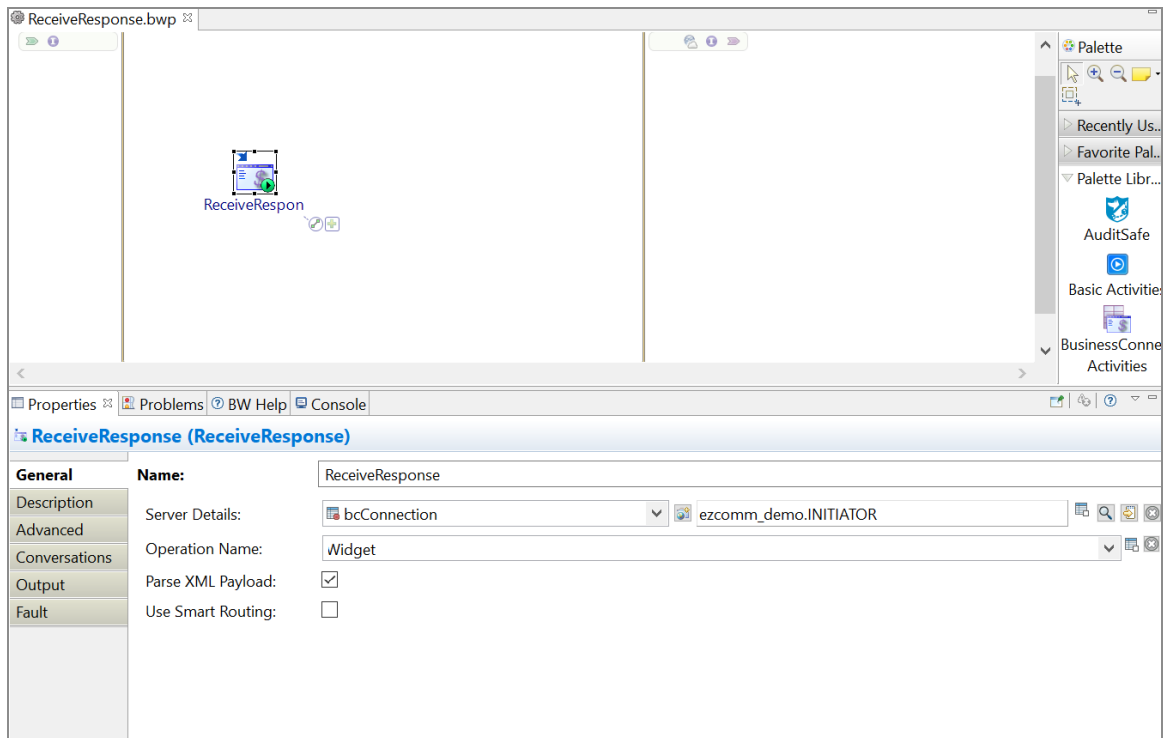
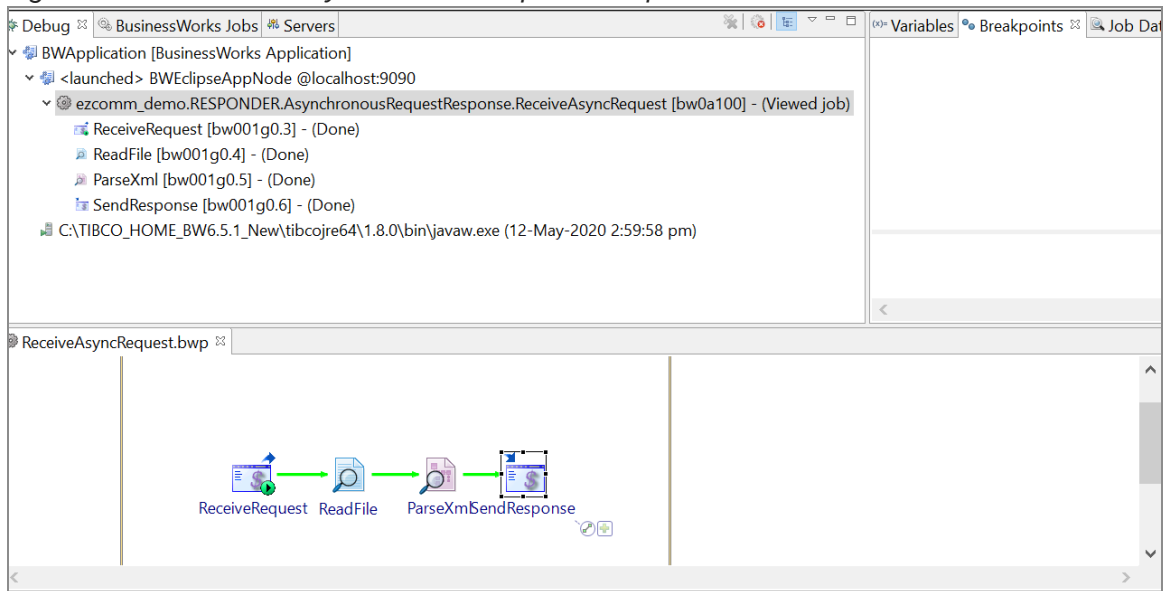


Figure 5: RESPONDER AsynchronousRequestResponse Process



# BusinessConnect Container Edition – Services Plug-in URIs

---

This section describes about the BusinessConnect Container Edition – Services Plug-in Uniform Resource Identifiers (URIs).

## Exchanging URIs

To transact e-commerce, trading partners must exchange URIs as part of the business agreement.

For BusinessConnect Container Edition – Services Plug-in, the URI, the subject, and the headers can encode information such as the from trading partner, to trading partner, and the operation ID of the transaction. For an outgoing HTTP message, BusinessConnect Container Edition always populates these values in the HTTP URL. However, for an incoming HTTP message it can interpret these values from the HTTP header or the HTTP URL, in that order.



**Note:** BusinessConnect Container Edition – Services Plug-in populates trading partner and operation information in the outgoing URI only if the URI ends with /EZComm.

Additional information in the URI, such as **toTP** and **fromTP**, is available only for transports other than AS1, AS2, and EMAIL, since the same information is derived from the internet headers such as AS2 TO or FROM ID and the EMAIL FROM or TO address. Such information becomes redundant and ambiguous if provided in the URI.

The following sections describe the available transports and their URI formats.

- [Email Transport](#)
- [File Transport](#)
- [FTP Transport](#)
- [HTTP/S Transport](#)

# Email Transport

URI format: <mailto://username@domain>

Example: <mailto://john@acme.com>

When using Email transport, you have the option of specifying the mail subject. If the subject contains the string `operationID="category/version_number/operation_name"` then OperationID is taken as the operation ID for that transaction.

If the operation ID is not specified in the subject, then the value is what is sent by the private process.

# File Transport

URI format: `file://BaseDir/*.*`

This causes all the directories under `BaseDir` to be checked for the files. For the files to be handled by BusinessConnect Container Edition – Services Plug-in, include the following information:

- Default behavior for the operation `BC/version/Notify`:

*BaseDir/EZComm/TpName*

- Non-default behavior for other operations:

*BaseDir/EZComm/TpName/Category\_version\_OperationID*

Where *BaseDir* is a base directory selected by the user, *TpName* is the name of the trading partner, *Category* is the operation category, *version* is the operation version, and *OperationID* is the operation ID.

If *OperationID* is not provided, then it defaults to `BC/version/Notify`.

You must provide a file mask (`*.*`) to ensure that the file is picked up by File transport.



**Note:** For more information about specifying the file mask field in File transport, see the "Outbound File Transport" topic in *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.

# FTP Transport

URI format: <ftp://server:port/dir>

Where *dir* is a directory and it can be anything or absent.

**Note:**

- For more information about specifying the file mask field in the FTP transport, see the "Outbound File Transport" topic in *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.
- With BusinessConnect Container Edition – Services Plug-in, the FTP inbound transactions always default to the BC/version/Notify operation.

## HTTP/S Transport

### URI for the HTTP Transport

URI format: <http://server:port/dmz/EZComm>

Example: <http://www.gizmo.com:555/dmz/EZComm>

For HTTP transport, the partner name, host name, and operation ID can be specified as parameters in the request URI or as transport headers.

The expected parameters or headers for BusinessConnect Container Edition – Services Plug-in are as follows:

- **fromTp**: This is a required field for the incoming message.
- **toTp**: If this parameter is missing, it is set to the default host.
- **operationID**: If this parameter is missing, the default is set to BC/version\_number/Notify.
- **fileName**: If you specify the parameters in the URI, the format is:  
<http://host:port/dmz/>

[EZComm?fromTp=fromTP&toTp=toTP&operationID=opID&fileName=fileName](#)

**i Note:** The `fileName` feature is not supported for the AS2-HTTP transport.

## URI for the HTTPS Transport

URI format: [https://server:port/dmz/EZComm](#)

Example: [https://www.gizmo.com:555/dmz/EZComm](#)

**i Note:** BusinessConnect 6.x still supports the older BusinessConnect 5.x URI format ([Configuring Private Processes](#) or [Configuring Private Processes](#)) for backward compatibility, but is deprecated starting with the BusinessConnect 6.0 release.

## Populating URIs

**i Note:** The AS2 specification does not support custom headers.

Ensure that the following parameters are followed for populating URIs:

- On the outbound side, URI fields have precedence over the headers.
- On the inbound side, if values are specified in headers and URI places, the transport headers take precedence over the request URI values.

# Managing BusinessConnect Container Edition – Services Plug-in Operations

---

This section describes how to manage the BusinessConnect Container Edition – Services Plug-in operations.

The exchange of business documents is known as the process flow. In any BusinessConnect Container Edition process flow, two types of messages are exchanged:

- Public messages or operations
- Private messages. See [Private Messages](#).

