TIBCO BusinessConnect™ Container Edition

Trading Partner Management

Version 1.2.0
October 2022

Contents

The Login Page

To log in to the TIBCO BusinessConnect™ Container Edition, provide the following default credentials:

- Username: `admin`
- Password: `Password`

Note: An SMTP Proxy Server should be already enabled on the BusinessConnect Container Edition Admin UI if you want to recover your forgotten password.

Note: If the sample certificate used to connect to the Gmail server expires, download a new Gmail server certificate (if required).

For more information, see the following topics:

- Email Inbound POP3 Service Configurations
- Email Outbound Proxy Server Configuration

Dashboard

From this page, you can go to the different features of TIBCO BusinessConnect Container Edition.

Data Viewer

Displays transaction search page on Audit Trail.

Partner Management

Manages the participants and business agreement between them.

B2B Administration

Manages different operations for the business protocols.

User Management

Defines different access privileges for users and roles .

System Settings

Provides access to modify and configure different parameters such as transport protocols, servers, certificates, and metadata.

Hosts Overview

Hosts are the participants who sponsor a trading community, where standardized business transactions can occur between trading partners. A host can be a retailer, manufacturer, or any sponsor who creates a trading community.

You can manage hosts as follows:

- Searching for a Host
- Creating a Host
- Configuring a Host
- Deleting Hosts

Note: On the Hosts page, you can enable or disable the switch in the **Status** column to activate or deactivate a host.

Searching for a Host

In addition to entering the host's name or selecting it from the list, you can use the Search function to find a specific host.

Procedure

1. On the **Partner Management** tile, click **Hosts**.
2. Enter the search string in the Search field to search for hosts.

   The names of one or more hosts that correspond to the search criteria only are displayed.

Creating a Host

To create a new host, perform the following steps:

Procedure

1. On the **Partner Management** tile, click **Hosts**.
2. On the Hosts page, click **Create Host**, which is in the upper-right corner of the page.
3. On the Create New Host page, in the **Host Name** field, enter the name of the host you want to create, and then click any one of the push buttons:

Option	Description
Done	To create the host.
Proceed	To instantly configure the data of the new host

> **Note:** Click **Proceed** button before you click **Done** button. After you click **Proceed** button, you can configure the protocols for that host.

For detailed information on configuring the host data, see Configuring a Host.

> **Note:** The first host that you create automatically becomes the default host. If you have created multiple host participants, you can assign any one of them as the default host by selecting Make this as Default Host check box while creating or configuring a host. The default host is displayed in the upper-right corner of the table on the Hosts page.

4. After you have provided all the required information, click **Done**.

   The status of the newly created host is by default enabled.

Configuring a Host

The configuration of a host includes tasks such as setting up the protocols, editing the configurations of the protocols, credentials, and business locations.

To edit the host data, perform the following steps:

> **Note:** You can either configure the data when creating the host or later configure the data of the already-created host.

Procedure

1. On the **Partner Management** tile, click **Hosts**.
2. On the Hosts page, select the host whose information you want to edit.

   The three tabs: Protocols, Credentials, and Business Location are displayed.
3. To provide detailed information about the host, provide information for the following tabs:

Option	Description
Protocols	To enable or edit configurations of protocols, click the **Protocols** tab. For more information on configuring the protocols, see Configure Protocols for Hosts.
Credentials	To add new credentials, click the **Credentials** tab. For more information on uploading the credentials, see Manage Credentials for Hosts.
Business Locations	To add information about the address and contact information for the company headquarters, click the **Business Locations** tab. For more information, see Add Business Locations of Hosts.

Configure Protocols for Hosts

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

To configure the protocols of a host, perform the following steps:

Procedure

1. On the Hosts page, click a host whose protocols you want to configure.
2. On the Edit Host page, select the business protocols that are available to use for the future communication with the selected host.
3. To edit the configurations of protocols, click the **Edit Configurations** tab.

   For more information on editing the protocols, see the appropriate documentation for the specific protocol.

4. Click **Done.**

Manage Credentials for Hosts

You can search, add, and delete credentials for hosts.

> **Note:** You can only add keys in the host credentials tab.

Searching Credentials

To search for the credentials, perform the following steps:

Procedure

1. Enter the search string in the **Search** field to search the credentials.

   One or more credentials that correspond to the search criteria are only displayed.

Adding a Credential

To add credentials for a host, perform the following steps:

Procedure

1. On the Edit Host page, on the **Credentials** tab, click the **Add** icon and select any one of the following options to create the respective key:

Option	Description
New Private Key	New private key for the host.
New PGP Private Key	Private key for encryption at host side.
New SSH Private Key	SSH keys are used to support the SSHFTP transport.

Based on which option you choose, the respective dialog box opens in which you can upload the key.

2. In the dialog box, provide the following details:

New Private Key/New PGP Private Key/New SSH Private Key

Field	Description
Alias	Enter the name of the key.
Upload file	Click **Add files or drop files** to browse and go to the file containing the key.
Password	Enter the password. The default password for sample keys is `Password1`.

The newly created key for the host is now listed in the credentials table.

To add more credentials to the list, click the **Add** icon on the **Credentials** tab on the Edit Host page.

Deleting Credentials

To delete one or more credentials:

Procedure

1. In the **Credentials** tab, select the credential that you want to delete, and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Add Business Locations of Hosts

A business location is the address and other identifying information of a host. One host often has multiple departments or other distinct groups at various locations. You can set up multiple locations for one host to simplify shipping and billing procedures. It can also include contact information such as name, phone number, and email address of a person associated with a particular location. Each business location can have multiple contacts.

Note: The Headquarters location is created when the RosettaNet Protocol is enabled for the Host.

To add a business location for a host, perform these steps:

Procedure

1. On the **Business Locations** tab, click the **Add** icon .

   The **Add Location** dialog box is displayed.

2. In the **Add Location** dialog box, enter the following details:

   Details

Field	Description
Location Name	Enter the name of the location.
Email	Enter email ID.
Phone	Enter contact number.
FAX	Enter fax number.
Web URL	Enter web URL.
Address	Enter address.
Primary Legal Contact	Select the legal contact information from the drop-down list.
Primary Support Contact	Select the support contact from the drop-down list.

3. To assign either primary legal or support contacts to the business location, or to add contacts to the host, click **New Contact** on the **Contacts** tab or click the **add** icon in the **Primary Legal Contact** or **Primary Support Contact** fields and provide the following details:

Field	Description
Contact Type	Select the type of the contact from the drop-down list: General, Support, Legal, or Business.
First Name	Enter the first name.
Last Name	Enter the last name.
Phone	Enter the contact number.
FAX	Enter the fax number.
Email	Enter the email address.

Your contact is displayed in the **Primary Legal Contact** and the **Primary Support Contact** drop-down lists.

4. Click **Add.**

Deleting Business Locations

Procedure

1. In the **Business Locations** tab, to delete the business locations, select the business location you want to delete from the table and click the **Delete** icon.

Deleting Hosts

To delete one or more hosts, perform the following steps:

Note:

- To delete a default host, you are first required to assign a different host participant as the default host by creating a new host participant.
- You cannot delete a host,
  - If you have only one host participant
  - If host has a Business Agreement

Procedure

1. On the Hosts page, select one or more hosts that want wish to delete and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Partners

Partners are the participants who are outside the host's company and establish business agreements with the host. For example, a partner can be a vendor, a customer, or a healthcare provider.

You can manage partners as follows:

- Searching for a Partner
- Creating a Partner
- Configuring a Partner
- Deleting Partners

Note: On the Partners page, you can enable or disable the switch under the **Status** column to activate or deactivate a partner.

Note: On the Partners page, you can directly go to the Edit Business Agreement window, by clicking the host in the **Agreements** column.

Searching for a Partner

In addition to entering the partner's name or selecting it from the list, you can use the **Search** function to find a specific partner.

Procedure

1. On the **Partner Management** tile, click **Partners**.
2. Enter the search string in the **Search** field to search a partner.

   The names of one or more partners that correspond to the search criteria only are displayed.

Creating a Partner

To create a new partner, perform the following steps:

Procedure

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click **Create Partner**, which is in the upper-right corner of the page.
3. On the Create New Partner page, in the **Partner Name** field, enter the name of the partner you want to create, and then click any one of the push buttons:

Option	Description
Done	To create the partner.
Proceed	To instantly configure the data of the new partner.

> **Note:** Click the **Proceed** button before you click the **Done** button. After you click the **Proceed** button, you can configure the protocols for that partner.

   For more information on configuring the partner data, see **Configuring a Partner**.
4. After you have provided all the required information, click **Done**.

   The status of the newly created partner gets enabled by default.

Configuring a Partner

The configuring of a partner includes tasks such as setting up the protocols, editing the configurations of the protocols, setting the proxy servers or adding transports, credentials, and business locations.

To edit the partner data, perform the following steps:

Note: You can either configure the data when creating the partner or later configure the data of the already-created partner.

Procedure

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click the partner whose information you wish to edit.

   The three tabs: Protocols, Credentials, and Business Locations are displayed.
3. To provide more information about the partner, provide information for the following tabs:

Option	Description
Protocols	To enable or edit configurations of protocols, click the **Protocols** tab. For more information on configuring the protocols, see Configure Protocols for Partners.
Credentials	To add new credentials, click the **Credentials** tab. For more information on uploading the credentials, see Manage Credentials for Partners.
Proxy Settings	To activate the proxy that BusinessConnect Container Edition uses as a default connection for any outgoing traffic with a specific trading partner. For more information, see Configure Proxy Settings for Partners.
Business Locations	To add information about the address and contact information for the company headquarters, click the **Business Locations** tab. For more information, see Add Business Locations of Partners.

Configure Protocols for a Partner

You can enable or disable protocols for a partner, or edit their configurations using **Protocols** tab.

To configure the protocols of a partner, perform the following steps:

Procedure

1. On the Partners page, click the partner whose protocols you want to configure.
2. On the Edit Partner page, select the business protocols that are available to use for the future communication with the selected partner.
3. To edit the configurations of protocols, click the **Edit Configurations** tab.

   Note: For more information on editing the protocols, see the appropriate documentation for the specific protocol.

4. Click **Done.**

Adding Outbound Transports for Partners

To add and configure transports for a partner, perform the following steps:

Procedure

1. On the **Protocols** tab, select a protocol and click **Edit Configurations**.
2. On the Protocol Configurations page, click **Transports**.

   For more information on configuring outbound transports for partners, see the following topics:

   - Setting Up FILE for a Trading Partner
   - Setting Up HTTP/S for a Trading Partner
   - Setting Up FTP/S for a Trading Partner
   - Setting Up SSHFTP for a Trading Partner
   - Setting Up Email for a Trading Partner
   - Setting Up AS1 Email for a Trading Partner
   - Setting Up AS2-HTTP/S for a Trading Partner

Manage Credentials for Partners

You can search, add, and delete credentials.

Note: You can only add certificates in the partner's Credentials tab.

Searching Credentials

To search for the credentials, perform the following steps:

Procedure

1. Enter the search string in the **Search** field to search the credentials.

   One or more credentials that correspond to the search criteria are only displayed.

Adding a Credential

To add credentials for a partner, perform the following steps:

Procedure

1. On the Edit Partner page, on the **Credentials** tab, click the **Add** icon ⊕ of the following options to create the respective key:

Option	Description
New Certificate	New certificate key for the partner.
New PGP Public Key	Public Key for encryption at the partner side.
New SSH Public Key	SSH keys are used to support the SSHFTP transport.

   Based on which option you choose, the respective dialog box opens in which you can upload the key or the certificate.

2. In the dialog box, provide the following details:

New Certificate/New PGP Public Key/New SSH Public Key

Field	Description
Alias	Enter the name of the key or certificate.
Upload file	Click **Add files or drop files** to browse and go to the file containing the key or the certificate.

The newly created key for the partner is now listed in the Credentials table.

To add more credentials to the list, click the **Add** icon in the **Credentials** tab on the Edit Partner page.

Deleting Credentials

To delete one or more credentials, perform the following steps:

Procedure

1. In the **Credentials** tab, select the credential that you wish to delete, and then click **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Configure Proxy Settings for Partners

You can use the **Proxy Settings** tab to activate the proxy that BusinessConnect Container Edition uses as a default connection for any outgoing traffic with a specific trading partner.

To configure the proxy settings of a partner, perform the following steps:

Procedure

1. On the Partners page, click the partner whose proxy settings you wish to configure.
2. On the Edit Partner page, click the **Proxy Settings** tab.
3. Select proxies using the information provided in the following table:

Selecting Proxy Settings for the Partner

Field	Description
Proxy Servers	Enable or disable the proxies using the toggle.
Connection Defaults	If the proxies are disabled, no proxy can be used regardless of any selections in the proxy list or in the **System Settings > Outbound Protocols > Proxy Server**s. **Note:** For SMTP, even if a TIBCO BusinessConnect Container Edition user disables the use of proxy for a specific trading partner, the system level SMTP proxy can still be used to send email. If the proxies are enabled and a proxy is selected from the list, the selected proxies are used for this partner: the default system settings is overridden. Using the Default option from the list means that BusinessConnect Container Edition uses the proxy defined under **System Settings > Outbound Protocols > Proxy Servers**. Therefore, if the proxy is not specified on the partner level, the BusinessConnect Container Edition user indicates that there is no preference, and whatever is defined on the system level should be used for this trading partner.
FTP Proxy	Enable the previously configured FTP proxy. Available FTP and SOCKS4/SOCKS5 proxy servers are displayed for selection.

Field	Description
HTTP Proxy	Enable the previously configured HTTP proxy. Available HTTP proxy and SOCKS4/SOCKS5 proxy servers are displayed for selection. Only HTTP 1.1 is supported for the HTTP Proxy.
SMTP Server	Enable the previously configured SMTP server. Available SMTP proxy servers are displayed for selection.

4. Click **Save**.

Add Business Locations of Partners

A business location is the address and other identifying information of a partner. One partner often has multiple departments or other distinct groups at various locations. You can set up multiple locations for one partner to simplify shipping and billing procedures. It can also include contact information such as name, phone number, and email address of a person associated with a particular location. Each business location can have multiple contacts.

Note: The default Headquarters location is created when user enables RosettaNet protocol for a partner.

To add a business location for a partner, perform the following steps:

Procedure

1. On the **Business Locations** tab, click **Add Location**.

   The **Add Location** dialog box is displayed.

2. In the **Add Location** dialog box, enter the following details:

Details

Field	Description
Location Name	Enter the name of the location.
Email	Enter the email ID.
Phone	Enter the contact number.
FAX	Enter the fax number.
Web URL	Enter the web URL.
Address	Enter the address.
Primary Legal Contact	Select the legal contact information from the drop-down list.
Primary Support Contact	Select the support contact from the drop-down list.

3. To assign either primary legal or support contacts to the business location, or to add contacts to the partner, click **New Contact** on the **Contacts** tab or click the **Add** icon in the **Primary Legal Contact** or **Primary Support Contact** fields and provide the following details:

Contacts

Field	Description
Contact Type	Select the type of the contact from the drop-down list: General, Support, Legal, or Business.
First Name	Enter the first name.
Last Name	Enter the last name.
Phone	Enter the contact number.

Field	Description
FAX	Enter the fax number.
Email	Enter the email address.

Your contact is displayed in the **Primary Legal Contact** and **Primary Support Contact** drop-down lists.

4. Click **Add.**

Deleting Business Locations

Procedure

1. In the **Business Locations** tab, to delete the business locations, select the business location you wish to delete from the table and click delete icon.

Deleting Partners

To delete one or more partners, perform the following steps:

Note: You cannot delete a partner, if a partner has a Business Agreement or associated with an external user.

Procedure

1. On the Partners page, select one or more partners that you wish to delete and then click **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Business Agreement Overview

A business agreement provides detailed information on which trading partners must agree before they can exchange business documents with each other.

For each protocol enabled for document exchange between the two participants, the following protocol-specific information is required:

- Transport method
- Valid operations
- Security

Note: Most of the information required to create a business agreement is protocol specific. Therefore, you need to fully configure both parties to the agreement.

The following tasks are required to create a valid business agreement:

- Identify the participants and define the agreement validity period.
- Configure a protocol.
- Configure an operation.

You can manage the business agreements as follows:

- Searching for a Business Agreement
- Creating a Business Agreement
- Configuring a Business Agreement
- Deleting Business Agreements

On the Business Agreements page, the protocols that are enabled for a business agreement are displayed in the **In Use Protocol** column. You can click the protocol link in this column in order to go directly to the respective protocol configuration page.

Note: To activate or deactivate a business agreement on the Business Agreements page, you can enable or disable the switch in the **Current Status** column in the table.

Searching for a Business Agreement

You can use the Search function to find a specific business agreement.

Procedure

1. Enter the search string in the Search field to search for a specific business agreement.

   The names of one or more business agreements that correspond to the search criteria are displayed.

Creating a Business Agreement

To create a new business agreement, perform the following steps:

Procedure

1. On the **Partner Management** tile, click **Business Agreements**.
2. On the Business Agreements page, click **Create Agreement**, which is in the upper-right corner of the page.
3. In the Create New Business Agreement dialog box, search and select the participants in the **Host** field and the **Partner** field between which you want to create an agreement.
4. After you have selected the host and the partner you want, click any one of the push buttons:

Option	Description
Done	To create the business agreement between the selected host and partner.
Proceed	To instantly configure the data of the newly created business agreement.

For detailed information on configuring the business agreement, see Configuring a Business Agreement.

5. After you have provided all the required information of the business agreement, click **Done**.

   The status of the newly created business agreement is enabled by default.

Configuring a Business Agreement

The configuring of business agreement includes tasks such as defining the agreement period, adding protocol bindings to a business agreement, and editing the protocol configurations.

To edit the business agreement data, perform the following steps:

> **Note:** You can either configure the data when creating the business agreement or later configure the data of the already-created business agreement.

Procedure

1. On the **Partner Management** tile, click **Business Agreements**.
2. On the Business Agreements page, select the business agreement whose information you wish to edit.

   The two tabs: Bind Protocol and Validity are displayed.
3. To configure the business agreement, provide information for the following tabs:

Option	Description
Bind Protocol	To add protocol bindings to a business agreement, click the **Bind Protocol** tab. For more information on configuring the protocols, see Adding a Protocol Binding.
Validity	To define the agreement period, click the **Validity** tab. For more information, see Defining Business Agreement Validity.

Adding a Protocol Binding

Before you begin

Both the host and the trading partner must have protocols enabled before you can add protocol bindings to a business agreement.
To add the protocol binding to the business agreement, perform the following steps:

Procedure

1. In the **Bind Protocol** tab, select the business protocols that are available to use as the binding protocol.

   The list of protocols shows only those protocols that are common for both the host and the partner participant.

2. To edit the configurations of the selected protocol, click the **Edit Configurations** tab.

   For more information regarding protocol configurations, see the other appropriate protocol specific documents.

3. Click **Done**.

Defining Business Agreement Validity

To define the validity of a business agreement, perform the following steps:

Procedure

1. On the Business Agreement page, click the agreement for which you wish to provide

the validity details.

2. On the **Validity** tab, enter the start date and end date manually or click the calendar pickers to define the exact period during which the agreement is valid.
3. Enable the **Active** switch, and then click **Done**.

Deleting Business Agreements

To delete one or more business agreements, perform the following steps:

Procedure

1. On the Business Agreements page, select one or more business agreements that you wish to delete, and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Business Protocols

Business Protocols are the standard methods used to exchange business documents between the participants. The host and the partner have to agree upon a common protocol before exchanging business documents or any operation in the transaction. This simplifies business transactions between the trading partners. For example, RosettaNet, X12, EDIFACT, and EZComm are the business protocols with their own specifications on how trading partners should send and receive business documents and its format.

On the Business Protocols page, you can see the list of installed protocols with their respective plug-in names and version numbers.

You can search a business protocol with the help of the **Search** function.

For more information on searching for a business protocol, see Searching for a Business Protocol.

Searching for a Business Protocol

You can use the Search function to find a specific business protocol.

Procedure

1. Enter the search string in the **Search** field to search for business protocols.

   The names of one or more business protocols that correspond to the search criteria are displayed.

Operations Editor

The operations editor allows you to configure operations for specific protocols. An operation is the sending or receiving of a business document and the required processing of that document. It is also the set of information required to send or receive, and process a business document.

Different protocols use different terminology to refer to operations. In the most simple case, an operation includes the following information:

- Name of the operation
- Document (an XML file that clearly defines the electronic document that partners exchange as part of this operation)
- Root XML element name (the top-level XML element in the document). See the following table:

Protocol-Specific Terminology

Protocol	Term for Operation
EZComm	Operation
RosettaNet	Activity
X12	Transaction
EDIFACT	Message
Gateway	Transmission

You can manage the operations as follows:

- Searching for an Operation
- Creating an Operation
- Importing Operations
- Deleting Operations

Searching for an Operation

You can use the **Search** function to find a specific operation.

Procedure

1. Enter the search string in the **Search** field to search operations.

   The names of one or more operations that correspond to the search criteria are displayed.

Creating an Operation

To create an operation, perform the following steps:

Procedure

1. On the **B2B Administration** tile, click **Operations Editor**.
2. On the **Operations Editor** page, select one of the protocols from the list for which you wish to add operations.
3. On the protocol-specific **Operations Editor** page, click the **Add** icon to add operation.

   For more information about adding operations, see the documentation provided for a specific protocol.

Importing Operations

You can import the operations using the **System Settings** tile.
For more information on importing the operations, see the *General Tab* on the System Settings page.

Deleting Operations

To delete one or more operations, perform the following steps:

Procedure

1. On the Operation Editor page, select a protocol for which you wish to delete an operation. On the protocol page, select an operation, and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Roles

Roles are created based on the user personas and are associated with each user.

You can manage the roles as follows:

- Searching for a Role
- Creating a Role
- Editing Roles
- Deleting Roles

On the Roles page, you can view the access rights set for a role by clicking the **Expand/Collapse Row** icon in the **Roles** column.

Searching for a Role

In addition to entering the name of the roles or selecting it from the list, you can use the **Search** function to find a specific role.

Procedure

1. Enter the search string in the **Search** field to search roles.

   The names of one or more roles that correspond to the search criteria are displayed.

Creating a Role

To create a new role, perform the following steps:

Procedure

1. On the **User Management** tile, click **Roles**.
2. On the User Roles page, click **Create Role**.

3. In the Create Role window, enter the name and description of the role you want to create and set its appropriate access rights. For more information on how to set the access rights, see Setting Access Rights for User Roles.