## BusinessConnect Container Edition – Services Plug-in Operations

Public messages are exchanged over the internet between BusinessConnect Container Edition and another B2B installation. The following message types are supported in BusinessConnect Container Edition – Services Plug-in:

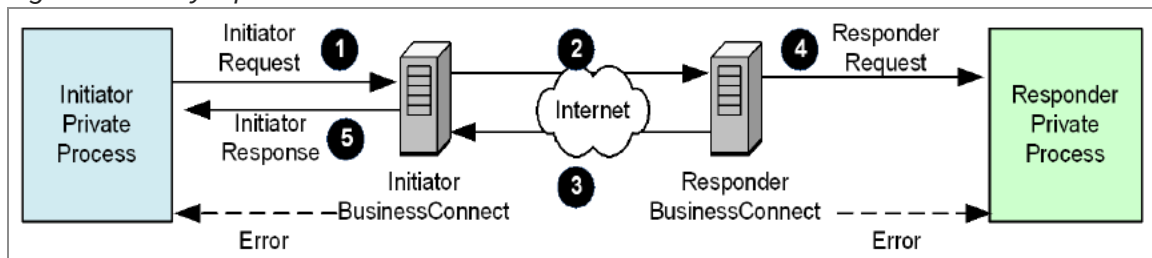
- [Notify Operation](#)
- [Synchronous Request Response Operation](#)
- [Asynchronous Request Response Operation](#)

### Notify Operation

Notify is a one-way operation that sends a document to the trading partner and receives an acknowledgment. It does not receive a response from the trading partner.

The flow of a Notify Operation is shown in the following figure.

Figure 6: Notify Operation



The following process flow occurs with the Notify Operation:

1. The Initiator private process sends a message to the Initiator BusinessConnect Container Edition.
2. The Initiator BusinessConnect Container Edition retrieves relevant information and sends the message to the Responder BusinessConnect Container Edition.
3. The Responder BusinessConnect Container Edition immediately sends a transport response (acknowledgment) to the Initiator BusinessConnect Container Edition on the same channel as the Initiator business request.
4. The Responder BusinessConnect Container Edition then forwards the message to the local private process.

See [Responder Messages](#). The Responder BusinessConnect Container Edition considers the operation as complete.

5. The Initiator BusinessConnect Container Edition sends an INITIATOR.RESPONSE message to the private process.

See [Initiator Inbound Response—BusinessConnect to Private Process](#). This message is sent independently from the Responder BusinessConnect Container Edition, which sends a RESPONDER.REQUEST message to the Responder private process.

Supported transports are: HTTP, HTTPS, HTTPSCA, File, FTP, FTPS, SSHFTP, Email, AS1, and AS2.

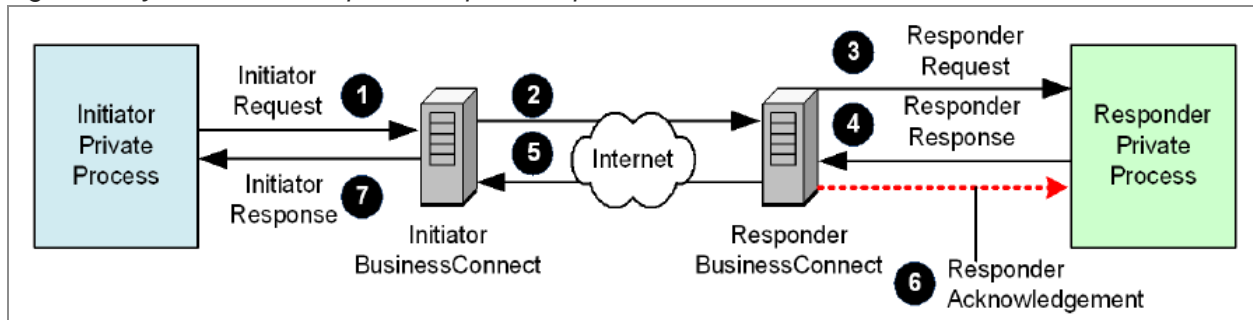
## Synchronous Request Response Operation

The Synchronous Request Response Operation sends a document to the trading partner and wait for a response. It waits until the response is received and suspends any further processing for that request. This operation is used to send documents to trading partners and require a response for further processing.



The flow of operation is shown in the following figure.

Figure 7: Synchronous Request-Response Operation



The following process flow occurs with the Synchronous Request-Response Operation:

1. The Initiator private process sends the request to the Initiator.
2. The Initiator sends the request to the Responder and waits for the response until the timeout specified in the appropriate transport has expired.
3. The Responder BusinessConnect Container Edition sends the request to the Responder private process.
4. The Responder private process sends a response. If the private process does not respond on time, the Responder BusinessConnect Container Edition times out and ends the transaction. If the response from the private process arrives after this time out, the message is rejected and an error occurs.
5. The response is forwarded to the Initiator BusinessConnect Container Edition.
6. The Responder acknowledgment is sent to the private process indicating whether the response has been forwarded to the trading partner. It does not indicate whether the trading partner has received it or not.
7. On receiving the response from the Responder, the Initiator sends the Initiator Response message. If the Initiator times out, an audit log entry is generated, a timeout error advisory is sent, and the connection is closed.

**i Note:** Resending of Responder.Request and Responder.Response for the Synchronous Request Response operation is not supported for BusinessConnect Container Edition – Services Plug-in.

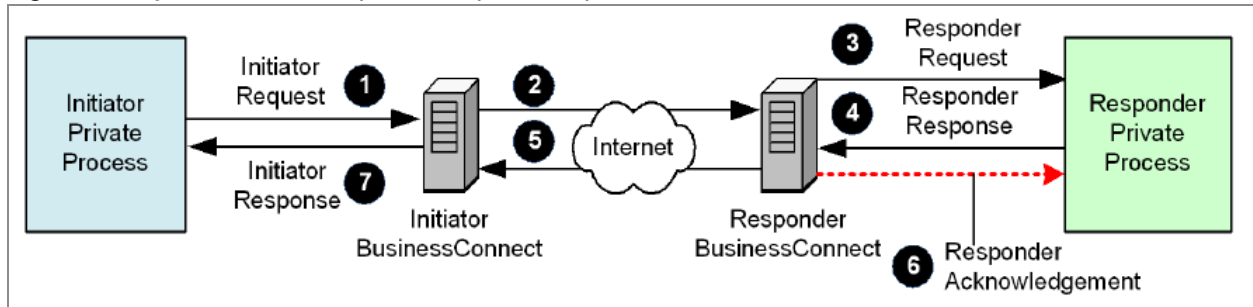
Supported transports are: HTTP, HTTPS, and HTTPSCA.

## Asynchronous Request Response Operation

The Asynchronous Request Response Operation sends a document to the trading partner and wait for a response. It allows further processing, irrespective of the arrival of the response from the partner.

The flow of operation is shown in the following figure.

Figure 8: Asynchronous Request Response Operation



The following process flow occurs with the Asynchronous Request Response Operation:

1. The Initiator private process sends a request to the Initiator BusinessConnect Container Edition.
2. The Initiator BusinessConnect Container Edition sends the request to the Responder and waits for the response until the timeout specified in the operation has expired.
3. The Responder BusinessConnect Container Edition sends a request to the Responder private process.
4. The Responder private process sends the response. If the private process does not respond on time, the Responder BusinessConnect Container Edition would time out and end the transaction.

If the response from the Responder private process arrives after the timeout, the message is rejected, and an error advisory is sent.

5. If the response from the Responder private process is received on time, the response is forwarded to the Initiator BusinessConnect Container Edition.
6. A Responder acknowledgment is sent to the Responder private process indicating whether the response has been forwarded to the trading partner.
7. After receiving the response from the Responder, the Initiator sends the Initiator Response message.

If the Initiator BusinessConnect Container Edition times out, an audit log entry is

generated and a timeout error advisory is sent out. In this case, the request is canceled. When the response arrives at a later time, no corresponding request is present, the advisory is rejected, an error advisory is published, and an internal system error is sent to the partner.

**i Note:** Resending of Responder .Response is supported for the Asynchronous Request Response operation.

Supported transports are: HTTP, HTTPS, HTTPSCA, AS2\_HTTP, AS2\_HTTPS, Email, and AS1\_EMAIL.

## Schema Validation in BusinessConnect Container Edition – Services Plug-in

Schema validation in BusinessConnect Container Edition – Services Plug-in is performed based on the following criteria:

- Schema type: XSD or DTD
- Direction of messages
- Whether the validation is done for a request or for a response

## Caching of Schemas

The referenced schema is updated in the validator cache during run time validation, in the same way as it would be saved through the GUI.

When a schema is used by reference, you do not observe any schema changes in the referenced object, but you could see the change on the reference instead. This means that the BusinessConnect Container Edition configuration store does not scan the referenced object each time the validation occurs, but it instead indicates if there is a change in the uploaded file object. You need to update the reference in the GUI — resave the schema reference—and the new referenced object is updated in the cache.

# Duplicate Message Detection

With BusinessConnect Container Edition – Services Plug-in, you can verify both incoming and outgoing public messages for duplicates. A message is determined to be a duplicate based on certain message field values such as `transactionID`, `operationID`, and so on.


For each message, a message digest from the predetermined fields is created and stored in a table. If any subsequent message has the same message digest, it is considered to be a duplicate message. If requested by the user, all incoming requests are checked for duplicates.

Both the inbound and outbound requests for a trading partner can be configured for the duplicate message detection.

If the duplicate detection for the outbound messages is enabled, all the incoming private process messages are checked for duplicates. If a request is found to be a duplicate, the transaction is ended and an error advisory is sent to the private process.


For the inbound requests, the private process is notified by setting the duplicate field as true, while it is up to the private process to take further action.

## Outbound Duplicate Detection Criteria

 **Note:** For asynchronous and synchronous responses, outbound duplicate detection is not supported (only inbound duplicate detection is supported).

The following fields from the private process are used to calculate the message digest for duplicate detection for outbound requests:

- `TransactionID` received from the user

 **Note:** When the outbound File Poller initiates a transaction, the `transactionID` element is used for calculating the message digest.

- Payload: `plainRequest`, `binaryRequest`, `inputFileName` (file content)
- Trading partner host name
- Operation ID

- Host name

## Inbound Duplicate Detection Criteria

**i Note:** For asynchronous and synchronous responses, only inbound duplicate detection is supported.

The following values from the incoming request are used to calculate the message digest for detection of duplicates for inbound requests:

- Payload
- Trading partner name
- Operation ID

## Configuring BusinessConnect Container Edition – Services Plug-in Operations

Perform the following steps to configure the BusinessConnect Container Edition – Services Plug-in operations:

### Procedure


1. On the B2B Administration tile, click **Operations Editor**.
2. Click the **EZComm** protocol.
3. Create a category, see [Adding a New Category](#).
4. Create a version to the category, see [Adding a New Version](#).
5. Create an operation to the version, see [Adding a New Operation](#).

## Adding a New Category

Category is used to group operations based on their type.

Perform the following steps to add a new category:

### Procedure


1. Click the **EZComm** link.  
The Operations Editor | EZComm page is displayed.
2. Click the **Add** icon  to create a new category.
3. Enter the following information in the **New Category** dialog:
  - (Required) In the **Name** field, enter the category name.
  - (Optional) In the **Description** field, enter the description for the category.
4. Click **Add**.

## Adding a New Version

Use versions for various subgroups of operations, such as `Notify only`, or `Notify and Synchronous Request Response`, and so on.

Perform the following steps to add a new version of a category:

### Procedure


1. Hover the mouse pointer over a category, click **Menu** , and select the **New Version**.
2. Enter the following information in the **New Version** dialog:
  - (Required) In the **Name** field, enter the version name.
  - (Optional) In the **Description** field, enter the description for the version.
3. Click **Add**.

## Adding a New Operation

Operations are added to a specific version. Each version can contain the same or different operation sets.

Perform the following steps to add a new operation:

## Procedure

1. Move the mouse pointer over version, click **Menu**  and select an operation from the list.
2. To configure the selected operation, perform the steps described in the following sections:
  - [Configuring New Notify Operation](#)
  - [Configuring Synchronous/Asynchronous Request-Response Operation](#)
3. Click **Add**.

## Configuring New Notify Operation

To configure the New Notify Operation, select or enter the details on the following tabs:

### Notify Operation Tab

Field	Description
<b>Name</b>	Name of the operation.
<b>Description</b>	(Optional) Brief description of the operation.
<b>Inbound</b>	
<b>Validate Message</b>	When selected, all the inbound messages (either request or response) are validated. Select the checkbox in the following cases: <ul style="list-style-type: none"><li>• If the Initiator needs a response from the Partner to be validated.</li><li>• If the Responder needs the request to be validated.</li></ul>
<b>Outbound</b>	
<b>Validate Message</b>	When selected, all the outbound messages (either request or response) are validated. Select the checkbox in the following cases: <ul style="list-style-type: none"><li>• If the Initiator needs a request to the Partner to be validated.</li><li>• If the Responder needs the response to be validated.</li></ul>

## Notify Request Action Tab

Field	Description
<b>Name</b>	Name of the request action.
<b>Description</b>	(Optional) Brief description of the request action.
<b>Direction</b>	(Pre-defined) Initiator to Responder.
<b>Validation Schema Name</b>	<p>Click <b>Upload file</b> and select the schema file in the BC_HOME\protocols\ezcomm\samples\sampleXML\xsd directory.</p> <div> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Services Plug-in supports XSD and DTD schema validation. For tutorial, the XSD validation is used.</li> <li>The file uploaded should match the validation type selected in the <b>XML Document Validation</b> field.</li> </ul> </div>
<b>Require Digital Signature</b>	Used for both HTTP and HTTPS transports. If selected, this option signs the outgoing messages and forces the incoming messages to be signed.
<b>Require Content Encryption</b>	Used for both HTTP and HTTPS transports. If selected, this option encrypts the outgoing messages and forces the incoming messages to be encrypted.
<b>For BC Palette use only</b>	
<b>XML Document Validation</b>	Select <b>XSD</b> or <b>DTD</b> from the <b>XML Document Validation</b> list.
<b>Root XML Element Name</b>	Root XML element name, which is the top-level XML element in the document.



## Configuring Synchronous/Asynchronous Request-Response Operation

These two operations are configured in a similar way, with small differences that are pointed out in the instructions.

To configure the Synchronous or Asynchronous Request-Response Operation, select or enter the details on the following tabs:

### Synchronous or Asynchronous Request-Response Operation Tab

Field	Description
<b>Name</b>	Name of the operation.
<b>Description</b>	(Optional) Brief description of the operation.
<b>Inbound</b>	
<b>Validate Message</b>	<p>When selected, all the inbound messages (either request or response) are validated. Select the checkbox in the following cases:</p> <ul style="list-style-type: none"> <li>• If the Initiator needs a response from the Partner to be validated.</li> <li>• If the Responder needs the request to be validated.</li> </ul>
<b>Outbound</b>	
<b>Validate Message</b>	<p>When selected, all the outbound messages (either request or response) are validated. Select the checkbox in the following cases:</p> <ul style="list-style-type: none"> <li>• If the Initiator needs a request to the Partner to be validated.</li> <li>• If the Responder needs the response to be validated.</li> </ul>

## Request Action Tab

Field	Description
<b>Name</b>	Name of the request action.
<b>Description</b>	(Optional) Brief description for the request action.
<b>Direction</b>	(Pre-defined) Initiator to Responder.
<b>Validation Schema Name</b>	<p>Click <b>Upload file</b> and select the schema file in the BC_HOME\protocols\ezcomm\samples\sampleXML\xsd directory.</p> <div> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Services Plug-in supports XSD and DTD schema validation. For tutorial, the XSD validation is used.</li> <li>The file uploaded should match the validation type selected in the <b>XML Document Validation</b> field.</li> </ul> </div>
<b>Require Digital Signature</b>	Used for both HTTP and HTTPS transports. If selected, this option signs the outgoing messages and forces the incoming messages to be signed.
<b>Require Content Encryption</b>	Used for both HTTP and HTTPS transports. If selected, this option encrypts the outgoing messages and forces the incoming messages to be encrypted.
<b>Wait time for Response (seconds)</b>	<p>This field is available only for the asynchronous Request-Response operation.</p> <p>The default value is set to 3600 seconds.</p>
<b>For BC Palette use only</b>	
<b>XML Document Validation</b>	Select <b>XSD</b> or <b>DTD</b> from the <b>XML Document Validation</b> list.
<b>Root XML Element Name</b>	Root XML element name, which is the top-level XML element in the document.

## Response Action Tab

Field	Description
<b>Name</b>	Name of the response action.
<b>Description</b>	(Optional) Brief description of the response action.
<b>Direction</b>	(Pre-defined) Responder to Initiator.
<b>Validation Schema Name</b>	Click <b>Upload file</b> and select the schema file in the BC_HOME\protocols\ezcomm\samples\sampleXML\xsd directory. <div> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Services Plug-in supports XSD and DTD schema validation. For tutorial, the XSD validation is used.</li> <li>The file uploaded should match the validation type selected in the <b>XML Document Validation</b> field.</li> </ul> </div>
<b>Require Digital Signature</b>	Used for both HTTP and HTTPS transports. If selected, this option signs the outgoing messages and forces the incoming messages to be signed.
<b>Require Content Encryption</b>	Used for both HTTP and HTTPS transports. If selected, this option encrypts the outgoing messages and forces the incoming messages to be encrypted.
<b>Private Process Wait (seconds)</b>	Specifies the amount of time that the Responder waits for the response from the private process. The default value is set to 3600 seconds.
<b>For BC Palette use only</b>	
<b>XML Document Validation</b>	Select <b>XSD</b> or <b>DTD</b> from the <b>XML Document Validation</b> list.
<b>Root XML Element Name</b>	Root XML element name, which is the top-level XML element in the document.

# Setting Up Trading Hosts and Partners

---

The following sections describe how to set up trading hosts and partners in BusinessConnect Container Edition for BusinessConnect Container Edition – Services Plug-in.

- [Configuring BusinessConnect Container Edition – Services Plug-in for a Host](#)
- [Configuring BusinessConnect Container Edition – Services Plug-in for a Partner](#)

For more information about setting up trading host and partner, see *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.

## Configuring BusinessConnect Container Edition – Services Plug-in for a Host

To create a host, see the "Creating a Host" topic in *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.


You can enable or disable the EZComm protocol, or edit its configurations for hosts using the **Protocols** tab.

Perform the following steps to configure the EZComm protocol for a host:

### Procedure

1. On the Hosts page, click the host's name whose EZComm protocol that you want to configure.
2. On the Edit Host page, select the **EZComm** protocol and click **Edit Configurations**.
3. On the **General** tab, select the AS2 identifier from the dropdown list. If no AS2 identifiers are present in the dropdown list, perform the following steps:

**Note:** Select an identifier to use in the AS2-From header field of the HTTP message. This identifier should be mutually agreed on between the trading partners.

- a. To add a new identifier, click the **Add** icon  on the **General** tab.
- b. Select or enter the following details on the **Add New** tab:

Field	Description
Domain Type	Select the domain type from the dropdown list.
ID	Enter an ID for the selected domain name.