Editing User Roles

To edit any of the listed administrative user roles, perform the following steps:

Procedure

1. On the **User Management** tile, click **Roles**.
2. On the User Roles page, click any role you wish to edit from the **Roles** column.
3. On the **Edit Role** tab, modify the name and description and expand the **Access** tab to add or modify the access rights for the selected user role.

   For more information on how to set the access rights, see Setting Access Rights for User Roles.

Setting Access Rights for User Roles

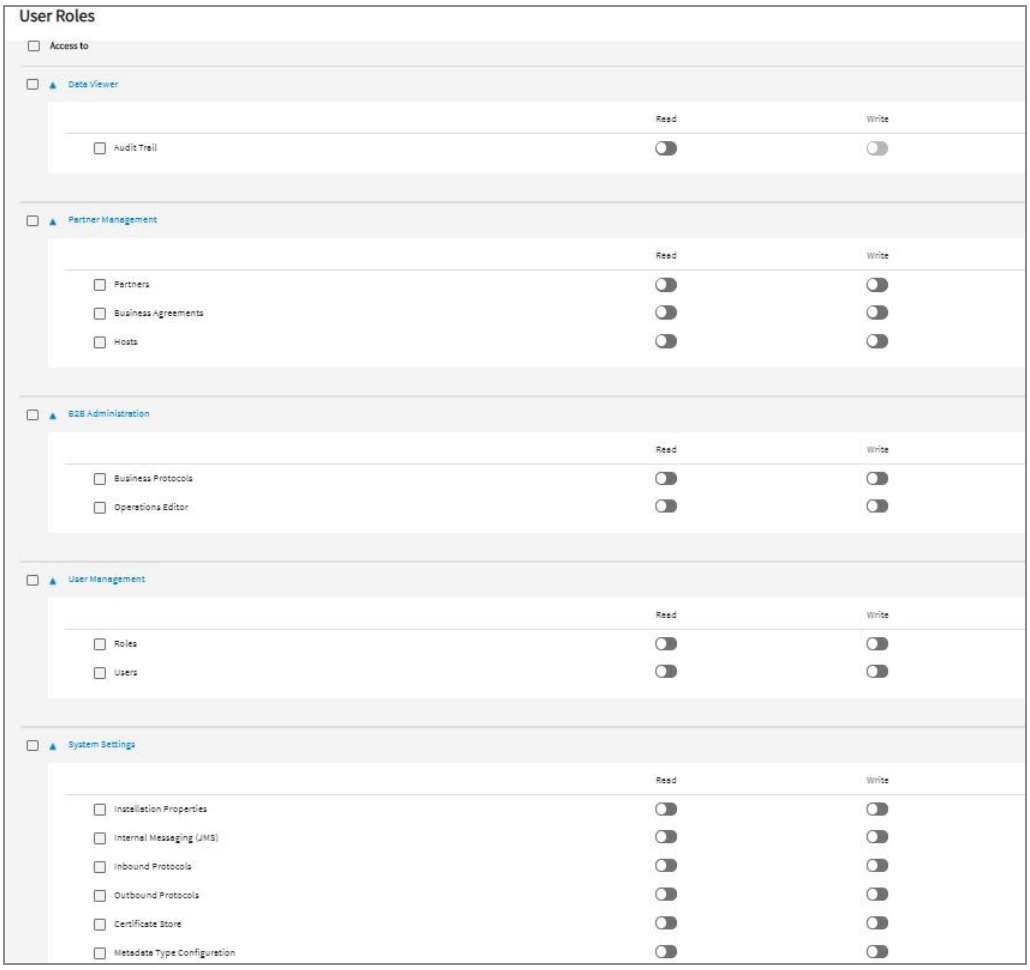
To set the access rights, log in as a user that has Admin access to the resources of TIBCO BusinessConnect Container Edition to which you wish to allow access for that user role.

> **Note:** You can enable these access rights for the user roles while creating new roles or while editing them.

To enable the access rights for the user roles, perform the following steps:

Procedure

1. On the **User Management** tile, click **Roles**.
2. On the User Roles page, click **Create Role** for creating a role or click any role from the list for editing them.
3. On the **Create Role** tab or **Edit Role** tab, enter the name and description of the role and expand the **Access** tab.



4. Select the appropriate check boxes for the different BusinessConnect Container Edition components to allow Read and Write privileges.

Deleting Roles

To delete one or more roles, perform the following steps:

Note: You cannot delete a role, if it is assigned to a user.

Procedure

1. On the User Roles page, select one or more roles that you wish to delete, and then click **Delete** icon.

2. On the pop-up dialog box, click **OK**.

Users

User Management allows you to create users, assign roles to the users, and assign access rights to different roles. You can give users Read or Write access to the TIBCO BusinessConnect Container Edition components. After creating users, you obtain a list of users with different access rights.

Note: You are required to update the email ID for the admin user which exists by default on the BusinessConnect Container Edition Users page.

There are two types of users available:

- Internal Users
- External Users

Internal Users

Internal Users in TIBCO BusinessConnect Container Edition are used for authentication of requests sent by Interior private process applications to manage participant, business agreement as well as operation level information for business protocols such as TIBCO BusinessConnect™ Container Edition - EDI Protocol powered by Instream®, TIBCO BusinessConnect™ Container Edition - RosettaNet Protocol, and TIBCO BusinessConnect™ Container Edition - Services Plug-in.

You can manage internal users as follows:

- Searching for an Internal User
- Creating an Internal User
- Editing Internal Users
- Deleting Internal Users

Searching for an Internal User

In addition to entering the name of the internal users or selecting it from the list, you can use the **Search** function to find a specific internal user.

Procedure

1. Go to **User Management > Users > Internal**.
2. Enter the search string in the **Search** field to search an internal user.

   The names of one or more internal users that correspond to the search criteria only are displayed.

Creating an Internal User

To create a new internal user, perform the following steps:

Procedure

1. On the **User Management** tile, click **Users**.
2. On the Business Connect Users page, click **Internal**.
3. On the **Internal** tab, click **Create User**.
4. In the Create New User window, enter the name, email ID, and password of the internal user.
5. Select any role from the list that you wish to assign to the internal user.

   All the access rights that are set to the role get automatically applied to the user.
6. Click **Save**.

Editing Internal Users

To edit any of the listed internal users, perform the following steps:

Procedure

1. On the **User Management** tile, click **Users**.

2. On the Business Connect Users page, click **Internal**.
3. On the **Internal** tab, click any internal user you wish to edit from the **User** column.
4. On the **Edit User** tab, modify the name, email ID, and password of the selected user. You can also modify the role assigned to that user.

Deleting Internal Users

To delete one or more internal users, perform the following tasks:

> **Note:** You cannot delete the Admin User.

Procedure

1. On the Internal tab, select one or more internal users that you wish to delete, and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

External Users

External users are specified only in the TIBCO BusinessConnect Container Edition Admin UI and they are associated with a trading partner, and not with a specific protocol.

You can manage external users as follows:

- Searching for a User
- Creating a User
- Editing Users
- Deleting Users

Searching for an External User

In addition to entering the name of the external users or selecting it from the list, you can use the **Search** function to find a specific external user.

Procedure

1. Go to **User Management** > **Users** > **External**.
2. Enter the search string in the **Search** field to search an external user.

   The names of one or more external users that correspond to the search criteria are displayed.

Creating an External User

To create a new external user, perform the following steps:

Procedure

1. On the **User Management** tile, click **Users**.
2. On the Business Connect Users page, click **External**.
3. On **External** tab, click **Create User**.
4. In the Create New External User window,
   a. Enter the name, last name, email ID, and password of the selected user.
   b. Select the name of the partner with which this external user will be associated.
5. Click **Save**.

Editing External Users

To edit any of the listed external users, perform the following steps:

Procedure

1. On the **User Management** tile, click **Users**.
2. On the Business Connect Users page, click **External**.
3. On the **External** tab, click the email ID of any external user you wish to edit from the **Email** column.
4. On the **Edit External User** tab, perform the following tasks:

a. Modify name, last name, email ID, and password of the selected user.

b. Modify the name of the partner with which this external user will be associated.

Deleting External Users

To delete one or more external users, complete the following steps:

Note: You cannot delete the Admin User.

Procedure

1. On the External tab, select one or more external users that you wish to delete, and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

User Groups

In TIBCO BusinessConnect Container Edition User Management, you can define groups to have particular access rights, and then internal users can be assigned to one or more groups. TIBCO BusinessConnect Container Edition groups are the equivalent of TIBCO Administrator roles and behave similarly but use the access rights which are specific to TIBCO BusinessConnect Container Edition.

You can manage user groups as follows:

- Searching for a User Group
- Creating User Group
- Editing User Groups
- Deleting User Groups

Searching for a User Group

In addition to creating a user group, you can use the **Search** function to find a specific user group.

Procedure

1. Go to **User Management > User Groups**.
2. Enter the search string in the **Search** field to search for a user group.

   The names of one or more user groups that correspond to the search criteria are displayed.

Creating User Group

To create a new internal user, perform the following steps:

Procedure

1. On the **User Management** tile, click **User Groups**.
2. On the User Groups page, click **Create User Group**.
3. In the **Create New User Group** window, enter name of the group, group description, and then click any one of the push buttons:

Option	Description
Done	To create the group.
Proceed	To instantly configure the settings of the new group.

4. For more information on configuring the user group, see Editing User Groups.
5. After you have provided all the required information, click **Done**.

Editing User Groups

To edit the settings of the user groups, perform the following steps:

Note: You can either configure the data when creating the user group or later configure the settings of the already created user group.

Procedure

1. On the **User Management** tile, click **User Groups**.
2. On the User Groups page, click the user group whose settings you wish to edit.

   The two tabs: Members and Partners are displayed.

Members Tab

The Members tab is used to add or remove group members.

Procedure

1. On the Members tab, click **Add New Users**.

2. In the pop-up dialog box, select the check box next to the users you want to join this group. These users have been previously generated. For more information, see Users.

You can select the Members check box for all the users to join the group.

Partners Tab

You can add or remove partners by using the Partners tab.

Procedure

1. On the Partners tab, click **Add New Partners**.
   The list of trading partners configured for the current TIBCO BusinessConnect Container edition installation is displayed.
2. In the pop-up dialog box, select the check box next to the partners you want to add to this group.

   You can select the **Partners** check box for all the partners to join the group.

Deleting User Groups

To delete one or more user groups, perform the following steps:

Procedure

1. On the User Groups page, select one or more user groups that you wish to delete, and then click the **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Audit Trail

The TIBCO AuditSafe is used to store information about the messages and documents processed by TIBCO BusinessConnect™ Container Edition.

Procedure

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

   The protocols you have installed are displayed on the Audit Trail page.

2. Click the protocol transaction you wish to see.

   For more information, see the protocol specific documentation.

System Settings

The System Settings tile provides you access to modify and configure different parameters such as transport protocols, servers, certificates, and metadata.

You can configure the following parameters:

- General
- Certificates
- Metadata Type Configuration
- Transport Protocols

General

The General tab allows you to manage the installation properties and internal messaging (JMS) using private process, Intercomponent JMS, and Intercomponent DMZ-JMS (Optional).

You can configure the following:

Installation Properties

Internal Messaging (JMS)

Installation Properties

You can modify the installation properties and import or export configuration data of TIBCO BusinessConnect Container Edition on the **Installation Properties** tab.

For more information of the fields, see the following table:

Installation Properties

Field	Description
Installation Name	The name of the BusinessConnect Container Edition installation. It names the installation automatically as BCCE-CONTAINER. You can change the name. **Note:** TIBCO BusinessConnect Container Edition uses the installation name within JMS subjects. If you rename the installation after deploying the BusinessConnect Container Edition server, subject names will be out of sync. Therefore, if you modify the installation name, export the Gateway Server token again after saving the changes, undeploy, and then redeploy the Interior Server and Gateway server.
Installation Prefix	The prefix BusinessConnect Container Edition appends to the subject of every message. The default value is AX.BCCE. **Note:** If you change the installation prefix after deploying the BusinessConnect server, subject names are out of sync. Therefore, if you modify the prefix, export the Gateway Server token again after saving the changes, undeploy, and then redeploy the Interior Server and Gateway server.
Description	An optional text description of the BusinessConnect Container Edition installation.

Import and Export Configuration Data

To import and export the configuration data, see fields in the following table:

Options	Descriptions
Import configuration	Imports configuration data from BusinessConnect like the `.csx` file, the `.bcce` file, and other configuration files. To import configuration data, perform the following steps: 1. In the **Importing Configuration Data** dialog box, click **Upload file**, go to your local directory to select the `.csx` file you wish to import, and click **Open**.

Options	Descriptions
	2. Enter a password (if required) and click **Start Importing**.
Export BCCE configuration	Exports configuration data from one BusinessConnect Container Edition to the other. 1. Go to **System Settings > General > Installation Properties**, and then click **Export BCCE configuration**. 2. A *installation_name*.bcce file is downloaded, where *installation_name* is the Installation Name entered in the **Installation Properties** dialog box.
Export GS configuration	Exports GS data from one BusinessConnect Container Edition to the other. To export GS configuration, perform the following steps: 1. Go to **System Settings > General > Installation Properties** and click **Export GS configuration**. 2. A GSToken.zip file is downloaded, which is required to be extracted, and files present in the folder are to be moved to the folder as mentioned in the README file for deployment.

Internal Messaging (JMS)

You can configure the JMS settings on TIBCO BusinessConnect Container Edition UI. To configure Private Process JMS, Intercomponent JMS, and Intercomponent DMZ-JMS (Optional) settings, go to **System Settings > Internal Messaging (JMS)** and click any tab you wish to configure the settings.

For more information, see *TIBCO BusinessConnect Container Edition, Administration Guide*.

Certificate Store

The Certificate Store page allows you to manage all credentials (certificates and private keys) and Server Identities and Certificates at one location. These credentials are owned by the participants.

For more information about certificates and security, see *TIBCO BusinessConnect Container Edition Security Guidelines*.

Note: To learn how to work with the keys, you can use the samples provided with this program in the directory `BCCE_HOME/samples/keys`. Ensure that the chosen password is `Password1`.

There are two tabs available:

- Credentials
- Server Identities & Certificates

Credentials

This tab allows you to add or to remove trusted root certificates from the system. Certificates are only valid if both trading partners trust the CA that signed the other's root certificate.

Uploading Server Certificate

To upload the server certificates, perform the following steps:

Procedure

1. On the **System Settings** tile, click **Certificates > Certificates Store**.
2. On the Certificate Store page, click the **Credentials** tab
3. On the Credentials tab, click the **Add** icon .

   The **Add Certificate Authority** option and the **Create New Identity** option are displayed.

Adding Certificate Authority

To add the certificate authority, perform the following steps:

Procedure

1. In the **Import CA Certificate** dialog box, enter the name of the certificate in the **Alias** field and click **Upload file** to browse and go to the file containing the certificate.
2. Click **Add**.

Creating New Identity

You can create new identities (private keys with X.509v3 leaf certificates) and add them to your system. To create a new public key certificate for your server, you will first create a Certificate Signing Request (CSR) and send it to a Certificate Authority (CA) for verification. When you create a CSR, a new private key is also created for decryption/ verification.

You will send the CSR, which only carries public information, to a CA. Once the signed certificate is returned, it is attached to the corresponding private key and this new identity becomes usable for decryption or verification, representing itself as stated in the certificate.

To create new identity, perform the following steps:

In the **New Identities** dialog box, enter the details as per the following table:

Field	Description
Alias	Enter the logical name of the host for which the certificate will be created using the verified certificate and the existing private key of the host. Example: MyCertificate.
Country Code	Only two digit entries are allowed, due to the restrictions posed by X.500. Example: US.
State	Enter the state where the host is located. Example: California.
Organization	Enter your company’s name. Example: Widgets Inc.

Field	Description
Organization Unit	Enter your organization unit's name. Example: HR.
Locality	Enter your locality. Example: San Jose.
Common Name	Fully qualified domain name (FQDN) of the server where the host is located. Example: widgets.com.
Key Length (bits)	Key length of the private key. Choose among 512, 1024, and 2048 bits. Example: 512.
Use Business Connect CA	Select the check box to enable CA.
Host	Select host from the drop-down list.

Searching Credentials

In addition to adding new credential or selecting it from the list, you can use the **Search** field to find a specific credential.

Procedure

1. Enter the name of the credential you wish to search.

   The names of one or more certificates that correspond to the search criteria are displayed.

Deleting Credentials

To delete one or more credentials, perform the following steps:

Procedure

1. On the **Credentials** tab, select one or more certificates that you wish to delete and then click the **Delete** icon..
2. On the pop-up dialog box, click **OK**.

Server Identities and Certificates

You can add an LDAP, a JMS, or an Email server certificate by using the **Server Identities and Certificates** tab. The JMS certificate is a credential of the JMS server, which is expected to be configured according to the corresponding guidelines. A server certificate is stored in the certificate store and must be created before it is assigned to a transport.

Adding Server Identities and Certificates

To create server identities and certificates, perform the following steps:

Procedure

1. On **System Settings** tile, click **Certificates > Certificates Store**.
2. On the Certificate Store page, click the **Server Identities & Certificates** tab
3. On the Server Identities and Certificates tab, click **add** icon .
   The **Add Third Party Server Certificate** option and the **Fetch Third Party Server Certificate** option are displayed.

Adding Third Party Server Certificate

To add third party server certificate, perform the following steps:

Procedure

1. In the **Add Third Party Server Certificate** dialog box, enter the name of the certificate in the **Alias** field and click **Upload file** to browse and navigate to the file containing the certificate.
2. Click Add
   The imported certificate will appear in the Name column on the Certificate page.

Fetching Third Party Server Certificate

Besides adding a server certificate, you can also fetch a server certificate in the **Fetch Third Party Server Certificate** tab.

For example, to fetch a Gmail SMTP server certificate, perform the following steps:

Procedure

1. In the **Fetch Server Certificates** dialog box, enter the name of the host (for example: smtp.gmail.com.)in the **Host** field and enter the port number (for example: 465) in the **Port** field.
2. Click Fetch

Searching Server Certificate

In addition to adding new server certificate or selecting it from the list, you can use the **Search** field to find a specific server certificate.

Procedure

1. Enter the name of the server certificate you wish to search.

   The names of one or more certificates that correspond to the search criteria only are displayed.

Deleting Server Certificates

To delete one or more server certificates:

Procedure

1. On the **Server Identities & Certificates** tab, select one or more certificates that you wish to delete and then click **Delete** icon..
2. On the pop-up dialog box, click **OK**.

Credential Expiry Alerter

The credential expiry alerter allows you to set up notification of expiring certificates, as well as for expired certificates that are still in the store. You can configure the following parameters:

- Polling interval: Checks the expiry dates of certificates at a specified interval.
- Number of days before a credential expires: Determine how far in advance you want

to know of an upcoming credential expiration.

- Notify email address: Sends the expiry notification to the specified email.

Note: To receive credential alert notification through emails, you have to configure the outbound SMTP proxy server.

Configuring the Credential Alerter

To configure the credential alerter, perform the following steps:

Procedure

1. On the **System Settings** tile, click **Credential Expiry Alerter**.
2. In the **Credential Expiry Alerter** dialog box, enter the details as per the following table:
3. *Credential Alerter*

Field	Description
Enable	Activate or deactivate the credential alerter by using the toggle.
Polling Interval (hours)	Specify the frequency with which the credential alerter keeps tracking and publishing alerts for the expiring credentials. The default value is 24 hours.
Days before Leaf Certificate Expiry	Specify the number of days before the leaf certificate expires.
Days before Key Expiry	Specify the number of days before the key expires.
Days before CSR Expiry	Specify the number of days before the CSR expires.

Field	Description
Days before CA Certificate Expiry	Specify the number of days before the CA certificate expires.
Notify email addresses	Provide one or more comma-separated email addresses for notification. **Note:** The email addresses must be different from the email addresses that you entered for the inbound mail POP3 servers. For more information, see *Inbound Mail POP3 Servers*.
From email addresses	Specify the initiating email address.

4. Click **Save** to save the values entered.

Transport Protocols

You can use **Transport Protocols** tab to configure the following types of protocols:

- Inbound Protocols
- Outbound Protocols

Inbound Protocol

The following inbound transport protocols are available for TIBCO BusinessConnect Container Edition:

- Email
- File
- FTP and FTPS

- SSHFTP
- HTTP, HTTPS, HTTPSCA

Each of the public transports can be enabled or disabled by selecting the appropriate check box associated with a specific transport.

Outbound Protocol

The following outbound transport protocols are available for TIBCO BusinessConnect Container Edition:

- FILE
- EMAIL
- Outbound HTTP/FTP Proxy and Mail SMTP Servers

Others

You can use **Others** tab to configure the following:

- Metadata Type Configuration
- Activate Protocol Plugins
- User Authentication Configuration
- Smart Routing

Activate Protocol Plugins

You can manage BusinessConnect Container properties by using the **Activate Protocol Plugins** tab. All the installed and activated protocols are displayed on the Activate Protocol Plugins page. In this window, you can perform the following tasks:

• Verify the names and the versions of installed protocols.

• Add, change, or remove TIBCO BusinessConnect Container Edition or protocol specific properties.

Activated Protocol Plug-ins and Properties

Plug-in	Title	Protocol
BCCE	BusinessConnect Container Edition **Note:** The default properties of TIBCO BusinessConnect Container Edition cannot be deleted by a user. For more information, see Editing Plug-in Properties.	• TIBCO BusinessConnect Container Edition AS1 Transport • TIBCO BusinessConnect Container Edition AS2 Transport
EZComm	BusinessConnect Container Edition - Services Plug-in	EZComm
RosettaNet	BusinessConnect Container Edition - RosettaNet Protocol	RosettaNet
tibEDI	BusinessConnect Container Edition - EDI Protocol powered by Instream	• EDIFACT • Gateway • X12

Managing Plug-in Properties of TIBCO BusinessConnect Container Edition

You can add, delete, and edit the Plug-in Properties of TIBCO BusinessConnect Container Edition.

Adding a Property

To add a property to any of the listed protocol plug-ins, perform the following steps:

1. In the Edit BCCE Plugin Settings, click **Add Property**.
2. Enter or select information as explained in the following table:

Adding New Property

Field	Description
Property Name	Specify the name of the property.
Property Type	Select a data type from the drop-down list: Boolean, String, or Integer.
Description	Specify description of the new property.