- c. Click **Add**.

The list of domains and their respective IDs are displayed on the **Identifiers List** tab. You can search or delete one or more identifiers from the list.

4. On the **General** tab, after you have selected the AS2 identifier from the dropdown list, enter the host's email address in the **Valid Email Address List** field.

**Note:** You can assign multiple email addresses.

5. Click **Save**.

## Assigning Default Host

Perform the following steps to assign a default host:

### Procedure

1. On the Partner Management tile, click **Hosts**.
2. On the Hosts page, click the host name that you want to set as default.
3. Select the **Make this as Default Host** checkbox.
4. Click **Done**.

# Configuring BusinessConnect Container Edition

## – Services Plug-in for a Partner

To create a partner, see the "Creating a Partner" topic in *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.

You can enable or disable the EZComm protocol, or edit its configurations for partners using the **Protocols** tab.

Perform the following steps to configure the EZComm protocol of a partner:


### Procedure

1. On the Partners page, click the partner's name whose EZComm protocol that you want to configure.
2. On the Edit Partner page, select the **EZComm** protocol and click **Edit Configurations**.
3. Select or enter the details on the [General Tab](#) and [Transport Tab](#).
4. Click **Save**.

## General Tab

1. On the **General** tab, select the AS2 identifier from the dropdown list. If no AS2 identifiers are present in the dropdown list, perform the following steps:

**i Note:** Select an identifier to use in the AS2-From header field of the HTTP message. This identifier should be mutually agreed on between the trading partners.

- a. To add a new identifier, click the **Add** icon  on the **General** tab.
- b. Select or enter the following details on the **Add New** tab:

Fields	Description
<b>Domain Type</b>	Select the domain type from the dropdown list.
<b>ID</b>	Enter an ID for the selected domain name.

- c. Click **Add**.

The list of domains and their respective IDs are displayed on the **Identifiers List** tab. You can search, edit, or delete one or more identifiers from the list.


2. On the **General** tab, after you have selected the AS2 identifier from the dropdown list, enter the host's email address in the **Valid Email Address List** field.

 **Note:** You can assign multiple email addresses.

## Transport Tab


You can search, add, configure, and delete the transports for a partner using the **Transport** tab.

1. To search for the transports enter the search string by using the wild card to substitute any characters before, after, or before and after the string that you are entering. The names of one or more transports that correspond to the search criteria are displayed.
2. To create new outbound transports, perform the following steps:
  - a. On the **Transport** tab, click **Add Outbound Transports**.

 **Note:** To add transports to the list of existing transports, click the **add-outline** icon.

- b. Select or enter the following details in the **Add Transport** dialog:

Field	Description
<b>Transport Name</b>	Enter the name of the transport.
<b>Choose Transport Type</b>	Select the type of transport from the dropdown list: FILE, HTTP, HTTPS, FTP, FTPS, SSHFTP, EMAIL, AS1_EMAIL, AS2_HTTP, and AS2_HTTPS

- c. Click **Add**.
3. To delete one or more types of outbound transports, perform the following steps:
  - a. On the **Transport** tab, select one or more transports that you want to delete and click the **Delete** icon .
  - b. Click **OK** when prompted to confirm the deletion of the transports.
4. Click **Save**.



# Configuring Business Agreements

---

The following sections describe how to configure business agreements and protocol bindings for BusinessConnect Container Edition – Services Plug-in.


- [Adding a New Business Agreement](#)
- [Configuring Agreement Protocol Binding for BusinessConnect Container Edition – Services Plug-in](#)

## Adding a New Business Agreement

### Before you begin



Configure both the trading partners before you configure their business agreement.

### Procedure

1. On the Partner Management tile, click **Business Agreements**.
2. On the Business Agreements page, click **Create Agreement** in the upper-right corner of the page.
3. Select a host from the **Host** field.
4. Select a partner from the **Partner** field.
5. Click **Proceed**.
6. Enabled the **Active**  toggle on the **Validity** tab to validate the agreement.

 **Note:** The **Active**  toggle is enabled by default.

To make the agreement valid for a certain time period, do the following:

- Specify the start date in the **Agreement Start on**  field.
- Specify the end date in the **Agreement Ends on**  field.

End date has to be later than the start date.

# Configuring Agreement Protocol Binding for BusinessConnect Container Edition – Services Plug-in

Perform the following steps to configure the BusinessConnect Container Edition – Services Plug-in agreement protocol bindings:

## Procedure

1. On the Edit Business Agreement page, **Bind Protocol** tab, select the **EZComm** checkbox.
2. Click **Edit Configurations**.

Select or enter the information in the following tabs to configure agreement protocol bindings:

- [Operations Tab](#)
- [Document Exchange Tab](#)
- [Transports Tab](#)
- [Override Configuration Tab](#)

## Operations Tab

Use the **Operations** tab to configure the Services Plug-in operations that each participant in a business agreement can initiate and respond to.

## Procedure

1. Select one of the following options on the **Allow All Operations**:

*Edit Protocol Binding: Operations Tab*

Field	Description
<b>Allow All Operations</b>	<p>If the checkbox is selected, you do not need to specify operation bindings that the host or partner can initiate.</p> <p>If the checkbox is cleared, you need to define the specific operation bindings.</p>

2. In the **Initiating Operations** section, click **Add Operations**.
3. Expand the operation tree and select the operation type checkbox.
4. Click **Done**.

## Document Exchange Tab

The **Document Exchange** tab is used to specify security settings for the business transaction that is being exchanged.

1. Configure the **Document Exchange** tab using the information in the following table.

Field	Description
<b>Outbound Document Exchange</b>	
<b>Signing Info Settings</b>	
<b>Signing Key</b>	Select the private key of the host from the list.
<b>Digest Algorithm</b>	Select a hash algorithm from the list: <b>SHA1</b> , <b>SHA256</b> , <b>SHA384</b> , or <b>SHA512</b> .
<b>PGP Signing Private Key</b>	Select the private PGP key of the host from the list.
<b>PGP Hash Algorithm</b>	Select the PGP hash algorithm from the list: <b>SHA1</b> or <b>RIPEMD160</b> .

Field	Description
<b>Encryption Info Settings</b>	
<b>Encryption Certificate</b>	Select the partner's certificate from the list.
<b>Encryption Algorithm</b>	Select an algorithm from the list: <b>DES3</b> , <b>AES-128</b> , <b>AES-192</b> , or <b>AES-256</b> .
<b>PGP Encryption Public Key</b>	Select the partner's PGP public key from the list.
<b>PGP Encryption Algorithm</b>	Select the PGP encryption algorithm from the list: <b>DES3</b> , <b>BLOWFISH</b> , <b>CAST5</b> , <b>AES-128</b> , <b>AES-192</b> , or <b>AES-256</b> .
<b>Inbound Document Exchange</b>	
<b>Signing Info Settings</b>	
<b>Verification Certificate</b>	Select the partner's certificate.
<b>PGP Signing Verification Public Key</b>	Select the partner's certificate.
<b>Encryption Info Settings</b>	
<b>Decryption Key</b>	Select the host's private key.
<b>PGP Decryption Private Key</b>	Select the host's private PGP key.

2. Click **Save**.

# Shadow Credential Usage for BusinessConnect Container Edition – Services Plug-in

## Sending Signed or Encrypted Messages

When sending signed or encrypted messages over HTTP, HTTPS, or HTTPSCA transports, you can use shadow credentials during the overlay and shadow credential period to sign or encrypt these messages.

## Receiving Signed or Encrypted Messages

When receiving signed or encrypted messages from a trading partner over HTTP, HTTPS, or HTTPSCA transports, credentials are picked during the overlay period in the following order:

1. Shadow credential is tried for authentication or decryption.
2. If this fails, the original credential is tried.

For the shadow credential period, only the shadow credential is tried.

## Transports Tab

The **Transports** tab is used to specify transports for a business agreement.

1. Select transports for the business agreement using the information in the following table.

Field	Description
<b>Outbound Transports for Host</b>	
<b>Primary Transport</b>	Select one of the transports that have been configured earlier for the partner participant.
<b>AS2 Async MDN</b>	Select any of the configured transports. The settings from the

Field	Description
<b>Reply Transport</b>	<p>specified AS2 MDN Async Reply Transport field are used for sending async MDN responses back to your trading partner. Configuring the AS2 MDN Async Reply Transport is not necessary unless you would like to specify different values for the following HTTP transmission related settings:</p> <ul style="list-style-type: none"> <li>• Retry Count – Default value: 3.</li> <li>• Retry Interval – Default value: 5 seconds.</li> <li>• Socket Timeout – Default value: 300 seconds.</li> </ul> <p>Any other settings specified in the AS2 MDN Async Reply Transport are ignored. The most common case for which you would specify this transport is when your trading partner is not acknowledging the receipt of your async MDNs within the default socket timeout period.</p>
<b>AS2 Async MDN Remote Server Certificate</b>	<p>The Remote Server Certificate for the AS2 HTTPS transport is an SSL certificate that should be used for encrypting the data sent using HTTPS.</p> <p>This list contains all the certificates that have been configured for the Trading Partner. You can select the one that is configured for SSL encryption.</p> <div> <p><b>Note:</b> The server certificate configuration is only required for Async MDNs via AS2 HTTPS transport.</p> </div>
<b>Client Authentication Identity for FTPS, HTTPSCA</b>	Select the host's private key from the list.
<b>Client Authentication Identity for SSHFTP</b>	Select the host's SSH private key from the list.



Field	Description
<b>Inbound Transports for Partner</b>	
(List of configured partner transports)	Select the appropriate checkboxes to allow certain inbound transports for the partner.

2. Click **Save**.



## Override Configuration Tab

Use this tab to configure additional settings for the host and partner in a business agreement.

1. To override general settings for the host, in the Host Configuration section, select information according to the following table.

Field	Description
<b>Override Settings for the Host</b>	
<b>Override Settings</b>	<p>If you enable the <b>Override Settings</b>  toggle, it overrides the values set on the host level. The AS2 identity selected from the identifier list overrides the default AS2 identity value configured for the host by using the procedure described in the following sections:</p> <ul style="list-style-type: none"> <li>• <i>TIBCO BusinessConnect™ Container Edition Trading Partner Management</i>, Set the Host's AS2 Identifier for a Protocol.</li> <li>• <i>TIBCO BusinessConnect™ Container Edition Trading Partner Management</i>, Disabling Session Cache for HTTPS.</li> </ul> <p>If you disable the <b>Override Settings</b> , the default AS2 identity for the host remains valid.</p>
<b>AS2 Identifier</b>	Select an AS2 identity that is used to override the default AS2 identity.

- To override general settings for the partner, in the Partner Configuration section, select information according to the following table.

Field	Description
<b>Override Settings for the Partner</b>	
<b>Override Settings</b>	<p>If you enable the <b>Override Settings</b>  toggle, this overrides the values set on the partner level. The AS2 identity selected from the AS2 identifier list is used to override the default AS2 identity for the host configured using the procedure described in the following sections:</p> <ul style="list-style-type: none"> <li><i>TIBCO BusinessConnect™ Container Edition Trading Partner Management</i>, Set the Host's AS2 Identifier for a Protocol.</li> <li><i>TIBCO BusinessConnect™ Container Edition Trading Partner Management</i>, Disabling Session Cache for HTTPS.</li> </ul> <p>If you disable the <b>Override Settings</b> , the default AS2 identity for the partner remains valid.</p>
<b>AS2 Identifier</b>	Select an AS2 identity that is used to override the default AS2 identity.
<b>Allow override of filename via HTTP parameter</b>	<p>If this checkbox is selected, and a file reference is being passed from the private process, then the name of the file is passed on to the Responder in an HTTP header called filename.</p> <p>Each partner has this checkbox. If it is selected and there is a <b>fileName</b> field in the HTTP message header or in <code>QueryString</code> (in that order), the message is written to a <code>fileName</code> file. This file is created in the shared directory located under the partner's name directory. The file size is irrelevant in this case.</p> <div> <p><b>Note:</b> This feature is fully supported for the Notify and Asynchronous Request Response operations. For the Synchronous Request Response operations, only request can send the filename to the partner while the partner cannot send the filename on the response: a synchronous response cannot be written to the file that the partner wants.</p> </div>



3. Click **Save**.

# Private Messages

---

This section describes how to configure the private messages for BusinessConnect Container Edition – Services Plug-in.

The exchange of business documents is known as the process flow. In any BusinessConnect Container Edition process flow, two types of messages are exchanged:

- Private messages
- Public messages (see [Managing BusinessConnect Container Edition – Services Plug-in Operations](#))

## About Private Messages

Private messages are exchanged between a private process and the local BusinessConnect Container Edition installation. Private messages can contain a request, response, or notification document. The private process handles conversion from internal to public data and back.

- On the Initiator side, the private process converts internal data to a notification document.
- On the Responder side, the private process receives a request and converts it to an internal company format.

You can generate private messages from TIBCO ActiveMatrix BusinessWorks private processes that use the TIBCO BusinessConnect Palette.

The BusinessConnect Container Edition server has two major roles:

- **Initiator:** This role receives request messages from private processes and transmits the Services Plug-in documents to your trading partners.
- **Responder:** This role receives Services Plug-in documents from trading partners and submits the converted request messages to their private processes.

# Initiator Messages

The following sections describe the messages used for private request and response document exchange in Services Plug-in. The message fields are packaged in the ^data^ control tag as part of the aeRvMsg format.

- [Initiator Outbound Request—Private Process to BusinessConnect](#)
- [Initiator Inbound Response—BusinessConnect to Private Process](#)

For more information, see the "Private Process Configuration" topic in the *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.

## Initiator Outbound Request—Private Process to BusinessConnect

The Initiator private process uses this message to handle outbound requests. Data that is sent is in a string or in binary form.

If both plainRequest and inputFile are passed, the plainRequest node is used.

If both binaryRequest and inputFile are passed, the binaryRequest node is used.

**Subject Name** *prefix.installation.EZComm.INITIATOR.REQUEST*

External example: AX.BC.BC-ACME.EZComm.INITIATOR.REQUEST

*Private Message: InitiatorRequest*

Field	Type	Required	Description
fromTp	String	No	Name of the trading partner initiating the transaction.
toTp	String	Yes	Name of the trading partner receiving the transaction.
transactionID	String	Yes	It is a unique ID for transactions in the Initiator private processes environment. The

Field	Type	Required	Description
			private process creates this ID.
closure	String	No	The private process generates the closure message and sends it to TIBCO BusinessConnect, it is required to return the contents of the closure to the InitiatorResponse to ensure that the private process can match it with the original Initiator.Request.
binaryRequest	base64 Binary	No	Private processes use the binaryRequest field to send binary data to BusinessConnect Container Edition.
as2-subject	String	No	A short string identifying the topic of the AS2 message.  The value in the <b>as2-subject</b> element overrides the value in the <b>MIME Subject</b> field.
content-type	String	No	Content type of the passed data.
content-disposition	String	No	Maps to MIME's content-disposition. This value, if provided, is set in the MIME Internet headers.
inputFile	String	No	If a file reference is being passed to BusinessConnect Container Edition, this field is used.
<b>httpAttributes</b>			
name	String	No	Name of the httpAttribute.  <b>Note:</b> It works only with <b>Request_Response</b> operations.
value	String	No	Value assigned to the httpAttribute.

Field	Type	Required	Description
<div> <b>Note:</b> It works only with <b>Request_Response</b> operations. </div>			
<b>Attachment</b>			
name	String	No	Name of the attachment file. For more information, see <a href="#">Multiple Attachments</a> .
content	Base64 Binary	No	Content for the attachment.
fileName	String	No	A file reference can be sent as an attachment. For more information, see <a href="#">Multiple Attachments</a> .
deleteFile	Boolean	No	If set to <b>true</b> , the file reference specified in the <b>filename</b> field is deleted after the completion (successful or otherwise) of the transaction.
content-id	String	No	Represents the content Id for the attachment. It must be specified and enforcement is performed at the BusinessWorks palette level.  If this field is not specified, it is populated as transactionID-sequence number.
content-type	String	No	Represents the type of the message content. For more information, see <a href="#">Multiple Attachments</a> .

## Initiator Inbound Response—BusinessConnect to Private Process

The Initiator private process uses this message to handle inbound responses.

**Subject Name** `prefix.installation.EZComm.INITIATOR.RESPONSE`

External example: AX.BC.ACME.EZComm.INITIATOR.RESPONSE

*Private Message: Initiator Response*

Field	Type	Required	Description
resend	Boolean	No	A boolean value indicating whether a message is resent.
standardID	String	Yes	Name of the protocol.
fromTp	String	No	Name of the trading partner initiating the transaction.
toTp	String	Yes	Name of the trading partner receiving the transaction.
operationID	String	No	A three-part ID of the form:  category/version_number/operation_Name.
transactionID	String	No	It is a unique ID for transactions in the Initiator private processes environment. The private process creates this ID.
statusCode	String	No	A code indicating the status of the message. 200 for success. Otherwise, a code that represents the type of error.
statusMsg	String	No	OK or a description of the cause of the error.
closure	String	No	The private process generates the closure message and sends it to BusinessConnect Container Edition. BusinessConnect Container Edition is required to return this closure contents back in the InitiatorResponse to ensure that the

Field	Type	Required	Description
			private process can match it with the original InitiatorRequest.
duplicate	Boolean	No	Specifies whether the incoming response is a duplicate.
binaryResponse	String	No	A response is sent to this field if it contains binary data.
responseFile	String	No	File name containing the response.
originalFileName	String	No	<p>This field contains the filename of the original response file in an Asynchronous request response operation:</p> <ul style="list-style-type: none"> <li>• If a response is received over the FILE or FTP transport, this is the actual filename that is in the directory or on the FTP server.</li> <li>• For HTTP/S transports, this is the filename that is sent as a file reference from the private process when the <b>Allow override of filename via HTTP parameter</b> checkbox for the partner is selected.</li> </ul> <p>See <a href="#">Allow override of filename via HTTP parameter</a> (applies only to HTTP/S transports).</p>
as2-subject	String	No	A short string identifying the topic of the AS2 message.
as2-to	String	No	<p>A short string aiding the receiving system in identifying the sending system.</p> <p>The as2-to and as2-from headers are used.</p>

Field	Type	Required	Description
as2-from	String	No	A short string aiding the receiving system in identifying the sending system.  The as2-to and as2-from headers are used.
email-subject	String	No	A string receiving an email subject by the EMAIL or AS1-EMAIL transport.
<b>Attachment</b>			
name	String	No	Name of the attachment file. For more information, see <a href="#">Multiple Attachments</a> .
content	any	No	Content for the attachment.
fileName	String	No	A file reference can be sent as an attachment. For more information, see <a href="#">Multiple Attachments</a> .
deleteFile	Boolean	No	If set to true, then the private process can decide to delete the inbound attachment file.
content-id	String	No	Represents the content Id for the attachment. It must be specified and enforcement is performed at the BusinessWorks palette level. If this field is not specified, it is populated as transactionID-sequence number.
content-type	String	No	Represents the type of the message content. For more information, see <a href="#">Multiple Attachments</a> .
<b>Body</b>			
stringData (plainResponse)	String	No	A response is sent to this field if it contains string data.