Editing Plug-in Properties

To edit the properties, perform the following steps:

1. On the Activate Protocol Plugins page, click **BCCE**.
2. In the **Edit BCCE Plugin Settings** dialog box, configure the properties as explained in the following table:

TIBCO BusinessConnect Container Edition Properties

Label	Field	Description
Database	bc.db.maxretry	The maximum number of retries for a database connection in case of failures. The default value is 3.
	bc.db.sleep.between.retry	The time interval between the successive attempts of connection in milliseconds. The default value is 1000.
	bc.db.auditlog.style	The format in which the audit and non-repudiation data is stored: Uncompressed or Compressed. Messages are compressed to save disk space, which also triggers the overhead

Label	Field	Description
		of compressing the messages. Therefore, choosing whether messages are stored in compressed or in uncompressed format depends on the priorities for a specific server: saving disk space or keeping better performance. **Note:** This property cannot be changed dynamically: the TIBCO BusinessConnect Container Edition server has to be restarted for this property to take effect.
HTTP	bc.http.threadPool.maximum	The maximum number of threads used for Outbound HTTP (or HTTPS) requests. The default value is 32.
SSL Caching	bc.ssl.disableSessionCache	Disables the session cache for outbound HTTPS and FTPS. HTTPS (SSL) transport endpoints (HTTPS, AS2-HTTPS) and FTPS use an internal SSL transport cache to significantly improve the performance of negotiating security parameters while establishing trusted connections. In some situations, problems might arise when third party server implementations are not able to properly handle cached sessions or renegotiation of security properties at the beginning of each application level communication session. For example, when the Initiator always wants to ensure that the peer's credential is the one that is trusted and has not changed during any cached session. The cache usually holds successfully negotiated

Label	Field	Description
		security parameters for about 5 minutes, so that large numbers of transactions between the Initiator and any given trading partner require a credential renegotiation in approximately 5 minutes. For TIBCO BusinessConnect Container Edition to enforce the renegotiation of the peer's credentials, this check box can be selected for any individual outgoing transport. If selected, each time TIBCO BusinessConnect Container Edition has business data to be delivered to the corresponding trading partner, the peer's credentials are requested and verified. **Note:** When session caching for outgoing HTTPS/FTPS transports is disabled, performance can be significantly degraded and this should be done only if there are known problems with the involved third party server application's handling of SSL session caching.
IPFilter	bc.ipfilter.enabled	Enable or disable the Gateway Service Network filtering.
	bc.ipfilter.default.noMatchPolicy	Default IP Filter Policy when no matching rules are evaluated on an inbound Gateway Service request where applicable. You can select Accept or Deny from the drop-down list.

Label	Field	Description
		On the Gateway engine, when the incoming trading partner IP address does not match any of the IP filters available at the Gateway Instance, then this selected no matching policy is evaluated to Accept the request or Deny the request. On the Interior server side, when the trading partner IP address does not match any available IP filters on the trading partner level, then this no matching policy is evaluated to either Accept the request or Deny the request
Scheduler Poller	bc.task.scheduler.polling.interval	The scheduler polling interval in seconds. The default value is 60.
Queue Poller	bc.queue.poller.enabled	Enable or disable the message queue poller. The Queue Poller monitors the message queue table to schedule sets of transactions to be sent as batches. By default, this property is enabled.
	bc.queue.poller.pollingInterval	The queue poller polling interval in seconds. The default value is 60.
MDN Poller	bc.mdn.poller.enabled	Enable or disable the MDN timeout poller. The MDN poller should be enabled when you use asynchronous MDNs (receipts) with the standard Email, AS1 Email or

Label	Field	Description
		AS2 HTTP/S transports. The MDN poller checks for expired receipt requests. By default, this property is enabled.
	bc.mdn.poller.pollingInterval	The MDN Poller Interval in seconds. The polling interval specified determines the number of checks TIBCO BusinessConnect Container Edition does for expired receipt (MDN) requests for the standard Email, AS1 Email and AS2 transports. A shorter polling interval allows MDN timeouts to be detected closer to the timeout period configured in the Receipt Timeout field of the Email, AS1, and AS2 transports. The polling interval should be less than or equal to the smallest timeout period specified in the Receipt Timeout field amongst all of the configured Email, AS1 and AS2 transports. The default value is 300.
Terminator Poller	bc.tx.terminator.enabled	The terminator poller is used to monitor the Poller table for any pending transactions that have been marked for termination by a user. By default, this property is enabled.
	bc.tx.terminator.pollingInterval	The polling interval of the terminator poller is responsible for terminating transactions that were marked for termination from the UI. The default value is 60.

Label	Field	Description
Resend Poller	bc.tx.resend.enabled	Enables or disables the resend poller. The resend poller is used to monitor the Resend table for any transactions that have been marked for resending by a user. By default, this property is enabled.
	bc.tx.resend.pollingInterval	Resend polling interval in seconds. Transactions can be selected and sent again from the UI. TIBCO BusinessConnect Container Edition keeps polling for such transactions at a regular interval, so that it can collect them and send them as requested. The polling interval specifies the look up frequency for the transactions that are sent. The default value is 120.
	bc.tx.resend.messagesPerPoll	This property specifies the maximum number of messages that BusinessConnect Container Edition sends again during one polling cycle. If there are many messages that need to be sent, memory is heavily utilized to reprocess them all at once. For example, if 2,000 transactions are selected for resend, they pick up 500 at a time until there are no more transactions to be sent again. This property along with the property `bc.tx.resend.pollingInterval` makes it possible to fine tune resend behavior by limiting the maximum number of messages to be processed in one polling

Label	Field	Description
		cycle. The default value is 500.
Hibernation Poller	bc.hibernation.pollingInterval	The Hibernation Poller periodically looks for hibernated messages that have exceeded their expiration time. A message is put into hibernation because it is waiting for a response from a trading partner. The request message from the Request/Reply transaction is put into hibernation until the reply is received or the reply timeout is exceeded. The request message from a receipt request for the standard Email, AS1 Email or AS2 HTTP/S transports are put into hibernation until the receipt is received or the receipt timeout is exceeded. The Hibernation Polling interval specifies how long TIBCO BusinessConnect Container Edition sleeps between each polling cycle for expired hibernated messages. The default value is 75.
	bc.hibernation.mode	Two hibernation modes are available: • db • ascache
FTP Poller	bc.ftpget.poller.enabled	Enables or disables the FTP Poller. By default, this property is enabled.
	bc.ftpget.poller.pollingInterval	FTP polling interval in seconds. The polling interval specifies how long TIBCO BusinessConnect Container

Label	Field	Description
		Edition sleeps between each cycle of retrieving files from the trading partners FTP sites. The default value is 120.
	bc.ftpget.timeout	FTP timeout in seconds. The value specified is used to set the socket timeout for an FTP GET command. The FTP GET command terminates if it does not complete within the timeout period. The default value is 300.
	bc.ftpget.workers	Max FTP/SSHFTP Workers per polling cycle. Each polling cycle can utilize one or more workers. Each worker can process an FTP/S or SSHFTP poller at a time and they are executed concurrently. One polling cycle checks if every participant's transport (that wanted to use the poller) has completed the polling cycle. For example, if you set up FTP GET (or SSHFTP GET) for 10 participants and specify 5 workers, then the 10 tasks will start processing with no more than 5 polls being executed at any given time. If no participant's transport is waiting for the execution, the polling cycle ends and the next cycle starts in the similar fashion as required by the polling interval. The default value is 5.

Label	Field	Description
	bc.ftp.enablecmd.passive	Enable the FTP Passive mode. In the FTP Passive mode, the FTP client initiates both data and command connections to the remote FTP server. By default, this property is enabled.
	bc.honorThreshold	Honor Inbound Threshold for FTP Large Files. When selected, this check box directs TIBCO BusinessConnect Container Edition to honor the preset inbound threshold for the large file sizes using FTP. If you change this setting, be sure to restart the BusinessConnect Container Edition for the changes to take effect. By default, this property is enabled.
SSHFTP	bc.sshftp.cache.tunnel	SSHFTP Tunnel Max Inactive Life in minutes. Only one SSH tunnel (per transport) exists between a host and a participant. If this tunnel is inactive for a longer time than described by this parameter, BusinessConnect Container Edition removes the tunnel and creates a new one, next time the BusinessConnect Container Edition needs to send or receive messages. If the tunnel is removed earlier because of other problems, such as the trading partner closed it or a disconnection occurred, BusinessConnect Container Edition will try to create a new tunnel automatically and fall back to that if possible.

Label	Field	Description
		The default value is 120.
EDIINT	bc.ediint.streamSize	A message size threshold. When reached, it will cause messages to be stored in temporary files on the file system while they are being processed, instead of being stored in memory. Consider setting this property to a low value when processing large messages, since it will help to conserve system memory. The default value is 5000000
	bc.ediint.suppress.foldedheader	Enabling this property removes any embedded CRLFs from the content-type header field of the following types of outbound HTTP messages: Signed messages and Message Disposition Notifications (receipts). The resulting content-type header are all on one line. This property can be set for a specific trading partner by creating a Boolean property with the following name format: `bc.ediint.suppress.foldedheader.<tpName>` Any spaces in the trading partner name should be replaced with underscores (_) when specifying the name of the property. By default, this property is enabled.
	bc.ediint.as2.inbound.filename.preservation	Enable file name preservation for the inbound AS2 Messages. If enabled, all inbound AS2 messages with a content

Label	Field	Description
		disposition type of “attachment” is stored on the file system after unpackaging. Files are stored in the shared directory for BusinessConnect Container Edition, under a subdirectory for the trading partner, and by date in the following way: If a file name has been specified in the content disposition header, it will be used when storing the message. If the file name already exists for that trading partner and date, it is generated based upon the filename specified in the content disposition header and has the following form: <specified filename base>_ <TP name>_ <GUID>_<inbound file number>.<specified filename extension> If a file name extension is not specified, none is used. **Note:** Various operating systems restrict the characters used in file names. Therefore, TIBCO BusinessConnect Container Edition does not allow use of the following characters in file names: embedded quotes, <, >, ?, :
	bc.ediint.as2.outbound.filename.preservation	Enable file name preservation for the outbound AS2 Messages. If enabled, BusinessConnect Container Edition will try to package all outbound AS2 messages as attachments with file names by including a content disposition header of the following form:

Label	Field	Description
		`Content Disposition: attachment;filename=specified_filename` The value of specified_filename is taken from the file name specified in the content disposition field of the message INITIATOR.REQUEST. If the outbound File poller is used to pass messages from the private process to BusinessConnect Container Edition, the name of the file containing the message from the outbound File poller is used as the value of specified_filename in the content disposition header. **Note:** Various operating systems restrict the characters used in file names. Therefore, TIBCO BusinessConnect Container Edition does not support the use of the following characters in file names: embedded quotes, <, >, ?, :
	bc.ediint.digestAlgorithmEnabled	Determines whether the AS1 and AS2 transports use the SHA1 message digest algorithm or pick up the digest algorithm setting from the Business Agreements. By default, `bc.ediint.digestAlgorithmEnabled` is disabled and the AS1 and AS2 handlers will always use SHA1 for the message digest algorithm as recommended by their respective specifications.

Label	Field	Description
DDTP	bc.ib.channel.force.plain	Gateway Server and Interior Server can use plain HTTP connections for DMZ Data Transfer Protocol (DDTP) data transferring after you enable this property in TIBCO Admin UI and set the value of the `java.property.bc.ib.channel.force.plain` property in all gsengine.tra files to true separately. This implementation reduces the communication time between Gateway Server and Interior Server when high performance is required and the data transfer security across the inner firewall is not a big concern. By default, this property is disabled.
	bc.ib.channel.maxProcessor	This property applies to the Interior Servers and is used to specify the maximum number of threads that each Interior Server can use to handle DDTP data transferring between Interior Server and Gateway Servers using the data-tunneling. The data streaming can come from Gateway Server or go to Gateway Server and eventually go to trading partners when trading partners download files using the SSHFTP or FTPS service. The default value of this property is 5. You can increase this value when high volumes or large payloads are processed. When you set a value for this property, it is good practice that the total value of this property in all Interior

Label	Field	Description
		Servers is close to the total value of the `java.property.gs.webengine.ddtp.maxProcessor` property in all Gateway Servers.
Miscelleneous	bc.useFLock	Two options are available in the drop-down list: File and Database. In TIBCO BusinessConnect Container Edition, some functions use locks to achieve synchronization among the servers. If you install TIBCO BusinessConnect Container Edition on a Linux platform, it is good practice to use the database-based lock instead of the file-based lock because the file-based lock is not stable. **Note:** If you deploy TIBCO BusinessConnect Container Edition in load balancing mode, you must set this property to the database-based lock.
	bc.securityLevel	Security Level when connecting to an HTTPS server. Select from the drop-down list: HIGH or LOW. All leaf certificates need to be checked and this value determines how the certificates are checked. This property is selected only on the client side and has the following values: • **LOW**: Used when testing with sample certificates. When the value is LOW, the

Label	Field	Description
		host name authentication is not done. • **HIGH**: Default setting. BusinessConnect Container Edition validates the remote server certificate to ensure that the host registered with that certificate is the same as the one receiving the POST: the certificate CN (common name) must match the URL host name.
	bc.securityVendor.sockets	Security vendor for inbound and outbound socket operations. Select SUN or IBM.
	bc.security.restrict	Version Security level is restricted to the specified version or later. The options available in the drop-down list are: All, SSLv3, TLSv1, TLSv1.1, or TLSv1.2. **Note:** If you select TLS version 1.1 or 1.2, you have to select SUN or IBM as the security vendor for inbound and outbound socket operations.
	bc.security.sslv2hello.enabled	Enables SSL agreement authentication between trading partners.
	bc.maxAuditLog.EntriesPerView	Maximum Log Viewer entries per view. You can set this value to control how many rows of data should be returned from the audit/non-repudiation database for viewing.

Label	Field	Description
		Note: If this value is set too high, it might consume all the available memory and put the system at risk. The default value is 300.
	bc.repo.fetch.limit	This property is used to limit the number of configuration items fetched and displayed initially when you open certain configuration pages. In systems with a large amount of configuration items, such as a large amount of users, participants, or business agreements and other items, the page response time is improved. The default value of this property is 500. Because only a limited amount of configuration items are fetched from the configuration store and displayed on the configuration page, you cannot paginate the displayed items beyond the limit. If a large amount of items are stored in the configuration store, you have to use the Search function to fetch the items you want.
Jasper	bc.repo.jasper.fetch.limit	The property is used to limit the number of records that are fetched for JasperReports Tabular data. The default value of this property is 500.
Inbox Transport	bc.inbox.sendEmail	Sends an Email to the Partner on successful Inbox storage when using Inbox Transport as the primary transport.

Label	Field	Description
	bc.inbox.notify.payload.Timeout	Default time for the Notify transaction payload to reside in Inbox before it is purged in minutes. The default value of this property is 1440.
	bc.inbox.response.payload.Timeout	Default time for the Response transaction payload to reside in Inbox before it is purged in minutes. The default value of this property is 1440.
File Based	bc.filebased.sfws.enabled	
	bc.filebased.sfws.threshold	
	bc.filebased.sfws.storelocation	
LDAP Configuration	bc.ldap.rolebasedn.attribute	The distinguished name of an LDAP entry that contains the role entries. For example, the following information can be a roleBaseDN: `CN=Users,DC=adldap,DC=com` The parts DC=adldap and DC=com are optional for the baseDN entry. The part CN=Users is mandatory, unless a role entry is created in baseDN. For more information, see Adding an Authentication Source.

Label	Field	Description
		Note: Ensure that an entry is created under the Base DN, which is specified in the **Base DN** field in the LDAP server configuration, on the LDAP server before you specify a value cn=entry_name for this property. The entry must have the object class organizationalRole on the Open LDAP server or IBM Tivoli Directory LDAP server, Container on the Microsoft Active Directory LDAP server, and nsContainer on the Sun ONE LDAP server.
JMS Configuration	bc.jms.destination.cache	A JMS destination cache is created after you enable this property. By using the cache, Interior Server does not have to discover the JMS destinations every time when it sends messages to a private process by using the JMS transport. This implementation improves the communication performance between Interior Server and the JMS server, and it is effective if the related EMS destinations used by the JMS server are not updated frequently. By default, this property is enabled.
TAS Audit Log	bc.auditlog.messageInAsync	This property specifies whether to save transaction messages in the audit log asynchronously. By default, this property is disabled.

Label	Field	Description
		Note: With the properties of bc.auditlog.messageInAsync, bc.auditlog.messageInAsync.maxMessages, bc.auditlog.messageInAsync.maxTotalSize, and bc.auditlog.messageInAsync.threadpool.size, you can save transaction messages in audit logs asynchronously. This function is useful when the message size is large and the database connection is not good, but fast delivery or quick response is required. When using this function, you must be cautious with the system memory consumption because more memory is consumed as a cache to temporarily store messages before the messages are written to the database.
	bc.auditlog.messageInAsync.maxMessages	This property specifies the maximum number of messages in asynchronous message audit log queue. The default value of this property is 2000.
	bc.auditlog.messageInAsync.maxTotalSize	This property specifies the maximum size of memory in MB that can be used for asynchronous message audit log. The default value of this property is 128. The limit for messages is controlled by both the maxMessage and maxTotalSize properties. The property that first

Label	Field	Description
		reaches the limit condition takes effect.
	bc.auditlog.messageInAsync.thread pool.size	This property specifies the size of thread pool that can be used for consuming the messages stored in memory temporarily and writing the messages to the database. The default value of this property is 10. You can increase this value if the memory occupied by the messages increases.

Note: For detailed information on editing the protocol plug-in properties, see the appropriate documentation for the specific protocol.

Deleting a Property

To remove the newly added properties, click Delete icon of the property you wish to delete in the **Edit BCCE Plugin Settings** dialog box.

Note: You can remove only user defined properties; default properties cannot be removed.

Metadata Type Configuration

The functionality in this section is protocol-specific:

RosettaNet Roles: Supported by RosettaNet. Roles display in the Roles tab for a host and trading partner and the Activity tab in the operations editor. Roles are explained in TIBCO BusinessConnect Container Edition - RosettaNet Protocol User Guide.

Domains: Supported by TIBCO BusinessConnect Container Edition Services Plug-in, TIBCO BusinessConnect Container Edition - RosettaNet Protocol, and TIBCO BusinessConnect™ Container Edition - EDI Protocol powered by Instream®, X12 variant. Each trading partner

involved in the exchange of documents has a domain. Look in the User's Guides for each of these protocols for more information.

RosettaNet Partner Classification Codes: Supported by RosettaNet. Example: Buyer. Partner Classification Codes are explained in TIBCO BusinessConnect Container Edition - RosettaNet Protocol User Guide.

RosettaNet Supply Chain Codes: Supported by RosettaNet. Example: Electronic Components. Supply Chain Codes are explained in TIBCO BusinessConnect Container Edition - RosettaNet Protocol User Guide.

Adding and Removing Metadata

You use the TIBCO BusinessConnect Container Edition UI to maintain RosettaNet roles, domains, partner classification codes, and supply chain codes.

After changing any of these items in the configuration store, the new options become available in the TIBCO BusinessConnect Container Edition UI. You can then use the new values in setting up the host or a trading partner.

To manage RosettaNet roles, partner classification codes, supply chain codes, and domains to the configuration store, perform the following steps:

1. On the **System Settings** tile, click **Metadata Type Configuration**.
2. To add new metadata, click the **Add** icon and perform the following tasks:
    - For creating new Domains, Partner Classification Codes, Supply Chain Codes: Enter name and description in the respective dialog boxes.
    - For creating RosettaNet Roles: Enter the name in the **Create RosettaNet Role** dialog box.
3. To delete any one of the data for RosettaNet roles, partner classification codes, supply chain codes, and domains, click the desired tab, select the data you wish to delete and click delete icon.
4. To search metadata value, enter the desired value in the **Search** field.

User Authentication Configuration

User Authentication Configuration allows you to add or remove the user authentication source for TIBCO BusinessConnect Container Edition. The user authentication source types

are as follows:

- Open LDAP server, which is used only for external users.
- TIBCO BusinessConnect Container Edition database, which is used both for internal and external users.

The user authentication sources are listed by priority on the User Authentication Configuration. At run time, the external user is authenticated against the source in the top to bottom order. However, when you manage the users on the **User Management** > **Users** page, only the source at the top is considered as the target source in your management activities.

You can manage the user authentication as follows:

- Searching for an LDAP Server
- Adding an Authentication Source
- Editing an Authentication Source
- Deleting Authentication Source

Searching for an LDAP Server

You can use the Search function to find the configured LDAP server.

- Enter the search string in the **Search** field to search configured LDAP server.

Adding an Authentication Source

To add an authentication source, perform the following steps:

1. On the **System Settings** tile, click **User Authentication Configuration**.
2. Click the **Add** icon in the User Authentication Configuration page.
   There are two types of authentication sources available:

- LDAP Server
- BC Database

Note: By default, the BC Database is available on the User Authentication Configuration page whereas the LDAP server is displayed in the **Source Alias** column after you configure it.

LDAP Server

In the **New Ldap Server** dialog box, enter the following information:

LDAP Server Settings

Field	Description
Alias	Alias name for the LDAP server.
Host Name	The IP address or name of the machine on which the LDAP server is deployed.
Port Number	The port number used for connecting to LDAP.
Bind DN and Bind Password	The LDAP server's Bind DN. The base DN is an X.500 distinguished name, which denotes the sub-tree of an LDAP directory where the to-be-authenticated user records are posted, such as: `ou=people,dc=unit,dc=company` The Bind DN provided can be an LDAP user that has both read and write permissions to LDAP. The user needs permission to: • Read and write LDAP user objects • Read and write LDAP group objects Authenticate other users to LDAP (that is, call the LDAP authenticate API or have read access to the password/credentials of LDAP user objects).
Base DN	Added prior to Bind DN when searching for users. This is the starting point in the LDAP hierarchy at which the search begins.

Field	Description
User Search Filter	You can specify a user search filter and only users that have the specified attribute are returned. Using the defaults for the user search filters, all users are returned. For example: • Base DN: `dc=na,dc=tibco,dc=com` • User Search Filter: `objectclass=person`
User Name Attribute	Provide the LDAP attribute name that represents the user name in the LDAP directory server. It is good practice to use the value of `cn` for all the supported LDAP servers.
User to Group or Role Membership Attribute	Provide the LDAP attribute that represents the User to Group (or Role) membership attribute in the LDAP directory server. The value for this attribute lists the Groups or Role the user is enrolled for the DN. **Note:** Different LDAP servers have different User to Group or Role membership attributes. For example, specify the value of memberOf for the Open LDAP server or Microsoft Active Directory LDAP server, nsrolsedn for the Sun ONE LDAP server, and ibm-allGroups for the IBM Tivoli Directory Server.
isSecure	Select this check box to check whether this is a secure LDAP URL.
isEnabled	Select this check box to check whether the LDAP connection is enabled. No operations are permitted for disabled connections.
isReadOnly	Select this check box to check whether the LDAP

Field	Description
	connection has Read Only permission. Read-only LDAP connections permit only read operations. However, read-only LDAP connections can update passwords.
Server Certificate	The server certificate used for secure LDAP communication. Select one of the certificates that was configured under **System Settings** > **Certificate Store** > **Server Identities & Certificates**.
Test Connection	Click the **Test Connection** tab to verify whether the connection works. If the test is not successful, review the configuration steps.

Note: The distinguished name of an LDAP entry that contains role entries must be set.

For more information about the LDAP Role BaseDN Attribute, see Activate Protocol Plugins, LDAP Configuration.

BC Database

The BC Database option is added by default when a user chooses it and uses it as a source of user information.

Authentication Source Defaults

The added and configured authentication sources are displayed in the **Source Alias** column. TIBCO BusinessConnect Container Edition uses the sources to authenticate the external users as per the order in which all the sources are listed or as per the status of the source (enabled or disabled).

For example, if you add BC Database and then LDAP as authentication sources, BCDB (the BC Database alias) is listed first in the **Source Alias** column and LDAP is listed second in the **Source Alias** column.

When authenticating external users, TIBCO BusinessConnect Container Edition uses BCDB first. If authentication fails with that source, TIBCO BusinessConnect Container Edition retries the authentication using LDAP.

You can use **Move Up** and **Move Down** options or drag and drop the sources in the **Source Alias** column to adjust the priority of the authentication source.

Editing an Authentication Source

To edit the configured LDAP server or a BC Database, perform the following steps:

1. On the User Authentication Configuration page, click any authentication source in the **Source Alias** column.
2. Based on your selection of the authentication source, perform the following:

- For LDAP Server: Modify the data in Edit Ldap: *Alias* dialog box. For the more description of the fields, see Adding an Authentication Source table.
- For BC Database: Modify the alias in the Edit Ldap: *Alias* dialog box.

Deleting Authentication Source

To delete one or more authentication sources:

1. On the User Authentication Configuration page, select the configured LDAP server or a BC Database and click the **Delete** icon.

2. On the pop-up dialog box, click **OK**.

Smart Routing

In TIBCO BusinessConnect Container Edition, you can define business rules to route messages to specific private processes. For more details, see *TIBCO BusinessConnect Container Edition Concepts, Smart Routing*.

Private Process Smart Routing

You can perform following tasks on the business rules for Private Process Smart Routing:

- Searching for Business Rules
- Creating New Business Rule
- Managing Business Rules
- Editing Business Rules
- Deleting Business Rules

Searching for Business Rules

You can use the Search function to find a specific business rule.

Enter the search string in the **Search** field to search a business rule.

The names of one or more business rules that correspond to the search criteria are displayed.

Creating New Business Rule

A smart routing business rule defines a smart ID and a set of conditions to which BusinessConnect Container Edition can compare all the messages.

To create a business rule for Smart Routing, perform the following steps:

1. In the Admin UI, go to **System Settings** > **Smart Routing** > **Private Process Smart Routing**.
2. In the Private Process Smart Routing window, click the **Add New Smart Route** tab or the **Add** icon.
   The **New Entry** dialog box is displayed.
   In the New Entry dialog box, enter the following information:

New Rule for the Private Process Smart Routing

Field	Description
Enabled	Select this check box to enable the new Smart Routing rule.
Protocol	Choose the protocol for the message from the drop-down list. To select all the protocols from the list, select the asterisk character (*).
From (Required)	The name of the trading partner that sends the original message. If Host (your company) sends a request to Partner and Partner sends a response, you might want to use Smart Routing for the response. In this case, this field is matched by Host because Host is the originator of the business transaction. Use the asterisk character (*) to match all hosts and partners, but do not use the asterisk character with a string. For example, do not use TIB*.
To (Required)	The name of the trading partner that receives the original message. If Partner sends a request to Host (your company), you might want to use Smart Routing for the request. In this case, this field is matched by Host because Host is the recipient of the request. Use the asterisk character (*) to match all hosts and partners, but do not use the asterisk character with a string. For example, do not use TIB*.

Field	Description
Direction	Choose the business direction of the message as follows: • Inbound: If a Partner sends a request to a Host (your company), both the business direction and the message direction are inbound. • Outbound: If a Host sends a request to a Partner and the Partner sends back a response, the message direction of the response is inbound and the business direction of the response is outbound because the original message was outbound. • * : The asterisk character selects both the directions.
Operation ID (Required)	Enter the location and identifier of the operation. This takes the form of a series of nodes. For example: BC/1.0/Notify. Use one asterisk character (*) to match all the operations directly under a specific node. For example: BC/*/* matches BC/MyNotify/Test but not BC/MyNotify/Test/notify1 Use two asterisk characters (**) to match operations recursively. Use double asterisks alone or use

Field	Description
	them as the last node. For example: BC/MyNotify/** matches BC/MyNotify/1.3/Test BC/MyNotify/**/notify1 and is same as BC/MyNotify/**. The software ignores any nodes after the double asterisk. You can use both a single asterisk and a double asterisk. For example: BC/*/1.0/** matches BC/Test-01/1.0/A/B
CMName	Enter the name of the listening CM (certified messaging) transport for the private process. If you provide the CM name for the listening CM transport, BusinessConnect Container Edition pre-registers the CM name, assuring creation of a ledger and persistence of messages in the event that the listening transport is down. If the CM name is not preregistered, BusinessConnect Container Edition has not created a ledger, and the listening CM transport is down, the messages do not persist.

Field	Description
	Note: Do not use the asterisk character (*) in this field. Verify the accuracy of the CM name before deploying the rule. If the CM name you provide does not exist, the ledger increments indefinitely.
Smart ID	Enter an ID for smart routing business rule. You can enter any combination of alphanumeric characters with a minimum of one character and a recommended maximum of 25 characters.

4. Click **Add**.
The rules that you create are displayed in the Private Process Smart Routing window, with a serial number associated for each rule.

Managing Business Rules

After the rules for Private Process Smart Routing are added, they are displayed on the Private Process Smart Routing page with their serial numbers.

You can manage the order of the business rules in the **Serial Number** column by using the following tabs:

• **Move To**: Select the overflow menu next to the serial number and to click this tab.

In the **Move Route** dialog box, enter the index number at which you want to move the business rule.

• **Insert After**: Select the overflow menu next to the serial number to click this tab.

The **New Entry** dialog box is displayed for you to add a new rule.
For more information, see Creating New Business Rule.

Editing Business Rules

To edit a Business Rule, perform the following steps:

1. In the Admin UI, goto **System Settings** > **Smart Routing** > **Private Process Smart Routing**.
2. In the Private Process Smart Routing window, click the serial number of the rule you want to edit and modify the configured data in the **Edit Entry** dialog box.
   For more information on editing data of the selected business rule, see the description of the fields in New Rule for the Private Process Smart Routing table.
3. Click **Save**.

Deleting Business Rules

To delete one or business rules, perform the following steps:

1. On the Private Process Smart Routing page, select one or more business rules that you wish to delete, and click **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Public Process Smart Routing

You can perform the following tasks on the business rules for Public Process Smart Routing:

- Adding New Business Rule
- Editing Business Rules
- Searching for Business Rules
- Deleting Business Rules

Adding New Business Rule

To create a business rule for Public Process Smart Routing, perform the following steps:

1. In the Admin UI, go to **System Settings** > **Smart Routing** > **Public Process Smart Routing**.
2. In the Public Process Smart Routing window, click the **Add** icon.
   The **New Entry** dialog box is displayed.
   In the New Entry dialog box, enter the following information:

   New Rule for the Public Process Smart Routing

Field	Description
Cluster Name	Enter the name of the cluster. This is a logical name of the location where messages are routed. The cluster name must begin with an alphanumeric character and be followed by zero or more alphanumeric characters such as '_' (underscore), '-' (hyphen) or '.' (dot); for example, `CLUSTER_LARGE_MESSAGES`, `BC_CLUSTER_03`, `SERVER-POOL-19`, `C001` The value is not case sensitive.
Transport Type	Pre-populated with the name of the transport you have selected.
Rule Expression	Expression for the rule is populated from the selection made in the added conditions for the attribute, operator, and operand.
Enabled	Enable or disable the routing

Field	Description
	mechanism by selecting or clearing this check box.
Add New Condition (icon)	Each time you click this button, a new row of attributes is added. Condition Type can be set to the following: • if all conditions are met: more restrictive rule • if any conditions are met: less restrictive rule A new condition is now displayed with the configurable options: Attribute, Operator, and Operand.

3. Enter data as explained in the following tables for the respective transports:
   - Rule Options for the HTTP/S, HTTPCA, and AS2_HTTP/S Transports
   - Rule Options for the FTP/S and SSHFTP Transports
   - Rule Options for the File Transport
   - Rule Options for the Email and AS1_Email Transports

   The defined rules are displayed in the field Rule Expression.
4. Click **Add**.
   The rules that you create are displayed in the Public Process Smart Routing window.

Rule Options for the HTTP/S, HTTPCA, and AS2_HTTP/S Transports

Attribute	Operator	Operand1, Operand2	Explanation
HTTP_Host	matches, =	(host name)	Enter the host name
HTTP_Version	matches, =	(HTTP version)	Define whether to use a certain HTTP version.
Large_Content	is	false true	Define whether the file size is large (true or false)
Query_String	matches, =	(query)	Define whether to use a certain query.
Request_URI	matches, =	(URI)	Define whether to use a certain URI.
Secure_SSL	is	false true	Define whether the transport is secure (true or false)
Client_Auth	is	false true	Define whether client authentication is true or false
Content_Size	=, greater_than, less_ than, range	(value)	Define whether the file size is equal to, bigger, smaller, or in the range of a certain value.

Attribute	Operator	Operand1, Operand2	Explanation
AS2_From (AS2 only)	matches, =	(partner name)	Enter the AS2_ID of the partner sending the message
AS2_To (AS2 only)	matches, =	(partner name)	Enter the AS2_ID of the partner receiving the message

Rule Options for the FTP/S and SSHFTP Transports

Attribute	Operator	Operand1, Operand2	Explanation
File_Name	matches, =	(file name)	Define the name of the file to be sent. The whole path with the file name must be specified.
File_Size	=, greater_than, less_than, range	(value)	Define whether the file size is equal to, bigger, smaller, or in the range of a certain value.
From_ Partner	matches, =	(partner name)	Enter the name of the partner sending the message
To_Partner	matches, =	(partner name)	Enter the name of the partner receiving the message
Large_File	is	false true	Define whether the file size is large (true or false)
Protocol	matches, =	(protocol name)	Define whether to use a certain protocol.

Rule Options for the File Transport

Attribute	Operator	Operand1, Operand2	Explanation
File_Name	matches, =	(file name)	Enter the full path for the file name
File_Size	=, greater_than, less_than, range	(value)	Define whether the file size is equal to, bigger, smaller, or in the range of a certain value.
Large_File	is	false true	Define whether the file size is large (true or false)
Protocol	matches, =	(protocol name)	Define whether to use a certain protocol.

Rule Options for the Email and AS1_Email Transports

Attribute	Operator	Operand1, Operand2	Explanation
Sender	matches, =	(host email address)	Enter the email of the host sending the message.
Subject	matches, =	(email transport subject)	Define whether to use a certain subject.
Content_ Size	=, greater_than, less_than, range	(value)	Define whether the file size is equal to, bigger, smaller, or in the range of a certain value.
Large_ Content	is	false true	Define whether the file size is large.
Recipient	matches, =	(partner's	Enter the email address of the partner

Attribute	Operator	Operand1, Operand2	Explanation
		email address)	receiving the message.

Editing Business Rules

To edit a Business Rule, perform the following steps:

1. In the Admin UI, go to **System Settings** > **Smart Routing** > **Public Process Smart Routing**.
2. In the Public Process Smart Routing window, click the name of the rule you want to edit and modify the configured data in the **Edit Entry** dialog box.
   For more information on editing data of the selected business rule, see the description of the fields in the New Rule for the Public Process Smart Routing table.
3. Click **Save**.

Searching for Business Rules

You can use the Search function to find a specific business rule.

Enter the search string in the **Search** field to search a business rule.

The names of one or more business rules that correspond to the search criteria are displayed.

Deleting Business Rules

To delete one or business rules, perform the following steps:

1. On the Public Process Smart Routing page, select one or more business rules that you wish to delete, and click the **Delete** icon.

2. On the pop-up dialog box, click **OK**.

Map Cluster

Clusters are mapped using the configured rules into fault tolerance groups.

Adding Map Cluster

To add map cluster, perform the following steps:

1. In the Admin UI, navigate to **System Settings** > **Smart Routing** > **Map Cluster**.
2. Click **Add New Map Cluster**.

   The **New Entry** dialog box is displayed.

   > **Note:** The Rule Name is displayed in the **New Entry** dialog box only if the rule is enabled.

3. Select the Rule Name that you want to add and click **Add**.

Searching for Map Cluster

You can use the Search function to find a specific map cluster.

Enter the search string in the **Search** field to search a map cluster.

The names of one or more map clusters that correspond to the search criteria are displayed.

Deleting Map Cluster

To delete one or more map clusters:

1. On the Map Cluster page, select one or more map clusters that you wish to delete and then click **Delete** icon.
2. On the pop-up dialog box, click **OK**.

Email Transport

TIBCO BusinessConnect™ Container Edition provides the ability to communicate with trading partners using email. The BusinessConnect Container Edition Email transport can be used to send or receive messages from email clients.

The BusinessConnect Container Edition Email transport has the following features:

- It enables users of email clients to exchange documents securely by signing the message with their private key and encrypting the message with the public certificate of their trading partner.
- It conforms to the S/MIME standards.
- It also offers the ability to send your business document as an attachment to a plain text message for exchanging messages with email clients that require a non-attachment (inline) message body.

The following options are available for the TIBCO BusinessConnect Container Edition Email transport:

- Authentication Supported through digital signatures.
- Security Supported through message encryption.
- Non-repudiation Supported through digital signatures and email receipts.
- Compression Supported through the compression before signing.

Message Compression

For large messages, compression is highly recommended. Do not use compression on smaller messages, since this might create a compressed message that is larger than the original. Compression is always performed before signing (if it is also applied). When outbound messages are compressed, files are in GZIP file format. For inbound messages which are compressed, files are decompressed automatically.

Attachments

TIBCO BusinessConnect Container Edition Email transport supports the sending of documents as attachments. When the option Send Data as Attachment is selected, the outbound document will be sent in a multipart/mixed MIME message as follows:

- The first body part of the multipart message will contain a static string message, which can be ignored by the receiver of the message.
- The second body part of the multipart message will contain the outbound document. This second body part will have a MIME Content Disposition header with a type of “attachment.”

When using TIBCO BusinessConnect Container Edition Email transport, it is also possible to include other attachments with the outbound document whether the main document is sent as an attachment or not. These attachments are included as additional body parts to the outbound MIME message. The body parts of all attachments will contain a Content Disposition header with a type of “attachment”.

When an email message containing attachments is signed, the entire multipart/mixed MIME message is signed. Likewise, when an email message containing attachments is encrypted, the entire multipart/mixed MIME message is encrypted.

Note: Not all TIBCO BusinessConnect Container Edition protocols support sending attachments with the Email transport. Those protocols which have support for passing attachment information in their messages to/from the private process can be used to send attachment with the Email transport. See the User Guide of your TIBCO BusinessConnect Container Edition protocol to verify whether it supports sending attachments with the Email transport.

Content Disposition Filename

Some TIBCO BusinessConnect Container Edition protocols provide the ability for the private process to specify a filename to be used as the value of the filename parameter in the Content Disposition MIME header of outgoing MIME messages, including the messages sent using the TIBCO BusinessConnect Container Edition Email transport. The filename can be specified for the Content Disposition header associated with the main document and/or any attachments.

The TIBCO BusinessConnect Container Edition protocols that support specifying the filename value for the Content Disposition header will also pass the value of the filename parameter from the Content Disposition header of inbound email messages to the private process.

See the User’s Guide of the respective TIBCO BusinessConnect Container Edition protocol to verify whether it supports passing of the Content Disposition header filename to/from the private process.

Email Client Limitations

The following limitations exist:

TIBCO BusinessConnect Container Edition does not support receipts from Microsoft Outlook email clients. This could happen when TIBCO BusinessConnect Container Edition sends an email message that contains a document requesting a Receipt from Outlook email clients.

- When sending a document from Outlook email clients to TIBCO BusinessConnect Container Edition, do not use any properties such as rich text, fancy colors, fonts supported by the respective clients.
- When sending a document from Outlook email clients as inline and not as attachment, you must always choose a proper Content-Transfer-Encoding. Examples: base64, quoted-printable. Do not send the document as 7-bit encoding, which is the default for most email clients. Plain text documents could be altered by some mail agents and must be avoided when sending to TIBCO BusinessConnect Container Edition.

Configuring Email transport involves configuration tasks in the trading host and trading partner.

Identifying the Sender and Receiver

TIBCO BusinessConnect Container Edition Email transport uses standard To and From email addresses as defined in SMTP standard (RFC 2821). These email addresses must be defined in the

Valid Email Address List field in **Partner Management > Partners > Partner Name > Protocol > Edit Configuration > General**. When email is received from the mail server:

- The **To address** is matched against the email address entered in the host's Valid Email Address List.
- The **From address** is matched against the trading partner's Valid Email Address List.

Email Inbound POP3 Service Configurations

You can use this part of the section to create and configure mailboxes on your inbound mail POP3 servers.

Note: If you want to configure Gmail as the inbound Mail POP3 server in System Settings, you must change Google account settings first. In the Gmail account at https://mail.google.com/settings/security/lesssecureapps, you must turn on Allow less secure apps.

Creating Email Poller

To create a new email poller, perform the following steps:

1. On the **System Settings** tile, click **Transport protocols > Inbound Protocols**.
2. In the Inbound window, select **EMAIL** check box, and click **Save**.
3. After enabling the EMAIL transport, click the **Configure Service** tab.
4. On **Email Inbound POP3 Service Configurations**, click the **Add** icon.
5. In the **Create Email Poller** dialog box, enter the required information in all the fields displayed. For more information about the fields, see the Edit Email Poller table.

On the Email Inbound POP3 Service Configurations page, you can enable or disable the switch in the **Enable** column to activate or deactivate an Email Poller.

Configuring the POP3 Server Polling Service

TIBCO BusinessConnect Container Edition allows you to configure unlimited POP3 Email servers, so that email messages from all these servers can be received. All POP3 servers are configured in the following way:

1. On the Admin UI, expand **System Settings > Transport Protocols > Inbound Protocols**.
2. On the Email Inbound POP3 Service Configurations page, select the mail POP3 server you wish to configure. In the **Edit Email Poller**, configure the fields using the information displayed in the following table:

Edit Email Poller

Field	Description
Enabled	Select the checkbox to enable the mail poller.

Field	Description
Mail POP3 Server	Name of the POP3 server. For example: pop.gmail.com:995 **Note:** If the SSL check box is selected, the port number is required in this field.
User Name	Name of the user for this mailbox. **Note:** The username should be unique.
Password	Password of the user for this mailbox.
Polling Interval (seconds)	Sets the polling interval to specify the frequency which the credential alert keeps tracking and publishing alerts on expiring credentials. The default value is 180 seconds.
SSL	Secure Sockets Layer (SSL) configuration. For inbound messages, when this check box is selected, SSL/TLS protocols are used to ensure secure communication.
Trusted Certificates	Uploads an X.509 certificate file encoded in Privacy-enhanced Electronic Mail (PEM) format. This PEM encoded file contains the server X.509 certificate along with all the CAs in the certificate path. Note: Only the PEM encoded X.509 files are supported. If the certificate expires, download the latest certificate.
Verify Host Name	When selecting this check box, verification of the host is made, confirming the host you are connecting to is the expected host. The host name in the host's digital certificate is compared against the value you specified. If the host name does not match the expected host name, the connection is refused. This is optional.
Strong Cipher Suites Only	Only cipher suites with strong encryption can be used, if they are available on the host you are connecting to. This is optional.

Field	Description
Number of Dispatch Attempts	Number of attempts to deliver inbound emails from the email event source component to the internal component. The default value is 3.
Dispatch Interval (Time interval for next retry in seconds)	Intervals between delivery attempts for emails sent from the email event source component to the internal component. The default value is 300 seconds.
Dispatch Timeout (seconds)	Timeout on the email event source component waiting for an email delivery acknowledgement from the internal component. The default value is 3600 seconds.

After you enter the required data, click **Save** and redeploy the Interior Server.

Outbound HTTP/FTP Proxy and Mail SMTP Servers

Proxy servers allow you to connect to resources that otherwise are unavailable. They can also provide additional security and cache resources, allowing frequently accessed resources to be served more rapidly. to provide for different types of outbound transports protocols.

Note: Only SMTP proxy server is supported for outbound EMAIL transport protocol.

Different proxy server types are supported to provide for different types of outbound transports protocols:

- **HTTP** : For outbound HTTP transport protocols
- **SMTP** : For outbound Email transport protocols
- **FTP** : For outbound FTP transport protocols

To select a proxy for a partner participant, see Configure Proxy Settings for Partners.

Adding New Proxy Server

To add a new proxy server, perform the following steps:

1. Expand **System Settings > Transport Protocols > Outbound Protocols**.
2. In the Proxy Servers dialog box, click **Configure Service** for the proxy server you wish to add.
3. On the configuration page of the selected proxy server, click the **Add** icon.
4. In the New Proxy Server dialog box, enter a name in the **Proxy Name** field and select the proxy server from the drop-down list of the **Proxy Type** field.

   In the expanded dialog box, fill the required information as per the fields explained in the Edit Proxy Server table.

Configuring a Proxy Server

To configure the proxy server, click **SMTP** enter the following information:

Edit Proxy Server

Field	Description
Host Name	Enter the name of the host on which the proxy server is installed.
Port Number	Enter the number of the port that the proxy server is using.
Proxy User Name	Enter a valid user name for the proxy server, if applicable.
Proxy Password	Enter the password associated with the user name, if applicable.
For SMTP only:	
SMTP Server Name	An SMTP server name with port number. For example: smtp.gmail.com:587.