# Responder Messages

- [Responder Inbound Request—BusinessConnect to Private Process](#)
- [Responder Outbound Response—Private Process to BusinessConnect](#)
- [Responder Acknowledgment—Private Process to BusinessConnect](#)

## Responder Inbound Request—BusinessConnect to Private Process

The Responder private process uses this message to handle inbound requests.

**Subject Name** `prefix.installation.EZComm.RESPONDER.REQUEST`

External example: AX.BC.BC-ACME.EZComm.RESPONDER.REQUEST

*Private Message: ResponderRequest*

Field	Type	Required	Description
resend	Boolean	No	A boolean value that indicates whether a message is resent.
standardID	String	Yes	Name of the protocol.
fromTp	String	Yes	Name of the trading partner who initiated the transaction.
toTP	String	Yes	Name of the trading partner who received the transaction.
operationID	String	No	A three-part ID of the form: category/version_ number/operation_Name.
transactionID	String	Yes	A unique ID generated by BusinessConnect Container Edition

Field	Type	Required	Description
			when publishing the transaction to the private process's environment.
closure	String	No	A closure message generated by the private process and sent to BusinessConnect Container Edition.
binaryRequest	base64Binary	No	Used by BusinessConnect Container Edition to send data when binary data is being passed to a partner.
isBinaryFile	Boolean	No	This field shows whether the file specified in the field <code>inputFile</code> is a binary file.
inputFile	String	No	Used for a file reference that was passed to BusinessConnect Container Edition.
operationType	String	No	Represents the type of the operation, such as Notify, Synchronous Request Response, or Asynchronous Request Response.
duplicate	Boolean	No	Specifies whether the incoming request is a duplicate.
originalFileName	String	No	<p>This field contains the filename of the original response file in an Asynchronous Request Response operation:</p> <ul style="list-style-type: none"> <li>For the FILE and FTP transport, this is the actual filename that is in the directory or on the FTP server.</li> <li>For HTTP/S transports, this is the filename that is sent as a</li> </ul>

Field	Type	Required	Description
			<p>file reference from the private process when the <b>Allow override of filename via HTTP parameter</b> checkbox for the partner is selected.</p> <p>See <a href="#">Allow override of filename via HTTP parameter</a> (applies only to HTTP/S transports).</p>
as2-subject	String	No	A short string identifying the topic of the AS2 message.
as2-to	String	No	<p>A short string that helps the receiving system to identify the sending system.</p> <p>The as2-to and as2-from headers are used.</p>
as2-from	String	No	<p>A short string that helps the receiving system to identify the sending system.</p> <p>The as2-to and as2-from headers are used.</p>
email-subject	String	No	A string that receives an email subject from the EMAIL or AS1-EMAIL transport.
<b>Attachment</b>			
name	String	No	Name of the attachment file. For more information, see <a href="#">Multiple Attachments</a> .
content	any	No	Content of the attachment.
fileName	String	No	A file reference can be sent as an attachment. For more information,

Field	Type	Required	Description
			see <a href="#">Multiple Attachments</a> .
deleteFile	Boolean	No	If set to true, then the private process can decide to delete the inbound attachment file.
content-id	String	No	Represents the content Id for the attachment. It must be specified and enforcement is performed at the BusinessWorks palette level. If this field is not specified, it is populated as transactionID-sequence number.
content-type	String	No	Represents the type of the message content. For more information, see <a href="#">Multiple Attachments</a> .

## Responder Outbound Response—Private Process to BusinessConnect

The Responder private process uses this message to handle outbound responses.

**Subject Name** *prefix.installation.EZComm.RESPONDER.RESPONSE*

External example: AX.BC.BC-ACME.EZComm.RESPONDER.RESPONSE

*Private Message: Responder.Response*

Field	Type	Required	Description
statusCode	Integer	Yes	A code indicating the status of the message (200 for success). Alternatively, a code that represents the type of error.

Field	Type	Required	Description
statusMsg	String	Yes	OK or a description of the cause of the error.
binaryResponse	Base64Binary	No	A response is sent to this field if it contains binary data.
responseFile	String	No	This is the name of the file that contains the response.
deleteResponseFile	Boolean		Deletes the response file if the value is true.
closure	String	Yes	This is the closure that is received from the Responder Request Based on this value, this response is correlated to the request.
content-type	String	No	Content type of the response. If not specified, BusinessConnect Container Edition interprets this value.
content-disposition	String	No	Maps to MIME's content-disposition. This value, if provided, is set in the MIME Internet headers.
as2-subject	String	No	A short string identifying the topic of the AS2 message.  By default, the value in the as2-subject element is the same as the one in the MIME Subject field.
<b>Attachment</b>			
name	String	No	Name of the attachment file. For more information, see <a href="#">Multiple</a>

Field	Type	Required	Description
			<a href="#">Attachments.</a>
content	Any	No	Content of the attachment.
fileName	String	No	A file reference can be sent as an attachment. For more information, see <a href="#">Multiple Attachments</a> .
deleteFile	Boolean	No	If set to true, the file reference specified in the <b>filename</b> field is deleted after the completion (successful or otherwise) of the transaction.
content-id	String	No	Represents the content Id for the attachment. It must be specified and enforced at the BusinessWorks palette level. If this field is not specified, it is populated as transactionID-sequence number.
content-type	String	No	Represents the type of the message content. For more information, see <a href="#">Multiple Attachments</a> .
<b>Body</b>			
stringData (plainResponse)	String	No	A response is sent to this field if it contains string data.

## Responder Acknowledgment—Private Process to BusinessConnect

The Responder TIBCO BusinessConnect sends this acknowledgment after it receives the Responder Response. The acknowledgment indicates whether the Responder Response has been forwarded to the trading partner.

**Subject Name** *prefix.installation.EZComm.RESPONDER.ACK*

External example: AX.BC.BC-ACME.EZComm.RESPONDER.ACK

*Private Message: Responder.Ack*

Field	Type	Required	Description
statusCode	String	Yes	A code indicating the status of the message (200 for success). Otherwise, the code represents the type of error.
statusMsg	String	Yes	OK or a description of the cause of the error.
operationType	String	No	Represents the type of the operation. In this case it is ack, indicating that the message is of the type Acknowledgment.
closure	String	Yes	A closure sent by the Responder Response message.

## General Messages

### Error Messages

BusinessConnect Container Edition uses the error message to publish status information.

**Subject Name** *prefix.installation.EZComm.ERROR*

Example: AX.BC.BC-ACME.EZComm.ERROR

Field	Type	Required	Description
statusCode	String	No	One of the private party-defined status and error codes.

Field	Type	Required	Description
statusMsg	String	No	The string representing the cause of one of the private party-defined status or error codes.
details	String	No	Additional information.
msgDirection	String	No	It indicates the flow of the message, either inbound or outbound.
closure	String	No	Reserved.
operationID	String	No	A three-part ID of the form: category/version_number/operation_Name.
transactionID	String	No	A unique ID generated by BusinessConnect Container Edition when publishing the transaction to the private process's environment.
standardID	String	Yes	Name of protocol.
timestamp	String	No	Time stamp for this message.
host	String	No	Name of host name.
tpName	String	No	Name of trading partner.
extraInfo	String	No	This field contains the originalFileName when available.
<b>Body</b>			
stringData	String	No	

## Multiple Attachments

You can send attachments to the trading partner by using Services Plug-in. The current private process schema accommodates attachments so that the attachment field represents a sequence that allows any number of attachments to be specified.



The following fields are available for configuring an attachment:

- **name:** This represents the name of the attachment. If none is specified, it is named `AttachmentsequenceNumber.second part of the content type`.

Example, if you are sending a `.xml` file, the content type is `text/xml` and the attachment name is `Attachment0.xml`. (1 is the sequence number for the first element of the attachment sequence).

- **content:** Content of the attachment.
- **fileName:** A file reference can be sent as an attachment. The content of this file is read and set to the content of the attachment.
  - If both the `content` and `fileName` fields are specified, then `content` is set as the attachment data.
  - If neither the `content` nor the `fileName` fields are specified, then this attachment element is not processed.

Specifying these fields is not enforced by the private process.

- **deleteFile:** This is a Boolean field. If set to `true`, the file reference specified in the **filename** field is deleted after the completion (successful or otherwise) of the transaction.
- **contentID:** Represents the content ID for the attachment. It must be specified and enforcement is performed at the BusinessWorks palette level. If this field is not specified, it is populated as `transactionID-sequence number`.
- **contentType:** Represents the type of the message content. If not specified, it is inferred by the protocol. If this field is set to `text/foo`, the content field must hold a `Java.lang.String` object. If this field is not set and the content field holds a `java.lang.String` object, the `contentType` field defaults to `text/plain`. If `contentType` is not set and the content field does not hold a `java.lang.String` object, the `contentType` defaults to `application/octet-stream`.

**i Note:** If a `contentType` field is not specified, such as when neither `content` or the `fileName` fields are specified, the attachment is not processed.

# Resending Services Plug-in Private Process Messages

The Services Plug-in can resend the private process messages that are in audit states `RECEIVED_FROM_PP` and `SEND_TO_PP`.

The following is the relationship between the audit states and private process message types:

- On the Initiator side:  
`RECEIVED_FROM_PP` `INITIATOR.REQUEST`  
`SEND_TO_PP` `INITIATOR.RESPONSE`
- On the Responder side:  
`RECEIVED_FROM_PP` `RESPONDER.RESPONSE`  
`SEND_TO_PP` `RESPONDER.REQUEST`

The message `RESPONDER.REQUEST` is not resendable for the synchronous transactions: it is only resendable for notify and asynchronous transactions.