Field	Description
	Note: If you select the SSL or TLS protocol with encrypted SMTP, the port number is normally 465. If you select the STARTTLS protocol with encrypted SMTP, the port number is normally 587. For the SMTPS transport, if port number is not given, the default port number 25 is used.
Server Certificate	Server certificate of this SMTPS used for the STARTTLS, SSL, and TLS protocols. Certificate Authorities can be added under **System Settings** > **Certificates** > **Certificate Store**. You have to add server certificates according to your own needs. The sample certificates are in the `TIBCO_HOME/bcce/version/samples/keys/email_ssl` directory. If the certificate expires, download the latest certificate. The sample certificate used to connect to the Gmail server might expire depending on the Gmail service. Download a new Gmail server certificate if needed.
Secure Transport Mode	The secure protocol employed in the transport layer. The STARTTLS, SSL, and TLS protocols are listed in the list. SSL stands for secure sockets layer. TLS stands for transport layer security and is the successor of SSL v3. It is an open standard under RFC 2246. STARTTLS is a way to take an existing insecure connection and upgrade it to a secure connection using SSL/TLS.

Setting Up Email for a Host

You can set Email transport for a host by selecting transport protocols on the Business Agreement tab and setting email ID of the host for the specific protocol.

Setting up Email Transport for the Trading Host in the Business Agreements

Procedure

1. On the **Partner Management** tile, click **Business Agreements**.
2. In the Business Agreement window, click the business agreement for which you wish to set the Email transport.
3. In the Edit Business Agreement window, on the **Bind Protocol** tab, enable any protocol you wish to use and click **Edit Configurations**.
4. On the Transports tab, select **email** from the drop-down list of the **Primary Transport** field in the Outbound transport for Host section.

> **Note:** Only the transport protocols that are selected in **System Settings > Transport Protocols > Inbound Protocols** are displayed in the **Primary Transport** field.

Setting the Host's Email Address for a Protocol

Procedure

1. On the **Partner Management** tile, click **Hosts**.
2. On the Hosts page, click any one of the hosts whose email address you wish to set.
3. On the Edit Host page, click ***protocol*** **> Edit Configurations**.
4. In the **General** tab of the *protocol* configuration page, enter host's email address in the **Valid Email Address List** field.
5. Click **Save**.

Setting Up Email for a Trading Partner

To make a transport available for a trading partner, you have to perform the following tasks:

1. Configuring Email for a Trading Partner
2. Select this transport for the partner in the Inbound transport for Partner section on

the **Business Agreements** > **Bind Protocol** > **Available Protocols** > **Edit Configurations** > **Transports**.

Note: Only the transport protocols that are selected in **System Settings > Transport Protocols > Inbound Protocols** are displayed in the Inbound transport for Partner section.

Configuring Email for a Trading Partner

To configure Email transport for a trading partner, perform the following steps:

Procedure

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any partner you wish to configure this transport.
3. In the Edit Partner window, on the Protocol tab, click **Edit Configurations** for any protocol you wish to configure.
4. On the *protocol* configurations page, click the **Add** icon.
5. In the **Add Transport** dialog box, enter required information in the following fields:

Email Transport Settings

Field	Description
Transport Name	An identifier for these transport settings.
Transport Type	Select EMAIL transport from the drop-down list.
URL (mailto)	The URL for the trading partner is: mailto: e-mailID@domain.com.
Subject	A short string identifying the topic of the email message; for example, “Purchase Order from ABC Company”. For more information on the Subject Header field for MIME messages, see RFC C2822, Internet Message Format.

Field	Description
Base64 Encode Clear Text Messages	Base64 encode plain outbound email messages. Plain messages are those messages which are not signed, not encrypted, and not compressed.
Non Repudiation of Receipt	Enable logging of receipts in the non-repudiation table. If you check this option, you must also check the Sign check box and set Request Receipt to Signed. This means that outbound messages are signed and signed receipts are requested from the Responder. The original signed request from the Initiator and the signed receipt from the Responder are logged in the Initiator's non-repudiation table.
Sign	Enable outbound request messages or acknowledgments to be signed using your private key. Your trading partner uses your public key to authenticate your message. The 1024-bit key length is used for signatures. TIBCO BusinessConnect Container can process messages which contain message digests computed using the SHA1 hash algorithm. However, TIBCO BusinessConnect Container Edition computes its message digests using the digest algorithm setting specified for the business agreement in the Document Exchange tab. Whether an outbound receipt is signed or not is controlled by the setup in the requesting partner's Request Receipt list.
Signature Scheme	Select the desired signature algorithm from the list of options: RSA, RSA-PSS. The default option is RSA. **Note:** Ensure to enable the Sign check box to apply the signature scheme.
Encrypt	Enables each outgoing message to be encrypted using your partner's

Field	Description
	public key. Your partner uses their private key to decrypt your message. The encryption algorithm specified for the business agreement in the Document Exchange screen is used to encrypt the email messages.
Encryption Scheme	Select the desired encryption algorithm from the list of options: RSA-PKCS1-v1_5, RSA-OAEP, and RSA-OAEP-sha256, RSA-OAEP-sha384, and RSA-OAEP-sha512. The default option is RSA-PKCS1-v1_5. **Note:** Ensure to enable the Encrypt check box to apply the encryption scheme.
Compress	File compression is always performed before message signing. If selected, each outgoing message is compressed in GZIP file format.
Send Data as Attachment	If selected, the outbound business documents will be sent as file attachments to email messages. Normally, the business documents are sent inline, as the main body of an email message.
Use Attachment Filename as Subject	If selected, the file name of the first attachment of the email is used as the message subject. This file name is presented in the Content Disposition MIME header with a type of "attachment" of the first attachment. **Note:** This feature is introduced for TIBCO BusinessConnect Container Edition - EDI Protocol powered by Instream, EDIFACT Protocol, and cannot be used by other protocols.

Field	Description
Request Receipt	The type of receipt returned from the trading partner. The following options are available: **None** No receipt is requested from the trading partner for a message. **Signed** A signed receipt is requested from the trading partner for each message. After the Responder gets the document and verifies the content for integrity, a signed receipt is created and sent by the trading partner. **Unsigned** An unsigned receipt is requested from the trading partner for each message. If you choose to request a receipt of any kind, you must have a valid email address set for the trading host. If you checked Non Repudiation of Receipt, you should select Signed. For computing the message digest, BusinessConnect Container Edition uses the digest algorithm that was configured for the business agreement in the Document Exchange page. For more information on receipts, see Message Disposition Notification Receipts.
Receipt Timeout (minutes)	The amount of time within which a receipt should be returned by the trading partner. Example: 5

6. Click **Add**.

Setting the Partner's Email Address for a Protocol

Procedure

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any one of the partners whose email address you wish to

set.

3. On the Edit Partner page, click ***protocol*** **> Edit Configurations**.
4. In the **General** tab of the *protocol* configuration page, enter partner's email address in the **Valid Email Address List** field.
5. Click **Save**.

SSHFTP Transport

The SSHFTP (SFTP) transport, one of the public transports in TIBCO BusinessConnect Container Edition, is used to establish secured SSH tunnels for the communication between TIBCO BusinessConnect Container Edition server and the trading partners' SSH servers. Based on its use, the SSHFTP transport should not be confused with other methods of securing FTP, such as with SSL/TLS (FTPS).

It is used to establish multiple tunnels for secure communication between two participants. The established secure tunnels, if inactive, will be removed by TIBCO BusinessConnect Container Edition

Implementation of the SSHFTP transport is based on the following

- SSH The Secure Shell (SSH) standard is available in the public domain, as described in RFC 4250 - 4254: http://www.ietf.org/rfc/rfc4250.txt?number=4250.

  Note: Only the SSH2 standard is supported: no SSH connections can be established with a server that is limited to using only SSH1.

- SFTP TIBCO BusinessConnect Container Edition is compliant with the SFTP specification available at http://tools.ietf.org/html/draft-ietf-secsh-filexfer-03.

Cache Timeout

The cache timeout is the time after which a tunnel will be removed if it is not in use (default is 2 hours). Properties for configuring the cache timeout are available on the server side. When changing the cache timeout configuration, ensure that any new or pending transactions will use the tunnel that has been open after the configuration was changed.

For more information about configuring SSHFTP for trading participants, see the following topics:

- Setting Up SSHFTP for a Trading Host
- Setting Up SSHFTP for a Trading Partner

Setting Up SSHFTP for a Trading Host

To set up SSHFTP inbound for a trading host, perform the steps in the following sections:

- Enabling SSHFTP Inbound
- Selecting and Configuring SSHFTP Inbound

Enabling SSHFTP Inbound

Procedure

1. On the **System Settings** tile, click **Inbound Protocols** under Transport protocols.
2. On the Inbound page, select the **SSHFTP** check box, and click **Save**.

Selecting and Configuring SSHFTP Inbound

Procedure

1. On the **Partner Management** tile, click **BusinessAgreements**.
2. On the Business Agreement page, click the business agreement for which you wish to configure this transport.
3. On the Protocol tab, select the protocol you wish to bind and configure and click **Edit Configuration**.
4. On the *protocol* configuration page, click the Transports tab.
5. In Inbound transport for Partner section, select SSHFTP and click **Edit Settings** to configure the fields explained in the following table:

> **Note:** Only the transport protocols that are selected in **System Settings** >**T ransport Protocols** > **Inbound Protocols** are displayed in the Inbound transport for Partner section.

SSHFTP Settings

Field	Description
URL	The URL for the directory on the SSHFTP server, which is sshftp://host_name:port/path_name/, where host_name is the name of the machine (server) where the SSHFTP server is running. Port is the port on the machine to which the SSHFTP server is listening to. path_name is the relative path that starts from the base directory of the SSHFTP server.
Authentication Mode	You can choose the following modes from this list: • Password User account's password must be configured. • Keyboard Interactive It is a generic authentication method that can be used to implement different types of authentication mechanisms. • Public Key BusinessConnect Container Edition Server SSH private key must be configured. • Public Key and Password BusinessConnect Container Edition Server SSH private key and user account's password must be configured. **Note:** ClientAuthenticationIdentity (for SSHFTP) under Business Agreement must have the TIBCO BusinessConnect Container Edition Server SSH private key if either Public Key or Public Key and Password is selected.
Username	The user name for the trading partner's SSHFTP server. The user name must always be configured.
Password	The password for the user account with the name specified in the Username field on the trading partner's SSH server.
Server Certificate	The SSH server's public key must be specified.
Preferred Cipher	Choose among the following ciphers:

Field	Description
	• AES128_CBC • AES192_CBC • AES256_CBC • AES128_CTR • AES192_CTR • AES256_CTR • ARCFOUR • ARCFOUR128 • ARCFOUR256 • BLOWFISH_CBC • BLOWFISH_CTR • CAST128_CBC • 3DES_CBC • 3DES_CTR • RIJNDAEL_CBC@LYSATOR.LIU.SE • ANY (accept the server's preference if available)
Preferred MAC	Choose among these options: • HMAC_SHA1 • HMAC_MD5 • HMAC_RIPEMD160 • ANY (accept the server's preference if available)
Preferred Compression	Choose among these compression algorithms: • ANY (accept the server's preference if available)

Field	Description
	• None (do not use compression even if the server offers this choice) • ZLIB • ZLIB@OPENSSH.COM
File Processing	The mechanism for deciding which files to retrieve. There are two choices: • File Mask Choose to control file renaming. Enter a mask in the File Mask field. • Script Choose to process files. Specify a script in the Scripts field
File Mask	Controls which files to retrieve. If you enter an asterisk (*), BusinessConnect Container Edition searches for all files in the specified FTP directory. To prevent the retrieval of files that have already been retrieved, there are two options: • Select the Delete File check box, which causes each file to be deleted after it is retrieved, if this is allowed by the FTP server. • Specify a file mask that prevents the retrieval of the same files again For more information, see Supported File Mask Options.
Include Full File Path	The complete file path is enabled to distinguish this file from other files. If the complete file path is required, select this check box to send the getting request by SSHFTP poller file full path to the original file field of the BusinessConnect Container Edition ReceiveRequest palette.
Scripts	Click Upload file to upload a SSHFTP script. For information on how

Field	Description
	to write scripts, see Scripts.
Scripts Engine	The scripts engine that you want to use to execute custom scripts. You can select **Nashorn** or **FESI** from the list. **Note:** You are required to download and save FESI jar in machine's folder, and provide the reference of this folder in "configurations.properties" of <bcce-1.1.0/config/".
Start Time	The start time of the scheduled window where polling from the external FTP server occurs. You can modify the start time by using increment or decrement arrow buttons .
End Time	The end time of the scheduled window where polling from the external FTP server occurs.You can modify the end time by using increment or decrement arrow buttons .
Frequency (seconds)	This field defines how often polling occurs. By default, the frequency is 5 minutes (300 seconds).
Delete File	Enable files to be deleted after retrieval. This option is intended for test purposes so that duplicate files are not retrieved from an SSHFTP server.
Require PGP Processing	Select this check box if PGP unpackaging is required for an incoming message, which includes signature verification, decryption and/or decompression. This also assumes that the incoming messages are PGP packaged, otherwise the messages are rejected. This check box does not take effect if an SSHFTP script is used. When the SSHFTP script is used, the PGP options and policies are set up in SSHFTP script through PGP API.

Field	Description
	If PGP unpackaging is required, the PGP keys used for the unpackaging are configured in the Inbound Document Exchange portion of the Document Exchange tab in a Business Agreement. If unselected, the message is sent to back office as pass through, even if the message is PGP packaged.
PGP Policy Select one item from this list.	PGP policy only takes effect if the Require PGP Processing check box is selected. The following options are available in the list: • **None** No specific policies are mandated for the incoming message; the message can be signed and/or encrypted, with or without compression. However the message has to be PGP packaged in a certain way. Otherwise, it is rejected. • **Must Sign** The incoming message must be and only be signed, with or without compression; • **Must Encrypt** The incoming message must and only be encrypted with or without compression; • **Must Sign and Encrypt** The message must be both signed and encrypted, with or without compression. • **Pass-Through** In this mode, the software does not package the data in any way. The software takes the original notify message that the private process sent and forwards it over the Internet to the trading partner.
TCPNoDelay	Select this check box to enable the TCP No Delay feature. This property is used to manage the TCP_NODELAY option that controls the Transmission Control Protocol (TCP) packet batching on the TCP level. By default, this property is enabled.

Field	Description
	• If the property is enabled, the client sends TCP packets by using the SSHFTP transport regardless of the packet size, which increases the volume of network traffic. • If the property is disabled, the client does not send a TCP packet by using the SSHFTP transport until it has collected a significant amount of outgoing data. You can weigh the network efficiency versus your application requirements to decide whether to enable this property. Disable this property if the SSHFTP client or server of your trading partner does not handle the message well with the property enabled.

Setting Up SSHFTP for a Trading Partner

To make a transport available for a trading partner, you have to:

1. Configuring SSHFTP Outbound.
2. Select this transport for the partner in a specific business agreement.

Configuring SSHFTP Outbound

To configure SSHFTP for a trading partner, perform the following steps:

Procedure

1. On the **Partner Management** tile, click **Partners** > ***partner's name***.
2. In the Edit Partner window, select a *protocol* and click **Edit Configurations**.
3. On the *Protocol* configurations page, click **Transport > Add Outbound Transport** or ***transport*** respectively and configure the options listed in the following table:

Outbound SSHFTP Settings

Field	Description
Transport Name	Specify an identifier for these transport settings.
URL	Specify the URL for the directory on the FTP server, which is sshftp://host_name:port/path_name/, where • host_name is the name of the machine (server) where the SSHFTP server is running • port is the port on the machine to which the SSHFTP server is listening to • path_name is the relative path that starts from the base directory of the SSHFTP server
Authentication Mode	Select one authentication mode that you want to use from this list. • Password The user account's password must be configured. • Keyboard Interactive It is a generic authentication method that can be used to implement different types of authentication mechanisms. • Public Key BusinessConnect Container Edition Server SSH private key must be configured • Public Key and Password BusinessConnect Container Edition Server SSH private key and user account's password must be configured **Note:** ClientAuthenticationIdentity (for SSHFTP) under Business Agreement must have the TIBCO BusinessConnect Container Edition Server SSH private key if either Public Key or Public Key and Password is selected.
Username	Specify the user name for the trading partner's SSHFTP server. The user name must always be configured.

Field	Description
Password	Specify the password for the user account with the name specified in the Username field on the trading partner's SSH server.
Preferred Cipher Preferred MAC Preferred Compression File Processing File Mask Scripts Scripts Engine	For information about these fields, see SSHFTP Settings.
Retry Count	Specify the number of retries.
Retry Interval	Specify the interval between retries.
PGP Processing When PGP processing is selected, the PGP keys used for the processing are configured in the Outbound Document Exchange portion of the Document Exchange tab for a Business Agreement. These settings do not take effect if an SSHFTP script is uploaded and used. If the SSHFTP script is used, the PGP options are set up in the script using PGP API.	
Sign	Specify whether the files have to be signed.
Encrypt	Specify whether the files have to be encrypted.
Compress	Specify whether the files have to be compressed.

Field	Description
Compression Algorithm	Select the compression algorithm: ZIP or ZLIB.
ASCII Armor	Specify whether the files have to be sent in the ASCII armor format.
TCPNoDelay	Select this check box to enable the TCP No Delay feature. This property is used to manage the TCP_NODELAY option that controls the Transmission Control Protocol (TCP) packet batching on the TCP level. By default, this property is enabled. • If the property is enabled, the client sends TCP packets by using the SSHFTP transport regardless of the packet size, which increases the volume of network traffic. • If the property is disabled, the client does not send a TCP packet by using the SSHFTP transport until it has collected a significant amount of outgoing data. You can weigh the network efficiency versus your application requirements to decide whether to enable this property. Disable this property if the SSHFTP client or server of your trading partner do not handle the message well with the property enabled.

Selecting SSHFTP Transport in the Business Agreement

Procedure

1. On the TIBCO BusinessConnect Container Edition UI, expand **Partner Management** > **Business Agreements**.
2. Click the business agreement for which you wish to select SSHFTP transport.
3. On the **Protocols** tab, select the protocol you wish to configure and click **Edit Configurations**.

4. On the **Transport tab**, select SSHFTP (or the name you provide while creating an SSHFTP transport) as Primary Transport, and click **Save**.

   You can edit settings for the selected transport. For more information on configuring these settings, see Outbound SSHFTP Settings.

File Transport

There are three types of communications supported with the File transport:

- Outbound File Transport
- Outbound File Pollers
- Inbound File Pollers

The outbound File transport is normally used for file exchange within an enterprise.

Using an Inbound File poller as a transport, a trading partner can check for documents, while Outbound File pollers provide a simple way for private processes to transmit documents to TIBCO BusinessConnect Container Edition. This is different from other transports that are used for communication between trading partners.

Outbound File Transport

You can configure File outbound transport to perform these tasks:

- Rename outbound files according to a mask.
- Manage file processing using scripts

To make the outbound File transport available for a trading partner, you have to perform the following tasks:

1. Configuring Outbound File Transport for a Partner.
2. Select this transport for the partner in the **Primary Transport** field on the **Business Agreements > Edit Business Agreements > Bind Protocols > Available Protocols > Edit Configurations > Transports**.

Configuring Outbound File Transport for a Partner

1. To configure outbound File transport for a trading partner, perform the following steps:

2. On the **Partner Management** tile, click **Partners**.
3. On the Partners page, click any partner you wish to configure this transport.
4. In the Edit Partner window, on the Protocol tab, click **Edit Configurations** for any protocol you wish to configure.
5. On the *protocol* configurations page, click the **Add** icon.
6. In the Add Transport dialog box, enter required information in the following fields:

Outbound File Transport

Field	Description
Transport Name	An identifier for these transport settings.
URL	The directory in which the outbound files are to be stored.
File Processing	The mechanism for deciding how files are sent to the trading partner. There are two choices: • File Mask: Choose this option to control file renaming and enter a mask in the File Mask field. • Script: Choose Script for processing files and specify a script in the Scripts field.
Output File Mask	The mask to control file naming. The value entered in the field is used as the name of the file. For more information, see Supported File Mask Options . If no value is entered, Business Connect generates the outbound request in a predefined format.
Scripts	Specify a File script. See Scripts for information on how to write scripts and File Specification Dialog for information on how to upload a script.
Scripts Engine	The scripts engine that you want to use to execute custom scripts. You can select one of the items from the list: • FESI

Field	Description
	• Nashorn **Note:** You are required to download and save FESI jar in machine's folder, and provide the reference of this folder in "configurations.properties" of <bcce-1.1.0/config/".

Note: On Kubernetes, NFS installation is mandatory, and are required to configure the mount path in mount_path property of `deployment.configurations` file in config folder of the deployment package.

Outbound File Polling Service

Outbound File Polling Services are protocol specific. This section provides global information on their configuration, while the specific information is explained for each of the protocols.

Note: By default, the Outbound File Polling Service picks up the existing files when the Poller Server engine starts up.

Enabling and Configuring Outbound File Polling Service

To enable an Outbound File Polling Service, perform these steps:

1. On the **System Settings** tile, click **Transport Protocols > Outbound Protocols**.
2. Click **Configure Service** of FILE Outbound.
3. Click the protocol you want to enable and edit the options listed below:

Outbound File Poller Configuration

Field	Description
Enable	Select the **Enable** check box to enable Outbound File polling service.
Monitor Directory (e.g. /...///*.*)	The name of the file fileName and directory location, if desired, to monitor. Either provide the fileName or use the asterisk (*.*) character as a wildcard to specify a collection of files. Do not provide a directory location only. TIBCO BusinessConnect Container Edition searches subdirectories recursively. The directory `C:\` is not taken as a base directory: specify `C:\BaseDir` instead. A better configuration is `C:\BaseDir\*.*`, which specifies the directory for the Outbound File poller. **Note:** Directories for Inbound and Outbound File pollers should not be the same ones that are used for storing shared or local files.
Directory to Place Error Files	Designate a directory where the files will be placed if an error occurs during the processing of the outgoing files.
Polling Interval (seconds)	The duration for which the polling occurs. Default is 300.
Delete File	Enable files to be deleted after processing. In order to avoid that the same files are picked up on the subsequent startup of the TIBCO BusinessConnect Container Edition engine, it is advised to select this check box and have the files removed after processing has been completed.

4. Click **Save**.

Note: You must set up Network File System (NFS) for Outbound File Polling to work in the Kubernetes environment.

Inbound File Pollers

The inbound File poller enables a trading host to monitor directories for documents placed on its local file system by a trading partner. To use BusinessConnect Container Edition with an inbound File poller, you have to perform two basic steps, which are described in the following sections:

- Enabling and Configuring Inbound File Poller
- Selecting File Inbound in the Business Agreement

Note: Directories for Inbound and Outbound File pollers should not be the same ones that are used for storing large, shared, or local files.

Note: By default, the Inbound File poller picks up the existing files when the Poller Server engine starts up.

Enabling and Configuring Inbound File Poller

1. To enable and configure an inbound File poller on the BusinessConnect Container Edition server, perform the following steps:
2. On the Admin UI, expand **System Settings > Transport Protocols > Inbound Protocols**.
3. On the Inbound page, select the check box next to the File transport, and click **Save**.
4. Click **Configure Service** and enter the fields as explained in the following table:

FILE Inbound Service Configurations

Field	Description
Enable	Select the check box to enable the transport.
Monitor Directory	Specify the directory to be monitored by the File Poller. This directory must start with '/' or '\' or '//' or '[a-zA-Z]:' and must end with '/' or '\'.

Field	Description
	Example: C:\tibco\bcce\1.0\monitorFiles\file.txt
Delete Files after Processing	Select this check box to delete the files after processing. By default, this check box is selected.
Polling Interval (secs)	Specify a period of time in seconds. The Poller monitors the specified location for the new and updated files. The default value is 300 seconds.
Directory to Place Error Files	Specify a directory where the error files are saved. This directory must start with '/' or '\' or '//' or '[a-zA-Z]:' and must end with '/' or '\'.

Note: When you import `.csx` file from TIBCO BusinessConnect to TIBCO BusinessConnect Container Edition, the inbound file polling **Monitor Directory** field and **Directory to Place Error Files** field do not reflect. You are required to manually configure the file path after importing the configuration.

Selecting File Inbound in the Business Agreement

This option is used to allow a particular business agreement to receive messages if the option is not enabled, then the host will not be able to receive any messages over the File transport from the partner with whom he has this business agreement.

1. On the TIBCO BusinessConnect Container Edition UI, expand **Partner Management** > **Business Agreements**.
2. Click the business agreement for which you wish to select File transport.
3. On the **Protocols** tab, select the protocol you wish to configure and click **Edit Configurations**.
4. On the **Transport tab**, in the Inbound transport for Partner section, select the File transport.

HTTP, HTTPS, and HTTPSCA Transports

TIBCO BusinessConnect Container Edition supports the following HTTP transports:

- **HTTP**: This is a request/response protocol between clients and servers. TIBCO BusinessConnect Container Edition supports the HTTP transport for the trading hosts and trading partners.
- **HTTPS**: This is an HTTP transport over a secure connection. The server uses its private key when setting up the secure connection.

  Before configuring HTTPS, you must set up a private key for the server as described in Certificates topic. TIBCO BusinessConnect Container Edition supports the HTTPS transport for the trading hosts and trading partners.
- **HTTPCA**: With HTTPS (Client Authentication), trading partners authenticate themselves to the host by signing messages with their private key. The host uses the public key in the partner's certificate file to authenticate the partner. Before configuring HTTPS (Client Authentication), you must set up a certificate file for the trading partner. For more information, see Manage Credentials for Partners.

Setting Up HTTP/S for a Trading Partner

To make a transport available for a trading partner, perform the following tasks:

1. Configuring HTTP/S for a Trading Partner.
2. Select this transport for the partner in the **Primary Transport** field on the **Business Agreements > Edit Business Agreement > Bind Protocol > Available Protocols > Edit Configurations > Transports**.

Configuring HTTP/S for a Trading Partner

To configure HTTP/S for a trading partner, perform the following steps:

> **Note:** The following steps are only for Transport tabs in EZComm protocol and X12 protocol.

Procedure

1. On the **Partner Management** tile, click **Partners**> ***partner's name***.
2. In the Edit Partner window, select **EZComm** and click **Edit Configurations**.
3. On the protocol configurations page, enter the following fields for General tab:

Configuring HTTP/S for a Trading Partner: General Tab

Field	Description
AS2 Identifier	Add a new AS2 Identifier or select from the list.
Valid Email Address List	This email address list can be a list of email addresses for this participant, separated by semicolon or by a comma. For an outbound document sent to the trading partner through SMTP transport, the first email address is used in the From header. For incoming email from the mail server, the To email address from the email is matched to one of the email addresses in this list. This only applies when using AS1, AS2, or Email transport.
Allow override of fileName via HTTP parameter	This option only applies to the HTTP and HTTPS transports for the TIBCO BusinessConnect Container Edition -Services Plug-in. This option does not apply to the AS2 and AS1 Email transports. For more information, see *TIBCO BusinessConnect Container Edition - Services Plug-in, User Guide.*

4. To add the transport for the partner, click **`partner name` > `protocol link` > Transport > Add Outbound Transport** or ***transport link*** respectively and configure the options listed in the following table:

> **Note:** The fields described in the following table are applicable for all the protocols.

Configuring HTTP/S for a Trading Partner: Transports Tab

Field	Description
Transport Name	An identifier for these transport settings.
Transport Type	Select the transport type from the drop-down list: HTTP or HTTPs.
URL	The URL of the trading partner.
HTTP 1.0 Compatible	Whether to exclude "Expect: 100 continue" in the HTTP header of the outbound HTTP/S request when the request is sent to the server of the trading partner.
Server Certificate (HTTPS only)	The participant's certificate used to encrypt communication.Note: You must configure the credentials in advance, before creating this transport.
Use HTTP Basic Authentication	Enable basic authentication at the trading partner. The user name and password supplied in those fields are provided when accessing the trading partner. The trading partner will service requests only if it can validate the supplied user name and password. Note that the password is passed in plain text across the network.
Username	Specify a user name for authenticating the host on the partner HTTP/S service.
Password	Specify a password for authenticating the host on the partner HTTP/S service.
Retry Count	The maximum number of times BusinessConnect Container Edition attempts to reconnect to the remote HTTP server, in case of failures.
Retry Interval	The interval BusinessConnect Container Edition waits before another re-connect is attempted.

Field	Description
Socket Timeout (seconds)	The amount of time a socket blocks on a read operation. **Note:** If you want to receive the timeout error when no response is received from your partner, the value in this field must be less than the value set in the Response Wait Time field in the Configuration tab of the SendRequest activity.
Cipher Suite Grade (HTTPS only)	Select the cipher grade (strength) from the list. The following options are available: • All • Only Stronger Than Export • Only 128-Bit and Stronger • Only stronger Than 128-Bit • Only 256-Bit and Stronger All ciphers are listed in *TIBCO BusinessConnect Container Edition Security Guidelines, Cipher Suites*.
Can Use TLS (HTTPS only)	TLS protocol is supported. If you select this check box, TLS protocol is used to establish connection to the trading partner server.
TLS Version (HTTPS only)	Select the version of TLS protocol. TLS protocol versions 1.0, 1.1, 1.2, and 1.3 are supported. **Note:** If you select TLS version 1.1 or 1.2, you have to select SUN or IBM as the security vendor for inbound and outbound socket operations.
Can Use SSLv3	SSL protocol version 3.0 is supported.

Field	Description
(HTTPS only)	If you select this check box, SSL protocol version 3.0 is used to establish connection to the trading partner server.
GISB/NAESB	
GISB/NAESB Package	Select this check box to package outbound messages in the NAESB Internet ET format. By default, this check box is cleared.
GISB/NAESB Version	Specify the GISB/NAESB version. The default value is 2.0.
Receipt Signature Required (X12 Protocol only)	Select this check box to support the receipt signature. When you select this check box, the outbound NAESB message contains a "receipt-security-selection" data element that instructs the responder to sign the receipt (including the synchronous receipt and asynchronous error notification) that is sent back. By default, this check box is cleared.
PGP Encrypt (X12 Protocol only)	Select this check box to enable PGP encryption. By default, this check box is selected. PGP encryption in ASCII Armor format is mandatory for requests. This setting takes effect only for a regular outbound request and not for an outbound Error Notification, which is never encrypted according to the NAESB standard.
PGP Sign (X12 Protocol only)	Select this check box to support PGP signature. This is optional. By default, this check box is cleared. This setting takes effect only for a regular outbound request and not for an outbound Error Notification. The "receipt-security-selection" data element in the original inbound NAESB message defines whether an error notification is signed. Note that other PGP features, such as Compression and Compression Algorithm, are not configured since NAESB messages are not compressed.

5. Click **Add > Save**.

Configuring Gateway Services for HTTP

To configure the Gateway services for HTTP perform the following tasks:

Procedure

1. On the **System Settings** tile, click **Inbound Protocols**
2. On the Inbound page, select **HTTP** protocol and click **Configure Service**.
3. On the Gateway Service Configurations page, click http or the **Add** icon to create new gateway service.
4. In the Edit Gateway Service dialog box, enter the information in the fields displayed. For more information about the fields, see *TIBCO BusinessConnect Container Edition Administration Guide, Configuring Gateway Services*.

Selecting HTTP, HTTPS, and HTTPSCA Transports for Trading Host

This option is used to allow a particular business agreement to receive messages if the option is not enabled, then the host will not be able to receive any messages over these transports from the partner with whom he has this business agreement.

Procedure

1. On the TIBCO BusinessConnect Container Edition UI, expand **Partner Management** > **Business Agreements**.
2. Click the business agreement for which you wish to select HTTP, HTTPS, or HTTPSCA transport.
3. On **Protocols** tab, select the protocol you wish to configure and click **Edit Configurations**.
4. On the **Transport tab**, in the Inbound transport for Partner section, select HTTP, HTTPS, or HTTPSCA.

   You can edit settings for the selected transport.

   - For HTTP/S: Select the **Require HTTP Basic Authentication** check box to do the

basic authentication for inbound messages.

- For HTTPSCA , select the **Client Authentication Identity** from the list and click **OK**.

  Select the **Require HTTP Basic Authentication** check box to do the basic authentication for inbound messages.

Only the transport protocols that are selected in **System Settings** > **Transport Protocols** > **Inbound Protocols** are displayed in the Inbound transport for Partner section.

FTP and FTPS Transports

This topic describes how to use FTP and FTPS transports for document exchange.

FTP Transport Overview

TIBCO BusinessConnect Container Edition supports FTP transport, which enables users to send or receive large documents by connecting to the trading partner's FTP server. It uses a store and retrieve mechanism of putting and getting files from the trading partner's FTP server. In some cases, a trading partner requires that the exchange of document happens securely so that the integrity of the transmission is not compromised. To accommodate this, TIBCO BusinessConnect Container Edition provides different ways of sending files through FTP transport.

To understand and set up FTP operations, review the following steps:

- The initiating partner uses the trading partner setup area to specify the address of the FTP server that receives the FTP put operations for a particular trading partner.
- A responding partner that receives FTP put operations must specify an FTP server to receive the Initiator’s FTP files. This server name and directory must match the URL specified in the preceding step. The responding TIBCO BusinessConnect Container Edition uses a poller to monitor that location.
- A partner that receives FTP put operations from an Initiator must specify the directory into which it places its response.
- The Initiator that receives the FTP response from the Responder must specify a directory that it polls for the Responder’s response. This server name and directory must match the URL specified in the preceding step.

If you use asynchronous request-response, you can mix HTTP, HTTPS, Email, and FTP. For example, you can send an asynchronous request document using FTP and the Responder can use HTTP. You are responsible for monitoring the directory on the FTP external server and removing files as needed.

Explicit and Implicit FTPS Connections

TIBCO BusinessConnect Container Edition supports FTPS in explicit mode, which means that the BusinessConnect Container Edition server assumes it is configured to connect to the security enabled FTP server's standard FTP port (usually TCP port 21). On this port, it negotiates security properties by issuing an AUTH SSL or AUTH TLS command (as per the transport's configuration), made on the server's admin GUI and the corresponding specifications (see specification RFC2228). Implicit FTPS connections (usually for connecting to TCP port 990) are not supported.

Supported File Mask Options

The supported file mask options for file names using FTP/S, SSHFTP, and File transports are as follows:

Supported File Mask Options

User Provides	TIBCO BusinessConnect Container Edition Uses
TpName	The receiving participant's name
HostName	The sending participant's name
DDD	Day in a year
YY	Last two digits of a year
YYYY	Year
MMM	Month abbreviated to three characters
MM	Month on two digits (1-base)
DD	Day of the month on two digits (1-base)
HH	Hour of the day (0-24)
MN	Minutes of the hour
SS	Seconds of the minute

User Provides	TIBCO BusinessConnect Container Edition Uses
NN	Milliseconds of the second on three digits
TransactionID	ID of the transaction
FileName	Name of the file
GUID	Globally unique identifier
DocumentID	ID of the sent document
OperationID	ID of the operation

Example:

```
My-#(YYYY)-#(MMM)-#(DD)-#(HH)-#(MN)-#(SS)-#(NN)-#(OperationID)-file.txt
```

will print:

My-2020-Feb-17-14-01-45-093-BC_1.0_Notify-file.txt

FTP/S Inbound

A host uses the FTP and FTPS inbound transports to periodically retrieve messages from one or more trading partners' FTP servers. This is in contrast to FTP outbound, which allows a host to send messages to a partner.

There are two ways that you can use FTP/S to get files from the FTP server of a trading partner:

- Retrieve files according to a mask
- Manage file processing using scripts

FTP inbound operations use the temporary local file storage, which exists inside the container.

FTP transfers over the Internet are not secure because intruders can look at the data transfer and even modify the commands or data before they reach their intended trading partner. To avoid that, use FTPS inbound, which is an FTP inbound transport over a secure connection. The FTP server and the FTP client, in this case BusinessConnect Container

Edition, exchange certificates and create a secure, encrypted connection before sending or receiving data or FTP commands.

Before configuring FTPS inbound, you must set up a certificates file for the trading partner and a key for the trading host.

Setting Up FTP/S for a Trading Host

To set up FTP/S inbound for a trading host, follow the instructions in the following sections:

- Enabling FTP/S Inbound
- Selecting and Configuring FTP/S Inbound

Enabling FTP/S Inbound

1. Go to **System Settings** tile > **Transport Protocols** > **Inbound Protocols**.
2. Select the **FTP** or **FTPS** check box.
3. Click **Save**.

Selecting and Configuring FTP/S Inbound

1. On the **Partner Management** tile, click **Business Agreements**.
2. In the Business Agreement page, click the business agreement for which you want to configure FTP/S Inbound.
3. In the Edit Business Agreement page, on the **Bind Protocol** tab, enable any protocol you wish to use and click **Edit Configurations**.
4. Click the **Transports** tab select **FTP** or **FTPS** in the **Inbound transport for Partner** section.
5. Click **Edit Setting** of the selected Inbound transport and edit the options listed below.

Inbound FTP/S Settings

Field	Description
URL	The URL for the directory on the FTP server, which is `ftp://host_name:port/path_name/`, where • `host_name` is the name of the machine (server) where the FTP server is running. • `port` is the port on the machine to which the FTP server is listening to. • `path_name` is the relative path that starts from the base directory of the FTP server.
Server Certificate	(FTPS only) The partner certificate used to encrypt transport communication.
Client Authentication Identity	(FTPS only) The host key to be used when the remote server requires authentication of the SSL sender.
Data Transfer	The format for transferring files: ASCII or Binary.
Username	The user name for authenticating the host on the partner FTP/S service.
Password	The password for authenticating the host on the partner FTP/S service.
File Processing	The mechanism for deciding which files to retrieve. There are two choices: • **File Mask** Select it to control file renaming. Enter a mask in the File Mask field. • **Script** Select it for processing files. Specify a script in the Scripts field.
File Mask	Controls which files to retrieve. If you enter an asterisk (*), BCCE

Field	Description
	searches for all files in the specified FTP directory. To prevent the retrieval of files that have already been retrieved, there are two options: • Select the Delete File check box, which causes each file to be deleted after it is retrieved, if this is allowed by the FTP server. • Specify a file mask that prevents the retrieval of the same files again.
Include Full File Path	The complete file path is enabled to distinguish this file from other files. If the complete file path is required, select this check box to send the getting request by FTP/FTPS poller file full path to the original file field of the Business Connect ReceiveRequest palette.
Scripts	Specify an FTP script.
Scripts Engine	Use the Nashorn or FESI engines to execute custom scripts. **Note:** You are required to download and save FESI jar in the machine's folder, and provide the reference of this folder in "configurations.properties" of <bcce-1.1.0/config/".
Secure Transport Mode	(FTPS only) The secure protocol employed in the transport layer. You can select one of the items from the list: • SSL_ONLY • SSL • TLS SSL stands for Secure Sockets Layer. TLS stands for Transport Layer Security, and is the successor of SSL v3. It is an open standard under RFC 2246.

Field	Description
Start Time	The start time of the scheduled window where polling from the external FTP server occurs.
End Time	The end time of the scheduled window where polling from the external FTP server occurs.
Frequency (seconds)	This field defines how often polling occurs. By default, the frequency is 5 minutes (300 seconds). **Note:** Additional overhead is incurred when the polling interval is reduced, as each poll requires logging on to the remote FTP server and checking for available files for retrieval. To reduce unnecessary overhead, an optimized value for the polling interval should be entered based on the volume of inbound documents from your trading partners.
Delete File	Enable files to be deleted after retrieval. This option is intended for test purposes so that duplicate files are not retrieved from an FTP server. **Note:** This option does not work for all FTP servers.
Require PGP Processing	Select this check box if PGP unpackaging is required for an incoming message, which includes signature verification, decryption and/or decompression. This also assumes that the incoming messages are PGP packaged, otherwise the messages are rejected. This check box does not take effect if an FTP script is used. When the FTP script is used, the PGP options and policies are set up in FTP script through PGP API. If PGP unpackaging is required, the PGP keys used for the unpackaging are configured in the Inbound Document Exchange portion of the **Document Exchange** tab in a Business Agreement. If unselected, the message is sent to back office as pass through,

Field	Description
	even if the message is PGP packaged.
PGP Policy	The PGP policy only takes effect if the Require **PGP Processing** check box is selected. Four policies are available: • **None** No specific policies are mandated for the incoming message; the message can be signed and/or encrypted, with or without compression. However, the message has to be PGP packaged in certain way, otherwise it will be rejected. • **Must Sign** The incoming message must be and only be signed, with or without compression. • **Must Encrypt** The incoming message must and only be encrypted with or without compression. • **Must Sign and Encrypt** The message must be both signed and encrypted, with or without compression. • **Pass-Through** In this mode, the software does not process the receiving data from the trading partner server, but forwards it to the private process directly.

6. Click **Save**.

FTP/S Outbound

The FTP and FTPS outbound transports are used for storing files on the trading partner's FTP server. You can configure FTP outbound transport to perform the following operations:

- Rename outbound files according to a mask.
- Manage file processing using scripts.

FTP transfers over the Internet are not secure because intruders can look at the data transfer and even modify the commands or data before they reach their intended trading partner.

FTPS outbound is an FTP outbound transport over a secure connection. The FTP server and the FTP client, in this case TIBCO BusinessConnect Container Edition, exchange certificates

and create a secure, encrypted connection before sending or receiving data or FTP commands.

Before configuring FTPS, you must set up a certificate file for the trading partner.

Setting Up FTP/S for a Trading Partner

To make a transport available for a trading partner, you have to perform the following tasks:

1. Configuring FTP/S Outbound.
2. To select this transport for the partner in the Primary Transport field, click **Business Agreements > Edit Business Agreement > Bind Protocol > Available Protocols > Edit Configurations > Transports**.

Configuring FTP/S Outbound

To make a transport available for a trading partner, you have to perform the following tasks:

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any partner you wish to configure this transport.
3. In the Edit Partner page, on the **Protocol** tab, click **Edit Configurations** for any protocol you wish to configure.
4. On the protocol configurations page, click the **Add** icon.
5. Enter the transport name.
6. Select FTP/S from the **Transport Type** list.
7. Configure the options listed in below table.

Outbound FTP/S Settings

Field	Description
Transport Name	An identifier for these transport settings.

Field	Description
URL	The URL for the directory on the FTP server, which is `ftp://host_name:port/path_name/`, where • *host_name* is the name of the machine (server) where the FTP server is running. • *port* is the port on the machine to which the FTP server is listening to. • *path_name* is the relative path that starts from the base directory of the FTP server.
Server Certificate	(FTPS only) The partner's certificate used to encrypt transport communication.
Data Transfer	The format for transferring files: ASCII or Binary.
Username	The user name for the trading partner's FTP server.
Password	The password for the trading partner's FTP server.
File Processing	The mechanism for deciding which files to retrieve. There are two choices: • **File Mask** Select it to control file renaming. Enter a mask in the File Mask field. • **Script** Select it for processing files. Specify a script in the Scripts field.
File Mask	(FTPS only) The mask that controls file renaming. The value entered in the field works as a template for the actual file name. For more information, see Supported File Mask Options.
Output File Mask	(FTP only) The mask that controls file renaming. The value

Field	Description
	entered in the field works as a template for the actual file name. For more information, see Supported File Mask Options.
Scripts	Specify an FTP script. For information on how to write scripts, Scripts and File Specification Dialog for information on how to upload a script.
Scripts Engine	Use Nashorn or FESI engines to run the custom scripts. **Note:** You are required to download and save FESI jar in machine's folder, and provide the reference of this folder in "configurations.properties" of <bcce-1.1.0/config/".
Secure Transport Mode	(FTPS only) The secure protocol employed in the transport layer. SSL stands for secure sockets layer. TLS stands for transport layer security and is the successor of SSL v3. It is an open standard under RFC 2246.
Retry Count	Number of retries.
Retry Interval	Time between retries.
PGP Processing When PGP processing is selected, the PGP keys used for the processing are configured in the Outbound Document Exchange portion of the Document Security tab for a Business Agreement. These settings do not take effect if an FTP script is uploaded and used. If the FTP script is used, the PGP options are set up in the script using PGP API.	
Sign	Specifies whether the files have to be signed.
Encrypt	Specifies whether the files have to be encrypted.

Field	Description
Compress	Specifies whether the files have to be compressed.
Compression Algorithm	Selects the compression algorithm: ZIP or ZLIB.
ASCII Armor	Specifies whether the files have to be sent in the ASCII armor format.

8. Click **Add**.

AS2 Transport

This topic describes how to use AS2 Transport for document exchange.