The message `RESPONDER.RESPONSE` is not resendable for any transaction type.



**Note:** Once a message is sent in the Services Plug-in format, the resent message is also in the same format.

For more information about how to resend transactions and view their transaction history, see the [Resending Transactions](#) and [Viewing Resend History](#) topics.

# Viewing Logs

---

This section explains how to view the transaction logs in Audit Trail of BusinessConnect Container Edition – Services Plug-in.

TIBCO® AuditSafe stores information about the messages and documents processed by BusinessConnect Container Edition.



**Note:** The entire AESchema is stored in the fields REQUEST\_FROM\_PP and SEND\_TO\_PP fields in TIBCO® AuditSafe, since this is required for the resend.

You can use the TIBCO AuditSafe to follow the processing states of inbound or outbound documents. Some of the types of information stored in the audit log include: sent and received documents; document originator; trading partner name; processing status; and validation errors.

To view the logs, on the Data Viewer tile, click **Audit Trail > EZComm**.

All the transactions are displayed on [Transactions Screen](#).

## Transactions Screen

On the Transactions screen, you can perform the following tasks:

- **Sort** transactions
- **Search Transactions** by using filters
- View **Transaction Details**
- Change the columns that you view by selecting the categories from the **Settings** dialog.

# Customizing Transactions Screen

## Procedure


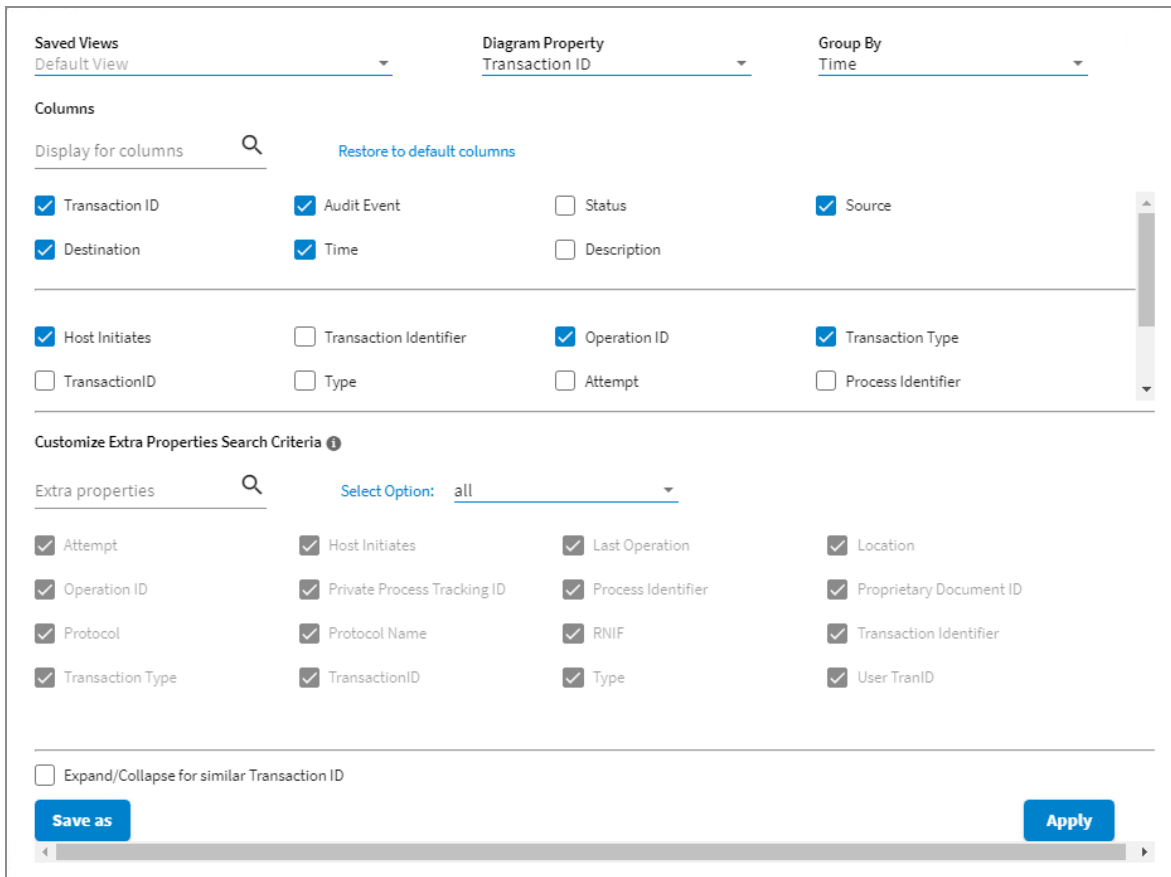
1. Click the **Gear**  icon.
2. In the **Settings** dialog:
  - Select the checkboxes for the columns that you want to view on the Transaction page.
  - Clear the checkboxes for the columns that you do not want to view on the Transaction page.
3. Click **Apply** to save your transaction screen settings.

Figure 9: Settings



The screenshot shows the 'Settings' dialog for customizing the Transactions screen. It features three main sections: 'Saved Views', 'Columns', and 'Customize Extra Properties Search Criteria'.

**Saved Views:** A dropdown menu showing 'Default View'.

**Diagram Property:** A dropdown menu showing 'Transaction ID'.

**Group By:** A dropdown menu showing 'Time'.

**Columns:** A section with a search bar and a 'Restore to default columns' link. It contains a grid of checkboxes for various columns:

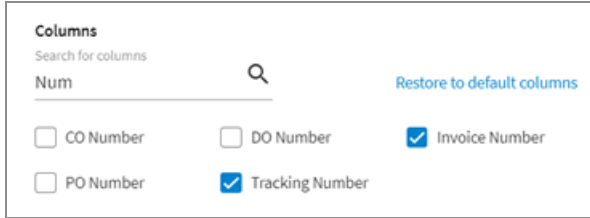
Column	Checked
Transaction ID	Yes
Audit Event	Yes
Status	No
Source	Yes
Destination	Yes
Time	Yes
Description	No
Host Initiates	Yes
Transaction Identifier	No
Operation ID	Yes
Transaction Type	Yes
TransactionID	No
Type	No
Attempt	No
Process Identifier	No

**Customize Extra Properties Search Criteria:** A section with a search bar and a 'Select Option: all' dropdown. It contains a grid of checkboxes for various search criteria:

Search Criteria	Checked
Attempt	Yes
Host Initiates	Yes
Last Operation	Yes
Location	Yes
Operation ID	Yes
Private Process Tracking ID	Yes
Process Identifier	Yes
Proprietary Document ID	Yes
Protocol	Yes
Protocol Name	Yes
RNIF	Yes
Transaction Identifier	Yes
Transaction Type	Yes
TransactionID	Yes
Type	Yes
User TransID	Yes

At the bottom, there is an unchecked checkbox for 'Expand/Collapse for similar Transaction ID', a 'Save as' button, and an 'Apply' button.

4. You can also use the following options:

Option	Description
<b>Group By</b>	Use this option to group results by category. To do this, select a category from the dropdown list.
<b>Columns</b>	<p>Select the checkbox next to the category to display the columns you want to view. You can also search for a category by entering a partial word to display all categories containing that string as shown in the following example.</p> 

- Each page displays up to 20 records with the newest transactions listed first as default. Page through the display to see the older records. You can sort the transactions by category, or search for records of a specific type. The number of records returned are limited to 10,000 audit events or a maximum of 500 pages.

**Note:** A "No records found" error is generated if your selection exceeds 500 pages.

## Sort Transactions

Click the arrows on a column (category) heading to sort transactions.

- ↑ : Sort first to last.
- ↓ : Sort last to first.

To reorder the columns, click the category name to select it, and drag it to a different location on the page.

Transactions are sorted according to date and time by default, so the newest transactions appear at the top of the list.

## Search for Transactions

The search feature of TIBCO AuditSafe is powerful and easy-to-use.



You can search for values in multiple categories and find matching records even if a category (or column) is not displayed. You can hide or show categories by selecting them from the **Settings** dialog.

While searching for values, use the following options:


- **Keyword:** To search for a term in all categories.
- **Audit Event:** To search for an audit event in all categories.
- **OR:** To search for values or keywords within the same category.  
Example: Search **Status** for in PROCESSING **OR** COMPLETED to find all the transactions that contain those values.
- **AND:** To search for values between two or more categories.  
Example: Search **Status** for COMPLETED **OR** PENDING, **AND** search **Audit Event** for Request\_TO\_PP.

The system automatically segments your query into **OR** and **AND** searches as shown in the following example:

Showing search results for:

Status: = COMPLETED  or = PENDING 

AND

Audit Event: = REQUEST\_TO\_PP 


## Using Search

Search contains the following options:

- **Time:** To define the start and end range for your search.
- **Keyword:** To search for the term in all categories.

Search Option	Description
=	<b>Equals:</b> Finds an exact match for a term.

Search Option	Description
	Entering the first few letters list matching options. Select one and press ENTER. If an exact match is not available, no items are listed.
!=	<b>Not Equal to:</b> Use this option to exclude terms from your search.
~	<b>Like:</b> Enter a few letters to list items containing a matching string.

1. Click the **Select** dropdown to choose a category.
2. In the **Search Transaction** field, select a [Search Option](#) , and enter a word.
3. Select an option from the ones that are displayed when you enter a word, and add it to your query.  
Continue adding options to narrow your search results.
4. After creating your query, click **Find** to list the results.
5. Click the **Remove** icon  to remove a search term.

## Transaction Details

Click a transaction in the list to see more details. You can view the transactions using either a Diagram view or a List view.