AS2 Transport Overview

AS2 (Applicability Statement 2) is the name given to implementations of RFC 4130 (MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP) from the IETF. AS2 involves the exchange of documents over the internet using S/MIME, HTTP, and HTTPS.

AS1 and AS2 are widely recognized standards for the exchange of documents between businesses: these standards allow users to exchange data securely and reliably using the internet. This results in reduced costs for users by eliminating the need for VANs (Value Added Networks).

To date, over 25 different companies offer products which support AS1 or AS2 or both. These products have all undergone interoperability testing facilitated by Drummond Group Inc. and are certified by eBusinessReady as being interoperable.

AS2 transport supports:

- Documents signing
- Documents encryption
- Documents compression
- Attachments

AS2 Transport

AS2 Transport allows you to exchange documents over the Internet using S/MIME and HTTP/S. When using AS2, data is encoded in a MIME message according to the Internet Engineering Task Force (IETF) AS2 RFC standard (RFC 4130).

Message Compression

Compression is available for large AS2 messages if a trading partner can send AS2 messages according to the IETF AS2 standard (RFC 4130) and the trading partner's AS2 product has passed interoperability testing with the Drummond Group.

There are different algorithms that can be used for compression of MIME messages. The Drummond Group AS2 interoperability test specification calls for a particular specification (draft-ietf-ediint-compression-12) to be followed when doing compression.

For large messages, compression is highly recommended. Do not use compression on smaller messages, since this might create a compressed message that is larger than the original.

Attachments

AS2 Transport supports single and multiple attachments in messages when used with TIBCO BusinessConnect Container Edition Services Plug-in (EZComm protocol).

AS2 MIME messages with attachments, described in RFC 6362 (Multiple Attachments for Electronic Data Interchange - Internet Integration (EDIINT)), are constructed in a single multipart/related MIME body part. The message payload is the first body part and any attachments are contained in subsequent body parts. Header elements indicate whether a message has an attachment and the type of attachment.

Filename Preservation

Some back-end systems require that data to be processed be stored in files with particular filenames. So for some trading partners it might be necessary to associate filenames with the contents of messages you send to them.

For AS2 messages, there is a draft specification (http://tools.ietf.org/id/draft-harding-ediint-filename-preservation-03.txt) that has been written to address this problem. The filename preservation draft specification requires that systems which conform to the specification provide the ability to specify the filename for storing the message content in the filename parameter of the Content Disposition header. For inbound messages, the ability to pass the filename from the Content Disposition header to the back-end systems must be provided.

Some TIBCO BusinessConnect Container Edition protocols also provide the ability for the private process to specify a filename to be used as the value of the filename parameter in the Content Disposition MIME header of outgoing MIME messages, including AS2 messages.

TIBCO BusinessConnect Container Edition protocols which support specifying the filename value for the Content Disposition header will also pass the value of the filename parameter from the Content Disposition header of inbound AS2 messages to the private process.

See the User Guide of the TIBCO BusinessConnect Container Edition protocol you are using to verify whether it supports passing the Content Disposition header filename to/from the private process.

AS2-HTTP and AS2-HTTPS

TIBCO BusinessConnect Container Edition AS2 Transport provides the ability to communicate with trading partners using AS2-HTTP/S. The following options are available:

- **Authentication** Supported through digital signatures.
- **Security** Supported through message encryption.
- **Non-repudiation** Supported through digital signatures and message receipts.
- **Filename Preservation** Supported through the use of the filename parameter in the Content Disposition header as specified in the draft-ietf-ediint-filename-preservation-02 specification.
- **Compression** Supported through the compression option as specified in the draft-ietf-ediint-compression-12 specification.

Note: Synchronous request-response transactions are not supported with AS2-HTTP or AS2-HTTPS.

Message Digest Algorithm

The AS2 specification, RFC 4130, recommends that the SHA-1 hash algorithm be used to calculate the message digest for all outbound messages. By default, the TIBCO BusinessConnect Container Edition AS2 transport will always use the SHA-1 hash algorithm regardless of the Digest Algorithm setting for the business agreement.

For messages with multiple attachments, the message digest is calculated over the whole multipart MIME package, not just the message payload, as described in RFC 3335 (MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet) and RFC 5402 (Compressed Data within an Internet Electronic Data Interchange (EDI) Message).

To override the default use of SHA-1 for the hash algorithm by the AS2 transport, you can set the TIBCO BusinessConnect Container Edition property bc.ediint.digestAlgorithmEnabled as follows:

- If bc.ediint.digestAlgorithmEnabled is set to true, the AS2 transport will use the digest algorithm that is specified in the business agreement Document Security settings.
- If bc.ediint.digestAlgorithmEnabled is false (the default), the AS2 transport will ignore the digest algorithm setting in the business agreement and use SHA-1.

Use of the MD5 hash algorithm with AS2 should not be required. Drummond Group certified AS2 products all use SHA-1 for the hash algorithm during interoperability testing. However, the AS2 specification also states that AS2 products should be able to accept messages which use the SHA-1 hash algorithm. TIBCO BusinessConnect Container Edition will process inbound messages using either hash algorithm.

Disabling Session Cache for HTTPS

HTTPS (SSL) transport endpoints (HTTPS, AS2-HTTPS) use an internal SSL transport cache to significantly improve the performance of negotiating security parameters while establishing trusted connections.

In some situations, problems might arise when third party server implementations are not able to properly handle cached sessions or renegotiation of security properties at the beginning of each application level communication session. For example, the Initiator always wants to ensure that the peer's credential is the one that is trusted and hasn't changed during any cached session.

The cache usually holds successfully negotiated security parameters for about 20 minutes, which means that large numbers of transactions between the Initiator and any given trading partner will require a credential renegotiation in approximately 20 minutes.

In order for BusinessConnect Container Edition to enforce the renegotiation of the peer's credentials, the Disable Session Cache check box can be selected for any individual outgoing transport. When selected, each time when TIBCO BusinessConnect Container Edition has business data to be delivered to the corresponding trading partner, the peer's credentials are requested and are again verified.

For more information and the right location for disabling and enabling session cache see bc.ssl.disableSessionCache.

AS2 Identifiers

TIBCO BusinessConnect Container Edition provides the ability to communicate with trading partners using AS2-HTTP and AS2-HTTPS. For AS2 transport, two headers are added in addition to the HTTP headers: AS2-From and AS2-To. When TIBCO BusinessConnect Container Edition sends an AS2 MIME message, the values in the message’s AS2-From and AS2-To fields will be set with the AS2 Identifier values entered during configuration of the trading partners. AS2 identifiers are selected in the AS2 Identifier list in the **Partner**

Management > Partners > Partner Name > Protocol> Edit Configurations > General tab.

Note: If the AS2 Identifier lists are left as blank, an error will show up reminding that the AS2 trading partner identifier is missing.

Sending and Receiving

When a document is sent from a host to a partner using AS2, the header AS2-From contains the value agreed for the trading host and the header AS2-To contains the value agreed for the trading partner. When an AS2 message is received by TIBCO BusinessConnect Container Edition, the AS2-To header is matched against the AS2 Identifier value entered for the host, and the AS2-From header is matched against the AS2 Identifier entered for the partner. If there is no match, then an error is logged to indicate that an AS2 message was received from an unknown trading partner.

Adding AS2 Identifiers

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any partner you wish to configure this transport.
3. In the Edit Partner page, on the **Protocol** tab, click **Edit Configurations** for any protocol you wish to configure.
4. On the protocol configurations page, click the **Add** icon.
5. Select an AS2 domain from the **Domain Type** list and enter the AS2 Domain ID.
6. Click **Add**.

   The AS2 specification includes formatting rules for the AS2 Identifier field. AS2-To and AS2-From header information is available in section 4.2 at the following URL: http://www.ietf.org/rfc/rfc4130.txt.

Setting Up AS2-HTTP/S for a Trading Host

To set up AS2-HTTP/S for a host, follow the instructions in the sections:

Setting the Host's AS2 Identifier for a Protocol

1. On the **Partner Management** tile, click **Hosts**.
2. On the Hosts page, click any host you wish to configure this transport.
3. In the Edit Partner window, on the Protocol tab, click **Edit Configurations** for any protocol you wish to configure.
4. Select the host's AS2 Identifier from the **AS2 Identifier** list.
5. Click **Save**.

Setting Up AS2-HTTP/S for a Trading Partner

To make a transport available for a trading partner, you have to perform the following tasks:

1. Configuring AS2-HTTP/S for a Trading Partner.
2. Select this transport for the partner in the **Primary Transport** field on the **Business Agreements > Edit Business Agreement > Bind Protocol > Available Protocols > Edit Configurations > Transports**.

Configuring AS2-HTTP/S for a Trading Partner

To configure AS2-HTTP/S for a trading partner, perform these steps:

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any partner you wish to configure this transport.
3. In the Edit Partner window, on the Protocol tab, click **Edit Configurations** for any protocol you wish to configure.
4. Select or enter data as described in AS2-HTTP/S Transport.
5. Click the **Transports** tab and select the transports.
6. Click **Save**.

   The New Transport dialog is displayed. Select or enter data as described in below

table.

In the New AS2-HTTP/S Transport dialog, configure the options according to

AS2-HTTP/S Transport

Field	Description
Name	Name the transport.
Type	Select AS2-HTTP or AS2-HTTPS from the Transport Type list. This action adds the AS2-HTTP/S item to the list in the Primary Transport areas described in Transports Tab of protocol.
Transport Name	An identifier for these transport settings.
URL	Required. The URL for the trading partner. Syntax: `https://host:port/dmz/protocol.` Example: `https://host_machine8:6705/dmz/EZComm.`
HTTP 1.0 Compatible	Whether to exclude "Expect: 100 continue" in the HTTP header of the outbound AS2 HTTP/S request when the request is sent to the server of the trading partner.
Server Certificate	(Required, HTTPS only) The certificate used to encrypt communication.
MIME Subject	A short string identifying the topic of the AS2 message; for example, “Purchase Order from ABC Company”. For more information on the Subject Header field for MIME messages, refer to RFC C2822, Internet Message Format.
Non Repudiation of Receipt	Enable logging of receipts in the non-repudiation table. If you check this option, you must also check the Sign check box and set Request Receipt to Signed. This means that outbound messages are signed and signed receipts are requested from the

Field	Description
	Responder. The original signed request from the Initiator and the signed receipt from the Responder are logged in the Initiator's non-repudiation table. For more information, see TIBCO BusinessConnect Container Edition Concepts, "Non-Repudiation."
Sign	Enable outbound request messages or acknowledgments to be signed using your private key. Your partner uses your public key to authenticate your message. The 1024-bit key length is used for signatures. TIBCO BusinessConnect Container Edition can process messages which contain message digests computed using the SHA1 hash algorithm. By default, TIBCO BusinessConnect Container Edition will use the SHA1 hash algorithm when signing outbound messages for the AS1 and AS2 transports. To override this behavior, set the TIBCO BusinessConnect Container Edition property bc.ediint.digestAlgorithmEnabled to true under System Settings. This will cause TIBCO BusinessConnect Container Edition to compute the message digests for AS1 and AS2 using the digest algorithm setting specified for the business agreement in the Document Security screen. Whether an outbound receipt is signed or not is controlled by the setup in the requesting partner's Request Receipt list.
Signature Scheme	Select the desired signature algorithm from the list of options: RSA, RSA-PSS. The default option is RSA. **Note:** Ensure to enable the Sign check box to apply the signature scheme.
Encrypt	Enable each outgoing message to be encrypted using your partner's public key. Your partner uses their private key to decrypt your

Field	Description
	message. The encryption algorithm specified for the business agreement in the Document Security screen will be used to encrypt the email messages.
Encryption Scheme	Select the desired encryption algorithm from the list of options: RSA-PKCS1-v1_5, RSA-OAEP, RSA-OAEP-sha256, RSA-OAEP-sha384, and RSA-OAEP-sha512 The default option is RSA-PKCS1-v1_5. **Note:** Ensure to enable the Encrypt check box to apply the encryption scheme
Compress	If selected, each outgoing message is compressed in ZLIB format.
Compression Order	File compression is performed in the following orders: • Before Signing File compression is performed before signing. • After Signing File compression is performed after signing.
Request Receipt	The type of receipt returned from the trading partner. The following options are available: • **None** No receipt is requested from the trading partner for a message. • **Signed** A signed receipt is requested from the trading partner for each message. After the Responder gets the document and verifies the content for integrity, a signed receipt is created and sent by the trading partner. • **Unsigned** An unsigned receipt is requested from the trading partner for each message. If you choose to request a receipt of any kind, you must have a valid email address set for the trading host.

Field	Description
	If you checked Non Repudiation of Receipt, you should select Signed. For computing the message digest, BusinessConnect Container Edition uses the digest algorithm that was configured for the business agreement in the Document Security screen. For more information on receipts, see Message Disposition Notification Receipts.
Return Receipt URL	The URL to which receipts are sent if you selected asynchronous receipts in the Request Receipt list. "http://" or "https://" prefix is mandatory for Return Receipt URL in the BCCE environment.
Receipt Timeout (minutes)	The amount of time within which a receipt should be returned by the trading partner.
Retry Count	The maximum number of times TIBCO BusinessConnect Container Edition will try to re-connect to the remote HTTP server, in case of failures.
Retry Interval	The interval TIBCO BusinessConnect Container Edition will wait before another re-connect is attempted.
Socket Timeout (seconds)	Socket timeout is the maximum amount of time (in seconds) to wait for a response before disconnecting the socket. **Note:** If you want to receive the timeout error when no response is received from your partner, the value in this field must be less than the value set in the Response Wait Time field in the Configuration tab of the SendRequest activity.
Use HTTP Basic Authentication	HTTP basic authentication uses a user name and password.
Username	Specify a user name for authenticating the host on the partner

Field	Description
	HTTP/S service.
Password	Specify a password for authenticating the host on the partner HTTP/S service.
Cipher Suite Grade	(HTTPS only) Select the cipher grade (strength) from the list. The options are: • All • Only Stronger Than Export • Only 128-Bit and Stronger • Only Stronger Than 128-Bit • Only 256-Bit and Stronger All ciphers are listed in TIBCO BusinessConnect Container Edition Concepts, "Cipher Suites."
Can Use TLS	(HTTPS only) Whether the TLS protocol is supported. If you select this check box, the TLS protocol is used to establish connection to the trading partner server.
TLS Version	(HTTPS only) Select the version of the TLS protocol. TLS protocol versions 1.0, 1.1, 1.2, and 1.3 are supported. **Note:** If you select TLS version 1.1 or 1.2, you have to select SUN or IBM as the security vendor for inbound and outbound socket operations.
Can Use SSLv3	(HTTPS only) SSL protocol version 3.0 is supported. If you select this check box, the SSL protocol version 3.0 is used to establish connection to the trading partner server.

7. click **Save**.

Synchronous and Asynchronous Receipts

Synchronous Receipts

The following synchronous options are available:

Sync Signed A signed, synchronous receipt is requested from the trading partner for each message. This is automatically selected if you check Non Repudiation of Receipt. An Initiator asks for signed or unsigned sync receipts if it wants to receive the receipts in the same HTTP connection so that it does not have to wait for the receipts to arrive on a separate connection.

Sync Unsigned An unsigned, synchronous receipt is requested from the trading partner for each message.

For synchronous receipts, the receipt should be returned by the trading partner in the reply to the HTTP request.

For more information on receipts, see Message Disposition Notification Receipts.

Asynchronous Receipts

The following asynchronous options are available:

Async Signed A signed, asynchronous receipt is requested from the trading partner for each message. An Initiator asks for signed or unsigned async receipts if it wants to receive the receipts in a separate HTTP connection. After the Responder gets the document and verifies the content for integrity, it opens a connection back to the Initiator to send out the receipt that was requested.

Async Unsigned An unsigned, asynchronous receipt is requested from the trading partner for each message.

For asynchronous receipts, the trading partner could return the receipt to another URL. MAILTO, HTTP, and HTTPS URLs are supported.

For more information on receipts, see Message Disposition Notification Receipts.

AS1 Transport

This topic describes how to use AS1 Transport for document exchange.

AS1 Transport Overview

AS1 (Applicability Statement 1) is the name given to implementations of RFC 3335 (MIME-Based Secure Peer-to-Peer Business Data Interchange Over the Internet) from the IETF (Internet Engineering Task Force). AS1 involves the exchange of documents over the internet using S/MIME and SMTP.

AS1 and AS2 are widely recognized standards for the exchange of documents between businesses: these standards allow users to exchange data securely and reliably using the internet. This results in reduced costs for users by eliminating the need for VANs (Value Added Networks).

To date over 25 different companies offer products which support AS1 or AS2 or both. These products have all undergone interoperability testing which is facilitated by Drummond Group Inc. and are certified by eBusinessReady as being interoperable.

AS1 transport supports:

- Documents signing
- Documents encryption
- Documents compression

AS1 Transport, hereafter referred to as AS1 Email transport, allows you to exchange documents over the Internet using S/MIME and email. It only specifies how to connect to a trading partner, deliver data, and get a receipt in a secure manner.

When data is transmitted to a trading partner using normal email such as Outlook email, a MIME content-type of text/plain is normally used. The AS1 standard specifies the use of the content-types application/X12 and application/EDIFACT for sending either X12 or EDIFACT EDI data, respectively. The content-type application/xml is used for sending XML documents.

It might not be possible for a trading partner using email to communicate successfully to a trading partner using AS1 email. The trading partner using AS1 email expects to receive

messages that use the AS1 content-types. That trading partner also sends messages using these content-types.

A trading partner using email might not recognize these AS1 content-types and therefore might not be able to process the email messages.

Message Compression

If a trading partner can send email messages according to the IETF AS1 standard (rfc3335.txt) and the trading partner's AS1 product has passed interoperability testing with the Drummond Group, compression is available for large email messages. There are different algorithms that can be used for compression of MIME messages. The Drummond Group AS1 interoperability test specification calls for a particular specification (draft-ietf-ediint-compression-12) to be followed when doing compression.

For large messages, compression is highly recommended. Do not use compression on smaller messages, as this might create a compressed message that is larger than the original message.

Attachments

The AS1 Email transport supports the sending and receiving of attachments as part of an AS1 message. This support is outside of the scope of the AS1 specification and might not be supported by other E-commerce vendors who offer AS1 support in their products. When attachments are added to an AS1 message, a multipart/mixed MIME message is created. The first body part of the MIME message contains the main document, while the subsequent body parts contain the attachments.

When an AS1 message with attachments is signed, the entire multipart/mixed MIME message is signed. Likewise, when an AS1 message with attachments is encrypted, the entire multipart/mixed MIME message is encrypted.

When an AS1 message is received that contains a multipart/mixed MIME message, the first body part is processed as the main document, while the subsequent body parts are processed as attachments. All inbound attachments are saved onto the file system and their file references are passed to the private process.

Not all TIBCO BusinessConnect Container Edition protocols support sending attachments with the AS1 Email transport. Those protocols which have support for passing attachment information in their messages to or from the private process can be used to send attachments with the AS1 Email transport. See the User Guide of your TIBCO

BusinessConnect Container Edition protocol to see whether it supports sending attachments with the AS1 Email transport.

Content Disposition Filename

Some back-end systems require that data to be processed be stored in files with particular filenames. Therefore, for some trading partners it might be necessary to associate filenames with the content of messages that were sent to them. For AS1 messages, this can be achieved by specifying the filename to use for storing the message content in the filename parameter of the Content Disposition header.

Some TIBCO BusinessConnect Container Edition protocols also provide the ability for the private process to specify a filename to be used as the value of the filename parameter in the Content Disposition MIME header of outgoing MIME messages, including AS1 messages. The filename can be specified for the Content Disposition header associated with the main document and/or any attachments. TIBCO BusinessConnect Container Edition protocols which support specifying the filename value for the Content Disposition header will also pass the value of the filename parameter from the Content Disposition header of inbound AS1 messages to the private process.

See the User Guide of the TIBCO BusinessConnect Container Edition protocol you are using to see whether it supports passing the Content Disposition header filename to/from the private process.

Options for Configuring AS1 Email for the Trading Partner

To use TIBCO BusinessConnect Container Edition AS1 Email Transport, select the AS1 Email transport when configuring your trading partner. The following options are available:

- **Authentication** Supported through digital signatures.
- **Security** Supported through message encryption.
- **Non-repudiation** Supported through digital signatures and email receipts.
- **Compression** Supported through the compression option as specified in the draft-ietf-ediint-compression-12 specification.

Message Digest Algorithm

The AS1 specification, RFC 3335, recommends that the SHA-1 hash algorithm be used to calculate the message digest for all outbound messages. By default, the TIBCO

BusinessConnect Container Edition AS1 transport will always use the SHA-1 hash algorithm regardless of the Digest Algorithm setting for the business agreement.

To override the default use of SHA-1 for the hash algorithm by the AS1 transport, you can set the TIBCO BusinessConnect Container Edition property bc.ediint.digestAlgorithmEnabled as follows:

- If bc.ediint.digestAlgorithmEnabled is set to true, the AS1 transport will use the digest algorithm that is specified in the business agreement Document Security settings.
- If bc.ediint.digestAlgorithmEnabled is false, the default, the AS1 transport ignores the digest algorithm setting in the business agreement and use SHA-1.

Use of the MD5 hash algorithm with AS1 should not be required.Drummond Group certified AS1 products all use SHA-1 for the hash algorithm during interoperability testing. However, the AS1 specification also states that AS1 products should be able to accept messages which use the SHA-1 hash algorithm. TIBCO BusinessConnect Container Edition will process inbound messages using either hash algorithm.

Note: Inbound AS1 messages that do not contain a content-type of application/x12, application/edifact, or application/consent cannot be determined to be AS1 email messages as opposed to plain email messages. Therefore, when an inbound email message is received that requests a signed receipt, the message digest for the email will be calculated using the Digest Algorithm setting of the business agreement regardless of how the email was sent (AS1 or plain email).

Identifying the Sender and Receiver

The AS1 Email transport uses standard To and From email addresses as defined in SMTP standard (RFC 2821). These email addresses are defined in the Valid Email Address List field in the **Partner Management > Partners > Partner Name > Protocol> Edit Configurations > General** tab. When email is received from the mail server:

- The **To address** is matched against the email address entered in the host's Valid Email Address List.
- The **From address** is matched against the trading partner's Valid Email Address List.

Configuring POP3 and SMTP Servers for AS1 Email

Configuring the POP3 AS1 Email Server

1. On the **System Settings** tile, click **Inbound Protocols**.
2. On **Email Inbound POP3 Service Configurations**, click the **Add** icon.
3. Configure the POP3 Server as explained in Email Inbound POP3 Service Configurations.