Switch between the two views by clicking the icon on the top right. The diagram view also displays related transactions.

## Resend Transactions

The Resend Transactions page allows users to manage and resend transactions that have been previously processed. This page provides two main functionalities: searching for and resending transactions, and viewing the history of resent transactions.

The Resend Transactions page has the following tabs:

- **Resendable Transactions:** Search for and resend transactions. For more information, see [Resending Transactions](#).


**Note:**

- For the state RECEIVED\_FROM\_PP, the Outbound File Poller messages are not listed in the **Resendable Transactions** tab and therefore cannot be resent.
- For the state SEND\_TO\_PP, the Outbound File Poller messages are listed in the **Resendable Transactions** tab.

- **Resend History:** View the history of resent transactions. For more information, see [Viewing Resend History](#).

The **Resend Transactions** tab provides a log of transaction activities with key details for tracking and management. Refer to the following table for column descriptions:

Column	Description
Business Process	Indicates the type of business process associated with the transaction.
Description	A brief description of the transaction.
Destination	The recipient or endpoint of the transaction.
Source	The originator or starting point of the transaction.
Audit Event	The specific audit event associated with the transaction.
Status	The current status of the transaction.
Time	The date and time the transaction occurred.
Transaction ID	The unique identifier for the transaction.
Host Initiates	Indicates whether the host participant initiated the transaction.  For the Initiator, this value is <b>true</b> for any type of transaction (Notify , Synchronous Request Response, or Asynchronous Request Response). For the



Column	Description
	Responder, this value is always false. This value is true for outgoing requests, while for incoming requests and for outgoing responses this value is false.
Protocol Name	The name of the protocol used for the transaction.
Operation ID	A protocol-specific value identifying the type of the transaction.
Transaction Type	The type of transaction. For example: EZComm-Notify, EZComm-Async, or EZComm-Sync.
User TranID	<p>The user transactionID column displays the transaction ID received from the private process on the Initiator side.</p> <p>Initiator forwards this ID to the Responder and at the same displays it in this column. This way, a transaction initiated by the Initiator can be cross-referenced on the Responder side. This feature works only for HTTP/S and Email transports. For File and FTP/S transports, this column is left blank.</p>

## Resending Transactions

To resend transactions, perform the following steps:

### Procedure

1. On the Data Viewer tile, click **Resend Transactions**.  
The Resend Transactions page displays a list of available protocols.
2. Click **EZComm** in the list of protocols.
3. Go to the **Resendable Transactions** tab to view the list of available transactions.  
All resendable transactions are displayed by default. The default settings are **Status:** ANY, **Audit Event:** ANY, and the **From** and **To** fields are set to a 24-hour range from the current time.
4. To filter the transactions, select the following fields and click **Find**:

- **Status:** Select a status from the dropdown menu. The following statuses are available: ANY, CANCELED, COMPLETED, ERROR, ERROR SECURITY, PENDING, and RECEIPT PENDING.
- **Audit Event:** Select an audit event from the dropdown menu. The following audit events are available: RECEIVED\_FROM\_PP and SEND\_TO\_PP.
- **From** and **To:** Select the date range for the transactions.

The list of transactions is displayed based on the applied filters.

5. From the list of transactions, select the checkboxes next to the transactions you want to resend.



**Tip:** Select the checkbox on the header to select all transactions.

6. Click **Resend** to resend the selected transactions.

The resent transaction is recorded and can be viewed on the **Resend History** tab only after completion of transaction, regardless of success or failure. If a transaction is in process, it does not appear on the **Resendable Transactions** tab. After the transaction is processed and sent, it becomes available to resend again on the **Resendable Transactions** tab.

## Result

You have now successfully resent transactions using the EZComm protocol.

# Viewing Resend History

To view the resend history for the Services Plug-in:

## Procedure

1. On the Data Viewer tile, click **Resend Transactions**.  
The Resend Transactions page displays a list of available protocols.
2. Click **EZComm** in the list of protocols.
3. Click the **Resend History** tab to view the history of resent transactions.

All resent transactions are displayed by default. The default settings are **Status:** ANY and **From** and **To** fields are set to a 24-hour range from the current time.

**i Note:** If the same event is resent multiple times, only the last sent transaction is shown with its timestamp. Multiple instances of the same transaction are not displayed.

4. To filter the history, select the following fields and click **Find**:

- **Status:** Select a status from the dropdown menu. The following statuses are available: ANY, CANCELED, COMPLETED, ERROR, ERROR SECURITY, PENDING, and RECEIPT PENDING.
- **From** and **To:** Select the date range for the transactions.

The list of resent transactions is displayed based on the applied filters.

## Result

You have now successfully viewed the resend history.

# File Pollers

---

The following sections describe outbound and inbound File pollers for BusinessConnect Container Edition – Services Plug-in.

- [Outbound File Pollers for BusinessConnect Container Edition – Services Plug-in](#)
- [Inbound File Pollers for BusinessConnect Container Edition – Services Plug-in](#)

## Outbound File Pollers for BusinessConnect Container Edition – Services Plug-in

The outbound File Poller provides a simple way for private processes to transmit documents to BusinessConnect Container Edition. This contrasts with the other transports, which are used for communication between trading partners.



**Note:** The sending partner for outbound File pollers is assumed to be the default host.

## URI Format for Outbound File Pollers

For the Outbound File Poller, the directory structure format is `/BaseDir/*.*`

Example: `/opt/inbound/*.*`

This ensures that all the directories under `BaseDir` are checked for files.

The format for the monitor directory path is as follows:

`xxx/ProtocolName/partner/Operation_Name`

Example: `xxx/EZComm/partner/BC_1.0_Notify`

For the file to be handled by Services Plug-in, the document must be structured in the following format:

- Default behavior, such as for the operation BC/1.0/Notify:  
BaseDir/TpName
- Non-default behavior, for other operations:  
BaseDir/TpName/Category\_Version\_OperationID

where

- BaseDir is a user-selected base directory
- TpName is the name of the trading partner
- Category is the operation category
- Version is the operation version
- OperationID is the operation ID

If Category\_Version\_OperationID is not provided, then it defaults to BC/1.0/Notify.

Since the default operation has changed from BC/Notify to BC/1.0/Notify, files in the Category\_operationID directory are treated as Category\_Empty\_operationID. For example, BusinessConnect Container Edition looks for an operation Category/Empty/operationID in the configuration store. For more information about enabling an outbound File Poller, see the "Outbound File Pollers" topic in *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.

## Inbound File Pollers for BusinessConnect Container Edition – Services Plug-in

When File outbound is used as a transport, the trading partner uses an inbound File Poller to check for the documents.

The format for the monitor directory paths is as follows:

*xxx/ProtocolName/partner/Operation\_Name*

Example: xxx/EZComm/partner/BC\_1.0\_Notify



**Note:** For the inbound File pollers, the receiving partner is assumed to be the default host.

For more information about enabling an inbound File Poller, see *TIBCO BusinessConnect™ Container Edition Trading Partner Management*.

## Copying Large Files to NFS (Sharing)

Perform the following steps to copy files (greater than 5 MB as configured by default) to the NFS (sharing) folders.

1. Go to **System Settings > Others > Activate Protocol Plugins**.
2. Click **EZComm**.
3. In the Edit EZComm Plugin Settings dialog, click **Add Property**.
4. Set the following fields.

Field	Value
Property Name	ezcomm.interior.pp.file.copy.nfs.path
Property Type	String

5. Click **Add**.
6. On the **Custom Property** tab, configure the `ezcomm.interior.pp.file.copy.nfs.path` field to NFS path.

Example: `/mnt/FilePoller`

**Custom Properties:**

`ezcomm.interior.pp.file.copy.nfs.path`  
`/mnt/FilePoller`  
`nfspace`



**Note:** You must set the `ezcomm.interior.pp.threshold` value to 5000.

7. Click **Save**.
8. Similarly, create a custom property for TIBCO BusinessConnect™ Container Edition with the following values.

Field	Value
Property Name	<code>audit.tas.logging.payload.limit</code>
Property Type	Integer

This limits the view or downloadable payload size on AuditSafe. The maximum limit is 5 MB.

**i Note:** You must set the `audit.tas.logging.payload.limit` value to 5000000.

**Custom Properties:**

`audit.tas.logging.payload.limit`

`audit.tas.logging.payload.limit`



# TIBCO Documentation and Support Services

---

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

## How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [Product Documentation website](#), mainly in HTML and PDF formats.

The [Product Documentation website](#) is updated frequently and is more current than any other documentation included with the product.

## Product-Specific Documentation

The documentation for this product is available on the [TIBCO BusinessConnect™ Container Edition – Services Plug-in Documentation](#) page.

## How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our [product Support website](#).
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the [product Support website](#). If you do not have a username, you can request one by clicking **Register** on the website.

## How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature

requests from within the [TIBCO Ideas Portal](#). For a free registration, go to [TIBCO Community](#).

# Legal and Third-Party Notices

---

SOME CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

USE OF CLOUD SG SOFTWARE AND CLOUD SERVICES IS SUBJECT TO THE TERMS AND CONDITIONS OF AN AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER AGREEMENT WHICH IS DISPLAYED WHEN ACCESSING, DOWNLOADING, OR INSTALLING THE SOFTWARE OR CLOUD SERVICES (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH LICENSE AGREEMENT OR CLICKWRAP END USER AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE SAME TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, ActiveMatrix BusinessWorks, BusinessConnect, Business Studio, and TIBCO Business Studio are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the “readme” file for the availability of a specific version of Cloud SG software on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. CLOUD SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "README" FILES.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>.

Copyright © 2001-2024. Cloud Software Group, Inc. All Rights Reserved.