Configuring an SMTP Server for a Host

To enable communication for a host through an SMTP server, see the following sections:

- Adding New Proxy Server
- Setting Up Email for a Host

Configuring an SMTP Server for a Partner

To enable use of an SMTP server for a partner, see Setting Up Email for a Trading Partner.

Setting Up AS1 Email for a Trading Host

Selecting AS1 Email for the Trading Host

1. On the **Partner Management** tile, click **Business Agreements**.
2. In the Business Agreement page, click the business agreement for which you wish to set the Email transport.

3. In the Edit Business Agreement page, on the **Bind Protocol** tab, enable any protocol you wish to use and click **Edit Configurations**.
4. On the **Transports** tab, **Inbound transport for Partner** section, select the **Email** check box.
5. Click **Save**.

Setting the Host's Email Address for a Protocol

1. On the **Partner Management** tile, click **Hosts**.
2. On the Hosts page, click any one of the hosts whose email address you wish to set.
3. On Edit Host page, click ***protocol*** **> Edit Configurations**.
4. In the **General** tab of the *protocol* configuration page, enter host's email address in the **Valid Email Address List** field.

   Note: You can add multiple email address. Make sure that addresses are separated by a semicolon (;) or by a comma (,).

5. Click **Save**.

Setting Up AS1 Email for a Trading Partner

To make a transport available for a trading partner, you have to perform the following tasks:

1. Configuring AS1 Email for a Trading Partner.
2. Select this transport for the partner in the Inbound transport for Partner section on the **Business Agreements > Edit Business Agreement > Bind Protocol > Available Protocols > Edit Configurations > Transports** tab.

Note: Only the transport protocols that are selected in **System Settings > Transport Protocols > Inbound Protocols** are displayed in the Inbound transport for Partner section.

Configuring AS1 Email for a Trading Partner

To configure AS1 Email for a trading partner, perform these steps:

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any partner you wish to configure this transport.
3. In the Edit Partner page, on the Protocol tab, click **Edit Configurations** for any protocol you wish to configure.
4. On the *protocol* configurations page, click the **Add** icon.
5. In the **Add Transport** dialog box.
6. Enter the transport name.
7. Select AS1_Email from the list and, enter required information in the following fields:

AS1_Email Transport Settings

Field	Description
Transport Name	An identifier for these transport settings.
URL	(Required) The URL for the trading partner. mailto: *e-mailID@domain.com*.
Subject	A short string identifying the topic of the email message; for example, “Purchase Order from ABC Company”. For more information on the Subject Header field for MIME messages, refer to RFC C2822, Internet Message Format.
Base64 Encode Clear Text Messages	Base64 encode plain outbound email messages. Plain messages are those messages which are not signed, not encrypted, and not compressed.
Non Repudiation of Receipt	Enable logging of receipts in the non-repudiation table. If you check this option, you must also select the **Sign** check box and set Request Receipt to Signed. This means that outbound messages

Field	Description
	are signed and signed receipts are requested from the Responder. The original signed request from the Initiator and the signed receipt from the Responder are logged in the Initiator's non-repudiation table. For more information, see TIBCO BusinessConnect Container Edition Concepts, "Non-Repudiation."
Sign	Enable outbound request messages or acknowledgments to be signed using your private key. Your partner uses your public key to authenticate your message. The 1024-bit key length is used for signatures. TIBCO BusinessConnect Container Edition can process messages which contain message digests computed using the SHA1 hash algorithms. By default, TIBCO BusinessConnect Container Edition will use the SHA1 hash algorithm when signing outbound messages for the AS1 and AS2 transports. To override this behavior, set the TIBCO BusinessConnect Container Edition property bc.ediint.digestAlgorithmEnabled to true under System Settings. This will cause TIBCO BusinessConnect Container Edition to compute the message digests for AS1 and AS2 using the digest algorithm setting specified for the business agreement in the Document Security screen. Whether an outbound receipt is signed or not is controlled by the setup in the requesting partner's Request Receipt list.
Signature Scheme	Select the desired signature algorithm from the list of options: RSA, RSA-PSS. The default option is RSA. **Note:** Ensure to enable the Sign check box to apply the signature scheme.

Field	Description
Encrypt	Enable each outgoing message to be encrypted using your partner's public key. Your partner uses their private key to decrypt your message. The encryption algorithm specified for the business agreement in the Document Security screen is used to encrypt the email messages.
Encryption Scheme	Select the desired encryption algorithm from the list of options: RSA-PKCS1-v1_5, RSA-OAEP, RSA-OAEP-sha256, RSA-OAEP-sha384, and RSA-OAEP-sha512. The default option is RSA-PKCS1-v1_5. **Note:** Ensure to enable the Encrypt check box to apply the encryption scheme.
Compress	If selected, each outgoing message is compressed in ZLIB format.
Compression Order	File compression is performed in the following orders: • **Before Signing** File compression is performed before signing. • **After Signing** File compression is performed after signing.
Request Receipt	The type of receipt returned from the trading partner. The following options are available: • **None** No receipt is requested from the trading partner for a message. • **Signed** A signed receipt is requested from the trading partner for each message. After the Responder gets the document and verifies the content for integrity, a signed receipt is created and sent by the trading partner. • **Unsigned** An unsigned receipt is requested from the trading partner for each message. If you choose to request a receipt of any kind, you must have a valid email address set for the trading host.

Field	Description
	If you checked Non Repudiation of Receipt, you should select Signed. For computing the message digest, BusinessConnect Container Edition uses the digest algorithm that was configured for the business agreement in the Document Security screen. For more information on receipts, see Message Disposition Notification Receipts.
Receipt Timeout (minutes)	The amount of time within which a receipt should be returned by the trading partner. Example: 5

8. Click **Add**.

Setting Up the Partner's Email for a Protocol

To set up the partner's email for a specific protocol, perform the following steps:

1. On the **Partner Management** tile, click **Partners**.
2. On the Partners page, click any partner you wish to configure this transport.
3. In the Edit Partner page, on the Protocol tab, click **Edit Configurations** for any protocol you wish to configure.
4. Add the partner's email address in the field **Valid Email Address List**.

   Make sure that addresses are separated by a semicolon (;) or by a comma (,).
5. Click **Save**.

Configuring AS1 Email for a Business Agreement

To configure the AS1 Email transport for a business agreement, see the Transports tab in User Guide of protocol.

Message Disposition Notification Receipts

A message disposition notification (MDN) receipt is a transport level acknowledgement.

When an Initiator sends a request, it can request a signed or unsigned MDN receipt from the Responder. The Responder then creates and sends the appropriate MDN receipt to notify the Initiator that its request message was successfully delivered. If the content of a signed, or encrypted, or signed and encrypted document cannot be verified for integrity, then the MDN receipt indicates the failure.

An MDN receipt does not guarantee that the document from the Initiator has been validated by the Responder's translator. An MDN receipt merely states that the document was received and its contents were verified for integrity.

When an Initiator is configured to request an MDN receipt from a trading partner, TIBCO BusinessConnect Container Edition adds MIME message headers to the outbound message.

Three types of headers are possible.

- The presence of a Disposition-Notifications-To MIME header indicates that a MDN receipt was requested. This header is valid for AS2-HTTP/S, AS1, and Email.
- The presence of a Disposition-Notification-Options MIME header indicates that a signed MDN receipt was requested. This header is valid for AS2-HTTP/S and Email.
- A third MIME header distinguishes between sending MDN receipts synchronously or asynchronously. This message header can be activated by putting a value in the Request Receipt URL field. For more information, see Request Receipt.

This field should have a valid URL for asynchronous MDN receipts. This header is valid for AS2-HTTP/S.

If the Initiator requests and receives a signed MDN receipt, the Initiator can authenticate that the Responder received the request by verifying the Responder's digital signature on the MDN receipt. Only signed MDN receipts can be logged in the TIBCO BusinessConnect Container Edition non-repudiation scheme.

For Email, TIBCO BusinessConnect Container Edition follows the AS1 specification for MDN receipts. For AS2-HTTP/S, TIBCO BusinessConnect Container Edition follows the AS2 specification for MDN receipts. For AS2-HTTP/S, synchronous or asynchronous receipts can be requested. See http://www.ietf.org/rfc/rfc2298.txt?number=2298 for more information on how MDN receipts are constructed and handled.

Configuring MDN Receipts

You can configure MDN Receipts using Transports tab for Business Agreement. For more information, see Business Agreements section in the specific protocol's documentation.

Enabling Receipts

You can enable MDN receipts in the Request Receipt list when configuring a transport for the trading partner. In this field, you can specify a signed or unsigned receipt. For AS2-HTTP/S you can also specify whether the receipt is to be sent synchronously or asynchronously. Asynchronous MDN receipts for AS2-HTTP/S transport can be returned on Email transport, and not just on HTTP/S transport.

Note: Asynchronous receipts appear in the audit log as a BCCE/Receipt entry.

Setting Up Receipt Timeouts

When TIBCO BusinessConnect Container Edition is configured to accept MDN receipts within a certain timeout and if they are not received within this timeout, the request is timed out. To set a value for the time that the Initiator should wait for an MDN receipt from the Responder, enter a value in the Receipt Timeout field in the Transports tab.

Setting Up the Asynchronous Receipt SSL Certificate

The Remote Server Certificate or the Server Certificate for the AS2 HTTPS transport is a SSL certificate that is used for encrypting the data sent using HTTPS. For more information on how to configure the remote server certificate for AS2 transport, see information about AS2 Async MDN Remote Server Certificate field for Business Agreement Transport tab in the protocol-specific documentation.

Setting Up the AS2 MDN Asynchronous Reply Transport

When an asynchronous MDN is requested, the Disposition-Notification-To header of the inbound request contains the URL that is used for returning the MDN. If this is an HTTP/S URL, the settings for the socket timeout, retry count, and retry interval are taken from the inbound AS2 transport configuration for the trading partner who sent the MDN request. If you want to use different values for the HTTP/S socket timeout, retry count, or retry interval when returning the MDN request, you can create an AS2 HTTP/S transport

configuration that has the proper values and specify this alternate AS2 transport configuration for the MDN reply. For more information, see information about AS2 Async MDN Reply Transport field for the Business Agreement Transport tab in the protocol-specific documentation.

MDN Receipts and Business Acknowledgments

An MDN receipt is a transport-level acknowledgment that does not guarantee that the document from the Initiator was validated by the Responder's translator. An MDN receipt merely states that the document was received and its contents were verified for integrity. No document validation takes place before an MDN receipt is sent back. An acknowledgment is a business level response that is sent back if required by the specified protocol in use.

A Responder might refuse an MDN receipt if the Responder does not recognize from which trading partner a message originated and is not listed in the Responder's list of trading partners.

Here are some conditions in which the Responder sends back an ERROR MDN receipt:

- The Responder does not have the certificates of the trading partner installed, so it cannot verify the contents of the inbound document if a signed document was sent and an MDN receipt was requested.
- The Responder cannot decrypt the inbound message from the trading partner as it might have not been encrypted with a valid set of certificates.

MDN Messages Sent to Private Processes

Miscellaneous message types are available for the protocol of the specified TIBCO BusinessConnect Container Edition shared configuration resource. These messages can occur when the AS1, AS2 or Email transports are used and receipts (MDNs) are utilized.

The miscellaneous messages that can be received for MDN receipts are MDN Alert messages and MDN Timeout messages. An MDN Alert is sent to the private process when an MDN receipt is sent to or received from a trading partner.

If the MDN receipt is requested but was not received from the trading partner before the configured timeout occurs, an MDN Timeout is sent to the private process. See documentation for a specific business protocol for more information.

Since protocols such as RosettaNet do not use AS1, AS2 or the Email transport, these messages will not occur for RosettaNet.

Note: See documentation for specific protocols to ensure the support of AS1 and AS2 transports and MDN Messages.

To learn more about MDN messages sent to Private Processes, see TIBCO BusinessConnect Plug-in Reference, Receive Misc. Msg.

Troubleshooting Transport Problems

This topic offers advice on resolving transport problems.

Error message when From and To identifiers are the same

Error while retrieving protocol binding for partner Company2 and host Company1.

The From and To identifiers for the participants are probably the same; for example, the To and From fields might both identify the partner instead of identifying the host and the partner.

Issues with encryption and decryption of S/MIME messages

Keys and certificates are set properly for the host and the partner at the business agreement level. For more information see Business Agreement: Document Exchange Tab in protocol-specific documentation.

Email Transport

Error message when email address is missing

If while receiving inbound email, the email address for the host is missing or incorrect, BusinessConnect Container Edition returns the following error message:

Error retrieving Host or Trading Partner. Check email configuration.

BusinessConnect Container Edition logs the message to the protocol log. See Identifying the Sender and Receiver, for information about providing the email address for the host.

Error message when email address is missing or incorrect

If while receiving inbound email, the email address for the partner is missing or incorrect, BusinessConnect Container Edition returns the following error message:

Email was received from <xxx> for <yyy>. No valid sender participant can be found with email address <xxx>

See Identifying the Sender and Receiver, for information about providing the email address for the host.

Scripts

TIBCO BusinessConnect Container Edition supports the use of scripts to manage file processing for FTP inbound and outbound transport and File outbound transport.

See FTP/S Inbound, FTP/S Outbound, and Configuring Outbound File Transport for a Partner for information on how to specify scripts in transport configuration dialogs. Script activities can be captured as audit trails using the logging object available in the context of the script. See Audit Logging in Scripts. In addition, an error advisory is also published when error is logged using the Java object.

Scripts should use Java methods to throw exceptions for script failures. If no exceptions are thrown, TIBCO BusinessConnect Container Edition considers the scripts as having completed successfully.

TIBCO BusinessConnect Container Edition provides a Java API for use within scripts. For information on this API, see the Viewing the Java API Reference Pages.

This topic also explains how to use the file specification dialog, which is used to specify DTD, guideline, and script files.

FTP Scripts

FTP scripts allow you to control the retrieval of files from and the storage of files on an FTP server. When FTP scripts are used, the normal file retrieval from or file storage to an FTP server is bypassed. Instead, the designated FTP script is called and the FTP script is responsible for retrieving or storing the files. It is also possible to perform pre- and post-processing, as appropriate for your application, from within your script.

For reference, see FTPClient, FTPReply, and UserLogAccess scripts on Viewing the Java API Reference Pages.

Secure FTP

Secure FTP (FTPS) is supported within FTP scripts by using the FTPClient API in secure mode. Secure mode is activated by providing the certificate specified for the trading partner to the setSSLCertificate(java.lang.String) method. If the FTP server supports SSL with client authentication, then the host private key should also be set with setSSLHostKey (java.lang.String).

The default secure transport version is obtained from the FTPS configuration settings, see Selecting and Configuring FTP/S Inbound and Configuring FTP/S Outbound. You can modify the transport version with the method setTransportType(java.lang.String).

SSHFTP Scripts

For reference, see FileAttr, SSHFTPClient, SSHFTPReply, and IFTPFlavorReply scripts on Viewing the Java API Reference Pages.

Document Security through PGP

PGP (Pretty Good Privacy) packaging and un-packaging is also supported through FTP/FTPS/SSHFTP scripts to provide document security. PGP is supported within FTP/FTPS/SSHFTP script also by using FTP/FTPS/SSHFTP Client API. You can set up PGP options (sign, encrypt, compress, format, and so on) by using methods defined in the FTP/FTPS/SSHFTP Client object; however, PGP keys and cipher algorithms used in PGP packaging or un-packaging still need to be configured in the business agreements' Document Exchange. For more inform, see the Document Exchange tab in the protocol specific documentation.

File Scripts

File scripts allow you to control the storage of files on the file system when using File outbound transport. When scripts are used, the normal file storage to the file system is bypassed. Instead, the designated script is called and the script is responsible for storing the files. You can also perform pre- and post-processing, as appropriate for your application, from within your script.

FTP Inbound

For FTP inbound operations, the script that is uploaded is executed instead of running pre-defined get or mget operations. During script execution, files are placed in a temporary directory.

To access this property on TIBCO BusinessConnect Container Edition UI:

1. Expand **Partner Management > Business Agreements > protocol link > Transports** tab.
2. Select **FTP** and click **Edit settings**.

3. Upload the scripts file in the FTP settings dialog box.

Job Variables

A client interface is available for developing the script and the object implementing the interface is available in the job slot variable.

• ftpObj The slot to retrieve the FTP client object.

Example: var ftpClient = job.get("ftpObj");

In addition, you can use the following job variables in scripts:

• getTmpDir The variable for the temporary directory on the local machine to retrieve files from the FTP server.

Example: var getdir = job.get("getTmpDir");

• hostName The variable containing the trading host name from whom the file came.

Example: var hostName = job.get("hostName");

• logObj The slot variable to retrieve the UserLogAccess object that does audit logging.

• tpName The variable containing a trading partner for whom the file is intended to be stored.

Example: var tpName = job.get("tpName");

• ibPGPHandler The variable to be used for inbound PGP un-packaging in an FTP session. Users can use the handler to set the inbound PGP processing policy.

Example: var ibPGPHandler = job.get("ibPGPHandler");

var policy = ... //options: "None", "Must Encrypt", "Must Sign", "Must Sign and Encrypt",

"Pass-through"

ibPGPHandler.setPGPPolicy(policy);

You might also need to set the operation id for the current inbound message:

ibPGPHandler.setOperationID(...);

and then to un-package the received file:

ibPGPHandler.unpackageMessage(filefullname);

FTP and File Outbound

Job Variables

A client interface is available for developing the script and the object implementing the terrifies is available in the job slot variable.

• ftpObj The variable to retrieve the client object.

Example: var ftpClient = job.get("ftpObj");

In addition, you can use the following job variables in scripts:

• dataObj An in-memory object containing the data to be transmitted.

Example: var dataObject = job.get("dataObj");

• deleteFileRef Set to false to prevent TIBCO BusinessConnect Container Edition from deleting the outbound file from the local machine at the end of script execution. The default value for this variable is true, and the outbound file gets deleted at the end of script execution.

• fileURL Variable entered in the URL field for File transport. You can use this to dynamically store the file in the file system.

Example: var fileURL = job.get("fileURL");

• hostName The variable containing the trading host name from whom the file came.

Example: var hostName = job.get("hostName");

• logObj The variable to retrieve the UserLogAccess object that does audit logging.

Example: var logClient = job.get("logObj");

• srcFileName The variable for the file name on the local machine that has the outbound file ready to be stored in the FTP server.

Example: var localfile = job.get("srcFileName")

• Skip Content Threshold If BusinessConnect Container Edition uses the Outbound File poller to get the file from the private process and the file size is smaller than the threshold set as Skip Content Threshold, then the file will be directly read into memory and the value of localFile will be null. In such cases, you should use job.get("dataObject") to access the data to be transmitted;

The default for the property Skip Content Threshold set in the dialog Edit Application Configuration is 10000 KB. This property defines a threshold for large files. Any file with the

size that exceeds this threshold will not be fully written into memory, which increases the available memory for the system.

To find out how to define this property, see TIBCO BusinessConnect Container Edition Administration, "Intercomponent Advanced."

• srcFilePath The directory on the local machine that has the outbound files ready to be stored in the FTP server.

Example: var localdir = job.get("srcFilePath");

• tpName The variable containing the trading partner for whom the file is intended to be stored.

Example: var tpName = job.get("tpName");

• obPGPHandler The variable to be used for outbound PGP packaging in an FTP session. Users can use the handler to set the PGP process options.

Example: var obPGPHandler = job.get("obPGPHandler");

var sign = ...

var encryption = ...

var compress = ...

//sign, encryption and compress are boolean values (true or false);

obPGPHandler.setPGPOptions(sign, encryption, compress);

You can also set the format of the payload after PGP processing, and the compression algorithm:

obPGPHandler.setCompressionAlgo("ZLIB"); //"ZLIB" or "ZIP"

obPGPHandler.setFormat("armored"); //"amored" or "binary"

and then you can package the payload with PGP processing:

obPGPHandler.packageMessage();

Supported FTP Commands

The commands available in the FTP specification 959 are supported:

• USER Logs in

• PASS Sends a password

• CWD Changes the working directory

• PASV Asks the server-DTP to listen on a data port and to wait for a connection rather than initiate one upon receipt of a transfer command. This command is executed only

if the FTP server supports the command. A server socket is opened if the FTP server does not support the command.

TYPE The argument specifies the representation type. The following types are supported, depending on the FTP server implementation:

— A (ASCII)

— I (Image)

— E (EBCDIC)

— L (Local byte size) byte size

• RETR Requests a file to be retrieved

• STOR Sends the request to store the data as a file in FTP server

• APPE Causes the server-DTP to accept the data transferred through the data connection and to store the data in a file at the server site. If the file specified exists at the server site, then the data is appended.

• PWD Prints the working directory

• DELE Sends the command to the server site to delete the file that is sent as the argument

• RMD Removes a directory at the FTP server

• MKD Creates a new directory at the FTP server

• LIST Retrieves the directory listing

• NLST Retrieves the filenames for the directory. This command is used to do multiple gets/delete.

• SITE Provides services specific to its system that are essential to file transfer but not sufficiently universal to be included as commands in the protocol.

• STAT Causes the status response to be sent over the control connection in the form of a reply

• SYST Finds the operating system of the server

• RNFR Renames filename from

- RNTO Renames filename to
- STOU Stores unique filename (system generated)
- REIN Reinitializes user

File Outbound

A new interface com.tibco.ax.fw.runtime.transport.file/FILEClient has been added to the JavaDoc. See Viewing the Java API Reference Pages.

This interface is used when a customer wants to implement custom scripts on the outbound File transport.

The script example for the outbound File transport is available at BC_HOME/samples/bc/filescripts/copyexample.txt.

Viewing the Java API Reference Pages

To access the TIBCO BusinessConnect Container Edition Java API reference, see Java API Reference Pages.

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 TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for TIBCO BusinessConnect™ Container Edition is available on the TIBCO BusinessConnect™ Container Edition page.

- *TIBCO BusinessConnect™ Container Edition Release Notes*
- *TIBCO BusinessConnect™ Container Edition Installation and Deployment*
- *TIBCO BusinessConnect™ Container Edition Concepts*
- *TIBCO BusinessConnect™ Container Edition Trading Partner Management*
- *TIBCO BusinessConnect™ Container Edition Administration*
- *TIBCO BusinessConnect™ Container Edition Security Guidelines*

How to Contact TIBCO Support

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to TIBCO Support website. If you do not have a user name, 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